分类号：O157.2　　单位代码：10335
密　级：　　学　　号：11106008

浙江大学

博士学位论文

中文论文题目：代数组合与代数编码中若干离散构型研究

英文论文题目：Several Discrete Configurations in Algebraic Combinatorics and Algebraic Coding Theory

申请人姓名：胡思煌
指导教师：葛根年　教授
合作导师：冯涛　研究员
专业名称：应用数学
研究方向：代数组合与代数编码
所在学院：理学院数学系

论文提交日期：二〇一四年四月

代数组合与代数编码中若干离散构型研究

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：	李学良\教授\南开大学
委员 3：	殷剑兴\教授\苏州大学
委员 4：	李雨生\教授\同济大学
委员 5：	葛根年\教授\浙江大学
委员 6：	冯涛\研究员\浙江大学

答辩日期：二〇一四年四月

致　谢

首先我要感谢培养了我五年的我的导师——葛根年教授。自我进入浙江大学读博以来，葛老师在科研和生活上都给予了我很多的指导和建议。葛老师鼓励我去开阔视野，将研究主题扩展到代数组合和代数编码上，这极大地培养了我的独立科研能力。葛老师在科研和教学上严谨认真、一丝不苟的态度更是为我树立了榜样，而这必将使我终身受益。

我还要感谢我的第二导师——冯涛博士。冯老师在科研上给予了我许多悉心和具体的指导。在和冯老师一起解决问题的过程中，我学到了很多的知识，并慢慢地体会到了科研的乐趣。

另外我还要感谢这五年中在学习和生活上给予过我指导的各位老师，特别是特拉华大学的向青教授、上海交通大学的坂内英一教授、福建师范大学的张胜元教授、同济大学的杨亦挺老师和范翠玲老师等。在他们到浙江大学访问及教学期间，我从他们那里学到了许多的新课题和新方法。

同时也要感谢浙江大学在研究生学习期间提供的各类补助和奖学金，以及教育部授予的博士研究生学术新人奖和国家奖学金等，这些都在很大程度上改善了我的生活和科研条件，使我能全身心地投入到学术研究中。

我还必须要感谢在一起学习、科研的同门：张先得师姐、张会师姐、高斐师兄、朱明志师兄、魏恒嘉、李抒行、林浩、张一炜、上官冲、汪馨、张韬、顾玉杰、马景学、丁报昆、陈寿长、李林林等。在这共同学习和生活的岁月里我们一起留下了许多美好的回忆。

最后，我要感谢我的祖父、祖母、父亲、母亲和女友。谢谢你们的关心和支持，让我在科研的道路上可以安心地一直走下去。

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

摘 要

代数组合学是组合数学的一个重要分支，它研究具有高度对称性和优美结构的组合对象. 编码理论是现代计算机科学和数字通信技术的核心，它研究如何对信息本身加入冗余，以对抗传输过程中发生的错误. 代数学、组合数学、编码理论的研究对象都具有离散的性质，三门学科之间存在着天然的联系. 在本学位论文中，我们将从代数的观点出发来考察组合与编码中一些离散构型，包括 Whist 赛程设计、差集、结合方案、循环码等.

在论文的第一部分，我们将应用代数的方法来解决组合问题. 在第 2 章中，我们主要研究 Whist 赛程设计的存在性问题. 它最早是由 Moore 于1896年提出，之后便吸引了 Wilson、Baker、Hartman 等众多组合设计学者的注意. 在这里我们引入了 $\mathbb{Z}$CPS-Wh frames 的概念，并且利用它统一了许多关于 $\mathbb{Z}$CPS-Whs 的构造方法. 我们还构造了许多新参数的 $\mathbb{Z}$CPS-Whs，由此大大地推进了这方面的存在性结果. 我们的主要工具是代数数论中著名的关于特征和的 Weil 估计.

差集是一类十分重要的组合结构，对其研究已十分深入. 所有已知的差集可以被划分成以下的三类：Singer 参数的差集、分圆差集和满足 $\gcd(v,n) > 1$ 的差集. 其中满足 $\gcd(v,n) > 1$ 的差集又可以被划分成以下的五类：Hadamard 差集、McFarland 差集、Spence 差集、Davis 和 Jedwab 构造的一类与 Spence 差集相似的差集、Chen 构造的推广的 Hadamard 差集. 我们注意到目前所有已知的满足 $\gcd(v,n) > 1$ 的差集都具有所谓的 character divisibility 性质. 于是 Jungnickel 和 Schmidt 提出了下面的问题：构造满足 $\gcd(v,n) > 1$ 但不具有 character divisibility 性质的差集. 在第 3 章中我们将把只具有三个非平凡特征值的差集作为主要的研究对象，并由此推导出一系列的必要条件.

在论文的第二部分，我们将主要考察组合与编码之间的一些交叉应用. 在第 4 章中，我们在 $\mathcal{DG}$ 码关于 Lee 重量划分的基础上构造了一族 9 类结合方案，并且利用复杂的指数和计算显式地决定出了这个结合方案的对偶方案的划分. 除此之外，

我们还得到了其他三个无穷类的结合方案；它们是这个 9 类方案的 fusion 方案和 quotient 方案.

为了构造奇特征有限域上的射影平面，Dembowski 和 Ostrom 引进了平面函数的概念. 基于其对差分攻击的最优抵抗性，人们将它们用于构造类似 DES 的迭代密码系统、纠错码、秘密分享方案等. 最近，Zhou 在偶特征的有限域上提出了一个新的“伪平面函数”的定义，由它我们可以得到有限射影平面. 在第 5 章中我们将构造三类新的伪平面二项式函数，其中的两类是无穷类. 另外我们发现任一伪平面函数都将给出一个定义在 Galois 环上的 5 类结合方案.

循环码的重量分布计算牵涉到 Gauss 和与指数和的计算. 虽然在有些情况下，我们可以得到一些简洁的表达式，但是绝大多数情况下这类计算是非常困难的. 在第 6 章中，我们决定了一类可约循环码的重量分布. 特别地，它的对偶码可以具有任意多个零点. 我们的主要工作是建立了相关的指数和与 Hermitian 型图的谱之间的对应关系.

关键词：差集，结合方案，四元码，循环码，Whist 赛程设计

Abstract

Algebraic combinatorics is an area of mathematics that employs methods of abstract algebra in various combinatorial contexts and, conversely, applies combinatorial techniques to problems in algebra. Coding theory is the study of the properties of codes and their fitness for a specific application. They both study discrete configurations. In this dissertation, we will use algebraic methods to investigate several combinatorial objects in design theory and coding theory, such as whist tournaments, difference sets, association schemes and cyclic codes.

In the first part, we will use algebraic methods to study two problems in design theory. In Chapter 2, we focus on the whist tournaments. The whist tournament problem was introduced by Moore in 1896. Its existence attracted a lot of design theorists such as Wilson, Baker, Hartman et al. We will propose a general recursive construction, i.e., a frame construction, for $\mathbb{Z}$-cyclic patterned starter whist tournaments. As a consequence, we are able to unify many known constructions for $\mathbb{Z}$-cyclic patterned starter whist tournaments. The known existence results of such designs are then extended. Weil's theorem on character sums is used to get our main result.

In combinatorics, a (v, k, λ) difference set is a subset D of size k of a group G of order v such that every nonidentity element of G can be expressed as a product $d_1 d_2^{-1}$ of elements of D in exactly λ ways. The known families of difference sets can be subdivided into three classes: difference sets with Singer parameters, cyclotomic difference sets, and difference sets with $\gcd(v, n) > 1$. It is remarkable that all the known difference sets with $\gcd(v, n) > 1$ have the so-called character divisibility property. In 1997, Jungnickel and Schmidt posed the problem of constructing difference sets with $\gcd(v, n) > 1$ that do not satisfy this property. In an attempt to attack this problem, we use difference sets with three nontrivial character values as candidates, and get some necessary conditions in Chapter 3.

The second part consists of Chapters 4-6, in which the interaction of combinatorics

and coding theory is particularly strong. In Chapter 4, we construct an infinite series of 9-class association schemes from a refinement of the partition of Delsarte-Goethals codes by their Lee weights. The explicit expressions of the dual schemes are determined through direct manipulations of complicated exponential sums. As a byproduct, the other three infinite families of association schemes are also obtained as fusion schemes and quotient schemes.

Planar functions in odd characteristic were introduced by Dembowski and Ostrom in order to construct finite projective planes in 1968. They were also used in the constructions of DES-like iterated ciphers, error-correcting codes, and signal sets. Recently, a new notion of pseudo-planar functions in even characteristic was proposed by Zhou. These new pseudo-planar functions, as an analogue of planar functions in odd characteristic, also bring about finite projective planes. There are three known infinite families of pseudo-planar monomial functions constructed by Schmidt and Zhou, and Scherr and Zieve. In Chapter 5, three new classes of pseudo-planar binomials are provided. Moreover, we find that each pseudo-planar function gives an association scheme which is defined on a Galois ring.

The determination of weight distribution of cyclic codes involves the evaluation of Gauss sums and exponential sums. Despite of some cases where a neat expression is available, the computation is generally rather complicated. In Chapter 6, we determine the weight distribution of a class of reducible cyclic codes whose dual codes may have arbitrarily many zeros. This goal is achieved by building an unexpected connection between the corresponding exponential sums and the spectra of Hermitian forms graphs.

Keywords: Association scheme, cyclic code, difference set, quaternary code, whist tournament

目 次

表目录

1 绪论

1.1 代数组合与代数编码

1.1.1 代数组合学

代数组合学（Algebraic Combinatorics）是组合数学的一个重要分支，它研究具有高度对称性和优美结构的组合对象. 关于代数组合学的研究开始于上世纪七十年代，不过关于它的某些研究轨迹可以溯源到上世纪三十至六十年代群论学家 Schur、Wielandt 和 Higman 等人关于有限置换群的工作以及统计学家 Bose 和 Ray-Chaudhuri 等人关于试验设计方面的工作. 1973年，Delsarte 在它的著名的博士论文中指出：诸如码与设计等组合结构可以通过结合方案来给出统一的处理. 1984年，Bannai 与 Ito 出版了系统论述代数组合学的第一本专著[10]. 在专著中，他们把代数组合学称为“组合对象的表示理论”或“没有群的群论”. 1989年，Brouwer、Cohen 和 Neumaier 出版了关于距离正则图的专著[18]. 1993年，Godsil 出版了以“代数组合学”命名的专著. 1992年，为适应代数组合学研究蓬勃发展的需要，《代数组合学》（Journal of Algebraic Combinatorics）杂志创刊.

结合方案是代数组合学的核心概念，关于它的研究是代数组合学研究的重点. 关于这方面成果的系统论述可以参考专著[10,18].

1.1.2 代数编码

在利用有噪声的信道传输信息的过程中，信息的编码占据了核心的地位. 考虑传输一个长度为 k 的 $0-1$ 字符串，普遍存在的信道噪声可能使字符串的某些位置发生改变. 在接收端得到的 $0-1$ 字符串总是受噪声的干扰而在部分位置发生了错误. 因此，为了可靠地传输信息，必须要对信息进行编码，保证在接收端至少能以很大概率发现并且纠正这些错误. 纠错码的核心思想就是对信息本身加入冗余，以对抗传输过程中发生的错误. 例如，一个纠错码可以看作一个映射，把代表信息的

k 长字符串映到一个 n 长的字符串，其中 $n > k$. 多出来 $n - k$ 个字符就是加入的冗余，用来探测并纠正传输过程中发生的少量错误.

循环码是一种具有良好的代数结构的线性码. 由于循环码具备快速的译码算法，它在通信和数据存储中都有重要的应用. 当前，循环码的研究热点集中在它的重量分布方面. 循环码的重量分布给出了循环码的关键信息，可以用来计算译码算法出错的概率. 然而，重量分布的计算是非常困难的问题，人们只知道少数几类循环码的重量分布. 特别地，我们称对偶码有一个零点的循环码为不可约循环码. 即使在不可约循环码这种最简单的情形，重量分布的计算本质上仍然是困难的. McEliece指出，不可约循环码的重量分布可以表示为一系列高斯和的线性组合. 由于高斯和的计算本身是非常困难的问题，因而只在几类特别的情况下能够算出不可约循环码的重量分布. 关于重量个数不超过 2 的不可约循环码的分类，Schmitt 和 White 提出了一个重要的猜想. 当循环码的对偶码有两个零点时，情况更为复杂. 自20世纪中叶以来，伴随着信息时代的到来，编码理论在数学和应用中的地位越来越重要. 一个生动的例子是美国宇航局在探测太阳系行星的水手计划（Mariner Program）中，利用线性码传输人造探测器拍摄的火星表面图片（Mariner 7，1969）. 研究者们在构造好的编码的过程中，揭示出编码与组合设计、非线性函数、秘密分享方案等数学对象之间的联系. 除了实践中应用之外，编码本身作为一个独立的数学对象和重要的数学工具，必将发挥越来越大的作用. 对编码理论的更深入的研究，具有重大的理论和实际意义.

1.2 Whist 赛程设计

关于 v 名选手的 whist 赛程设计 (tournament) 是一类特殊的参数为 $(v, 4, 3)$ 的（拟）可分解平衡不完全区组设计 (RBIBD). Whist 赛程设计的存在性问题最早是由 Moore[75] 于1896年提出，之后便吸引了 Wilson、Baker、Hartman 等众多组合设计学者的注意. 自1970年以来，人们已经知道当 $v \equiv 0, 1 \pmod 4$ 时 Wh(v) 恒存在. 有关 whist 赛程设计的更多介绍，读者可以参考 Anderson 的文章[4].

当 v 是有限个模 4 余 1 的素数的积时，Watson[92] 在1954年便给出了 $\mathbb{Z}$CPS-Wh(v) 的一种构造方法. 之后 Bose 和 Cameron[14] 于1965年和 Baker[7] 于1975年又

分别独立地对 v 是模 4 余 1 的素数的情形给出了 $\mathbb{Z}$CPS-Wh(v) 新的两种构造方法. 在过去的二十来年里，很多学者都研究过 $\mathbb{Z}$CPS-Whs 的存在性问题，主要的文献有 Finizio[37]，Finizio 和 Leonard[38]，Leonard[56]，Leonard 和 Jones[57]，Abel、Anderson 和 Finizio[3]. 下面我们简要回顾一下它的研究历史.

在1994年，Finizio[37] 率先提出了 $\mathbb{Z}$-循环的 patterned starter whist 赛程设计的概念，并且对所有的 $5 \leq v \leq 41$，$v \equiv 1 \pmod 4$ 得到了完整的存在性结果. 随后 Leonard[56] 给出了 $\mathbb{Z}$CPS-Wh(q^2) 的一种构造方法，其中 q 是模 4余 3 的素数. Leonard[56]、Leonard 和 Jones[57] 则进一步利用这个方法对所有的 $7 \leq q \leq 5000$ 构造了 $\mathbb{Z}$CPS-Wh(q^2)，其中 q 是模 4 余 3 的素数. 除了上述例子之外，Abel、Anderson 和 Finizio[3] 构造了仅有的两个参数较小的 $\mathbb{Z}$CPS-Wh(v)，其中 $v \equiv 1 \pmod 4$. 对 $v \equiv 0 \pmod 4$ 的情形，人们目前只知道当 $v \in \{4, 28, 40, 76, 112, 148\}$ 时 $\mathbb{Z}$CPS-Wh(v) 存在，具体的例子请参见文献[3,38,75].

Frames 在可分解设计的构造中起着重要的作用[39,60,86]. 在第 2 章中，我们引入了 $\mathbb{Z}$CPS-Wh frames 的概念，并且利用它统一了之前的许多关于 $\mathbb{Z}$CPS-Wh 的构造. 我们还利用它构造了许多新参数的 $\mathbb{Z}$CPS-Whs，由此大大地推进了这方面的存在性结果. 本章内容已经发表在杂志《Discrete Applied Mathematics》和《Journal of Combinatorial Designs》上.

1.3 差集

差集是一类十分重要的组合结构，对其研究已十分深入，有关差集的研究结果参见[12,78]. 所有已知的差集可以被划分成以下的三类：Singer 参数的差集、分圆差集和满足 $\gcd(v, n) > 1$ 的差集. 其中满足 $\gcd(v, n) > 1$ 的差集又可以被划分成以下的五类：Hadamard 差集、McFarland 差集、Spence 差集、Davis 和 Jedwab[24] 构造的一类与 Spence 差集相似的差集、Chen[22] 构造的推广的 Hadamard 差集. 给定一个差集 D. 若对每一个 G 的非平凡特征 χ 均成立 $\sqrt{n} \,|\, \chi(D)$，则称差集 D 具有 character divisibility 性质. 注意到目前所有已知的满足 $\gcd(v, n) > 1$ 的差集都具有这种性质. 于是 Jungnickel 和 Schmidt 在他们的综述文章[54] 中提出了下面的问题：

问题： 构造满足 $\gcd(v, n) > 1$ 但不具有 character divisibility 性质的差集.

在第 3 章中，我们将尝试去解决这个问题. 对于一个差集 D，记 D 的所有非平凡的特征值的集合为

$$X = X(D) = \{\chi(D) \mid \chi \in \widehat{G}, \chi \neq \chi_0\}.$$

我们将主要考虑满足 $|X| = 3$ 的差集并由此推导出一系列的必要条件. 通过计算机搜索，我们找到了一些满足所有这些必要条件的可能参数. 另外我们也找到了一些几乎满足所有必要条件的参数. 这些参数在一定程度上表明是有可能存在满足 $\gcd(v, n) > 1$ 但不具有 character divisibility 性质的差集. 本章内容已经发表在杂志《Designs, Codes and Cryptography》上.

1.4 组合与编码的交叉应用

1.4.1 Delsarte-Goethals 码上的结合方案

自 Kerdock、Preparata、Goethals、Delsarte-Goethals 等码的 $\mathbb{Z}_4$-线性性质被发现以来[44]，学者们已经应用 $\mathbb{Z}_4$-线性码构造了很多的组合结构：例如 t-设计和结合方案. 根据 Solè[85] 的描述，$\mathbb{Z}_4$-线性性质的发现从 Liebler 和 Mena[58] 利用特征为 4 的 Galois 环构造结合方案中受到了启发. 有关从 $\mathbb{Z}_4$-线性码构造 t-设计的研究最早由 Harada[45] 提出. 之后 Helleseth 等人[83] 在这方面做了许多的工作.

结合方案是代数组合研究中的核心概念，并且已经在许多数学学科中发挥了重要的作用，例如 编码理论与图论. Henry Cohn 等人[8] 猜想一个在 $\mathbb{R}^{14}$ 中 64 个点上定义的 3 类的结合方案是一个*全局最优结构*（universally optimal configuration）. 随后 Abdukhalikov、Bannai 和 Suda[2] 利用二元和四元的 Kerdock、Preparata 码及 MUB 的最大集推广了这个结合方案.

具体的来说，他们根据 Lee 重量对缩短 Kerdock 码进行了划分，从而得到了一族 3 类的结合方案. 它的对偶方案恰定义在截短 Preparata 码上. 这启发我们去研究另外一类重要的四元码：Delsarte-Goethals ($\mathcal{DG}$) 码. 在第 4 章中，我们在 $\mathcal{DG}$ 码关于 Lee 重量划分的基础上构造了一族 9 类结合方案，并且我们利用复杂的指数和计算显式地决定出了这个结合方案的对偶方案的划分. 本章中的内容已经被《Journal of Algebraic Combinatorics》杂志接收.

1.4.2 偶特征的伪平面二项式函数

给定奇素数 p 和正整数 n. 令 $q = p^n$. 给定函数 $f : \mathbb{F}_q \to \mathbb{F}_q$. 若对任一 $\epsilon \in \mathbb{F}_q^*$, 映射

$$x \to f(x+\epsilon) - f(x) \tag{1.1}$$

都是 $\mathbb{F}_q$ 上的置换，则称 f 是一个 *平面函数*（planar function）. 为了构造奇特征有限域上的射影平面，Dembowski 和 Ostrom[28] 引进了平面函数的概念. 在密码学中，平面函数也被称作 *完全非线性函数*（perfect nonlinear functions）[72]. 基于其对差分攻击的最优抵抗性，人们将它们用于构造类似 DES 的迭代密码系统. Carlet、Ding 和 Yuan[21,29,95] 等研究者则利用平面函数构造纠错码，然后将其用于设计秘密分享方案. 平面函数还被用于构造验证码[30]、常重复合码[34] 和信号集[33]. 它们还被用于构造一些组合结构，比如斜 Hadamard 差集和 Paley 型的部分差集[93].

对于 $p = 2$ 的情形，不存在有限域 $\mathbb{F}_{2^n}$ 上的平面函数：因为若 x 满足 $f(x+\epsilon) - f(x) = d$，则 $x + \epsilon$ 亦满足. 此时我们称一个函数 $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ 是 *几乎完全非线性的*（almost perfect nonlinear），若对任一 $\epsilon \in \mathbb{F}_{2^n}^*$ 映射 (1.1) 都是 2-到-1 的. 遗憾的是，几乎完全非线性函数和有限射影平面没有多少直接的联系. 直到最近，Zhou[97] 在偶特征的有限域上提出了一个新的“伪平面函数”的定义，由它我们可以得到有限射影平面.

在第 5 章中我们将构造三类新的伪平面二项式函数，其中的两类是无穷类. 另外我们发现任一伪平面函数都将给出一个定义在 Galois 环上的 5 类结合方案. 我们的结果可以看作是 Liebler 和 Mena[58] 及 Bonnecaze 和 Duursma[13] 等人结果的推广. Abdukhalikov、Bannai 和 Suda[2] 及 LeCompte、Martin 和 Owens[55] 也构造过类似的 4 类结合方案. 本章中的内容已经被《Designs, Codes and Cryptography》杂志接收.

1.4.3 循环码的重量分布

给定素数 p 和有限域 $\mathbb{F}_p$ 上长为 l 的循环码 $\mathcal{C}$. 令 A_i 表示 $\mathcal{C}$ 中汉明重量（Hamming weight）等于 i 的码字数目. 关于重量分布 $\{A_0, A_1, \ldots, A_l\}$ 的研究是编码理论中非常重要的课题. 令 $h(x)$ 为 $\mathcal{C}$ 的校验多项式. 我们称 $\mathcal{C}$ 是 *不可约的*（*可约的*）若 $h(x)$ 在 $\mathbb{F}_p$ 上是不可约的（可约的）. 当 $h(x)$ 可以表示成 $h(x) =$

$h_0(x)h_1(x)\cdots h_{s-1}(x)$，其中 $h_i(x)$ 为 $\mathbb{F}_p$ 上不可约多项式，则码 $\mathcal{C}$ 是一个具有 s 个零点的循环码的对偶码.

McEliece[68] 证明了不可约的循环码的重量分布可以由 Gauss 和表示出来. 因此我们可以利用数论中的技巧来决定循环码的重量分布[40,68,69,87,94]. 遗憾的是，通常情况下计算 Gauss 和是非常困难的. 对于只具有一种非零重量的不可约循环码，Ding 等[33,88,89] 已经给出了很好的刻画. 而只具有两种非零重量的不可约循环码也已经被人们所广泛研究. Schmidt 与 White[81] 给出了一个不可约循环码具有至多两种非零重量的充要条件，并且他们进一步猜测所有的只具有两种非零重量的不可约循环码是由两个无穷类和另外 11 个散在的例子组成. 更多的信息可以在文献[33] 中找到.

对于可约的循环码，它的重量分布的计算则牵涉到指数和的计算. 尽管在一些文献中[31,38,50,61–65,71,96] 可以得到简洁的计算结果，但是通常情况下这都是非常复杂的. 在已知的绝大部分文献中，这类循环码的对偶码都具有两个或三个零点.

在第 6 章中，我们决定了一类可约循环码的重量分布. 特别地，它的对偶码可以具有任意多个零点. 我们的主要工作是建立了相关的指数和与 Hermitian 型图的谱之间的对应关系. 本章中内容已经发表在《IEEE Transactions on Information Theory》杂志上.

2 Whist 赛程设计

2.1 引言

关于 v 名选手的 whist 赛程设计 (tournament) 是一类特殊的参数为 $(v, 4, 3)$ 的（拟）可分解平衡不完全区组设计 (RBIBD). 它的每一个区组 (a, b, c, d) 代表一局 whist 比赛，且在这局比赛中 (a, c) 搭档对抗 (b, d) 搭档. 一个 whist 赛程设计 Wh(v) 需要满足以下的“whist”条件：任何一名选手与其他的每一名选手都恰好搭档过一次并且恰好对抗过两次. 它的每一个（部分）平行类代表了这个赛程设计的一轮比赛. Whist 赛程设计的存在性问题最早是由 Moore[75] 于1896年提出，之后便吸引了 Wilson、Baker、Hartman 等众多组合设计学者的注意. 自1970年以来，人们已经知道当 $v \equiv 0, 1 \pmod 4$ 时 Wh(v) 恒存在. 有关 whist 赛程设计的更多介绍，读者可以参考 Anderson 的文章[4].

下面令集合 $\mathcal{X} = \mathbb{Z}_m \cup \mathcal{A}$，其中当 $v \equiv 1 \pmod 4$ 时，$m = v$，$\mathcal{A} = \emptyset$；当 $v \equiv 0 \pmod 4$ 时，$m = v - 1$，$\mathcal{A} = \{\infty\}$. 为了方便，我们将一个 whist 赛程设计的所有 v 名选手依次标记为集合 $\mathcal{X}$ 中的元素，同时将它的所有（部分）平行类依次标记为 R_1，R_2，$\cdots$，R_m. 如果它的每一个平行类 R_{j+1} 均是由 R_j 中每个元素进行运算 $+1 \pmod m$ 后得到的，那么我们就称这个 whist 赛程设计是 $\mathbb{Z}$-循环的. 这里当集合 $\mathcal{X}$ 包含元素 ∞ 时，我们规定 $\infty + 1 \equiv \infty \pmod m$. 容易看出 $\mathbb{Z}$-循环的 whist 赛程设计由它的任一平行类完全确定，从而我们可以取定某一个平行类来代表这个设计. 特别地我们称之为初始平行类，并且规定当 $v \equiv 1 \pmod 4$ 时，元素 0 不能出现在初始平行类中. 对称差[5] 将会是我们用来判定一组区组是否构成一个 $\mathbb{Z}$-循环的 whist 赛程设计的初始平行类的重要工具.

设 G 是一个有限交换群，并且它的阶 $|G| \equiv 1 \pmod 2$. 集合 $\{(x, -x) : x \in G \backslash \{e_G\}\}$（其中 e_G 是群 G 的单位元）叫作是群 G 的 *patterned starter*. 类似地称集合 $\{(x, -x) : x \in G \backslash \{e_G\}\} \cup \{(\infty, e_G)\}$ 为 $\mathcal{X} = G \cup \infty$ 的 patterned starter. 进一步设 $G = \mathbb{Z}_m$，其中 m 如上一段中所定义. 若一个 $\mathbb{Z}$-循环的 Wh(v) 的初始平行类中所有

搭档构成的配对恰是 $\mathcal{X}$ 的 patterned starter，则称它是一个 $\mathbb{Z}$-循环的 patterned starter whist 赛程设计，简记为 $\mathbb{Z}$CPS-Wh(v).

当 v 是有限个模 4 余 1 的素数的积时，Watson[92] 在1954年便给出了 $\mathbb{Z}$CPS-Wh(v) 的一种构造方法. 之后 Bose 和 Cameron[14] 于1965年和 Baker[7] 于1975年又分别独立地对 v 是模 4 余 1 的素数的情形给出了 $\mathbb{Z}$CPS-Wh(v) 新的两种构造方法.

定理 2.1: [7,14,92] 当 v 是有限个模 4 余 1 的素数的积时，$\mathbb{Z}$CPS-Wh(v) 恒存在.

在过去的二十来年里，很多学者都研究过 $\mathbb{Z}$CPS-Whs 的存在性问题，主要的文献有 Finizio[37]，Finizio 和 Leonard[38]，Leonard[56]，Leonard 和 Jones[57]，Abel、Anderson 和 Finizio[3]. 下面我们简要回顾一下它的研究历史.

在1994年，Finizio[37] 率先提出了 $\mathbb{Z}$-循环的 patterned starter whist 赛程设计的概念，并且对所有的 $5 \leq v \leq 41$，$v \equiv 1 \pmod 4$ 得到了完整的存在性结果. 随后 Leonard[56] 给出了 $\mathbb{Z}$CPS-Wh(q^2) 的一种构造方法，其中 q 是模 4 余 3 的素数. Leonard[56]、Leonard 和 Jones[57] 则进一步利用这个方法对所有的 $7 \leq q \leq 5000$ 构造了 $\mathbb{Z}$CPS-Wh(q^2)，其中 q 是模 4 余 3 的素数.

除了上述例子之外，Abel、Anderson 和 Finizio[3] 构造了仅有的两个参数较小的 $\mathbb{Z}$CPS-Wh(v)，其中 $v \equiv 1 \pmod 4$. 对 $v \equiv 0 \pmod 4$ 的情形，人们目前只知道当 $v \in \{4, 28, 40, 76, 112, 148\}$ 时 $\mathbb{Z}$CPS-Wh(v) 存在，具体的例子请参见文献[3,38,75]. 最近 Abel、Anderson 和 Finizio[3] 证明了以下的必要条件.

定理 2.2: [3] 当 $v \equiv 9 \pmod{12}$ 时，$\mathbb{Z}$CPS-Wh(v) 只在 $v \equiv 81 \pmod{108}$ 的情形下才有可能存在.

2.2 不存在性结果

定理 2.3: 给定任一非负整数 k. 若 $v = 12k + 9$，则 $\mathbb{Z}$CPS-Wh(v) 不存在.

证明. 令 $h = 3k + 2$，于是 $v = 4h + 1$. 下面我们将用反证法证明. 首先假设存在一个 $\mathbb{Z}$CPS-Wh$(4h + 1)$. 不妨记它的初始平行类为

$$\{a_i, b_i, -a_i, -b_i\}, 1 \leq i \leq h.$$

根据定义，我们有

$$\{\pm a_i, \pm b_i \,|1 \le i \le h\} = \{\pm(a_i + b_i), \pm(a_i - b_i)|1 \le i \le h\} = \mathbb{Z}_v \setminus \{0\}.$$

于是

$$2\sum_{i=1}^{h}(a_i^2 + b_i^2) \equiv 4\sum_{i=1}^{h}(a_i^2 + b_i^2) \equiv S \pmod{v},$$

其中 $S = \sum_{i=0}^{v-1} i^2$. 从而

$$\begin{aligned} S &= 2S - S \\ &\equiv 2\left(2\sum_{i=1}^{h}(a_i^2 + b_i^2)\right) - \left(4\sum_{i=1}^{h}(a_i^2 + b_i^2)\right) \\ &\equiv 0 \pmod{v}. \end{aligned}$$

整理可得

$$S = \sum_{i=0}^{v-1} i^2 = \frac{(v-1)v(2v-1)}{6} \equiv 0 \pmod{v},$$

也就是说

$$(v-1)(2v-1) \equiv 0 \pmod{6}.$$

由此可知 $v \equiv 1, 5 \pmod{12}$，也就证明了 $\mathbb{Z}$CPS-Wh$(12k+9)$ 不存在. □

定理 2.4: 给定任一非负整数 k. 若 v 满足下述条件之一:

(i) $v = 12k$ 且 $v-1$ 无平方因子,

(ii) $v = 12k+8$ 且 $v-1$ 无平方因子,

则 $\mathbb{Z}$CPS-Wh(v) 不存在.

证明. 设 $v = 4h$. 下面我们用反证法证明. 首先假设存在一个 $\mathbb{Z}$CPS-Wh$(4h)$. 不妨记它的初始平行类为

$$\{\infty, \alpha, 0, -\alpha\}, \{a_i, b_i, -a_i, -b_i\}, 1 \le i \le h-1.$$

根据定义可知

$$\begin{aligned} \{\pm\alpha\} \cup \{\pm a_i, \pm b_i | 1 \le i \le h-1\} &= \mathbb{Z}_{v-1} \setminus \{0\}, \\ \{\pm\alpha\} \cup \{\pm(a_i + b_i), \pm(a_i - b_i) | 1 \le i \le h-1\} &= \mathbb{Z}_{v-1} \setminus \{0\}. \end{aligned}$$

从而有

$$2\alpha^2+2\sum_{i=1}^{h-1}(a_i^2+b_i^2)\equiv 2\alpha^2+4\sum_{i=1}^{h-1}(a_i^2+b_i^2)\equiv S \pmod{v-1},$$

其中 $S=\sum_{i=0}^{v-2} i^2$. 由此可得

$$\begin{aligned}2\alpha^2 &= 4\alpha^2-2\alpha^2\\ &= 2\left(2\alpha^2+2\sum_{i=1}^{h-1}(a_i^2+b_i^2)\right)-\left(2\alpha^2+4\sum_{i=1}^{h-1}(a_i^2+b_i^2)\right)\\ &\equiv 2S-S\\ &\equiv S \pmod{v-1}. \end{aligned} \tag{2.1}$$

若 $v=12k$，则

$$S=\frac{(v-2)(v-1)(2v-3)}{6}=(v-1)(6k-1)(8k-1)\equiv 0 \pmod{v-1}.$$

于是

$$2\alpha^2\equiv S\equiv 0 \pmod{v-1}.$$

又因为 $v-1$ 为奇数，所以

$$\alpha^2\equiv 0 \pmod{v-1}.$$

现在进一步假设 $v-1$ 无平方因子，那么就有 $\alpha=0$，而这与假设条件 $\alpha\neq 0$ 矛盾. 因此也就证明了当 $v=12k$ 且 $v-1$ 无平方因子时 $\mathbb{Z}$CPS-Wh(v) 不存在.

同样的分析可以证明结论 (ii). □

定理 2.5: 给定任一非负整数 k. 设 $v=12k+4$. 若 $\mathbb{Z}$CPS-Wh(v) 存在且 $\frac{v-1}{3}$ 无平方因子，则区组 $\{\infty,\alpha,0,-\alpha\}$，其中 $\alpha=\frac{v-1}{3}$ 或 $\alpha=\frac{2(v-1)}{3}$，必定出现在初始平行类中.

证明. 根据定理 2.4 的证明可得

$$\begin{aligned}S &= \frac{(v-2)(v-1)(2v-3)}{6}\\ &= \frac{v-1}{3}(6k+1)(24k+5)\\ &\equiv 0 \pmod{\frac{v-1}{3}}.\end{aligned}$$

再结合等式 (2.1)，我们得到

$$2\alpha^2 \equiv S \equiv 0 \pmod{\frac{v-1}{3}}.$$

又因为 $\frac{v-1}{3} = 4k+1$为奇数，所以

$$\alpha^2 \equiv 0 \pmod{\frac{v-1}{3}}.$$

根据条件 $\frac{v-1}{3}$ 无平方因子可知 $\frac{v-1}{3}$ 必整除 α，由此我们得到 $\alpha = \frac{v-1}{3}$ 或 $\alpha = \frac{2(v-1)}{3}$. □

定理 2.6: 给定一个正整数 v. 设 $v \equiv 4 \pmod{12}$，$v-1 = 3^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$，其中 p_i 为互不相同的素数且均不等于 3，$a_0 \geq 1$，a_i 是互不相同的非负整数. 则

(i) 当 a_0 为偶数时，$\mathbb{Z}$CPS-Wh(v) 不存在.

(ii) 当 a_0 为奇数时，若 $\mathbb{Z}$CPS-Wh(v) 存在，则 $p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s} \equiv 1 \pmod{12}$.

证明. 记 $v = 12k+4$，$r = (v-4)/4$. 下面我们用反证法证明. 假设存在一个 $\mathbb{Z}$CPS-Wh(v). 不妨记它的初始平行类为

$$\{\infty, \alpha, 0, -\alpha\},$$
$$\{a_i, b_i, -a_i, -b_i\}\ (1 \leq i \leq r).$$

根据定义可知

$$\{\pm\alpha\} \cup \{\pm a_i, \pm b_i \mid 1 \leq i \leq r\} = \mathbb{Z}_{v-1} \setminus \{0\};$$
$$\{\pm\alpha\} \cup \{\pm(a_i+b_i), \pm(a_i-b_i) \mid 1 \leq i \leq r\} = \mathbb{Z}_{v-1} \setminus \{0\}.$$

计算两边的平方和，可得

$$\begin{aligned} 2\alpha^2 + 2\sum_{i=1}^{r}(a_i^2+b_i^2) &\equiv 2\alpha^2 + 4\sum_{i=1}^{r}(a_i^2+b_i^2) \\ &\equiv \sum_{j=0}^{v-2} j^2 \pmod{v-1}. \end{aligned}$$

从而有

$$\begin{aligned} 2\alpha^2 &= 2\left[2\alpha^2 + 2\sum_{i=1}^{r}(a_i^2+b_i^2)\right] - \left[2\alpha^2 + 4\sum_{i=1}^{r}(a_i^2+b_i^2)\right] \\ &\equiv 2\sum_{j=0}^{v-2} j^2 - \sum_{j=0}^{v-2} j^2 \\ &\equiv \sum_{j=0}^{v-2} j^2 \pmod{v-1}. \end{aligned} \tag{2.2}$$

另外我们计算

$$\begin{aligned} \sum_{j=0}^{v-2} j^2 &= \frac{(v-2)(v-1)(2v-3)}{6} \\ &= \frac{v-2}{2}\cdot\frac{v-1}{3}\cdot(2v-3). \end{aligned}$$

因此

$$2\alpha^2 \equiv \sum_{j=0}^{v-2} j^2 \equiv 0 \pmod{\frac{v-1}{3}}.$$

又因为 $(v-1)/3 = 4k+1$ 为奇数，所以

$$\alpha^2 \equiv 0 \pmod{\frac{v-1}{3}}.$$

我们令

$$\alpha^2 = m\cdot\frac{v-1}{3},$$

并把它代入等式 (2.2)，可得

$$\begin{aligned} 2m\cdot\frac{v-1}{3} &\equiv \frac{v-2}{2}\cdot\frac{v-1}{3}\cdot(2v-3) \\ &\equiv (-1)\cdot\frac{v-2}{2}\cdot\frac{v-1}{3} \pmod{v-1}. \end{aligned}$$

整理可得

$$(2m+\frac{v-2}{2})\cdot\frac{v-1}{3} \equiv 0 \pmod{v-1},$$

也就是说

$$2m+\frac{v-2}{2} = 2m+6k+1 \equiv 0 \pmod{3}.$$

所以

$$m \equiv 1 \pmod{3}.$$

下面我们分两种情形来进行讨论：(i) a_0 为偶数，(ii) a_0 为奇数.

(i) a_0 为偶数：

根据

$$\alpha^2 = m \cdot \frac{v-1}{3} = 3^{a_0-1} \cdot (mp_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}),$$

$a_0 - 1$ 为奇数，$\gcd(mp_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}, 3) = 1$，可知等式两边因子 3 出现的次数不可能相等，由此得到矛盾，也就证明了此时 $\mathbb{Z}$CPS-Wh(v) 不存在.

(ii) a_0 为奇数：

记 $a_0 = 2c + 1$. 根据

$$\alpha^2 = m \cdot \frac{v-1}{3} = 3^{2c} \cdot (mp_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}),$$

可知 $mp_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ 必为平方数，所以

$$mp_1^{a_1}p_2^{a_2}\cdots p_s^{a_s} \equiv 1 \pmod 3.$$

从而

$$p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s} \equiv 1 \pmod 3. \tag{2.3}$$

另外从 a_0 为奇数可知

$$3^{a_0} \equiv 3 \pmod{12}.$$

根据上式和

$$v - 1 = 3^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s} \equiv 3 \pmod{12},$$

我们有

$$p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s} \equiv 1 \pmod 4. \tag{2.4}$$

再结合 (2.3) 和 (2.4), 我们推出

$$p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s} \equiv 1 \pmod{12}.$$

□

推论 2.1 ([3]): 给定任一非负整数 v. 设 $v \equiv 4 \pmod{12}$. 若 $\mathbb{Z}$CPS-Wh(v) 存在，则 $v \equiv 4 \pmod{36}$ 或 $v \equiv 28 \pmod{108}$.

证明. 我们首先排除 $v \equiv 16 \pmod{36}$ 的情形：设 $v = 36k + 16$，于是

$$v - 1 = 36k + 15 = 3 \times (12k + 5).$$

根据定理 2.6 (ii) 可知此时 $\mathbb{Z}$CPS-Wh(v) 不存在. 因此在 $v \equiv 4 \pmod{12}$ 的条件下，$\mathbb{Z}$CPS-Wh(v) 只在 $v \equiv 4 \pmod{36}$ 或 $v \equiv 28 \pmod{36}$ 时才可能存在. 特别地，如果 $v \equiv 28 \pmod{36}$，不妨记 $v = 36k + 28$，于是

$$v - 1 = 36k + 27 = 3^2 \times (4k + 3).$$

根据定理 2.6 (i)，3 必然整除 $4k + 3$，也就是说 $v \equiv 28 \pmod{108}$. □

2.3 $\mathbb{Z}$CPS-Whs 的 frame 构造

自1986年 Stinson[86] 首先引进了 frame 的概念之后，frame 就在可分解平衡不完全区组设计（RBIBD）的研究中发挥了重要的作用[39]. Lu 和 Zhu[60] 进一步提出了 triplewhist tournament frame 的概念，并利用它们几乎完整地解决了 triplewhist tournament designs 的存在性问题. 之后 Ge 和 Zhu[42] 定义并利用 $\mathbb{Z}$-cyclic triplewhist tournament frames 来构造 $\mathbb{Z}$-cyclic triplewhist tournaments[41].

令 S 是 v 个参赛选手的集合 （$|S| = v$），而 $\mathcal{H} = \{S_1, S_2, \cdots, S_n\}$ 是集合 S 的一个划分. 假设 $|S_i| = s_i$ 并且对于任意的 i，$1 \le i \le n$，都成立 $v - s_i \equiv 0 \pmod{4}$. 若集合 $S \backslash S_i$ 中任一元素在一组区组中恰好出现一次，也就是说这组区组恰好形成了集合 $S \backslash S_i$ 的一个划分，则我们称这组区组是一个*带“洞” S_i 的部分平行类*.

下面我们就来定义 whist tournament frame. 若一组区组的集合满足以下的条件：

(i) 所有的区组可以被分成一些带洞的部分平行类，并且其中恰有 s_i 个带洞 S_i 的部分平行类（易知每个部分平行类包含 $(v - s_i)/4$ 个区组）；

(ii) 除了 s_i 个带洞 S_i 的部分平行类之外，集合 $S \backslash S_i$ 中任一元素在其余每个带洞部分平行类中恰出现一次；

(iii) 各自分别来自两个不同洞的元素恰搭档一次；

(iv) 各自分别来自两个不同洞的元素恰对抗两次；

则称这组区组为一个型为 $(s_1, s_2, \cdots, s_n)$ 的 *whist tournament frame*（简记为 Wh-frame）.

我们将用以下的“指数”符号来标记一个 frame 的型：型 $t_1^{u_1} \ldots t_m^{u_m}$ 表示在多重集 $\{s_1, s_2, \cdots, s_n\}$ 中元素 t_i 出现的次数为 u_i，$1 \leq i \leq m$. 若 $s_1 = \cdots = s_n = s$, 则称这样的 Wh-frame 是型一致的（uniform type），简记为 Wh-frame(s^n). 特别地，当 $v \equiv 1 \pmod 4$ 时，一个型为 1^v 的 Wh-frame 就是一个 Wh(v).

设 $\mathcal{X} = \mathbb{Z}_v, v = hn$，且群 H 是 $\mathbb{Z}_v$ 的一个阶为 h 的子群. 若一个 Wh-frame(h^n) 中存在一个带洞 H 的平行类，并且其余的带洞平行类都可以通过对带洞 H 平行类中每个元素进行运算 $+1 \pmod v$ 后得到，则我们称它是 $\mathbb{Z}$-循环的. 特别地，称带洞 H 的平行类为初始平行类.

类似地，设 G 是一个有限交换群，并且它的阶 $|G| \equiv 1 \pmod 2$. 设 H 为 G 的一个子群. 集合 $\{(x, -x) : x \in G \backslash H\}$ 叫作是 $G \backslash H$ 的 *patterned starter*. 设 $G = \mathbb{Z}_v, v = hn$，且群 H 是 $\mathbb{Z}_v$ 的一个阶为 h 的子群. 若一个 $\mathbb{Z}$-循环的 Wh-frame(h^n) 的初始平行类中所有搭档构成的配对恰是 $\mathbb{Z}_v \backslash H$ 的 patterned starter，则称它是一个 $\mathbb{Z}$-循环的 patterned starter whist tournament frame，简记为 $\mathbb{Z}$CPS-Wh-frame(h^n).

例 2.1: 以下的 9 个区组构成了一个 $\mathbb{Z}$CPS-Wh-frame(3^{13}) 的初始平行类：

$$(5, 24, 34, 15), \quad (4, 27, 35, 12), \quad (7, 11, 32, 28), \quad (2, 36, 37, 3),$$
$$(1, 29, 38, 10), \quad (14, 31, 25, 8), \quad (6, 18, 33, 21), \quad (9, 16, 30, 23),$$
$$(17, 19, 22, 20).$$

引理 2.1: 若 $\mathbb{Z}$CPS-Wh-frame$(h^{(v/h)})$ 和 $\mathbb{Z}$CPS-Wh-frame$(t^{(h/t)})$ 都存在，则 $\mathbb{Z}$CPS-Wh-frame$(t^{(v/t)})$ 存在.

证明. 记 R_1 和 R_2 分别为前两个 $\mathbb{Z}$CPS-Wh-frames 的初始平行类. 将 R_2 中的每一个元素 x 替换成 $(\frac{v}{h})x$ 并将得到的区组集合记为 R_2^*. 容易验证 $R_1 \cup R_2^*$ 就构成了 $\mathbb{Z}$CPS-Wh-frame$(t^{(v/t)})$ 的一个初始平行类. □

令 $t = 1$，我们有：

引理 2.2: 给定非负整数 $h \equiv 1 \pmod 4$. 若 $\mathbb{Z}$CPS-Wh-frame(h^n) 和 $\mathbb{Z}$CPS-Wh(h) 都存在，则 $\mathbb{Z}$CPS-Wh(hn) 存在.

类似的，我们有：

引理 2.3：*给定非负整数* $h \equiv 3 \pmod 4$. *若* $\mathbb{Z}$CPS-Wh-frame(h^n) *和* $\mathbb{Z}$CPS-Wh$(h+1)$ *都存在，则* $\mathbb{Z}$CPS-Wh$(hn+1)$ *存在.*

证明. 记 R_1 和 R_2 分别为 $\mathbb{Z}$CPS-Wh-frame 和 $\mathbb{Z}$CPS-Wh 的初始平行类. 将 R_2 中的每一个元素 x 替换成 nx（元素 ∞ 保持不变）并将得到的区组集合记为 R_2^*. 容易验证 $R_1 \cup R_2^*$ 就构成了 $\mathbb{Z}$CPS-Wh$(hn+1)$ 的一个初始平行类. □

定理 2.7：*若* $\mathbb{Z}$CPS-Wh-frame(h^n) *存在，则参数* h, n *必然满足*

(i) *若* $h \equiv 1, 5 \pmod 6$，*则* $n \equiv 1, 5 \pmod{12}$，

(ii) *若* $h \equiv 3 \pmod 6$，*则* $n \equiv 1 \pmod{12}$.

证明. 根据定义可知

$$h(n-1) \equiv 0 \pmod 4.$$

从而

$$n \equiv 1 \pmod 4,$$

也就是说

$$n \equiv 1, 5 \text{ 或 } 9 \pmod{12}.$$

令 $r = h(n-1)/4$ 且以下的 r 个区组

$$\{a_i, b_i, -a_i, -b_i\}, 1 \le i \le r,$$

为 $\mathbb{Z}$CPS-Wh-frame(h^n) 的一个初始平行类. 同样地，根据定义可知

$$\begin{aligned}\{\pm a_i, \pm b_i \,|1 \le i \le r\} &= \{\pm(a_i + b_i), \pm(a_i - b_i) | 1 \le i \le r\} \\ &= \mathbb{Z}_{hn} \setminus \{0, n, 2n, \cdots, (h-1)n\}.\end{aligned}$$

因此

$$2\sum_{i=1}^{r}(a_i^2 + b_i^2) \equiv 4\sum_{i=1}^{r}(a_i^2 + b_i^2) \equiv \sum_{j=0}^{hn-1} j^2 - \sum_{k=0}^{h-1} k^2 n^2 \pmod{hn}.$$

从而

$$\begin{aligned}\sum_{j=0}^{hn-1} j^2 - \sum_{k=0}^{h-1} k^2n^2 &= 2\left[\sum_{j=0}^{hn-1} j^2 - \sum_{k=0}^{h-1} k^2n^2\right] - \left[\sum_{j=0}^{hn-1} j^2 - \sum_{k=0}^{h-1} k^2n^2\right] \\ &\equiv 2\left[2\sum_{i=1}^{h}(a_i^2+b_i^2)\right] - \left[4\sum_{i=1}^{h}(a_i^2+b_i^2)\right] \\ &\equiv 0 \pmod{hn}.\end{aligned}$$

所以

$$\begin{aligned}\sum_{j=0}^{hn-1} j^2 - \sum_{k=0}^{h-1} k^2n^2 &= \frac{(hn-1)hn(2hn-1)}{6} - \frac{(h-1)h(2h-1)}{6}n^2 \\ &= \frac{(hn-1)(2hn-1)-(h-1)(2h-1)n}{6}hn \\ &\equiv 0 \pmod{hn},\end{aligned}$$

也就是说

$$(hn-1)(2hn-1)-(h-1)(2h-1)n \equiv 0 \pmod 6. \tag{2.5}$$

如果 $h \equiv 1 \pmod 6$, 那么等式 (2.5) 就化为

$$(n-1)(2n-1) \equiv 0 \pmod 6.$$

由此我们可以得到 $n \equiv 1, 5 \pmod{12}$.

如果 $h \equiv 5 \pmod 6$, 那么等式 (2.5) 就化为

$$(5n-1)(4n-1) \equiv 0 \pmod 6.$$

同样地，我们也得到了 $n \equiv 1, 5 \pmod{12}$.

最后如果 $h \equiv 3 \pmod 6$, 那么等式 (2.5) 就化为

$$n-1 \equiv 0 \pmod 6.$$

容易看出此时 $n \equiv 1 \pmod{12}$. □

2.4 $\mathbb{Z}$CPS-Wh-frame(3^p) 的构造

在这一节中，我们将构造 $\mathbb{Z}$CPS-Wh-frame(3^n) 的一个无穷类，并利用它们来得到满足 $v \equiv 0 \pmod 4$ 条件的 $\mathbb{Z}$CPS-Wh(v). 根据引理 2.3 和文献[3] 中定理 3.2，我们有以下的必要条件.

引理 2.4: 若 $\mathbb{Z}$CPS-Wh-frame(3^n) 存在，则 $n \not\equiv 5 \pmod{12}$.

关于特征和的 Weil 定理将是我们这一节中证明的主要工具.

定理 2.8 ([59]): 设 ψ 为域 $GF(q)$ 的阶为 $m > 1$ 的乘法特征. 令 $f \in GF(q)[x]$ 是一个首 1 正次数多项式并且不能表示成一个多项式的 m 次方. 记 d 为 f 在 $GF(q)$ 的分裂域中互异根的数目. 则对任意的 $a \in GF(q)$，我们有

$$\left| \sum_{c \in GF(q)} \psi(af(c)) \right| \leq (d-1)\sqrt{q}.$$

给定一个素数 $p \equiv 1 \pmod{m}$ 和群 $\mathbb{Z}_p$ 的一个本原元 ω，我们用 C_0^m 来表示 $\mathbb{Z}_p$ 的乘法子群 $\{\omega^{im} \mid 0 \leq i < (p-1)/m\}$，用 C_j^m 来表示 C_0^m 的陪集，即 $C_j^m = \omega^j \cdot C_0^m$.

2.4.1 $p \equiv 13 \pmod{24}$ 的情形

从 $\gcd(p, 3) = 1$ 可知 $\mathbb{Z}_p \times \mathbb{Z}_3$ 同构于 $\mathbb{Z}_{3p}$. 我们首先给定以下 9 个基于加法群 $\mathbb{Z}_p \times \mathbb{Z}_3$ 上的区组：

$$\begin{aligned}
&B_1 = \{(1,0),(x,0)\}, && B_2 = \{(y^2,0),(y,1)\}, && B_3 = \{(y^3,0),(y^2,1)\},\\
&B_4 = \{(y^4,0),(y^3,1)\}, && B_5 = \{(y^5,0),(y^6,1)\}, && B_6 = \{(x^4,1),(x^5,1)\},\\
&B_7 = \{(z^7,1),(z^8,1)\}, && B_8 = \{(z^9,1),(z^{10},1)\}, && B_9 = \{(z^{11},1),(z^{12},1)\}.
\end{aligned}$$

需要说明的是：在这里我们用一个区组的前面两个元素来表示整个区组. 比如集合 $B_2 = \{(y^2,0),(y,1)\}$ 代表了区组 $((y^2,0),(y,1),(-y^2,0),(-y,2))$.

给定一个区组 $B = \{a, b\}$. 我们记 $\pm B = \{a, b, -a, -b\}$，$\Delta B = \{\pm(a+b), \pm(a-b)\}$. 不难验证

$$\begin{aligned}
\bigcup_{i=1}^{9} \pm B_i &= \bigcup_{j=0}^{2} \mathcal{A}_j \times \{j\}\,,\\
\bigcup_{i=1}^{9} \Delta B_i &= \bigcup_{j=0}^{2} \mathcal{B}_j \times \{j\}\,,
\end{aligned}$$

其中

$$\begin{aligned}
\mathcal{A}_0 &= \{\pm 1, \pm x, \pm y^2, \pm y^3, \pm y^4, \pm y^5\},\\
\mathcal{A}_1 &= \{y, y^2, y^3, x^4, x^5, y^6, z^7, z^8, z^9, z^{10}, z^{11}, z^{12}\},\\
\mathcal{A}_2 &= \{-a \mid a \in \mathcal{A}_1\},\\
\mathcal{B}_0 &= \{\pm(x+1), \pm(x-1), \pm x^4(x-1), \pm z^7(z-1), \pm z^9(z-1), \pm z^{11}(z-1)\},\\
\mathcal{B}_1 &= \{y(y+1), y^2(y+1), y^3(y+1), y^5(y+1)\}\\
&\quad \cup\{-y(y-1), -y^2(y-1), -y^3(y-1), y^5(y-1)\}\\
&\quad \cup\{-x^4(x+1), -z^7(z+1), -z^9(z+1), -z^{11}(z+1)\},\\
\mathcal{B}_2 &= \{-a \mid a \in \mathcal{B}_1\}.
\end{aligned}$$

如果 $\mathcal{A}_i$，$\mathcal{B}_i$，$0 \le i \le 2$ 中的任一集合都是 $\mathbb{Z}_p^*/C_0^{12}$ 的一个完全代表系，那么区组集合

$$\mathcal{F} = \{B_i \cdot (s, 1) \mid 1 \le i \le 9, s \in C_0^{12}\}$$

就构成了 $\mathbb{Z}$CPS-Wh-frame(3^p) 的一个初始平行类.

引理 2.5：*给定任一素数 $p \equiv 13 \pmod{24}$. 若 $p > 9150625$，则 $\mathbb{Z}$CPS-Wh-frame(3^p) 存在.*

证明. 容易验证如果元素 $x, y, z \in \mathbb{Z}_p$ 满足以下的条件：

$$\begin{aligned}
&\text{(a) } x \in C_1^{12}, \quad x+1 \in C_k^{12}, \quad x-1 \in C_{k-2}^{12},\\
&\text{(b) } y \in C_1^{12}, \quad y+1 \in C_{k-2}^{12}, \quad y-1 \in C_k^{12},\\
&\text{(c) } z \in C_1^{12}, \quad z+1 \in C_{k+1}^{12}, \quad z-1 \in \bigcup_{i \in \{0,2,4,6,8,10\}} C_{k+i}^{12},
\end{aligned}$$

其中整数 k 满足 $0 \le k \le 11$（此处 C^{12} 的下指标进行模 12 的运算），那么 $\mathcal{A}_i$，$\mathcal{B}_i$，$0 \le i \le 2$ 中任一集合均是 $\mathbb{Z}_p^*/C_0^{12}$ 的一个完全代表系. 根据前面的讨论可知区组集合 $\mathcal{F}$ 构成了 $\mathbb{Z}$CPS-Wh-frame(3^p) 的一个初始平行类.

现在我们就来证明存在满足前面所列条件的元素 $x, y, z \in \mathbb{Z}_p$. 给定 $\mathbb{Z}_p$ 的一个本原元 ω. 记 $f_1(x) = \omega^{11}x$，$f_2(x) = \omega^{12-k}(x+1)$，$f_3(x) = \omega^{14-k}(x-1)$. 条件 (a) 等价

于对 $1 \le j \le 3$，$f_j(x) \in C_0^{12}$. 令 χ 为一个阶为 12 的乘法特征，也就是说对 $x \in C_i^{12}$，有 $\chi(x) = \theta^i$, 其中 θ 是一个 12 次本原单位根. 记 $B_i = \chi(f_i(x)), 1 \le i \le 3$. 则

$$1 + B_i + B_i^2 + \cdots + B_i^{11} = \begin{cases} 12, & \text{if } f_i(x) \in C_0^{12}, \\ 0, & \text{if } f_i(x) \notin C_0^{12} \cup \{0\}, \\ 1, & \text{if } f_i(x) = 0. \end{cases}$$

令和式

$$S = \sum_{x \in \mathbb{Z}_p} \prod_{i=1}^{3} (1 + B_i + B_i^2 + \cdots + B_i^{11}). \tag{2.6}$$

则 $S = 12^3 n + d$，其中 n 是 $\mathbb{Z}_p$中满足条件 (a) 的元素 x 的个数，d 是当 $f_1(x)$、$f_2(x)$、$f_3(x)$ 中某个值等于 0 时上式右边的贡献值. 若 $f_1(x) = 0$，则 $x = 0$，$f_2(0) = w^{12-k}$，$f_3(0) = -w^{14-k}$. 根据条件 $p \equiv 13 \pmod{24}$ 可知 $-1 \in C_6^{12}$. 于是命题 $f_2(0) \in C_0^{12}$ 和 $f_3(0) \in C_0^{12}$ 无法同时成立. 因此它对和式 S 的贡献值为 0. 若 $f_2(x) = 0$，则 $x = -1$，$f_1(x) = -\omega^{11} \notin C_0^{12} \cup \{0\}$，于是它对和式 S 的贡献值亦为 0. 若 $f_3(x) = 0$，则 $x = 1$，$f_1(x) = \omega^{11} \notin C_0^{12} \cup \{0\}$，于是它对和式 S 的贡献值亦为 0. 综上所述，可知 d 总是等于 0. 于是如果我们能够证明 $|S| > 0$，也就立即可以推出存在满足条件 (a) 的元素 $x \in \mathbb{Z}_p$. 展开等式 (2.6) 的右边，

$$S = \sum_{x \in \mathbb{Z}_p} 1 + \sum_{r=1}^{3} \sum_{1 \le i_1 < \cdots < i_r \le 3} \sum_{1 \le j_1, \cdots, j_r \le 11} \sum_{x \in \mathbb{Z}_p} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r}. \tag{2.7}$$

现在我们用 Weil 定理来估计这个和式. 注意 $B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} = \chi(\prod_{l=1}^{r} (f_{i_l}(x))^{j_l})$ 且 χ 的阶为 12. 若存在 $p(x) \in \mathbb{Z}_p[x]$ 使得 $\prod_{l=1}^{r} (f_{i_l}(x))^{j_l} = [p(x)]^{12}$，又因为 $f_{j_l}(x)$ 是两两互素的，则必然成立 $j_1 \equiv j_2 \equiv \cdots \equiv j_r \equiv 0 \pmod{12}$. 现在我们可以应用定理 2.8. 对任意的 $r, 1 \le r \le 3$，我们有

$$\left| \sum_{x \in \mathbb{Z}_p} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \right| \le (r-1)\sqrt{p}. \tag{2.8}$$

根据等式 (2.6)-(2.8)，

$$|S| \ge p - \sum_{r=1}^{3} \binom{3}{r} 11^r (r-1)\sqrt{p} = p - 3025\sqrt{p}. \tag{2.9}$$

从而当 $p > 9150625$ 时 $|S| > 0$. 类似地，我们可以找到满足所需条件的元素 y 与 z. □

引理 2.6: *给定任一素数 $p \equiv 13 \pmod{24}$. 若 $1213 \leq p \leq 9150625$，则 $\mathbb{Z}$CPS-Wh-frame(3^p) 存在.*

证明. 对于任意的素数 $p \equiv 13 \pmod{24}$ 且 $1213 \leq p \leq 9150625$，我们通过计算机程序找到了分别满足条件 (a)、(b)、(c) 的元素 x、y、z. 限于篇幅我们只在表 2.1 中列出相应的数对 (p, R)，其中 $1213 \leq p \leq 6037$，$R = (\omega, x, y, z, k)$. □

2.4.2 $p \equiv 1 \pmod{24}$ 的情形

容易验证 $-1 \in C_0^6$. 根据 $\gcd(p, 3) = 1$，可知 $\mathbb{Z}_p \times \mathbb{Z}_3$ 同构于 $\mathbb{Z}_{3p}$. 首先我们给定以下 9 个定义在群 $\mathbb{Z}_p \times \mathbb{Z}_3$ 上的区组:

$$
\begin{aligned}
&B_1 = \{(1,0),(a,0)\},\\
&B_2 = \{(b,0),(e,1)\},\\
&B_3 = \{(c,0),(-b-c-e,1)\},\\
&B_4 = \{(d,0),(b+2c-d+e,1)\},\\
&B_5 = \{(b+c-d,0),(-c+d-e,1)\},\\
&B_6 = \{(-f,1),(-e,1)\},\\
&B_7 = \{(c-d+e,1),(b+c+e,1)\},\\
&B_8 = \{(f,1),(-b-2c+d-2e-f,1)\},\\
&B_9 = \{(b+2c-d+2e+f,1),(-b-2c+d-e,1)\}.
\end{aligned}
$$

于是我们有

$$
\begin{aligned}
\bigcup_{i=1}^{9} \pm B_i &= \bigcup_{j=0}^{2} \pm \mathcal{A}_j \times \{j\},\\
\bigcup_{i=1}^{9} \Delta B_i &= \bigcup_{j=0}^{2} \pm \mathcal{B}_j \times \{j\},
\end{aligned}
$$

其中

$$
\begin{aligned}
&\mathcal{A}_0 = \{1, a, b, c, d, b+c-d\},\\
&\mathcal{A}_1 = \mathcal{A}_2 = \{e, f, b+c+e, c-d+e, b+2c-d+e, b+2c-d+2e+f\},\\
&\mathcal{B}_0 = \{a+1, a-1, b+2c-d+2e+2f, 2b+4c-2d+3e+f, e-f, b+d\},\\
&\mathcal{B}_1 = \mathcal{B}_2 = \{b+e, -b+e, b+2c+e, b+2c-2d+e, b+2c-d+2e, e+f\}.
\end{aligned}
$$

现在设 S 为 $C_0^6/\{\pm 1\}$ 的一个完全代表系. 若 $\mathcal{A}_i$，$\mathcal{B}_i$，$0 \leq i \leq 2$ 中的任一集合都是 $\mathbb{Z}_p^*/C_0^6$ 的一个完全代表系，则区组集合

$$
\mathcal{F} = \{B_i \cdot (s,1) \mid 1 \leq i \leq 9, s \in S\}
$$

表 2.1 (p, R): $p \equiv 13 \pmod{24}$, $1237 \leq p \leq 6037$

p	(ω, x, y, z, k)	p	(ω, x, y, z, k)	p	(ω, x, y, z, k)
1237	(2,1167,306,155,2)	1381	(2,77,159,150,5)	1429	(6,312,656,38,7)
1453	(2,557,462,249,6)	1549	(2,1358,745,270,2)	1597	(11,954,33,83,3)
1621	(2,1316,1035,221,2)	1669	(2,557,1541,93,2)	1693	(2,991,649,70,5)
1741	(2,265,872,113,5)	1789	(6,194,683,91,3)	1861	(2,436,290,248,2)
1933	(5,681,487,57,3)	2029	(2,1797,22,334,3)	2053	(2,1707,1096,288,3)
2221	(2,6,1352,156,2)	2269	(2,1244,136,120,4)	2293	(2,83,173,52,2)
2341	(7,112,758,109,2)	2389	(2,817,2383,18,2)	2437	(2,43,1133,33,5)
2557	(2,943,2,2,6)	2677	(2,1274,822,301,2)	2749	(6,382,2070,6,2)
2797	(2,1860,696,145,2)	2917	(5,970,728,381,2)	3037	(2,752,77,623,2)
3061	(6,1373,462,197,2)	3109	(6,2312,6,487,2)	3181	(7,938,1380,55,3)
3229	(6,521,1269,126,2)	3253	(2,2832,1657,486,2)	3301	(6,776,1351,312,3)
3373	(5,1055,164,5,2)	3469	(2,3326,288,29,2)	3517	(2,7,1545,132,3)
3541	(7,3042,376,296,2)	3613	(2,2039,200,457,2)	3637	(2,312,353,1461,2)
3709	(2,3042,1270,114,3)	3733	(2,2620,3188,357,2)	3853	(2,622,2901,293,2)
3877	(2,2842,82,327,2)	4021	(2,982,2084,418,2)	4093	(2,498,435,811,2)
4261	(2,506,291,430,2)	4357	(2,4316,478,251,2)	4549	(6,1418,181,293,2)
4597	(5,433,1148,661,2)	4621	(2,901,916,193,2)	4789	(2,3658,1017,119,2)
4813	(2,1195,780,179,2)	4861	(11,2037,1749,62,2)	4909	(6,3027,4697,215,2)
4933	(2,280,2504,336,2)	4957	(2,4330,1018,433,2)	5077	(2,1081,83,139,2)
5101	(6,1066,624,229,2)	5197	(7,1456,84,53,2)	5413	(5,261,605,94,2)
5437	(5,2961,3320,791,2)	5557	(2,182,849,303,3)	5581	(6,3347,92,206,2)
5653	(5,731,255,245,2)	5701	(2,389,244,606,2)	5749	(2,1816,1884,96,2)
5821	(6,1475,26,70,2)	5869	(2,3338,3866,241,2)	6037	(5,362,1039,18,2)

便构成了 $\mathbb{Z}$CPS-Wh-frame(3^p) 的一个初始平行类.

给定整数 $e \geq 2, t \geq 1$ 和 $n \geq 0$. 记

$$Q(e,t,n) = \frac{1}{4}\left(U + \sqrt{U^2 + 4e^{t-1}(t+en)}\right)^2, \text{ 其中 } U = \sum_{h=1}^{t} \binom{t}{h}(e-1)^h(h-1).$$

特别地，我们将 $Q(e,t,0)$ 简记为 $Q(e,t)$. 易验证当 $t < t'$ 时，$Q(e,t,n) < Q(e,t',n)$.

下面的结论是 Weil 定理的一个直接推论.

定理 2.9 (定理 2.2[20]): 设 $q \equiv 1 \pmod{e}$ 为一个素数幂，$B = \{b_1, \cdots, b_t\}$ 为 $GF(q)$ 的任一 t-子集，$(\beta_1, \cdots, \beta_t)$ 为集合 $\mathbb{Z}_e^t$ 中任一元素. 记集合 $X = \{x \in GF(q) : x - b_i \in C^e_{\beta_i}, i = 1, \cdots, t\}$. 则

$$|X| \geq \frac{q - U\sqrt{q} - e^{t-1}t}{e^t}.$$

从而若 $q > Q(e,t,n)$，则 $|X| > n$. 特别地，当 $q > Q(e,t)$ 时集合 X 非空.

引理 2.7: 给定任一素数 $p \equiv 1 \pmod{24}$. 若 $p > 1.9 \times 10^{12}$，则 $\mathbb{Z}$CPS-Wh-frame(3^p) 存在.

证明. 容易验证如果元素 a、b、c、d、e、f 满足以下的条件（其中 C^6 的下指标进行模 6 运算）：

$a \in C_1^6$,	$a+1 \in C_0^6$,	$a-1 \in C_1^6$;
$b \in C_2^6$;		
$e \in C_0^6$,	$e+b \in C_0^6$,	$e-b \in C_1^6$;
$c \in C_3^6$,	$c+b+e \in C_2^6$,	$2c+b+e \in C_2^6$;
$d \in C_4^6$,	$d-b-2c-2e \in C_4^6$,	$d-c-e \in C_3^6$,
$d+b \in C_5^6$,	$d-b-2c-e \in C_4^6$,	$2d-b-2c-e \in C_3^6$,
$d-b-c \in C_5^6$;		
$f \in C_1^6$,	$f+b+2c-d+2e \in C_5^6$,	$2f+b+2c-d+2e \in C_2^6$,
$f-e \in C_4^6$,	$f+e \in C_5^6$,	$f+2b+4c-2d+3e \in C_3^6$;

则 $\mathcal{A}_i$，$\mathcal{B}_i$，$0 \leq i \leq 2$ 中任一集合均是 $\mathbb{Z}_p^*/C_0^6$ 的一个完全代表系.

不妨设 $\frac{1}{2} \in C_r^6$. 下面我们应用定理 2.9 证明当 $p > 1.9 \times 10^{12} > Q(6,7)$ 时存在满足上述条件的元素 a、b、c、d、e、f.

首先我们在定理 2.9 中给定 $e = 6, t = 3, B = \{0, -1, 1\}$ 和 $(\beta_1, \beta_2\ \beta_3) = (1, 0, 1)$. 根据条件 $p > Q(6,7) > Q(6,3)$，可知集合 $X_1 := \{x \in \mathbb{Z}_p \mid x \in C_1^6, x+1 \in C_0^6, x-1 \in C_1^6\}$ 非空. 由此取定一个元素 $a \in X_1$.

在定理 2.9 中给定 $e=6,t=1,B=\{0\}$ 和 $\beta_1=2$. 根据条件 $p>Q(6,7)>Q(6,1)$，可知集合 $X_2:=\{x\in\mathbb{Z}_p\mid x\in C_2^6\}$ 非空. 取定一个元素 $b\in X_2$.

在定理 2.9 中给定 $e=6,t=3,B=\{0,-b,b\}$ 和 $(\beta_1,\beta_2,\beta_3)=(0,0,1)$. 根据条件 $p>Q(6,7)>Q(6,3)$，可知集合 $X_3:=\{x\in\mathbb{Z}_p\mid x\in C_0^6,x+b\in C_0^6,x-b\in C_1^6\}$ 非空. 取定一个元素 $e\in X_3$.

在定理 2.9 中给定 $e=6,t=3,B=\{0,-b-e,-\frac{1}{2}(b+e)\}$ 和 $(\beta_1,\beta_2,\beta_3)=(3,2,2+r)$. 根据条件 $p>Q(6,7)>Q(6,3)$，可知集合 $X_4:=\{x\in\mathbb{Z}_p\mid x\in C_3^6,x+b+e\in C_2^6,x+\frac{1}{2}b+\frac{1}{2}e\in C_{2+r}^6\}$ 非空. 取定一个元素 $c\in X_4$.

在定理 2.9 中给定 $e=6,t=7,B=\{0,b+2c+2e,c+e,-b,b+2c+e,\frac{1}{2}b+c+\frac{1}{2}e,b+c\}$ 和 $(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7)=(4,4,3,5,4,3+r,5)$. 根据条件 $p>Q(6,7)>Q(6,3)$，可知集合 $X_5:=\{x\in\mathbb{Z}_p\mid x\in C_4^6,x-b-2c-2e\in C_4^6,x-c-e\in C_3^6,x+b\in C_5^6,x-b-2c-e\in C_4^6,x-\frac{1}{2}b-c-\frac{1}{2}e\in C_{3+r}^6,x-b-c\in C_5^6\}$ 非空. 取定一个元素 $d\in X_5$.

在定理 2.9 中给定 $e=6,t=6,B=\{0,-b-2c+d-2e,-\frac{1}{2}b-c+\frac{1}{2}d-e,e,-e,-2b-4c+2d-3e\},(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6)=(1,5,2+r,4,5,3)$. 根据条件 $p>Q(6,7)>Q(6,6)$，可知集合 $X_6:=\{x\in\mathbb{Z}_p\mid x\in C_1^6,x+b+2c-d+2e\in C_5^6,x+\frac{1}{2}b+c-\frac{1}{2}d+e\in C_{2+r}^6,x-e\in C_4^6,x+e\in C_5^6,x+2b+4c-2d+3e\in C_3^6\}$ 非空. 取定一个元素 $f\in X_5$.

综上所述，我们已经找到了满足所需条件的元素 a、b、c、d、e、f. 最后根据前面的讨论，可知区组集合 $\mathcal{F}$ 构成了一个 $\mathbb{Z}$CPS-Wh-frame(3^p) 的初始平行类. □

引理 2.8：*给定任一素数 $p\equiv 1\pmod{12}$. 若 $13\le p\le 1213$，则 $\mathbb{Z}$CPS-Wh-frame(3^p) 存在.*

证明. 例 2.1 给出了一个 $\mathbb{Z}$CPS-Wh-frame(3^{13}). 通过计算机程序，我们对素数 $p\equiv 1\pmod{12}$ 且 $37\le p\le 1213$ 的情形找到了相应的 $\mathbb{Z}$CPS-Wh-frame(3^p) 的一个初始平行类. 限于篇幅我们只在表 2.2 中列出 $37\le p\le 349$ 时的本原元 ω 和 9 个基区组. □

综上所述，我们有：

表 2.2　素数 $p \equiv 1 \pmod{12}$ 且 $37 \leq p \leq 1213$ 时对应的基区组

p	ω	基区组		
37	2	{(12,1),(18,1)};	{(35,0),(25,1)};	{(24,0),(22,1)};
		{(29,1),(3,1)};	{(9,0),(19,1)};	{(11,0),(33,0)};
		{(10,1),(34,1)};	{(6,0),(8,1)};	{(15,1),(27,1)}.
61	2	{(12,1),(58,1)};	{(8,0),(13,1)};	{(25,0),(48,1)};
		{(55,0),(32,1)};	{(41,0),(29,1)};	{(3,1),(2,1)};
		{(38,1),(49,1)};	{(35,0),(5,0)};	{(23,1),(59,1)}.
73	5	{(47,0),(34,1)};	{(24,0),(41,1)};	{(32,1),(28,1)};
		{(39,1),(46,1)};	{(27,1),(21,1)};	{(7,0),(19,1)};
		{(48,0),(14,0)};	{(4,0),(52,1)};	{(45,1),(54,1)}.
97	5	{(76,1),(28,1)};	{(91,0),(13,1)};	{(69,1),(1,1)};
		{(32,1),(96,1)};	{(17,0),(95,1)};	{(2,0),(84,1)};
		{(29,0),(2,1)};	{(34,0),(89,0)};	{(21,1),(65,1)}.
109	6	{(46,0),(85,1)};	{(39,0),(17,1)};	{(24,1),(22,1)};
		{(92,1),(93,1)};	{(28,0),(25,0)};	{(17,0),(87,1)};
		{(85,0),(29,1)};	{(16,1),(47,1)};	{(62,1),(80,1)}.
157	5	{(31,0),(4,1)};	{(57,1),(135,1)};	{(26,0),(135,0)};
		{(134,0),(50,1)};	{(107,1),(129,1)};	{(82,0),(100,1)};
		{(22,1),(153,1)};	{(76,0),(3,1)};	{(28,1),(154,1)}.
181	2	{(78,0),(154,1)};	{(170,1),(66,1)};	{(173,0),(97,1)};
		{(116,0),(27,1)};	{(46,0),(84,1)};	{(115,1),(71,1)};
		{(110,1),(16,1)};	{(52,0),(17,0)};	{(11,1),(165,1)}.
193	5	{(22,0),(135,1)};	{(46,0),(28,1)};	{(132,0),(58,1)};
		{(71,0),(69,0)};	{(7,1),(50,1)};	{(29,1),(146,1)};
		{(85,0),(165,1)};	{(47,1),(143,1)};	{(164,1),(186,1)}.
229	6	{(38,0),(17,1)};	{(118,1),(51,1)};	{(57,0),(212,1)};
		{(84,0),(105,1)};	{(50,0),(124,1)};	{(123,1),(166,1)};
		{(111,1),(106,1)};	{(82,0),(37,0)};	{(63,1),(178,1)}.
241	7	{(204,0),(51,1)};	{(35,1),(220,1)};	{(131,0),(61,0)};
		{(73,0),(226,1)};	{(206,1),(61,1)};	{(180,1),(119,1)};
		{(164,0),(190,1)};	{(113,0),(15,1)};	{(21,1),(122,1)}.
277	5	{(243,0),(112,1)};	{(32,0),(119,0)};	{(172,0),(94,1)};
		{(213,1),(39,1)};	{(154,0),(165,1)};	{(125,1),(238,1)};
		{(52,0),(183,1)};	{(64,1),(127,1)};	{(150,1),(152,1)}.
313	10	{(90,0),(83,1)};	{(111,0),(230,1)};	{(190,0),(96,0)};
		{(27,0),(167,1)};	{(139,0),(146,1)};	{(290,1),(81,1)};
		{(23,1),(79,1)};	{(21,1),(234,1)};	{(232,1),(292,1)}.
337	10	{(91,0),(47,0)};	{(303,1),(177,1)};	{(160,1),(74,1)};
		{(163,0),(268,1)};	{(196,0),(47,1)};	{(223,0),(263,1)};
		{(136,0),(96,1)};	{(34,1),(69,1)};	{(241,1),(290,1)}.
349	2	{(60,0),(205,1)};	{(177,0),(78,0)};	{(294,0),(259,1)};
		{(249,1),(328,1)};	{(109,0),(144,1)};	{(105,1),(16,1)};
		{(100,1),(244,1)};	{(6,0),(90,1)};	{(21,1),(333,1)}.

引理 2.9: *若素数 p 满足以下条件之一:*

(i) $p \equiv 13 \pmod{24}$，*或*

(ii) $p \equiv 1 \pmod{24}$ *且 p 小于等于 1213 或者大于 1.9×10^{12},*

则 $\mathbb{Z}$CPS-Wh-frame(3^p) *存在.*

证明. 根据引理 2.5，引理 2.6 和引理 2.8 易证情形 (i). 根据引理 2.7 和引理 2.8 易证情形 (ii). □

在引理 2.3 中取定 $h = 3$ 并结合引理 2.9，我们有：

定理 2.10: *若素数 p 满足以下条件之一:*

(i) $p \equiv 13 \pmod{24}$，*或*

(ii) $p \equiv 1 \pmod{24}$ *且 p 小于等于 1213 或者大于 1.9×10^{12},*

则 $\mathbb{Z}$CPS-Wh$(3p+1)$ *存在.*

2.5 $\mathbb{Z}$CPS-Wh-frame(27^p) 的构造

根据 $\gcd(p, 27) = 1$ 可知 $\mathbb{Z}_p \times \mathbb{Z}_{27}$ 同构于 $\mathbb{Z}_{27p}$. 容易验证元素 19 在乘法群 $(\mathbb{Z}_{27}, \cdot)$ 中阶为 3 （$19^2 \equiv 10 \pmod{27}, 19^3 \equiv 1 \pmod{27}$）. 我们在群 $\mathbb{Z}_{27}$ 考虑乘以元素 19 这个群作用. 容易验证这个群作用的轨道的长度只有 1 和 3 两种：

(i) $0, 3, 6, 9, 12, 15, 18, 21, 24$ 是所有的不动点，

(ii) $\{1, 19, 10\}$, $\{8, 17, 26\}$, $\{2, 11, 20\}$, $\{7, 25, 16\}$, $\{4, 22, 13\}$, $\{5, 14, 23\}$ 是所有长度等于 3 的轨道.

令 ω 为 $\mathbb{Z}_p$ 的一个本原元. 给定以下 27 个定义在群 $\mathbb{Z}_p \times \mathbb{Z}_{27}$ 上的基区组:

$$
\begin{aligned}
B_1 &= \{(1,1),(x_1,0)\}, & B_2 &= \{(x_1^7,2),(x_1^6,0)\},\\
B_3 &= \{(x_2^4,2),(x_2^5,3)\}, & B_4 &= \{(x_8,1),(x_8^2,3)\},\\
B_5 &= \{(x_1^2,2),(x_1^3,3)\}, & B_6 &= \{(x_1^3,2),(x_1^4,3)\},\\
B_7 &= \{(x_3,12),(x_3^2,6)\}, & B_8 &= \{(x_6^5,2),(x_6^4,6)\},\\
B_9 &= \{(x_5^2,12),(x_5^3,6)\}, & B_{10} &= \{(x_7^2,1),(x_7,6)\},\\
B_{11} &= \{(x_1^6,2),(x_1^5,9)\}, & B_{12} &= \{(x_2^3,9),(x_2^2,9)\},\\
B_{13} &= \{(x_1^3,1),(x_1^4,9)\}, & B_{14} &= \{(x_4^4,1),(x_4^3,12)\},\\
B_{15} &= \{(x_4^5,1),(x_4^4,12)\}, & B_{16} &= \{(x_5^6,1),(x_5^7,4)\},\\
B_{17} &= \{(x_1^8,4),(x_1^9,4)\}, & B_{18} &= \{(x_4^{10},22),(x_4^{11},4)\},\\
B_{19} &= \{(x_{10}^9,1),(x_{10}^{10},4)\}, & B_{20} &= \{(x_1^{10},2),(x_1^9,22)\},\\
B_{21} &= \{(x_1^{11},1),(x_1^{12},4)\}, & B_{22} &= \{(1,11),(x_2,4)\},\\
B_{23} &= \{(x_2,11),(x_2^2,4)\}, & B_{24} &= \{(x_2^3,11),(x_2^4,4)\},\\
B_{25} &= \{(x_1^{10}\cdot\omega^4,19),(x_1^{11}\cdot\omega^4,4)\}, & B_{26} &= \{(x_9^8\cdot\omega^4,19),(x_9^9\cdot\omega^4,2)\},\\
B_{27} &= \{(x_3^7\cdot\omega^4,19),(x_3^8\cdot\omega^4,2)\}.
\end{aligned}
$$

跟上一节一样：在这里我们用一个区组的前面两个元素来表示整个区组. 比如集合 $B_1 = \{(1,1),(x_1,0)\}$ 就表示区组 $((1,1),(x_1,0),(p-1,26),(p-x_1,0))$. 接下来我们要做的就是找到所需的元素 $x_i \in \mathbb{Z}_p$ 使得区组集合

$$\mathcal{F} = \{B_i \cdot (w^4,19)^j \mid 1 \le i \le 27, 0 \le j < \frac{p-1}{4}\}$$

构成 $\mathbb{Z}$CPS-Wh-frame(27^p) 的一个初始平行类. 首先我们将区组集合 $\mathcal{F}$ 中所有具有

相同第二坐标的元素的第一坐标取出来放在一起得到

$$
\begin{aligned}
\mathcal{A}_0 &= \{x_1, x_1^6\} \cdot C_0^2;\\
\mathcal{A}_3 &= \{x_8^2, x_1^3, x_1^4, x_2^5\} \cdot C_0^4;\\
\mathcal{A}_6 &= \{x_7, x_3^2, x_5^3, x_6^4\} \cdot C_0^4;\\
\mathcal{A}_9 &= \{x_2^2, x_2^3, x_1^4, x_1^5\} \cdot C_0^4;\\
\mathcal{A}_{12} &= \{x_3, x_5^2, x_4^3, x_4^4\} \cdot C_0^4;\\
\mathcal{A}_1 &= \{1, x_8, x_7^2, x_1^3, x_4^4, x_4^5, x_5^6, x_3^7, x_9^8, x_{10}^9, x_1^{10}, x_1^{11}\} \cdot C_0^{12};\\
\mathcal{A}_2 &= \{x_3^8\omega^4, x_9^9\omega^4, x_1^2, x_1^3, x_2^4, x_6^5, x_1^6, x_1^7, \omega^8, x_2\omega^8, x_1^{10}, x_2^3\omega^8\} \cdot C_0^{12};\\
\mathcal{A}_4 &= \{x_1^{12}, x_2, x_2^2, x_1^{11}\omega^4, x_2^4, x_1^9\omega^8, x_4^{10}\omega^8, x_5^7, x_1^8, x_1^9, x_{10}^{10}, x_4^{11}\} \cdot C_0^{12}.
\end{aligned}
$$

这里集合 $\mathcal{A}$ 的下指标表示第二坐标的值，比如 $\mathcal{A}_0 = \{a \mid (a,0) \in \mathcal{F}\}$. 接着我们将区组集合 $\mathcal{F}$ 中所有具有相同第二坐标的差的第一坐标取出来放在一起得到

$$
\begin{aligned}
\mathcal{B}_0 &= \{x_2^2(x_2-1), x_1^8(1-x_1)\} \cdot C_0^2;\\
\mathcal{B}_3 &= \{x_5^6(x_5-1), x_{10}^9(x_{10}-1), x_1^{11}(x_1-1), -x_1^9(x_1+1)\} \cdot C_0^4;\\
\mathcal{B}_6 &= \{x_3(1-x_3), x_5^2(1-x_5), -x_3^7(1+x_3)\omega^4, -x_9^8(1+x_9)\omega^4\} \cdot C_0^4;\\
\mathcal{B}_9 &= \{-x_3(1+x_3), x_4^{10}(x_4-1), -x_5^2(1+x_5), -x_2^2(x_2+1)\} \cdot C_0^4;\\
\mathcal{B}_{12} &= \{-(1+x_2), -x_2(1+x_2), -x_2^3(1+x_2), x_1^{10}(x_1-1)\omega^4\} \cdot C_0^4;\\
\mathcal{B}_1 &= \{1+x_1, 1-x_1, x_2^4(x_2-1), x_1^3(x_1-1), x_6^4(x_6+1)\omega^{14}\}\\
&\quad \cup \{x_1^3(1+x_1)\omega^4, x_1^3(1-x_1)\omega^8, x_3^7(1-x_3)\omega^{14}, x_9^8(1-x_9)\omega^{14}\}\\
&\quad \cup \{x_4^{10}(1+x_4)\omega^6, x_1^8(1+x_1)\omega^{14}, x_1^2(x_1-1)\} \cdot C_0^{12};\\
\mathcal{B}_2 &= \{x_1^6(x_1+1), x_1^6(x_1-1), x_8(x_8-1), x_7(x_7+1)\omega^{10}, (1-x_2)\omega^{10}\}\\
&\quad \cup \{x_2(1-x_2)\omega^{10}, x_2^3(1-x_2)\omega^{10}, x_1^9(x_1-1)\omega^{10}, x_1^5(x_1+1)\omega^8\}\\
&\quad \cup \{x_1^5(x_1-1)\omega^4, x_4^3(x_4-1)\omega^{14}, x_4^4(x_4-1)\omega^{14}\} \cdot C_0^{12};
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{B}_4 &= \{-x_2^4(1+x_2)\omega^8, x_8(1+x_8), x_1^2(1+x_1)\omega^2, x_1^3(1+x_1)\omega^2, x_6^4(1-x_6)\}\\
&\quad \cup \{x_7(1-x_7)\omega^2, x_5^6(1+x_5)\omega^2, x_{10}^9(1+x_{10})\omega^2, x_1^{11}(1+x_1)\omega^2\}\\
&\quad \cup \{-x_1^{10}(1+x_1)\omega^4, x_4^3(x_4+1)\omega^4, x_4^4(x_4+1)\omega^4\} \cdot C_0^{12}.
\end{aligned}
$$

容易验证若下面的条件都成立：

(i) 集合 $\mathcal{A}_0$ 与集合 $\mathcal{B}_0$ 分别都是 $\mathbb{Z}_p^*/C_0^2$ 的一个完全代表系，

(ii) $\mathcal{A}_3, \mathcal{A}_6, \mathcal{A}_9, \mathcal{A}_{12}, \mathcal{B}_3, \mathcal{B}_6, \mathcal{B}_9, \mathcal{B}_{12}$ 中任一集合都是 $\mathbb{Z}_p^*/C_0^4$ 的一个完全代表系，

(iii) $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_4, \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_4$ 中任一集合都是 $\mathbb{Z}_p^*/C_0^{12}$ 的一个完全代表系,

则区组集合 $\mathcal{F}$ 构成了 $\mathbb{Z}$CPS-Wh-frame(27^p) 的一个初始平行类.

引理 2.10: *给定任一素数 $p \equiv 13 \pmod{24}$. 若 $p > 9150625$，则 $\mathbb{Z}$CPS-Wh-frame(27^p) 存在.*

证明. 容易验证若存在元素 $x_i \in \mathbb{Z}_p$ 使得以下的条件成立：

$$\begin{array}{lll}
x_1 \in C_1^{12}, & x_1+1 \in C_0^{12}, & x_1-1 \in C_3^{12}; \\
x_2 \in C_1^{12}, & x_2+1 \in C_9^{12}, & x_2-1 \in C_0^{12}; \\
x_3 \in C_1^{12}, & x_3+1 \in C_1^{12}, & x_3-1 \in C_{10}^{12}; \\
x_4 \in C_1^{12}, & x_4+1 \in C_{11}^{12}, & x_4-1 \in C_9^{12}; \\
x_5 \in C_1^{12}, & x_5+1 \in C_6^{12}, & x_5-1 \in C_3^{12}; \\
x_6 \in C_1^{12}, & x_6+1 \in C_5^{12}, & x_6-1 \in C_{11}^{12}; \\
x_7 \in C_1^{12}, & x_7+1 \in C_0^{12}, & x_7-1 \in C_2^{12}; \\
x_8 \in C_1^{12}, & x_8+1 \in C_9^{12}, & x_8-1 \in C_7^{12}; \\
x_9 \in C_1^{12}, & x_9+1 \in C_2^{12}, & x_9-1 \in C_{10}^{12}; \\
x_{10} \in C_1^{12}, & x_{10}+1 \in C_1^{12}, & x_{10}-1 \in C_{11}^{12};
\end{array}$$

则集合 $\mathcal{A}_0$ 与集合 $\mathcal{B}_0$ 分别都是 $\mathbb{Z}_p^*/C_0^2$ 的一个完全代表系；$\mathcal{A}_3, \mathcal{A}_6, \mathcal{A}_9, \mathcal{A}_{12}, \mathcal{B}_3, \mathcal{B}_6, \mathcal{B}_9, \mathcal{B}_{12}$ 中任一集合都是 $\mathbb{Z}_p^*/C_0^4$ 的一个完全代表系；$\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_4, \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_4$ 中任一集合都是 $\mathbb{Z}_p^*/C_0^{12}$ 的一个完全代表系. 再根据前面的讨论可知区组集合 $\mathcal{F}$ 构成了 $\mathbb{Z}$CPS-Wh-frame(27^p) 的一个初始平行类.

给定群 $\mathbb{Z}_p$ 的一个本原元 ω. 记

$$f_1(x) = \omega^{11}x,\ f_2(x) = x+1,\ f_3(x) = \omega^9(x-1).$$

容易看出条件

$$x \in C_1^{12},\ x+1 \in C_0^{12},\ x-1 \in C_3^{12}$$

等价于

$$f_j(x) \in C_0^{12}, 1 \le j \le 3.$$

令 χ 为一个阶为 12 的乘法特征. 记 $B_i = \chi(f_i(x)), 1 \le i \le 3$. 则

$$1 + B_i + B_i^2 + \cdots + B_i^{11} = \begin{cases} 12, & \text{if } f_i(x) \in C_0^{12}, \\ 0, & \text{if } f_i(x) \notin C_0^{12} \cup \{0\}, \\ 1, & \text{if } f_i(x) = 0. \end{cases}$$

记和式

$$S = \sum_{x \in \mathbb{Z}_p} \prod_{i=1}^{3} (1 + B_i + B_i^2 + \cdots + B_i^{11}). \tag{2.10}$$

则 $S = 12^3 n + d$，其中 n 是 $\mathbb{Z}_p$ 中满足下述条件：

$$x \in C_1^{12},\ x+1 \in C_0^{12},\ x-1 \in C_3^{12}$$

的元素 x 的数目，d 是当某个 $f_i(x) = 0$ 时上述和式右边的贡献值. 若 $f_1(x) = 0$，则 $x = 0,\ f_2(0) = 1, f_3(0) = -\omega^9$. 又因为 $p \equiv 13 \pmod{24}$，可知 $-1 \in C_6^{12}$. 从而 $f_3(0) \notin C_0^{12} \cup \{0\}$，故它对和式右边的贡献值为 0. 若 $f_2(x) = 0$，则 $x = -1,\ f_1(-1) = -\omega^{11} \notin C_0^{12} \cup \{0\}$，所以它对和式的贡献值亦为 0. 若 $f_3(x) = 0$，则 $x = 1,\ f_1(1) = \omega^{11} \notin C_0^{12} \cup \{0\}$，故它对和式的贡献值亦为 0. 综上所述，可知 d 总是等于零. 于是如果我们能够证明 $|S| > 0$，也就立即可以推出存在满足条件 $x \in C_1^{12}, x+1 \in C_0^{12}, x-1 \in C_3^{12}$ 的元素 x. 展开等式 (2.10) 的右边，

$$S = \sum_{x \in \mathbb{Z}_p} 1 + \sum_{r=1}^{3} \sum_{1 \le i_1 < \cdots < i_r \le 3} \sum_{1 \le j_1, \cdots, j_r \le 11} \sum_{x \in \mathbb{Z}_p} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r}. \tag{2.11}$$

现在我们用 Weil 定理来估计这个和式. 注意 $B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} = \chi(\prod_{l=1}^{r} (f_{i_l}(x))^{j_l})$ 且 χ 的阶为 12. 若存在 $p(x) \in \mathbb{Z}_p[x]$ 使得 $\prod_{l=1}^{r} (f_{i_l}(x))^{j_l} = [p(x)]^{12}$，又因为 $f_{j_l}(x)$是两两互素的，则必然成立 $j_1 \equiv j_2 \equiv \cdots \equiv j_r \equiv 0 \pmod{12}$. 现在我们可以应用定理 2.8. 对任意的 $r, 1 \le r \le 3$，我们有

$$\left| \sum_{x \in \mathbb{Z}_p} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \right| \le (r-1)\sqrt{p}. \tag{2.12}$$

根据等式 (2.10)-(2.12)，

$$|S| \ge p - \sum_{r=1}^{3} \binom{3}{r} 11^r (r-1)\sqrt{p} = p - 3025\sqrt{p}. \tag{2.13}$$

从而当 $p > 9150625$ 时 $|S| > 0$. 类似地，我们可以找到满足所需条件的其余元素 $x_i, 2 \le i \le 11$. □

引理 2.11：*给定任一素数 $p \equiv 13 \pmod{24}$. 若 $8221 \leq p \leq 9150625$，则 $\mathbb{Z}$CPS-Wh-frame(27^p) 存在.*

证明. 对于任意的素数 $p \equiv 13 \pmod{24}$ 且 $8221 \leq p \leq 9150625$，我们通过计算机程序找到了分别满足所需条件的元素 x_i. 限于篇幅我们只在表 2.3 中列出相应的数对 (p, x_i)，其中 $8221 \leq p \leq 11317$. □

引理 2.12：*给定素数 $p \equiv 13 \pmod{24}$. 若 $37 \leq p < 8221$，则 $\mathbb{Z}$CPS-Wh-frame(27^p) 存在.*

证明. 通过计算机程序，我们对每个素数 $p \equiv 13 \pmod{24}$ 且 $37 \leq p < 8221$ 找到了相应的 $\mathbb{Z}$CPS-Wh-frame(27^p) 一个初始平行类. 限于篇幅我们在表 2.4 中只对区间 $37 \leq p \leq 349$ 列出对应的乘子 γ（元素 γ 在单位群 $U(\mathbb{Z}_{27p})$ 中阶为 $(p-1)/4$）和 27 个基区组. 表中的每一个区组 $(a, b, -a, -b)$ 被它的前两个元素 (a, b) 所表示. 通过对这 27 个区组乘以集合 $\{\gamma^i \mid 0 \leq i < (p-1)/4\}$ 中的所有元素，我们就得到了整个初始平行类. □

结合引理 2.10–2.12，我们得到了本节的主要结果.

引理 2.13：*给定任一素数 $p \equiv 13 \pmod{24}$. 若 $p \geq 37$，则 $\mathbb{Z}$CPS-Wh-frame(27^p) 存在.*

在引理 2.3 中取定 $h = 27$. 再结合引理 2.13，我们有下面的结果.

定理 2.11：*给定任一素数 $p \equiv 13 \pmod{24}$. 若 $p \geq 37$，则 $\mathbb{Z}$CPS-Wh$(27p+1)$ 存在.*

2.6 利用差矩阵的构造方法

在这一节中，我们利用一类特殊的（循环）差矩阵来构造 $\mathbb{Z}$CPS-Whs. 更多的处理方法请参阅文献[23].

给定一个 v 阶的 Abel 群 G，其运算为加法. 设 $A = [a_{ij}]$ 为 G 上的一个 $k \times v$ 矩阵. 若对任意取定的 $r, s \in \{1, 2, \cdots, k\}, r \neq s$，$G$ 中每个元素都恰有 1 次表成 $a = a_{rj} - a_{sj}$，$1 \leq j \leq v$ 的形式，则称 A 为 G 上的一个 $(v, k; 1)$-*差矩阵*（difference

表 2.3 (p, x_i): $p \equiv 13 \pmod{24}, 8221 \leq p \leq 11317$

p	ω	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
8221	2	3106	2612	2571	1649	1812	1371	250	3111	235	22
8269	2	2292	50	395	1750	1451	7174	297	5447	2881	1773
8293	2	1950	5978	1377	1304	7667	1275	836	3229	1082	6446
8317	6	447	354	423	434	6	2656	997	3698	638	1620
8389	6	113	2126	4992	429	1593	915	1092	3191	1580	2714
8461	6	578	114	1522	1026	1873	4694	1288	1817	200	2497
8581	6	726	301	2709	847	3184	356	4394	2306	116	1831
8629	6	274	6	515	3750	3240	229	1216	2295	2708	333
8677	2	123	1898	4381	2204	1977	187	5534	410	540	744
8821	2	5936	262	1057	2549	201	1585	1644	3201	2966	470
8893	5	3071	839	2505	3918	519	1479	80	700	271	1255
8941	6	2022	6176	925	5658	497	1314	1293	619	3240	2682
9013	5	2370	212	341	1731	2530	3589	26	1358	2620	478
9109	10	2190	1988	4062	1014	3097	88	1478	546	646	4635
9133	6	340	96	707	337	949	719	15	262	813	1613
9157	6	4050	3053	942	499	1624	2886	1316	3492	2983	3750
9181	2	1001	2097	265	1529	2385	658	467	493	1621	5132
9277	5	3554	17	1926	1660	2458	2442	1824	910	587	583
9349	2	224	3011	265	671	3176	73	170	6216	1238	350
9397	2	336	426	2592	4684	8980	645	1209	346	4116	118
9421	2	2571	58	897	105	457	1080	349	385	2547	3353
9613	2	2818	348	3283	850	2122	236	2897	1894	1488	4297
9661	2	3243	3283	6765	157	780	2636	250	2530	4688	1026
9733	2	1066	161	7945	3651	2205	3935	3942	417	1169	1218
9781	6	1604	667	640	897	705	1101	1090	689	814	1498
9829	10	2328	3252	376	1087	2573	909	1048	1248	742	3039
9901	2	2244	198	1042	1537	3445	3184	2103	2619	204	1894
9949	2	390	713	5032	87	3705	4281	1299	1475	1437	707
9973	11	99	106	2440	1809	1702	4687	4095	2223	1174	775
10069	2	47	1342	391	2933	3067	923	2548	1228	488	3987
10093	2	2105	1765	548	4789	63	1164	722	2154	3658	3270
10141	2	2244	1336	3177	2300	3608	3649	69	680	2361	827
10333	5	346	2722	636	772	2007	1351	9199	187	2173	3012
10357	2	5751	733	1778	1762	1672	1725	820	2112	74	1916
10429	7	2167	2169	1037	2754	1274	1582	133	1117	1792	1595
10453	5	306	302	1252	406	1078	408	131	5347	264	760
10477	2	4921	1542	1994	3840	387	1176	2843	1602	3082	1111
10501	2	988	725	1114	4056	120	786	421	138	1496	1953
10597	5	5888	228	170	1182	584	2542	80	1014	7196	4558
10789	2	5710	806	40	1070	323	153	436	2312	800	594
10837	2	1273	85	439	2734	9215	3716	1364	307	4951	14
10861	2	2393	1621	2131	92	527	3054	1848	878	701	2375
10909	2	5176	318	457	1686	1680	387	4221	927	1734	955
10957	5	563	349	1828	572	2332	1779	6840	2280	1656	5648
11149	10	1556	10	5154	1538	646	1363	3771	1965	281	159
11173	5	1668	2455	138	1694	1637	1263	4490	4062	279	4296
11197	2	295	6437	2609	1017	1971	1985	9088	298	3221	694
11317	2	689	198	1980	1125	4070	382	223	413	1966	1172

表 2.4　素数 $p \equiv 13 \pmod{24}$ 且 $37 \leq p \leq 349$ 时对应的基区组

p	γ	基区组					
37	7	$(10,329)$;	$(15,157)$;	$(25,946)$;	$(54,398)$;	$(3,674)$;	$(22,535)$;
		$(13,522)$;	$(1,751)$;	$(23,348)$;	$(16,65)$;	$(33,780)$;	$(5,844)$;
		$(12,129)$;	$(31,869)$;	$(6,810)$;	$(48,488)$;	$(2,712)$;	$(50,867)$;
		$(8,104)$;	$(9,727)$;	$(4,276)$;	$(29,805)$;	$(19,504)$;	$(24,331)$;
		$(18,116)$;	$(71,379)$;	$(88,487)$.			
61	73	$(43,1143)$;	$(46,459)$;	$(48,476)$;	$(9,252)$;	$(59,617)$;	$(1,1408)$;
		$(29,262)$;	$(3,691)$;	$(5,1453)$;	$(10,768)$;	$(7,1463)$;	$(6,12)$;
		$(8,1497)$;	$(2,613)$;	$(19,1615)$;	$(20,950)$;	$(11,1626)$;	$(27,1591)$;
		$(28,753)$;	$(31,910)$;	$(24,407)$;	$(35,1598)$;	$(52,1245)$;	$(26,765)$;
		$(16,779)$;	$(13,340)$;	$(60,177)$.			
109	7	$(75,1719)$;	$(46,2816)$;	$(16,598)$;	$(19,1878)$;	$(13,2597)$;	$(1,1573)$;
		$(3,1916)$;	$(26,1220)$;	$(10,227)$;	$(4,2430)$;	$(6,122)$;	$(74,826)$;
		$(2,1380)$;	$(8,514)$;	$(17,348)$;	$(36,2699)$;	$(23,748)$;	$(5,974)$;
		$(30,890)$;	$(25,138)$;	$(27,2452)$;	$(24,2817)$;	$(34,186)$;	$(32,473)$;
		$(48,617)$;	$(51,855)$;	$(52,1001)$.			
157	19	$(77,1222)$;	$(1,430)$;	$(3,517)$;	$(4,620)$;	$(5,996)$;	$(7,4225)$;
		$(9,342)$;	$(10,1942)$;	$(12,4216)$;	$(15,651)$;	$(16,4207)$;	$(25,48)$;
		$(27,71)$;	$(28,60)$;	$(31,72)$;	$(33,66)$;	$(36,85)$;	$(40,80)$;
		$(41,101)$;	$(43,120)$;	$(54,325)$;	$(56,142)$;	$(62,424)$;	$(67,349)$;
		$(6,730)$;	$(20,908)$;	$(30,710)$.			
181	13	$(75,796)$;	$(1,554)$;	$(3,302)$;	$(4,953)$;	$(6,566)$;	$(7,1369)$;
		$(5,991)$;	$(10,4868)$;	$(12,977)$;	$(16,297)$;	$(18,1839)$;	$(20,4849)$;
		$(21,4847)$;	$(24,51)$;	$(25,47)$;	$(35,89)$;	$(36,74)$;	$(42,84)$;
		$(54,134)$;	$(56,93)$;	$(59,315)$;	$(62,128)$;	$(73,886)$;	$(9,100)$;
		$(2,143)$;	$(22,534)$;	$(37,551)$.			
229	19	$(77,2048)$;	$(1,862)$;	$(3,1355)$;	$(4,2735)$;	$(6,407)$;	$(9,18)$;
		$(10,20)$;	$(12,23)$;	$(14,27)$;	$(15,33)$;	$(17,39)$;	$(24,53)$;
		$(28,56)$;	$(30,66)$;	$(34,68)$;	$(35,82)$;	$(36,85)$;	$(40,54)$;
		$(47,107)$;	$(51,106)$;	$(59,110)$;	$(60,368)$;	$(70,355)$;	$(71,511)$;
		$(72,484)$;	$(7,757)$;	$(13,3084)$.			
277	10	$(58,6743)$;	$(3,5)$;	$(29,425)$;	$(9,420)$;	$(7,14)$;	$(26,7426)$;
		$(21,2420)$;	$(20,1323)$;	$(55,1073)$;	$(73,2924)$;	$(18,41)$;	$(12,7454)$;
		$(6,1694)$;	$(19,806)$;	$(16,3050)$;	$(118,5136)$;	$(49,418)$;	$(23,1525)$;
		$(38,276)$;	$(1,1886)$;	$(24,927)$;	$(52,6102)$;	$(51,957)$;	$(104,1806)$;
		$(17,2961)$;	$(106,6711)$;	$(59,1898)$.			
349	19	$(10,2798)$;	$(3,5)$;	$(4,8)$;	$(72,1270)$;	$(27,1559)$;	$(9,25)$;
		$(6,555)$;	$(13,23)$;	$(17,30)$;	$(1,1084)$;	$(20,40)$;	$(91,2283)$;
		$(60,696)$;	$(54,284)$;	$(28,1087)$;	$(24,2220)$;	$(16,3997)$;	$(47,167)$;
		$(7,151)$;	$(18,3079)$;	$(59,89)$;	$(36,1048)$;	$(39,5981)$;	$(78,547)$;
		$(50,727)$;	$(26,3913)$;	$(15,3940)$.			

matrix），简记为 $(v,k;1)$-DM. 特别地当 $G=\mathbb{Z}_v$ 时，我们称 G 上的差矩阵是循环的(cyclic)，简记为 $(v,k;1)$-CDM. 若差矩阵的每一行恰是 $\mathbb{Z}_v$ 的全体元素，则我们称它是一个齐次的（homogeneous）$(v,k;1)$-CDM. 容易验证如果一个 $(v,k;1)$-CDM 包含元素全为 0 的行，那么剩下的行则构成一个齐次的 $(v,k-1;1)$-CDM，反之亦然.

若一个齐次的 $(v,4;1)$-CDM $A=[a_{ij}]$ 还满足性质 $a_{1j}=-a_{3j}, a_{2j}=-a_{4j}$，$1\le j\le v$，则称 A 为一个对称齐次（symmetric homogeneous）的循环差矩阵，简记为 $(v,4;1)$-SHCDM. 下面我们给出 $(v,4;1)$-SHCDM 存在的充分必要条件.

引理 2.14: $(v,4;1)$-SHCDM 存在当且仅当 $\gcd(v,6)=1$.

证明. 首先，我们假设 $\gcd(v,6)=1$. 令

$$A=\begin{bmatrix} 1 & 2 & \ldots & i & \ldots & v-1 & 0\\ 2 & 4 & \ldots & 2i & \ldots & 2(v-1) & 0\\ -1 & -2 & \ldots & -i & \ldots & -(v-1) & 0\\ -2 & -4 & \ldots & -2i & \ldots & -2(v-1) & 0 \end{bmatrix}.$$

直接验证可知 A 是一个 $(v,4;1)$-SHCDM.

接下来，我们假设 $A=[a_{ij}]$，$1\le i\le 4$，$1\le j\le v$，是一个 $(v,4;1)$-SHCDM. 根据定义可知 $a_{1j}=-a_{3j}, a_{2j}=-a_{4j}, 1\le j\le v$, 并且

$$\{a_{1j}\mid 1\le j\le v\}=\{a_{1j}-a_{3j}=2\,a_{1j}\mid 1\le j\le v\}=\mathbb{Z}_v, \tag{2.14}$$

$$\{a_{2j}\mid 1\le j\le v\}=\{a_{1j}-a_{2j}\mid 1\le j\le v\}=\{a_{1j}+a_{2j}\mid 1\le j\le v\}=\mathbb{Z}_v. \tag{2.15}$$

从等式 (2.14) 可得

$$\sum_{j=1}^{v} a_{1j}\equiv\sum_{j=1}^{v}2\,a_{1j}\equiv\sum_{j=0}^{v-1} j\equiv\frac{(v-1)v}{2}\pmod v.$$

因此

$$\frac{(v-1)v}{2}\equiv\sum_{j=1}^{v} a_{1j}\equiv\sum_{j=1}^{v}2\,a_{1j}-\sum_{j=1}^{v}a_{1j}\equiv 0\pmod v.$$

整理可得 $v\equiv 1 \pmod 2$. 结合等式 (2.14) 和 (2.15)，可知

$$\sum_{j=1}^{v} a_{1j}^2\equiv\sum_{j=1}^{v} a_{2j}^2\equiv\sum_{j=1}^{v}(a_{1j}+a_{2j})^2\equiv\sum_{j=1}^{v}(a_{1j}-a_{2j})^2\equiv S\pmod v,$$

其中 $S=\sum_{i=0}^{v-1} i^2$. 于是

$$\begin{aligned} 2S &= 2S+2S-2S \\ &\equiv 2\sum_{j=1}^{v} a_{1j}^2+2\sum_{j=1}^{v} a_{2j}^2-\left(\sum_{j=1}^{v}(a_{1j}+a_{2j})^2+\sum_{j=1}^{v}(a_{1j}-a_{2j})^2\right) \\ &\equiv 2\sum_{j=1}^{v} a_{1j}^2+2\sum_{j=1}^{v} a_{2j}^2-2\left(\sum_{j=1}^{v} a_{1j}^2+\sum_{j=1}^{v} a_{2j}^2\right) \\ &\equiv 0 \pmod{v}. \end{aligned}$$

又因为 $v\equiv 1 \pmod 2$，所以

$$S=\sum_{i=0}^{v-1} i^2=\frac{(v-1)v(2v-1)}{6}\equiv 0 \pmod{v},$$

从中可以推出 $v\equiv 1,5 \pmod 6$，整理得 $\gcd(v,6)=1$. □

下面我们利用 $(v,4;1)$-SHCDM 来构造 $\mathbb{Z}$CPS-Wh-frames.

引理 2.15：*若 $\mathbb{Z}$CPS-Wh-frame(h^n) 和 $(v,4;1)$-SHCDM 都存在，则 $\mathbb{Z}$CPS-Wh-frame$((vh)^n)$ 存在.*

证明. 令 $A=(a_{ij})$ 为一个 $(v,4;1)$-SHCDM. 对 $\mathbb{Z}$CPS-Wh-frame(h^n) 初始平行类中每一个区组 $(a,b,-a,-b)$，都构作区组 $(a+ga_{1j},b+ga_{2j},-a-ga_{1j},-b-ga_{2j})$，$g=hn$，$1\le j\le v$，这里的元素都进行模 vhn 的运算. 容易验证所有的这些区组构成了 $\mathbb{Z}$CPS-Wh-frame$((vh)^n)$ 的一个初始平行类. □

同样地，我们可以从一个 $\mathbb{Z}$CPS-Wh(v) 构造一个 $(v,4;1)$-SHCDM.

引理 2.16：*给定任一非负整数 v. 若 $v\equiv 1 \pmod 4$ 且 $\mathbb{Z}$CPS-Wh(v) 存在，则 $(v,4;1)$-SHCDM 存在.*

证明. 设 $v=4h+1$，$\mathbb{Z}$CPS-Wh(v) 初始平行类中区组为 $(a_i,b_i,-a_i,-b_i), 1\le i\le h$. 令

$$A=\begin{bmatrix} a_1 & \dots & a_h & b_1 & \dots & b_h & -a_1 & \dots & -a_h & -b_1 & \dots & -b_h & 0 \\ b_1 & \dots & b_h & -a_1 & \dots & -a_h & -b_1 & \dots & -b_h & a_1 & \dots & a_h & 0 \\ -a_1 & \dots & -a_h & -b_1 & \dots & -b_h & a_1 & \dots & a_h & b_1 & \dots & b_h & 0 \\ -b_1 & \dots & -b_h & a_1 & \dots & a_h & b_1 & \dots & b_h & -a_1 & \dots & -a_h & 0 \end{bmatrix}.$$

容易验证 A 恰是一个 $(v,4;1)$-SHCDM. □

根据引理 2.2，引理 2.15（取 $h=1$），引理 2.16，我们可以直接证明下面的乘积构造. 这个构造最先是由 Anderson 等人[6] 中提出.

定理 2.12：设 u,v 都为模 4 余 1 的正整数. 若 $\mathbb{Z}$CPS-Wh(u) 和 $\mathbb{Z}$CPS-Wh(v) 均存在，则 $\mathbb{Z}$CPS-Wh(uv) 存在.

同样地，根据引理 2.3 和 引理 2.15，我们有下面的结论。

定理 2.13：给定正整数 $v\equiv 1 \pmod 4$ 和 $q\equiv 3 \pmod 4$. 若 $\mathbb{Z}$CPS-Wh(v)，$\mathbb{Z}$CPS-Wh$(q+1)$ 和 $(q,4;1)$-SHCDM 都存在，则 $\mathbb{Z}$CPS-Wh$(qv+1)$ 存在.

2.7 小参数时 $\mathbb{Z}$CPS-Wh(v) 的存在性结果

在这一节中，我们整理了小参数时 $\mathbb{Z}$CPS-Wh(v) 的存在性结果. 首先，我们给出一些新的 $\mathbb{Z}$CPS-Whs.

例 2.2：存在一个 $\mathbb{Z}$CPS-Wh(161)，其初始平行类如下：

$$
\begin{array}{llll}
(46,118,115,43); & (90,84,71,77); & (27,38,134,123); & (52,147,109,14);\\
(159,151,2,10); & (143,79,18,82); & (51,73,110,88); & (50,3,111,158);\\
(108,92,53,69); & (97,39,64,122); & (56,86,105,75); & (54,152,107,9);\\
(133,85,28,76); & (94,138,67,23); & (102,66,59,95); & (1,25,160,136);\\
(49,34,112,127); & (37,65,124,96); & (62,7,99,154); & (61,141,100,20);\\
(30,98,131,63); & (125,31,36,130); & (101,87,60,74); & (120,21,41,140);\\
(47,135,114,26); & (17,126,144,35); & (139,13,22,148); & (145,33,16,128);\\
(156,45,5,116); & (113,155,48,6); & (81,157,80,4); & (129,42,32,119);\\
(70,68,91,93); & (8,83,153,78); & (121,11,40,150); & (89,29,72,132);\\
(117,12,44,149); & (58,57,103,104); & (15,19,146,142); & (24,55,137,106).
\end{array}
$$

例 2.3：存在一个 $\mathbb{Z}$CPS-Wh(209)，其初始平行类如下：

$(61,68,148,141)$; $(153,129,56,80)$; $(44,26,165,183)$; $(208,127,1,82)$;
$(119,152,90,57)$; $(71,50,138,159)$; $(59,151,150,58)$; $(185,5,24,204)$;
$(47,27,162,182)$; $(126,72,83,137)$; $(172,75,37,134)$; $(139,93,70,116)$;
$(15,99,194,110)$; $(16,12,193,197)$; $(198,28,11,181)$; $(147,113,62,96)$;
$(19,3,190,206)$; $(91,144,118,65)$; $(32,34,177,175)$; $(156,171,53,38)$;
$(78,73,131,136)$; $(145,95,64,114)$; $(160,85,49,124)$; $(140,8,69,201)$;
$(117,35,92,174)$; $(170,200,39,9)$; $(21,81,188,128)$; $(121,166,88,43)$;
$(173,101,36,108)$; $(187,111,22,98)$; $(48,186,161,23)$; $(106,7,103,202)$;
$(130,122,79,87)$; $(115,52,94,157)$; $(18,104,191,105)$; $(66,207,143,2)$;
$(40,84,169,125)$; $(133,29,76,180)$; $(189,192,20,17)$; $(112,4,97,205)$;
$(203,109,6,100)$; $(135,86,74,123)$; $(45,55,164,154)$; $(60,51,149,158)$;
$(168,195,41,14)$; $(184,178,25,31)$; $(196,155,13,54)$; $(176,163,33,46)$;
$(132,63,77,146)$; $(10,42,199,167)$; $(30,89,179,120)$; $(67,102,142,107)$.

例 2.4: *存在一个* $\mathbb{Z}$CPS-Wh(217)，*其初始平行类可以通过对以下的每个区组中每个元素乘以* $1,25,191 \pmod{217}$ *展开得到*:

$(20,191,197,26)$; $(10,74,207,143)$; $(5,82,212,135)$; $(14,64,203,153)$;
$(16,116,201,101)$; $(11,118,206,99)$; $(4,28,213,189)$; $(2,171,215,46)$;
$(12,45,205,172)$; $(21,180,196,37)$; $(6,32,211,185)$; $(7,102,210,115)$;
$(19,108,198,109)$; $(3,59,214,158)$; $(8,27,209,190)$; $(23,89,194,128)$;
$(31,107,186,110)$; $(47,56,170,161)$.

例 2.5: *存在一个* $\mathbb{Z}$CPS-Wh(253)，*其初始平行类如下*:

$(133,197,120,56)$; $(55,148,198,105)$; $(51,122,202,131)$; $(14,48,239,205)$;
$(153,92,100,161)$; $(91,187,162,66)$; $(242,177,11,76)$; $(213,19,40,234)$;
$(140,167,113,86)$; $(3,241,250,12)$; $(118,1,135,252)$; $(246,208,7,45)$;
$(20,245,233,8)$; $(176,71,77,182)$; $(28,27,225,226)$; $(227,178,26,75)$;
$(125,46,128,207)$; $(41,110,212,143)$; $(204,174,49,79)$; $(16,106,237,147)$;
$(107,190,146,63)$; $(83,32,170,221)$; $(194,90,59,163)$; $(62,4,191,249)$;
$(98,85,155,168)$; $(29,6,224,247)$; $(180,25,73,228)$; $(240,152,13,101)$;
$(65,67,188,186)$; $(119,129,134,124)$; $(33,53,220,200)$; $(181,145,72,108)$;
$(195,103,58,150)$; $(102,165,151,88)$; $(149,171,104,82)$; $(164,57,89,196)$;
$(130,141,123,112)$; $(64,111,189,142)$; $(132,37,121,216)$; $(206,209,47,44)$;
$(68,31,185,222)$; $(17,127,236,126)$; $(175,35,78,218)$; $(5,24,248,229)$;
$(93,52,160,201)$; $(22,215,231,38)$; $(54,87,199,166)$; $(251,70,2,183)$;
$(116,10,137,243)$; $(23,223,230,30)$; $(184,109,69,144)$; $(158,21,95,232)$;
$(219,60,34,193)$; $(159,9,94,244)$; $(203,179,50,74)$; $(211,81,42,172)$;
$(136,36,117,217)$; $(157,214,96,39)$; $(115,18,138,235)$; $(154,210,99,43)$;
$(169,80,84,173)$; $(15,61,238,192)$; $(97,114,156,139)$.

2.7.1 $v \equiv 1 \pmod 4$ 且 $v \leq 300$

跟据定理 2.3 可知当 $v \equiv 9 \pmod{12}$ 时不存在 $\mathbb{Z}$CPS-Wh(v). 所以我们只需考虑 $v \equiv 1,5 \pmod{12}$. 上一节中关于乘积构造的定理 2.12 将是我们的主要证明工具.

引理 2.17: *给定一个正整数* v. *设* $v \equiv 1 \pmod 4$ *且* $v \leq 300$. *则*

表 2.5　$\mathbb{Z}$CPS-Wh(v): $v \equiv 1 \pmod 4$ 且 $v \leq 300$

5	prime	13	prime	17	prime
25	5×5	29	prime	37	prime
41	prime	49	7^2	53	prime
61	prime	65	5×13	73	prime
77	例1.4[3]	85	5×17	89	prime
97	prime	101	prime	109	prime
113	prime	121	11^2	125	$5 \times 5 \times 5$
133	例1.6[3]	137	prime	145	5×29
149	prime	157	prime	161	例 2.2
169	13×13	173	prime	181	prime
185	5×37	193	prime	197	prime
205	5×41	209	例 2.3	217	例 2.4
221	13×17	229	prime	233	prime
241	prime	245	5×7^2	253	例 2.5
257	prime	265	5×53	269	prime
277	prime	281	prime	289	17×17
293	prime				

(i) 若 $v \equiv 9 \pmod{12}$，则 $\mathbb{Z}$CPS-Wh(v) 不存在.

(ii) 若 $v \equiv 1, 5 \pmod{12}$，则 $\mathbb{Z}$CPS-Wh(v) 都存在.

证明. Finizio[37]对 $5 \leq v \leq 41$ 构造了相应的 $\mathbb{Z}$CPS-Wh(v). 当 v 为素数时，我们可以通过定理 2.1 构造相应的 $\mathbb{Z}$CPS-Wh-(v). 对 $v = q^2$，其中 $q \equiv 3 \pmod 4$ 且 $7 \leq q \leq 11$，相应的 $\mathbb{Z}$CPS-Wh(v) 已经由 Leonard 等人[56,57] 构造出来. 若 v 可以表示成 $v = a_1 \times a_2 \times \cdots \times a_s$，其中 $a_i \equiv 1 \pmod 4$，并且 $\mathbb{Z}$CPS-Wh(a_i) 均存在，则根据定理 2.12 可知 $\mathbb{Z}$CPS-Wh(v) 存在. 详细的信息请参见表 2.5. □

2.7.2　$v \equiv 0 \pmod 4$ 且 $v \leq 300$

例 2.6: 存在一个 $\mathbb{Z}$CPS-Wh(176)，其初始平行类如下:

$(\infty, 35, 0, 140)$; $(3, 174, 172, 1)$; $(38, 166, 137, 9)$; $(11, 152, 164, 23)$;
$(10, 121, 165, 54)$; $(25, 28, 150, 147)$; $(40, 41, 135, 134)$; $(151, 6, 24, 169)$;
$(22, 93, 153, 82)$; $(48, 154, 127, 21)$; $(143, 75, 32, 100)$; $(15, 120, 160, 55)$;
$(13, 149, 162, 26)$; $(159, 126, 16, 49)$; $(12, 115, 163, 60)$; $(141, 109, 34, 66)$;
$(52, 74, 123, 101)$; $(170, 129, 5, 46)$; $(44, 86, 131, 89)$; $(161, 106, 14, 69)$;
$(145, 37, 30, 138)$; $(50, 67, 125, 108)$; $(80, 7, 95, 168)$; $(103, 51, 72, 124)$;
$(90, 8, 85, 167)$; $(68, 91, 107, 84)$; $(29, 57, 146, 118)$; $(61, 122, 114, 53)$;
$(128, 104, 47, 71)$; $(62, 87, 113, 88)$; $(173, 17, 2, 158)$; $(139, 133, 36, 42)$;
$(102, 111, 73, 64)$; $(18, 98, 157, 77)$; $(94, 144, 81, 31)$; $(19, 65, 156, 110)$;
$(76, 155, 99, 20)$; $(142, 132, 33, 43)$; $(92, 78, 83, 97)$; $(79, 116, 96, 59)$;
$(70, 39, 105, 136)$; $(4, 58, 171, 117)$; $(45, 56, 130, 119)$; $(148, 112, 27, 63)$.

引理 2.18: 对 $v \in A = \{4, 28, 40, 76, 112, 148, 184, 220, 292\}$，$\mathbb{Z}$CPS-Wh($v$) 均存在.

证明. 对 $v \in \{4, 28, 40, 76, 112, 148\}$，请参见文献[3,38,75]. 对 $v \in \{184, 220, 292\}$，我们在引理 2.3 中令 $h = 3, n = 61, 73, 97$. 对应的 $\mathbb{Z}$CPS-Wh-frames 的存在性参见引理 2.9. □

引理 2.19: 给定一个正整数 v. 若 v 满足 $v \equiv 4 \pmod{12}$，$v \leq 300$，$v \notin A \cup \{244, 256\}$，则 $\mathbb{Z}$CPS-Wh(v) 不存在.

证明. 对 $v = 136$，因为 $v-1 = 135 = 3^3 \times 5$，所以根据定理 2.6 可知 $\mathbb{Z}$CPS-Wh(136) 不存在. 对于剩下的值，可以应用推论 2.1 进行证明. □

引理 2.20: 给定一个正整数 v. 若 v 满足 $v \equiv 0, 8 \pmod{12}$，$v \leq 300$，$v \notin \{176, 276\}$，则 $\mathbb{Z}$CPS-Wh(v) 不存在.

证明. 根据定理 2.4 容易验证. □

最后我们总结一下本节中得到的结果：

引理 2.21: 设 $v \equiv 0 \pmod{4}$，$v \leq 300$ 且 $v \notin \{244, 256, 276\}$. 则

(i) 若 $v \in A \cup \{176\}$，则 $\mathbb{Z}$CPS-Wh(v) 存在，

(ii) 若 $v \notin A \cup \{176\}$，则 $\mathbb{Z}$CPS-Wh(v) 不存在.

2.7.3 $\mathbb{Z}$CPS-Wh-frame(3^{q^2})

例 2.7: 存在一个 $\mathbb{Z}$CPS-Wh-frame(3^{5^2})，其初始平行类为：

$(2,40,73,35)$; $(6,51,69,24)$; $(7,28,68,47)$; $(12,48,63,27)$;
$(20,32,55,43)$; $(15,49,60,26)$; $(1,3,74,72)$; $(5,64,70,11)$;
$(21,53,54,22)$; $(8,57,67,18)$; $(19,36,56,39)$; $(4,66,71,9)$;
$(13,59,62,16)$; $(14,33,61,42)$; $(10,34,65,41)$; $(17,31,58,44)$;
$(23,30,52,45)$; $(29,37,46,38)$.

例 2.8: *存在一个* $\mathbb{Z}$CPS-Wh-frame(3^{7^2})，*其初始平行类为*:

$(2,127,145,20)$; $(3,121,144,26)$; $(6,99,141,48)$; $(7,27,140,120)$;
$(11,73,136,74)$; $(12,13,135,134)$; $(16,146,131,1)$; $(17,22,130,125)$;
$(24,50,123,97)$; $(25,62,122,85)$; $(28,110,119,37)$; $(4,36,143,111)$;
$(5,40,142,107)$; $(18,113,129,34)$; $(29,90,118,57)$; $(31,58,116,89)$;
$(35,68,112,79)$; $(8,108,139,39)$; $(10,60,137,87)$; $(14,69,133,78)$;
$(15,61,132,86)$; $(30,38,117,109)$; $(41,47,106,100)$; $(45,126,102,21)$;
$(9,66,138,81)$; $(19,72,128,75)$; $(23,44,124,103)$; $(32,46,115,101)$;
$(33,71,114,76)$; $(42,54,105,93)$; $(43,56,104,91)$; $(51,55,96,92)$;
$(52,59,95,88)$; $(53,64,94,83)$; $(63,65,84,82)$; $(67,70,80,77)$.

命题 2.1: *给定任一素数* q. *若* $q \equiv 11 \pmod{12}$ *且* $11 \leq q \leq 359$，*则* $\mathbb{Z}$CPS-Wh-frame(3^{q^2}) *存在*.

证明. 不难看出 $\mathbb{Z}_{3q^2}$ 同构于 $\mathbb{Z}_{q^2} \times \mathbb{Z}_3$. 我们的构造将基于群 $\mathbb{Z}_{q^2} \times \mathbb{Z}_3$. 给定 $\mathbb{Z}_{q^2}$ 的一个本原元 ω. 记 C_0^{2q} 为单位群 $U(\mathbb{Z}_{q^2})$ 的乘法子群

$$\{\omega^{i2q} : 0 \leq i < (q-1)/2\},$$

C_j^{2q} 为 C_0^{2q} 在单位群 $U(\mathbb{Z}_{q^2})$ 中陪集，即

$$C_j^{2q} = \omega^j \cdot C_0^{2q}.$$

另外 C_0^{2q} 在 $\mathbb{Z}_{q^2}$ 中还有两个陪集:

$$q \cdot C_0^{2q} \text{ 和 } (-q) \cdot C_0^{2q}.$$

我们将把它们分别记作 $C(\infty)$ 和 $C(-\infty)$. 不难验证 C_0^{2q} 在 $\mathbb{Z}_{q^2}$ 中共有 $2(q+1)$ 个陪集:

$$C_j^{2q} \ (0 \leq j \leq 2q-1),\ C(\infty),\ C(-\infty).$$

为了构造 $\mathbb{Z}$CPS-Wh-frame(3^{q^2}) 的初始平行类，我们将寻找满足下述条件的由 $3(q+1)/2$ 个区组构成的集合 $\mathcal{B}$:

(i) $\frac{q+1}{6}$ 个区组 $\{(a_i,0),(b_i,0)\}, 1 \leq i \leq \frac{q+1}{6}$;

(ii) $\frac{2(q+1)}{3}$ 个区组 $\{(a_i,0),(b_i,1)\}$, $\frac{q+1}{6}+1\le i\le\frac{5(q+1)}{6}$;

(iii) $\frac{2(q+1)}{3}$ 个区组 $\{(a_i,1),(b_i,1)\}$, $\frac{5(q+1)}{6}+1\le i\le\frac{3(q+1)}{2}$.

跟前面一样，这里每个区组由它的前两个元素表示. 进一步，若下面的任一集合

(i) $\{\pm a_i \mid 1\le i\le\frac{5(q+1)}{6}\}\cup\{\pm b_i \mid 1\le i\le\frac{q+1}{6}\}$,

(ii) $\{a_i \mid \frac{5(q+1)}{6}+1\le i\le\frac{3(q+1)}{2}\}\cup\{b_i \mid \frac{(q+1)}{6}+1\le i\le\frac{3(q+1)}{2}\}$,

(iii) $\{\pm(a_i\pm b_i) \mid 1\le i\le\frac{q+1}{6}\}\cup\{\pm(a_i-b_i) \mid \frac{5(q+1)}{6}+1\le i\le\frac{3(q+1)}{2}\}$,

(iv) $\{a_i+b_i,b_i-a_i \mid \frac{q+1}{6}+1\le i\le\frac{5(q+1)}{6}\}\cup\{-(a_i+b_i) \mid \frac{5(q+1)}{6}+1\le i\le\frac{3(q+1)}{2}\}$,

都构成 C_0^{2q} 在 $\mathbb{Z}_{q^2}$ 中的完全代表系，则区组集合

$$\mathcal{F}=\{B\cdot(s,1)|s\in C_0^{2q}\}$$

就是 $\mathbb{Z}$CPS-Wh-frame(3^{q^2}) 的一个初始平行类. 通过计算机搜索，我们已经对每个素数 $q\equiv 11 \pmod{12}$ 且 $11\le q\le 359$ 找到了相应的初始平行类. 限于篇幅，我们只在表 2.6 中列出 $q=11,23,47$ 的数值. □

2.8 总结

Frames 在可分解设计的构造中起着重要的作用[39,60,86]. 在本章中，我们引入了 $\mathbb{Z}$CPS-Wh frames 的概念，并且利用它统一了之前的许多关于 $\mathbb{Z}$CPS-Wh 的构造. 我们还利用它构造了许多新参数的 $\mathbb{Z}$CPS-Whs，由此大大地推进了这方面的存在性结果. 我们相信 frame 构造方法将会继续在 $\mathbb{Z}$CPS-Whs 的构造中发挥重要的作用.

表 2.6　$\mathbb{Z}$CPS-Wh-frame(3^{q^2}): $q = 11, 23, 47$

q	ω	基区组			
11	2	(17,1),(55,1); (104,1),(15,1); (55,0),(49,1); (62,0),(83,1); (54,0),(26,0);	(57,0),(61,1); (3,1),(22,1); (54,1),(90,1); (37,0),(85,1); (16,1),(40,1).	(76,0),(64,1); (7,0),(37,1); (35,1),(100,1); (81,0),(82,0);	(46,0),(106,1); (95,1),(47,1); (80,1),(36,1); (48,0),(29,1);
23	118	(461,0),(331,1); (282,0),(141,1); (270,1),(155,1); (163,1),(212,1); (505,0),(6,1); (505,1),(276,1); (119,1),(387,1); (440,1),(136,1); (324,1),(7,1);	(471,0),(259,1); (43,1),(129,1); (370,1),(61,1); (460,0),(8,1); (13,0),(2,1); (47,1),(127,1); (204,0),(419,1); (449,0),(48,1); (452,1),(169,1);	(133,1),(520,1); (170,0),(340,0); (48,0),(24,1); (511,1),(199,1); (171,0),(179,0); (140,1),(70,1); (365,0),(466,1); (74,0),(263,1); (202,0),(109,1);	(196,0),(137,0); (413,1),(332,1); (91,0),(62,1); (387,0),(58,1); (166,0),(121,0); (433,0),(37,1); (489,0),(14,1); (437,1),(514,1); (11,1),(527,1).
47	53	(1482,1),(1218,1); (2069,0),(1438,1); (1317,1),(1176,1); (1279,1),(1602,1); (1310,1),(1198,1); (1854,1),(583,1); (1922,1),(1941,1); (1024,0),(1972,1); (1724,0),(2202,1); (1173,0),(2018,0); (1097,0),(1499,0); (1442,0),(1067,1); (891,1),(347,1); (1254,0),(398,1); (1549,0),(650,1); (1797,1),(655,1); (2074,0),(925,1); (1313,0),(762,1);	(132,1),(1110,1); (1080,1),(1426,1); (1783,0),(1410,1); (161,0),(1842,1); (1957,0),(1726,1); (1046,1),(1293,1); (1601,0),(791,1); (1840,1),(1334,1); (1957,1),(263,1); (1565,1),(141,1); (1784,0),(697,1); (1506,1),(849,1); (1581,1),(297,1); (1354,0),(2169,1); (1158,1),(977,1); (1412,0),(368,1); (1716,1),(758,1); (1779,0),(1892,1);	(732,0),(534,0); (1068,0),(1382,1); (1192,0),(2106,1); (638,1),(841,1); (1867,1),(1,1); (84,0),(1584,1); (925,0),(351,0); (958,0),(479,0); (1096,0),(571,1); (1072,0),(16,1); (481,1),(1008,1); (1625,1),(2197,1); (733,1),(348,1); (796,0),(229,1); (1492,0),(1155,1); (1122,0),(1106,1); (1716,0),(305,1); (1484,1),(2163,1);	(1855,1),(2148,1); (786,0),(2122,1); (258,1),(1738,1); (1030,0),(265,0); (994,0),(497,0); (1616,0),(1561,1); (1394,1),(29,1); (878,0),(2072,0); (1328,1),(440,1); (2036,0),(1112,1); (1537,0),(2098,1); (1612,0),(453,1); (1559,0),(411,1); (865,1),(1891,1); (1815,1),(2123,1); (1280,1),(166,1); (1880,0),(371,1); (2,1),(25,1).

3 具有少数特征值的差集

3.1 引言

给定一个 v 阶有限 Abel 群 G，其运算为乘法，单位元为 1_G，且 $\exp(G) = m$. 设 D 为 G 的一个 k 元子集. 给定一个正整数 λ. 若对任意的 $g \in G, g \neq 1_G$，都恰有 λ 个由 D 中元素组成的序对 (d_1, d_2) 使得 $g = d_1 d_2^{-1}$，则称 D 为 G 上的 (v, k, λ)-差集（difference set）. 我们称 $n = k - \lambda$ 为差集 D 的阶. 对于群 G 的一个子集 A，记 $A^{(-1)} = \{g^{-1} \,|\, g \in A\}$. 记号 A 同时也代表群环 $\mathbb{Z}[G]$ 中的元素 $\sum_{g\in A} g$. 容易验证 D 是群 G 上的一个 (v, k, λ)-差集当且仅当以下的群环等式成立：

$$DD^{(-1)} = n + \lambda G.$$

群的特征理论是除群环之外研究差集的又一重要工具. 给定一个有限 Abel 群 G，令 $\widehat{G}$ 表示它的特征群，χ_0 表示平凡特征. 在这一节中，我们将经常应用下面的 Fourier 反演公式.

引理 3.1：*设 G 为 v 阶有限 Abel 群. 若 $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$. 则对任意 $h \in G$，*

$$a_h = \frac{1}{v} \sum_{\chi\in\widehat{G}} \chi(A)\chi(h^{-1}),$$

其中 $\chi(A) = \sum_{g\in A} a_g \chi(g)$.

由 Fourier 反演公式不难看出：设 A 和 B 是群环 $\mathbb{Z}[G]$ 中两个元素. 则 $A = B$ 当且仅当对任一群 G 的特征 χ 均有 $\chi(A) = \chi(B)$. 下面我们利用特征给出差集的一个等价刻画.

命题 3.1：*给定一个 v 阶有限 Abel 群 G 和特征 $\chi \in \widehat{G}$. 令 k 和 λ 为正整数且满足 $k(k-1) = \lambda(v-1)$. 则 G 中的 k-子集 D 是一个 (v, k, λ) 差集当且仅当*

$$\chi(D)\overline{\chi(D)} = \begin{cases} n, & \text{若} \quad \chi \neq \chi_0, \\ k^2, & \text{若} \quad \chi = \chi_0. \end{cases}$$

有关差集的更多知识，读者可以参阅 Beth 等人的专著[12,78].

所有已知的差集可以被划分成以下的三类：Singer 参数的差集、分圆差集和满足 $\gcd(v,n)>1$ 的差集. 其中满足 $\gcd(v,n)>1$ 的差集又可以被划分成以下的五类：Hadamard 差集、McFarland 差集、Spence 差集、Davis 和 Jedwab[24] 构造的一类与 Spence 差集相似的差集、Chen[22] 构造的推广的 Hadamard 差集. 给定一个差集 D. 若对每一个 G 的非平凡特征 χ 均成立 $\sqrt{n}\,|\,\chi(D)$，则称差集 D 具有 character divisibility 性质. 注意到目前所有已知的满足 $\gcd(v,n)>1$ 的差集都具有这种性质. 于是 Jungnickel 和 Schmidt 在他们的综述文章[54] 中提出了下面的问题：

问题： 构造满足 $\gcd(v,n)>1$ 但不具有 character divisibility 性质的差集.

在这一章中，我们将尝试去解决这个问题. 对于一个差集 D，记 D 的所有非平凡的特征值的集合为

$$X=X(D)=\{\chi(D)\mid \chi\in\widehat{G},\chi\neq\chi_0\}.$$

我们将主要考虑满足 $|X|=3$ 的差集并由此推导出一系列的必要条件. 通过计算机搜索，我们找到了一些满足所有这些必要条件的可能参数. 另外我们也找到了一些几乎满足所有必要条件的参数. 这些参数在一定程度了表明是有可能存在满足 $\gcd(v,n)>1$ 但不具有 character divisibility 性质的差集.

在图论领域中也有一些与本节类似的研究结果. Bridges 和 Mena[15–17] 考察了一类具有 3 个特征值的图：multiplicative design. Ma[66] 则研究了一般群中具有少数几个特征值的 polynomial addition 集. 所有这些工作都是具有少数几个特征值的图[19] 的特殊情形.

这一章的结构安排如下：在第 3.2 节中，我们推导出一些关于具有 3 个非平凡特征值差集存在的必要条件. 然后根据引理 3.2，我们将分成三种情形分别在第 3.3-3.5 节中进行讨论. 最后我们在第 3.6 节中处理额外的三种特殊情形.

3.2 必要条件

在本节中我们总是假定：当群 G 的特征 χ 遍历所有的非平凡特征时，$\chi(D)$ 总共取到三个非平凡的特征值 a、b 和 c.

首先我们规定一些记号. 记 $\mathbb{Z}_m^*$ 为 $\mathbb{Z}_m$ 的乘法单位群. 对任意 $t \in \mathbb{Z}_m^*$，通过 $\sigma_t(\xi_m) = \xi_m^t$ 来定义 Galois 群 $\mathrm{Gal}(Q(\xi_m)/Q)$ 中的元素 σ_t，并且 $\mathrm{Gal}(Q(\xi_m)/Q)$ 中每个元素都可以表示成这种形式. 对任意的 $\chi \in \widehat{G}$ 和 $x \in G$，定义 $\chi^t(x) = \sigma_t(\chi(x))$；不难看出它也是群 G 的一个特征. 对于特征群 $\widehat{G}$ 的子集 U，定义 $U^{(t)} = \{\chi^t \,|\, \chi \in U\}$. 对每个 $z \in \{a, b, c\}$，规定

$$U_z = \{\chi \in \widehat{G} \backslash \{\chi_0\} \,|\, \chi(D) = z\}.$$

则集合 U_a、U_b 和 U_c 构成了 G 中所有非平凡特征的一个划分. 对于 G 的任一特征 χ，容易看出 χ^{-1} 也是 G 的一个特征，并且 $\chi^{-1}(D) = \sigma_{-1}(\chi(D))$. 因此

$$\{\sigma_{-1}(a), \sigma_{-1}(b), \sigma_{-1}(c)\} = \{a, b, c\}.$$

于是 σ_{-1} 至少固定集合 $\{a, b, c\}$ 中一个元素. 不妨设 $c = \sigma_{-1}(c)$，即 c 为实数. 则 $b = \sigma_{-1}(a) = \bar{a}$，$U_a^{(-1)} = U_b$.

令 χ 是集合 U_c 中一个特征，即 $\chi(D) = c$. 结合 $\chi(D)\overline{\chi(D)} = n$，我们有 $c = \pm\sqrt{n}$. 不妨设 $c = \sqrt{n}$；如若不然，则用 $G \setminus D$ 代替 D. 显然 a 与 $\bar{a}$ 均不等于 $\pm\sqrt{n}$. 因为 $\mathrm{Gal}(Q(\xi_m)/Q)$ 可交换，所以对任意 $t \in \mathbb{Z}_m^*$，

$$\sigma_{-1}(\chi^t(D)) = \sigma_t\sigma_{-1}(\chi(D)) = \chi^t(D).$$

由此可知对任一 $t \in \mathbb{Z}_m^*$ 都有 $\sigma_t(\sqrt{n}) = \chi^t(D) = \sqrt{n}$. 从而 $\sqrt{n}$ 是一个整数且对任意 $t \in \mathbb{Z}_m^*$ 成立 $U_c^{(t)} = U_c$.

类似地，容易验证子群 $T := \{t \in \mathbb{Z}_m^* | \sigma_t(a) = a\}$ 在群 $\mathbb{Z}_m^*$ 中的指数（index）等于 2，并且对任意的 $t \in T$ 成立 $U_a^{(t)} = U_a$，$U_b^{(t)} = U_b$. 由此可知对任意的 $\chi \in \widehat{G}$ 和 $t \in T$，都有 $\chi(D) = \chi^t(D) = \chi(D^{(t)})$ 成立. 根据反演公式，可知 D 被 T 所固定，即对任意的 $t \in T$ 均成立 $D^{(t)} = D$. 另外由 Galois 理论的基本定理可知 $Q(a)$ 是 $Q(\xi_m)$ 的二次子域. 所以存在某个无平方因子的整数 d 使得 $Q(a) = Q(\sqrt{d})$. 下面我们给出一些关于二次域和分圆域的结果. 读者可以参考 Ireland 等人的教材[53].

环 $\mathbb{Z}[1, \beta]$ 是 $Q(\sqrt{d})$ 的代数整数环，其中

$$\beta = \begin{cases} \sqrt{d}, & \text{若 } d \equiv 2, 3 \pmod 4, \\ (-1 + \sqrt{d})/2, & \text{若 } d \equiv 1 \pmod 4. \end{cases}$$

代数数域 $Q(\sqrt{d})$ 的判别式（discriminant）为

$$\Delta_d = \begin{cases} 4d, & \text{若 } d \equiv 2,3 \pmod 4, \\ d, & \text{若 } d \equiv 1 \pmod 4. \end{cases}$$

代数数域 $Q(\xi_m)$ 的判别式等于

$$(-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}.$$

它与 m 具有相同的素因子；除了当 $m \equiv 2 \pmod 4$ 时它与 m 具有相同的奇的素因子. 我们知道素数 p 在一个代数数域中分裂当且仅当 p 整除这个数域的判别式. 所以 Δ_d 的每一个素因子也都是 m 的因子. 由此推出 $d|m$ 和当 $4|m$ 时 Δ_d 为偶数.

给定整除 m 的一个素数 p. 记 G 的 Sylow p-子群为 G_p. 设 $G = G_p \times W$，其中 W 是一个阶为 w 的子群且 w 与 p 互素. 又设 $|G_p| = p^s$. 下面我们给出一个关于二次域 $Q(a)$ 的判别式的一个结果.

引理 3.2: 二次域 $Q(a)$ 的判别式 Δ_d 只可能有一个素因子. 下面是它所有可能的取值情况:

$$\Delta_d = \begin{cases} -p, & \text{若 } d = -p, \text{ 其中 } p \text{ 为素数且 } p \equiv 3 \pmod 4, \\ -8, & \text{若 } d = -2, \\ -4, & \text{若 } d = -1. \end{cases}$$

证明. 取定 Δ_d 的任一素因子 p，且设 $p^s||v$. 对于任一在 G_p 上的作用是平凡的群 G 的特征 χ，特征值 $\chi(D)$ 属于数域 $Q(\xi_{\text{ord}(\chi)})$. 而数域 $Q(\xi_{\text{ord}(\chi)})$ 的判别式与 p 互素. 因此 $\chi(D) = \sqrt{n}$. 利用反演公式，可知 D 在 $\bar{G} = G/G_p$ 中同态下的象为

$$\bar{D} = \sqrt{n} + \frac{k - \sqrt{n}}{w} \bar{G}, \tag{3.1}$$

其中 $w = v/p^s$. 于是

$$w|(k - \sqrt{n}),$$

等价于说 $v|p^s(k - \sqrt{n})$. 若 q 为 Δ_d 的另一素因子，则 $v|q^r(k - \sqrt{n})$ 且 $q^r||v$. 根据 $\gcd(p^s, q^r) = 1$ 可以推出 $v|(k - \sqrt{n})$，而这时不可能的. 所以 Δ_d 只有一个素因子. 于是 $\Delta_d = \pm p$，其中 p 为一个奇素数，或者 $\Delta_d = \pm 2^r$ 其中 r 为大于等于 2 的整数. 所以我们有

(i) $d = p^* = (\frac{-1}{p})p$，或

(ii) $d \in \{-1, -2, 2\}$.

在情形 (i) 中，根据 $\sigma_{-1}(\sqrt{p^*}) = (\frac{-1}{p})\sqrt{p^*} = -\sqrt{p^*}$ 可知 $p \equiv 3 \pmod 4$. 在情形 (ii) 中，根据 $\sqrt{2} = \xi_8 + \xi_8^7$ 被 σ_{-1} 固定可知 $d = 2$ 不可能出现. 这样我们就证明了整个结论. □

注：当 $p = 2$ 时，我们可以改进上述引理证明中的结论 $v|2^s(k - \sqrt{n})$. 令 N 为一个阶为 2^{s-t} 的子群并且使得 $\bar{G} = G/N$ 的 Sylow 2-子群是初等交换的. 令 $rk_2(G)$ 代表所有可能的 t 中最大的整数. 则通过类似的推导我们可以得到 $\bar{D} = \sqrt{n} + \frac{k-\sqrt{n}}{v/2^{s-rk_2(G)}}\bar{G}$. 于是 $v|(2^{s-rk_2(G)}(k - \sqrt{n}))$.

当 a 是一个纯虚数时，我们有下面的结果.

引理 3.3：若 $a + \bar{a} = 0$，则 $d = -1$.

证明. 根据 $a + \bar{a} = 0$ 和 $a\bar{a} = n$ 可知 $a = \pm i\sqrt{n}$. 从而 $Q(a) = Q(\sqrt{-1})$，所以 $d = -1$. □

为了方便，我们引入以下的几个符号：$\Delta = 2\sqrt{n} - a - \bar{a}$，$\Omega = (v(\sqrt{n} - a))/((a - \bar{a})\Delta)$ 和 $R = (k - \sqrt{n})/\Delta$. 记 $D = \sum_{g\in G} d_g g$ 和 $D^{(-1)} = \sum_{g\in G} d'_g g$，其中每个系数 d_g, d'_g 均为 0 或 1. 根据反演公式，对任意的 $g \in G$ 我们有

$$\begin{aligned} vd_g &= ag^{-1}(U_a) + \bar{a}g^{-1}(U_b) + \sqrt{n}g^{-1}(U_c) + k; \\ vd'_g &= \bar{a}g^{-1}(U_a) + ag^{-1}(U_b) + \sqrt{n}g^{-1}(U_c) + k; \\ v\delta_g &= g^{-1}(U_a) + g^{-1}(U_b) + g^{-1}(U_c) + 1, \end{aligned}$$

其中 $g^{-1}(U_z) = \sum_{\chi\in U_z} \chi(g^{-1})(z = a, b, c)$；$\delta_g = 1$ 若 $g = 1_G$，否则等于 0. 于是我们有：

$$\begin{aligned} g^{-1}(U_a) &= \frac{(vd_g - k + \bar{a})(\sqrt{n} - a) - (vd'_g - k + a)(\sqrt{n} - \bar{a}) - \sqrt{n}\bar{a}v\delta_g + \sqrt{n}av\delta_g}{(a - \bar{a})\Delta}; \\ g^{-1}(U_b) &= \overline{g^{-1}(U_a)}; \\ g^{-1}(U_c) &= \frac{v(d_g + d'_g) - (a + \bar{a})(v\delta_g - 1) - 2k}{\Delta}. \end{aligned}$$

表 3.1　特征表

d_g	d'_g	$g^{-1}(U_a)$	$g^{-1}(U_b)$	$g^{-1}(U_c)$
1	1	$-\frac{v}{\Delta}+R$	$-\frac{v}{\Delta}+R$	$\frac{2v}{\Delta}-1-2R$
1	0	$\Omega+R$	$\bar{\Omega}+R$	$\frac{v}{\Delta}-1-2R$
0	1	$\bar{\Omega}+R$	$\Omega+R$	$\frac{v}{\Delta}-1-2R$
0	0	R	R	$-1-2R$

特别地，当 $g=1_G$ 时上述等式给出：

$$\begin{aligned} |U_a| &= |U_b| = \frac{v(\sqrt{n}-d_1)}{\Delta}+R, \\ |U_c| &= \frac{v(2d_1-a-\bar{a})}{\Delta}-1-2R. \end{aligned}$$

当 $g\neq 1_G$，我们根据 d_g 和 d'_g 取值的情况在表 3.1 将其分为四种情形.

容易验证 $|D\cap D^{(-1)}|$ 就是 D^2 中 1_G 的系数. 根据反演公式，可得

$$v|D\cap D^{(-1)}| = |U_a|(a^2+\bar{a}^2)+|U_c|n+k^2.$$

由此推出

$$\begin{aligned} |D\cap D^{(-1)}| &= \frac{|U_a|(a^2+\bar{a}^2)+|U_c|n+k^2}{v} \\ &= \frac{1}{v}\left[|U_a|(-2n+a^2+\bar{a}^2)+(2|U_a|+|U_c|)n+k^2\right] \\ &= \frac{1}{v}\left[-(v(\sqrt{n}-d_1)+k-\sqrt{n})(2\sqrt{n}+a+\bar{a})+(v-1)n+k^2\right] \\ &= k-(\sqrt{n}-d_1+\frac{k-\sqrt{n}}{v})(2\sqrt{n}+a+\bar{a})<k \end{aligned}$$

接下来，我们定义以下的 4 个集合：$E_1=D\cap D^{(-1)}\setminus\{1_G\}, E_2=D\setminus D^{(-1)}, E_3=D^{(-1)}\setminus D$ 和 $E_4=G\setminus(D\cup D^{(-1)}\cup\{1_G\})$. 容易看出这 4 个集合构成了 $G\setminus\{1_G\}$ 的一个划分. 容易证明集合 E_2 和 E_3 均非空集：如若不然，由 $D=D^{(-1)}=D\cap D^{(-1)}$ 推出 $\chi(D)=\chi(D^{(-1)})=\overline{\chi(D)}$，而这对 $\chi\in U_a$ 不成立. 类似地，我们有集合 E_1 和 E_4 中至少一个是非空的：如若不然，则 $D+D^{(-1)}=G-1+2d_1$，从而当 χ 遍历所有的非平凡特征值时 $\chi(D)$ 只取到两个非平凡的特征值综上所述，集合 $E_i, 1\leq i\leq 4$ 中至少有三个是非空的.

值得注意的是：当 E_1 是空集而 E_4 非空的时候，我们在 $\widehat{G}$ 上能得到一个 3 类的结合方案. 设 $\widehat{G}$ 的全体共轭类为 $\{C_0, C_1, \ldots, C_d\}$，其中 $C_0 = \{\chi_0\}$. 我们定义 $(x, y) \in R_i$ 当且仅当 $yx^{-1} \in C_i$. 我们已经知道 $\mathscr{X} = (\widehat{G}, \{R_i\}_{0 \le i \le d})$ 构成了一个 d-类的结合方案[10]. 记 $\overline{C_i} = \sum_{x \in C_i} x$，$0 \le i \le d$. 则 $\{\overline{C_0}, \overline{C_1}, \ldots, \overline{C_d}\}$ 构成一个 Schur 环[67]. 依据 Bannai-Muzychuk 判别法则[9,76] 和表 3.1 中的信息，我们可以如下的类数为 3 的 $\mathscr{X}$ 的 fusion 方案. 这里我们给出它的第一特征阵：

$$P = \begin{array}{c} \\ 1 \\ E_2 \\ E_3 \\ E_4 \end{array} \begin{array}{c} \begin{array}{cccc} \chi_0 & U_a & U_b & U_c \end{array} \\ \begin{pmatrix} 1 & \frac{v(n-d_1)}{\Delta} + R & \frac{v(n-d_1)}{\Delta} + R & \frac{v(2d_1-a-\bar{a})}{\Delta} - 1 - 2R \\ 1 & \Omega + R & \bar{\Omega} + R & \frac{v}{\Delta} - 1 - 2R \\ 1 & \bar{\Omega} + R & \Omega + R & \frac{v}{\Delta} - 1 - 2R \\ 1 & R & R & -1 - 2R \end{pmatrix} \end{array},$$

其中

$$\det P = \frac{v^3}{(a - \bar{a})\Delta}.$$

接下来，我们将根据上面的讨论推导出一些必要条件. 我们记 p 为 Δ_d 唯一的素因子. 又记 $\sqrt{n} = p^x u$，其中 x 为某一非负整数且满足 $\gcd(p, u) = 1$，即 $p^x || \sqrt{n}$.

(1) $\Delta | v$, $\Delta | (k - \sqrt{n})$, $(a - \bar{a})\Delta | v(\sqrt{n} - a)$, $(a - \bar{a}) | v$.

根据表 3.1 中的数都是代数整数、E_2 和 E_3 都非空集和 E_1、E_4 中至少一个不是空集，我们容易验证上面的结论. 从 $\Omega - \bar{\Omega} = v/(a - \bar{a})$ 容易推出最后一个结论.

(2) $v \,|(k - \sqrt{n})(2\sqrt{n} + a + \bar{a})$.

这是因为 $|D \cap D^{(-1)}|$ 是一个整数.

(3) $w|(k-\sqrt{n}), \sqrt{n}+\frac{k-\sqrt{n}}{w} \leq p^s$.

这个结论可以从引理 3.2 的证明过程中直接推出. 若 $p=2$，事实上我们可以进一步得到 $v|2^{s-rk_2(G)}(k-\sqrt{n})$ 和 $\sqrt{n}+\frac{k-\sqrt{n}}{2^{rk_2(G)}w} \leq 2^{s-rk_2(G)}$.

(4) $p\,|(2\sqrt{n}+a+\bar{a})$.

如若不然，从 (2) 中我们推出 $p^s|(k-\sqrt{n})$. 又因为 $w|(k-\sqrt{n})$，所以我们有 $v|(k-\sqrt{n})$，而这是不可能的.

(5) $1 \leq 2d_1 - a - \bar{a}$.

这是因为 $g^{-1}(U_c)$ 是一个不大于 $|U_c|$ 的整数.

下面我们给出两个有关 $|G|$ 其它素因子性质的结论.

命题 3.2: *若 q 为 v 的一个不等于 p 的素因子，则 $q|(a-\bar{a})$.*

证明. 设 $q \nmid (a-\bar{a})$. 则 $q \nmid (\sqrt{n}-a)$：如若不然，则 $q \mid (\sqrt{n}-\bar{a})$，而两者之差给出 $q \mid (a-\bar{a})$，这是不可能的. 令

$$\bar{G} = G_p \times \langle \alpha : \alpha^q = 1 \rangle$$

为 G 的一个商群，并且定义 $\bar{D}$ 为 D 在 $\bar{G}$ 中的象.

当 $d=-p$ 其中 p 为一个奇素数时，我们有 $\sigma_t(\sqrt{d}) = \sigma_t(\sqrt{p^*}) = (\frac{t}{p})\sqrt{p^*}$. 因此 $T = \{t \in \mathbb{Z}_m^* | (\frac{t}{p}) = 1\}$. 当 $d=-1$ 时，我们有 $p=2$ 和 $4|m$. 根据 $\sqrt{-1} = \xi_4$ 可知 $T = \{t \in \mathbb{Z}_m^* | t \equiv 1 \pmod 4\}$. 当 $d=-2$ 时，我们有 $p=2$ 和 $8|m$. 根据 $\sqrt{-2} = \xi_8 + \xi_8^3$ 可知 $T = \{t \in \mathbb{Z}_m^* | t \equiv 1, 3 \pmod 8\}$. 于是不论 $d=-p$、-1 或 -2，我们均可以通过中国剩余定理对任意的 $i, 1 \leq i \leq q-1$ 找到一个整数 $t \in T$ 满足 $t \equiv 1 \pmod{p^s}$ 和 $t \equiv i \pmod q$.

由于 D 被 T 所固定，我们有

$$\bar{D} = D_0 + D_1(\langle \alpha \rangle - 1)$$

其中 $D_0, D_1 \in \mathbb{Z}[G_p]$. 将群 $\langle \alpha : \alpha^q = 1 \rangle$ 简记为 G_q，并设 $\chi_1 \times \chi_2$ 为 $G_p \times G_q$ 的一个特征. 若 χ_2 在 G_q 上是平凡的，则

$$\chi_1(D_0) + (q-1)\chi_1(D_1) = c_1, \tag{3.2}$$

反之，

$$\chi_1(D_0) - \chi_1(D_1) = c_2. \tag{3.3}$$

若 χ_1 在 G_p 上是非平凡的，则 $c_1, c_2 \in \{a, \bar{a}, \sqrt{n}\}$；反之 $c_1 = k, c_2 = \sqrt{n}$. 当 χ_1 是非平凡的特征时，通过对前面两个等式取差，我们有 $q\chi_1(D_1) = c_1 - c_2$. 再根据假设条件，我们有 $c_1 = c_2$ 和 $\chi_1(D_1) = 0$. 当 χ_1 是平凡的特征时，我们有 $\chi_1(D_1) = (k - \sqrt{n})/q$. 于是

$$D_1 = \frac{k - \sqrt{n}}{qp^s} G_p.$$

由此推出 $p^s | (k - \sqrt{n})$. 再结合 $w | (k - \sqrt{n})$，我们得到 $v | (k - \sqrt{n})$，而这是不可能的. 所以我们有 $q | (a - \bar{a})$. □

下面的结论是关于 D 的乘子的.

命题 3.3: 设 q 为一个素数. 若 q 整除 n 且 q 与 v 互素，则 $D^{(q)} = D$.

证明. 设 Q 为 $\mathbb{Z}[\xi_v]$ 的素理想，$Q|q$，则 $q|n$. 若 $Q|a$，$Q|\bar{a}$，则 $Q|\Delta = 2\sqrt{n} - a - \bar{a}$. 根据 $\Delta | v$ 可知 $Q|v$. 而这与条件 q 和 v 是互素的矛盾. 根据 $n = a\bar{a}$，我们有 Q 恰整除 $a, \bar{a}$ 中的某一个数. 又因为 $\sigma_q(Q) = Q$，$\{\sigma_q(a), \sigma_q(\bar{a})\} = \{a, \bar{a}\}$，故 $\sigma_q(a) = a$，$\sigma_q(\bar{a}) = \bar{a}$. 根据 $\chi(D^{(q)}) = \sigma_q(\chi(D))$ 和 $\chi(D)$ 只可能取值 $k, \sqrt{n}, a, \bar{a}$，我们可以得到当 χ 遍历所有的特征时恒成立 $\chi(D^{(q)}) = \chi(D)$. 于是从反演公式我们直接推出 $D^{(q)} = D$. □

注：

(i) 给定一个满足命题 3.3 中条件的素数 q. 根据 $\sigma_q(a) = a$，即 $\sigma_q(\sqrt{d}) = \sqrt{d}$，我们得到：$(\frac{q}{p}) = 1$ 若 $d = -p$ 其中 p 为奇素数；$q \equiv 1, 3 \pmod 8$ 若 $d = -2$；$q \equiv 1 \pmod 4$ 若 $d = -1$.

(ii) 给定一个不等于 p 的素数 q. 若 q 同时整除 n 和 v，则根据命题 3.2 我们有 $q | (a - \bar{a})$. 又因为 $4n = (a + \bar{a})^2 - (a - \bar{a})^2$，所以 $q | (a + \bar{a})$. 于是若 q 是一个奇数，则 $q|a$，$q|\bar{a}$.

3.3 $d=-p$ 的情形

在这一节中，我们将考虑 $d=-p$ 的情形，其中 p 为奇素数. 下面我们设 $d=-p$，其中 p 为一个奇素数且 $p\equiv 3 \pmod 4$.

根据引理 3.3 可知 $a+\bar{a}\neq 0$. 下面我们来推导出一些新的必要条件. 对任一整数 l，记最大的整数 z 使得 p^z 整除 l 为 $\mathrm{ord}_p(l)$.

(6') $p^x||(a+\bar{a}), p^x|(a-\bar{a}), p^x|k, s\geq x+1$.

根据 $d=-p\equiv 1 \pmod 4$，a 为 $\mathbb{Q}(\sqrt{-p})$ 中的一个代数整数，可知存在整数 e,f 使得 $a=e+f\frac{-1+\sqrt{-p}}{2}$. 于是 $a-\bar{a}=f\sqrt{-p}$，所以 $\mathrm{ord}_p((a-\bar{a})^2)$ 为奇数. 又根据 $4n=(a+\bar{a})^2-(a-\bar{a})^2$，$\mathrm{ord}_p((a-\bar{a})^2)$ 为奇数，可得 $p^x||(a+\bar{a})$. 从而我们有 $p^x|(a-\bar{a})$，$p^x|\Delta=2\sqrt{n}-a-\bar{a}$. 从 $\Delta|(k-\sqrt{n})$ 可知 $p^x|(k-\sqrt{n})$，于是 $p^x|k$. 从 $w|(k-\sqrt{n})$ 可知 $v|(k-\sqrt{n})p^{s-x}$，于是 $s\geq x+1$.

(7') $x\geq 1$.

取定一个特征 $\chi\in U_a$. 令 χ' 为 G 的另一特征且它在 W 上的作用与 χ 相同而在 G_p 上的作用是平凡的. 则 $\chi(D)=a$，$\chi'(D)=\sqrt{n}$. 根据 $(1-\xi_{p^s})|(\chi(D)-\chi'(D))$ 可知 $(1-\xi_{p^s})|(a-\sqrt{n})$. 类似的，我们可以得到 $(1-\xi_{p^s})|(\bar{a}-\sqrt{n})$. 我们已经知道 $p|(2\sqrt{n}+a+\bar{a})$，所以 $(1-\xi_{p^s})|4\sqrt{n}$. 于是 $p|4\sqrt{n}$，由此可以得到 $x\geq 1$.

(8') $p^x||k, p^x||(k-\sqrt{n}), p^s||(k+\sqrt{n}), \Delta|p^xw$.

根据 $k(k-1)=\lambda(v-1)$ 和 (1)，可知 $\mathrm{ord}_p(\lambda)=\mathrm{ord}_p(k)\geq x$. 又根据 $k^2=n+\lambda v$ 和 $\mathrm{ord}_p(n)=2x<x+s\leq\mathrm{ord}_p(\lambda v)$，我们有 $\mathrm{ord}_p(k)=x$，即 $p^x||k$. 从 $(k+\sqrt{n})-(k-\sqrt{n})=2\sqrt{n}$ 可以知道 $\mathrm{ord}_p(k+\sqrt{n}), \mathrm{ord}_p(k-\sqrt{n})$ 中至少一个数等于 x. 于是根据 $k^2-n=(k+\sqrt{n})(k-\sqrt{n})=\lambda v$ 可知 $\{\mathrm{ord}_p(k+\sqrt{n}), \mathrm{ord}_p(k-\sqrt{n})\}=\{s,x\}$. 若 $\mathrm{ord}_p(k-\sqrt{n})=s$，则从 $w|(k-\sqrt{n})$ 我们有 $v|(k-\sqrt{n})$，而这是不可能的. 因此 $\mathrm{ord}_p(k+\sqrt{n})=s$，$\mathrm{ord}_p(k-\sqrt{n})=x$. 最后一个结果 $\Delta|p^xw$ 可以从 $\Delta|v, \Delta|(k-\sqrt{n}), \gcd(v,(k-\sqrt{n}))=p^xw$ 中推出.

下面我们记

$$\gamma = \frac{k-\sqrt{n}}{p^x w}.$$

根据 $w|(k-\sqrt{n})$ 和 $p^x||(k-\sqrt{n})$，可知 γ 为一个与 p 互素的整数. 从

$$(k+\sqrt{n})(k-\sqrt{n}) = k^2 - n = \lambda v$$

可得

$$\gamma(\lambda + n + \sqrt{n}) = p^{s-x}\lambda.$$

于是

$$\begin{aligned}
\lambda &= \frac{(n+\sqrt{n})\gamma}{p^{s-x}-\gamma} = \frac{(p^x u+1)u}{p^{s-x}-\gamma}p^x\gamma, \\
k &= n+\lambda = \frac{p^{s-x}n+\sqrt{n}\gamma}{p^{s-x}-\gamma} = \frac{(p^s u+\gamma)u}{p^{s-x}-\gamma}p^x, \text{and} \\
w &= \frac{k-\sqrt{n}}{p^x\gamma} = \frac{(n-\sqrt{n})p^{s-x}+2\sqrt{n}\gamma}{\gamma p^x(p^{s-x}-\gamma)} = \frac{(p^x u-1)u}{\gamma} + \frac{(p^x u+1)u}{p^{s-x}-\gamma}.
\end{aligned}$$

记

$$\begin{aligned}
a+\bar{a} &= -p^x\alpha, \\
a-\bar{a} &= \eta p^x\sqrt{-p}
\end{aligned}$$

其中 $\alpha, \eta \in \mathbb{Z}$，$\gcd(p,\alpha) = 1$. 因为 $1 \le 2d_1 - a - \bar{a}$，$a+\bar{a} \neq 0$，所以我们必须有 $\alpha \ge 1$. 从 $4n = (a+\bar{a})^2 - (a-\bar{a})^2$ 可得 $4u^2 = \alpha^2 + p\eta^2$. 又从命题 3.2 可知 $\pi(w) = \pi(\eta) \setminus \{p\}$，其中 $\pi(w)$ 代表 w 的所有素因子的集合. 根据 $\sqrt{n} + \frac{k-\sqrt{n}}{w} \le p^s$ 我们得到 $u + \gamma \le p^{s-x}$. 经过整理，我们可以将上面所得到的必要条件简化为：

$$\begin{array}{llll}
\gamma|(p^x u-1)u, & (p^{s-x}-\gamma)|(p^x u+1)u, & 2u+\alpha|w, & p^{s-x}|p^x(2u-\alpha), \\
\eta|p^{s-x}w, & u+\gamma \le p^{s-x}, & \pi(w) = \pi(\eta)\setminus\{p\}, & 4u^2 = \alpha^2 + p\eta^2, \\
s \ge x+1, & x \ge 1, & \alpha \ge 1. &
\end{array}$$

注： (i) 根据 w 的表达式，我们可以得到 $v \ge 4n$，其中 γ 为取值在区间 $(0, p^{s-x})$ 中一个变量，且当 $\gamma = \frac{p^{s-x}}{2}$ 时取到最小值. 这里我们没有利用任何关于 $a, \bar{a}$ 的整除性条件. 根据 $(2u+\alpha)|w$ 和 $2u+\alpha \ge 3$ 可知 $w > 1$，即 G 不能为一个 p-群.

(ii) 从 $|U_c| \ge 0$ 可以得到 $v \ge \frac{2k-2d_1}{2d_1+p^x\alpha} + 1$.

(iii) 令 $\widetilde{U_c} = \{\chi \in U_c \mid \chi \text{ 在 } G_p \text{ 上作用不是平凡的}\}$. 则 $|\widetilde{U_c}| = |U_c| - (|W| - 1)$. 我们定义群 $\mathbb{Z}_{p^s}^*$ 在 $\widetilde{U_c}$ 上的如下作用: $(t, \chi) \to \chi^t$，其中 $t \in \mathbb{Z}_{p^s}^*, \chi \in \widetilde{U_c}$. 不难验证如此定义的群作用下的轨道的长度均被 $p-1$ 所整除. 因此 $(p-1)\big|(w(d_1 - \sqrt{n}) - (k - \sqrt{n}))$.

(iv) 令 $T_1 = \{t \in Z_{p^s}^* | (\frac{t}{p}) = 1\}$. 我们可以像 (3) 中一样类似地定义 T_1 在 U_a 上的群作用. 同样地，我们可以得到 $\frac{p-1}{2}\big|(w\sqrt{n} - d_1 + (k - \sqrt{n}))$.

我们已经通过计算机程序对以下参数区间 $p \in \{3, 5, 7, 11, 13, 17, 19\}, 1 \leq x, s \leq 10, 1 \leq \alpha, \eta \leq 10^4$ 进行了搜索，遗憾的是我们没有找到满足上述所有必要条件的参数. 下面我们给出两个几乎满足所有条件的例子.

例 3.1: 令 $p = 7$，$\alpha = 8$，$\eta = 24$，$u = 32$，$\gamma = 4$，$v = 2^3 \cdot 3^5 \cdot 7^3$，$k = 54656$，$n = 2^{10} \cdot 7^2$. 于是 $3|w$，$3|(k - \sqrt{n})$，$d_1 = 0$，且这一节中所有的必要条件均被满足除了 $(\sqrt{n} - d_1 + \frac{k-\sqrt{n}}{v})(2\sqrt{n} + a + \bar{a}) \leq k$.

例 3.2: 令 $p = 11$，$\alpha = 30$，$\eta = 48$，$u = 81$，$\gamma = 980$，$v = 2^{10} \cdot 3 \cdot 11^5$，$k = 364287561$，$n = 3^8 \cdot 11^4$. 于是 $w \equiv 2 \pmod 5$，$\sqrt{n} \equiv 1 \pmod 5$，$5|(k - \sqrt{n})$，$d_1 = 1$，且这一节中所有的必要条件均被满足除了 $\frac{p-1}{2}|(w\sqrt{n} - d_1 + (k - \sqrt{n}))$.

3.4 $d = -2$ 的情形

接下来，我们来考虑 $d = -2, \Delta_d = -8$ 的情形. 根据第 3.2 节中结论我们已经知道 $4|m$. 定义

$$l = \min\{|N| \,\big|\, G/N \text{ 的指数被 } 4 \text{ 严格整除}\}.$$

因此我们可以选取 G 的一个阶为 l 的子群 N 使得 $\exp(G/N)$ 被 4 严格整除. 与引理 3.2 中证明类似，我们考察 D 在 G/N 中的同态象. 容易看出

$$\sqrt{n} + \frac{k - \sqrt{n}}{v/l} \leq l.$$

不难验证 l 是 2 的幂次方且 $l \leq 2^{s-2}$. 根据 $\sqrt{-2}$ 属于 $Q(\xi_8)$ 但不属于 $Q(\xi_4)$，可知 $8|\exp(G)$. 所以 $l \geq 2$. 记 $k = \sqrt{n} + \gamma\Delta$，其中 γ 为某一正整数，$a = u_1 + u_2\sqrt{-2}$，其中 u_1, u_2 为满足 $u_1^2 + 2u_2^2 = n$ 的整数. 我们已经通过计算机程序对以下参数区间

$-10^4 \le u_1 \le 1, 1 \le u_2, \gamma \le 10^4$ 进行了搜索，并且找到了满足第 3.2 节中所有必要条件的参数. 下面我们给出两个例子.

例 3.3: 对 $a = 96(-1+2\sqrt{-2})t$，$\gamma = 216t$，$n = 2^{10}\cdot 3^4 \cdot t^2$，$v = 4n$，其中 $t \in \{2^i, 12\cdot 2^i, 20\cdot 2^i \,|\, i$ 为非负整数$\}$，第 3.2 节中所有必要条件均被满足. 若 $t = 1$，则 $l \ge \frac{1}{(1-\frac{k-\sqrt{n}}{v})}\sqrt{n} = 2\sqrt{n} = 2^6 \cdot 3^2$. 因此 $l \ge 2^{10}$. 从而 G 的 Sylow 2-子群必须是循环的，然而 Turyn [78] 已经证明这样的差集是不可能存在的.

例 3.4: 对 $a = 192(-7+4\sqrt{-2})t$，$\gamma = 972t$，$n = 2^{12}\cdot 3^6 \cdot t^2$，$v = 4n$，$k = 2n+\sqrt{n}$，其中 $t = 2^i$，i 为某一非负整数，第 3.2 节中所有必要条件均被满足. 若 $t = 1$，$l \ge 2\sqrt{n} = 2^7 \cdot 3^3$，则 $l \ge 2^{12}$. 跟上面的例子一样，这样的差集不可能存在.

3.5 $d = -1$ 的情形

对 $d = -1, \Delta_d = -4$ 情形的分析与上面的 $d = -2$ 的情形是相似的. 首先定义

$$l = \min\{|N| \,\big|\, G/N\text{的指数被 2 严格整除}\}.$$

跟上一节类似，我们有

$$\sqrt{n} + \frac{k-\sqrt{n}}{v/l} \le l, \tag{3.4}$$

其中 l 是 2 的幂次方且 $2 \le l \le 2^{s-1}$. 设 $k = \sqrt{n} + \gamma\Delta$ 其中 γ 为某一正整数，$a = u_1 + u_2\sqrt{-1}$，其中 u_1, u_2 为满足 $u_1^2 + u_2^2 = n$ 的整数. 同样地我们利用计算机对参数区间 $-10^4 \le u_1 \le 1, 1 \le u_2, \gamma \le 10^4$ 进行了搜索，由此找到了许多满足第 3.2 节中所有必要条件的参数. 下面我们给出一个例子.

例 3.5: 对 $a = 160(-3+4\sqrt{-1})t$，$\gamma = 500t$，$n = 2^{10}\cdot 5^4 \cdot t^2$，$v = 4n$，$k = 2n+\sqrt{n}$，其中 $t = 2^i, i$ 为某一非负整数，第 3.2 节中所有必要条件均被满足.

3.6 一些特殊的情形

在这一节中，我们将考虑以下三种特殊的情形：

(i) D 为一个 Hadamard 差集且满足 $a + \bar{a} = 0$；

(ii) G 为一个 p-群；

(iii) $U_c \cup \{\chi_0\}$ 为 $\widehat{G}$ 的一个子群.

3.6.1 D 为一个 Hadamard 差集且满足 $a + \bar{a} = 0$

给定一个 Hadamard 差集 D. 设 D 只有 3 个非平凡的特征值 $\sqrt{n}, a, \bar{a}$. 根据条件 $a + \bar{a} = 0$ 和引理 3.3，可得 $d = -1$，$a = \pm i\sqrt{n}$. 另一方面，$1 \leq 2d_1 - a - \bar{a}$，所以我们可以推出 $d_1 = 1$，即 $1_G \in D$. 下面我们将根据 D 的参数分成两种情况来进行讨论.

若 D 的参数为 $(v, k, \lambda) = (4n, 2n + \sqrt{n}, n + \sqrt{n})$，则它满足所有的必要条件，除了 (3.4). 在我们的假设下，条件 (4) 化为 $l \geq 2\sqrt{n}$. 根据第 3.2 节中结果，可知 $\Delta = 2\sqrt{n}, R = \sqrt{n}$，$\Omega = -\sqrt{n} - i\sqrt{n}$，$|D \cap D^{(-1)}| = 2\sqrt{n}$. 记 $H = D + D^{(-1)} - G$. 容易验证 群环元素 H 中有 $2\sqrt{n}(= |D \cap D^{(-1)}|)$ 个元素的系数为 1，其余元素的系数为 0 或 -1. 另一方面，H 中所有元素的系数和等于 $2\sqrt{n}(= 2k - v)$. 由此可知 H 为 G 的一个子集. 令 $M = U_c \cup \{\chi_0\}$. 则

$$\chi(H) = \chi(D) + \chi(D^{(-1)}) - \chi(G) = \begin{cases} 2\sqrt{n}, & \text{若 } \chi \in M; \\ 0, & \text{若 } \chi \in \widehat{G} \setminus M. \end{cases}$$

利用反演公式可得 $H^2 = 2\sqrt{n}H$，$H = H^{(-1)}$，即 H 为 G 的一个阶为 $2\sqrt{n}$ 的子群. 下面我们称 G 的一个特征 χ 零化（annihilates）它的一个子群 H 若 $\chi(h) = 1$ 对所有的 $h \in H$ 都成立. 群 G 的所有零化 H 的特征组成的集合叫作是 H 在 $\widehat{G}$ 中的零化子群，简记为 $H^{\perp}$. 不难验证 $M = H^{\perp}$，$|M| = |H^{\perp}| = |G/H| = 2\sqrt{n}$. 与引理 3.2 的证明类似，我们有 $G_2^{\perp} \leq M$，$|G_2^{\perp}| = |G/G_2| = w$. 由此导出 $w \,|2\sqrt{n}$，所以 $w^2 \,|4n$. 另一方面，我们有 $v = 4n = 2^s w$，这里 $\gcd(w, 2) = 1$. 从而 $w^2 \,|2^s w$，于是 $w = 1$，即 G 是一个 2-群. 整理可得 $n = 2^{s-2}$，这里 s 必为一个偶数，因为 $\sqrt{n}$ 为一个整数. 设 $s = 2m$，m 为某一非负整数. 则 D 的参数为 $(v, k, \lambda) = (2^{2m}, 2^{2m-1} + 2^{m-1}, 2^{2m-2} + 2^{m-1})$. 现在我们可以将表 3.1 简化为 表 3.2.

下面我们设 D 的参数为 $(v, k, \lambda) = (4n, 2n - \sqrt{n}, n - \sqrt{n})$. 我们来证明这种情况是不可能发生的. 首先易知 $|D \cap D^{(-1)}| = 1$，$|U_c| = 1 + 2\sqrt{n}$. 记 $H = G + 1 - D - D^{(-1)}$.

表 3.2　Hadamard 差集的特征表

d_g	d'_g	$g^{-1}(U_a)$	$g^{-1}(U_b)$	$g^{-1}(U_c)$
1	1	$-\sqrt{n}$	$-\sqrt{n}$	$2\sqrt{n}-1$
1	0	$-i\sqrt{n}$	$i\sqrt{n}$	-1
0	1	$i\sqrt{n}$	$-i\sqrt{n}$	-1

不难验证 H 是 G 的一个大小为 $1+2\sqrt{n}$ 的子集. 直接验证，可得

$$\chi(H)=\begin{cases}1+2\sqrt{n}, & \text{若 } \chi=\chi_0,\\ 1-2\sqrt{n}, & \text{若 } \chi\in U_c,\\ 1, & \text{若 } \chi\in\widehat{G}\setminus M,\end{cases}$$

和

$$g^{-1}(U_c)=\begin{cases}1+2\sqrt{n}, & \text{若 } g=1_G,\\ 1-2\sqrt{n}, & \text{若 } g\in H,\\ 1, & \text{若 } g\in G\backslash H, g\neq 1_G.\end{cases}$$

根据反演公式，我们有

$$H^2=(2\sqrt{n}-1)+(2-2\sqrt{n})H+2G,$$

和

$$U_c^2=(2\sqrt{n}-1)+(2-2\sqrt{n})U_c+2\widehat{G}.$$

因为 H^2 的系数都是非负的，所以 $2-2\sqrt{n}+2\geq 0$，于是 $\sqrt{n}\leq 2$. 若 $n=1$，则 $D=\{1_G\}$，因为 $|D|=k=1$ 且 D 中包含单位元. 然而这与 $\chi(D)$ 有三个非平凡的特征值矛盾. 若 $n=4$，则 $v=16$，$U_c^2=3+2(\widehat{G}-U_c)$. 所以对 U_c 中的每个元素，它在 U_c^2 中的系数为零. 最后根据 Turyn[78] 的结论，可知 G 不可能是循环群，所以它必然同构于 $\mathbb{Z}_8\bigoplus\mathbb{Z}_2$ 或 $\mathbb{Z}_4\bigoplus\mathbb{Z}_4$. 另一方面，由于 $\widehat{G}\cong G$，所以在 $\widehat{G}$ 中恰有 3 个阶为 2 的元素，并且都属于 U_c. 因此这三个阶为 2 的元素中至少有一个满足它在 U_c^2 中的系数是正的. 而这跟前面的结论矛盾.

综上所述，我们有下面的结论.

引理 3.4：给定一个阶为 v 的 *Abel* 群 G. 设 D 为 G 上的一个 (v,k,λ)-Hadamard 差集且 D 恰有三个非平凡的特征值 $\sqrt{n},a,\bar{a}$. 若 $a+\bar{a}=0$，则 D 的参数必为 $(v,k,\lambda)=$

$(2^{2m}, 2^{2m-1}+2^{m-1}, 2^{2m-2}+2^{m-1})$，其中 m 为某一非负整数. 特别地，G 为一个 2-群. 令 $H = D + D^{(-1)} - G$. 则 H 为 G 的一个子群，且 $H^{\perp} = \chi_0 \cup \{\chi \in G | \chi(D) = \sqrt{n}\}$.

3.6.2 G 为一个 p-群

前面我们已经证明若 p 为奇素数，则 $w > 1$. 所以我们有 $p = 2$. 根据 Menon[74] 的一个结论，D 的参数可以表示成 $(v, k, \lambda) = (4n, 2n \pm \sqrt{n}, n \pm \sqrt{n})$. 记 $v = 4n = 2^s$，其中 s 为某一非负整数. 因为 $\Delta | v$，所以我们不妨设 $\Delta = 2\sqrt{n} - a - \bar{a} = 2^u$，$u$ 为某一非负整数. 根据 $\Delta = 2\sqrt{n} - a - \bar{a} < 4\sqrt{n}$，$-a - \bar{a} \geq 1 - 2d_1 \geq -1$，可知 $2^{s/2} - 1 \leq 2^u < 2^{s/2+1}$. 于是 $2^u = 2^{s/2} = 2\sqrt{n}$，从而推出 $a + \bar{a} = 0$. 所以 D 满足引理 3.4 中的条件. 因此 D 的参数必然可以表示成 $(v, k, \lambda) = (2^{2m}, 2^{2m-1} + 2^{m-1}, 2^{2m-2} + 2^{m-1})$，其中 m 为某一非负整数. 令 $H = D + D^{(-1)} - G$. 不难验证 H 为 G 的一个子群，并且 $H^{\perp} = \{\chi_0\} \cup \{\chi \in \widehat{G} | \chi(D) = \sqrt{n}\}$.

下面我们进一步假设 $\exp(G) = 4$. 根据

$$\sqrt{n} + \frac{k - \sqrt{n}}{2^{rk_2(G)}} \leq 2^{s - rk_2(G)},$$

可得 $m \geq rk_2(G)$. 由 $rk_2(G)$ 的定义不难验证 $m = rk_2(G)$，$G \cong \mathbb{Z}_4^m$. 另外，$a = \pm i\sqrt{n}$，所以每一个 $\chi \in U_a \cup U_a^{(-1)}$ 的阶均为 4. 注意到 $\widehat{G} \cong \mathbb{Z}_4^m$ 中有 $2^m - 1 = 2\sqrt{n} - 1$ 个阶为 2 的元素，且 $|U_c| = 2\sqrt{n} - 1$. 于是 U_c 且包含所有的阶为 2 的特征. 也就是说，$H^{\perp} = \{\chi_0\} \cup \{\chi \in \widehat{G} | \chi(D) = \sqrt{n}\}$ 是 $\widehat{G}$ 中唯一的极大初等 *Abel* 子群. Davis 和 Polhill[25] 已经构造出了这样的差集.

3.6.3 $U_c \cup \{\chi_0\}$ 为 $\widehat{G}$ 的一个子群

令 $M = U_c \cup \{\chi_0\}$. 由于 M 是一个子群，所以对 $\widehat{G}$ 中任意非平凡特征 ψ，$\psi(M)$ 只可能取两个特征值 0 与 $|M|$. 另一方面，由表 3.1 可知

$$\psi(M) \in \left\{ -2R, \frac{v}{\Delta} - 2R, \frac{2v}{\Delta} - 2R \right\}.$$

于是

$$\frac{v}{\Delta} - 2R = 0, \quad \frac{2v}{\Delta} - 2R = |M|,$$

因为 $-2R<0$，$\frac{v}{\Delta}-2R<\frac{2v}{\Delta}-2R$. 根据已知结论 $R=\frac{k-\sqrt{n}}{\Delta}$ 可得 $v=2(k-\sqrt{n})$，$|M|=\frac{v}{\Delta}$. 另外，我们有 $k^2=n+(k-n)v$. 于是 $v=4n$，$k=2n+\sqrt{n}$，$\lambda=n+\sqrt{n}$，即 D 的参数为 $(v,k,\lambda)=(4n,2n+\sqrt{n},n+\sqrt{n})$. 令 $H=D+D^{(-1)}-G$. 则

$$\chi(H)=\begin{cases}2\sqrt{n}, & \text{若 } \chi\in M;\\ a+\bar{a}, & \text{若 } \chi\in\widehat{G}\setminus M.\end{cases}$$

根据反演公式可得 $H=a+\bar{a}+M^{\perp}$. 比较等式两边 1_G 的系数，可知

$$a+\bar{a}=\begin{cases}0, & \text{若 } d_1=1;\\ -2, & \text{若 } d_1=0.\end{cases}$$

若 $a+\bar{a}=-2$，则 $\Delta=2\sqrt{n}-a-\bar{a}=2\sqrt{n}+2$. 由于 $\Delta|(k-\sqrt{n})$，所以 $(\sqrt{n}+1)|n$，而这是不可能的. 故而 $a+\bar{a}=0$. 因此 D 满足引理 3.4 的条件.

现在我们可以看到在上面的这两种特殊情形中，D 均满足引理 3.4 的条件. 现在我们来总结一下本节中我们所得到的结论.

定理 3.1：给定一个阶为 v 的 *Abel* 群 G. 设 D 为 G 上的一个 (v,k,λ)-Hadamard 差集且 D 恰有三个非平凡的特征值 $\sqrt{n},a,\bar{a}$. 令 $M=\{\chi_0\}\cup\{\chi\in\widehat{G}\,|\,\chi(D)=\sqrt{n}\}$. 若下述条件之一成立:

(i) D 为一个 Hadamard 差集且满足 $a+\bar{a}=0$，

(ii) G 为一个 p-群，

(iii) M 为 $\widehat{G}$ 的一个子群，

则 D 具有参数 $(v,k,\lambda)=(2^{2m},2^{2m-1}+2^{m-1},2^{2m-2}+2^{m-1})$，其中 m 为某一非负整数. 特别地，G 为一个 2-群. 令 $H=D+D^{(-1)}-G$. 则 H 是 G 的一个子群，且 $H^{\perp}=M$.

3.7 总结

在这一章中，我们尝试去构造不具有 character divisibility 性质的差集. 我们将只具有三个非平凡特征值的差集作为我们的考察对象，并由此得到了一系列的必要条件. 我们发现它们的特征值都属于数域 $Q(\sqrt{-d})$，其中 $d=1$，$d=2$，或 d 是一个模 3 余 4 的奇素数. 利用计算机搜索，我们找到了一些可能的参数. 对于 $d=1$ 或

2 的情况，我们找到了几个满足所有本章中得到的必要条件的参数，见例 3.3-3.5. 于是我们不禁要问这样的参数集合是否真的存在. 如果存在的话，我们就也就找到了不具有 character divisibility 性质的差集.

4 Delsarte-Goethals 码上的结合方案

4.1 引言

自 Kerdock、Preparata、Goethals、Delsarte-Goethals 等码的 $\mathbb{Z}_4$-线性性质被发现以来[44]，学者们已经应用 $\mathbb{Z}_4$-线性码构造了很多的组合结构：例如 t-设计和结合方案. 根据 Solè[85] 的描述，$\mathbb{Z}_4$-线性性质的发现从 Liebler 和 Mena[58] 利用特征为 4 的 Galois 环构造结合方案中受到了启发. 有关从 $\mathbb{Z}_4$-线性码构造 t-设计的研究最早由 Harada[45] 提出. 之后 Helleseth 等人[83] 在这方面做了许多的工作.

结合方案是代数组合研究中的核心概念，并且已经在许多数学学科中发挥了重要的作用，例如 编码理论与图论. Henry Cohn 等人[8] 猜想一个在 $\mathbb{R}^{14}$ 中 64 个点上定义的 3 类的结合方案是一个*全局最优结构*（universally optimal configuration）. 随后 Abdukhalikov、Bannai 和 Suda[2] 利用二元和四元的 Kerdock、Preparata 码及 MUB 的最大集推广了这个结合方案.

具体的来说，他们根据 Lee 重量对缩短 Kerdock 码进行了划分，从而得到了一族 3-类的结合方案. 它的对偶方案恰定义在截短 Preparata 码上. 这启发我们去研究另外一类重要的四元码：Delsarte-Goethals ($\mathcal{DG}$) 码.

$\mathcal{DG}$ 码具有 6 种不同的 Lee 重量. 与 Kerdock 码不同的是，根据 Lee 重量对 $\mathcal{DG}$ 作划分并不能得到一个结合方案. 我们需要更精细的划分以期得到一个 9 类的结合方案. 通过复杂的特征和计算，我们完全决定了它的对偶方案与特征阵.

当 $m = 3$ 时，$\mathcal{DG}$ 码在 Gray 映射下的象是线性的，并且此时原来的 9 类的结合方案的象同样也是一个结合方案，不过有着不同的参数. 当 $m > 3$ 时，$\mathcal{DG}$ 码在 Gray 映射下的象不再是线性的. 我们目前还不清楚是否能在初等交换 2 群中找到与我们构造的结合方案具有相同参数的结合方案.

本章的结构安排如下：在第 4.2 中，我们介绍一些与结合方案、Galois 环和四元码相关的预备知识. 在第 4.3 中，我们详细地给出了如何从 $\mathcal{DG}$ 码的 Lee 重量分

布来构造 9 类结合方案，并且计算了它的对偶方案及其特征阵. 具体的特征阵可以在本章附录 A 中找到. 主要结果的证明将被安排在第 4.4 节中.

4.2 预备知识

4.2.1 结合方案

给定一个非空的有限集 X. 令对称的关系 $R_0, R_1, \cdots, R_d$ 为 $X \times X$ 的一个划分且 $R_0 = \{(x, x) | x \in X\}$. 对任一 i，记 A_i 为 R_i 的邻接矩阵：$A_i(x, y) = 1$ 若 $(x, y) \in R_i$；反之等于 0. 若存在非负整数 $p_{i,j}^k$ 使得

$$A_i A_j = \sum_{k=0}^{d} p_{i,j}^k A_k,$$

则称 $(X, \{R_i\}_{i=0}^d)$ 为一个 d-*类结合方案*(association scheme). 数 $p_{i,j}^k$ 叫作是这个方案的相交数（intersection numbers）. 矩阵集合 $A_0, A_1, \cdots, A_d$ 在 $\mathbb{C}$ 上的线性扩张形成了一个 $d+1$-维的半单代数，称作是 Bose-Mesner 代数. 根据矩阵 A_i 相对于基 $A_0, A_1, \cdots, A_d$ 的乘法作用，我们记

$$A_i(A_0, A_1, \cdots, A_d) = (A_0, A_1, \cdots, A_d) B_i,\ 0 \leq i \leq d.$$

由于每一个 A_i 都是对称的，所以这个代数是交换的. 于是存在极小幂零元（minimal idempotents）$E_0, E_1, \cdots, E_d$，且它们也构成这个代数的一组基. 如下定义的 $(d+1) \times (d+1)$ 矩阵 P:

$$(A_0, A_1, \cdots, A_d) = (E_0, E_1, \cdots, E_d) P$$

叫作是这个结合方案的 *第一特征阵*（first eigenmatrix）. 对应地，如下定义的 $(d+1) \times (d+1)$ 矩阵 Q:

$$(E_0, E_1, \cdots, E_d) = \frac{1}{|X|} (A_0, A_1, \cdots, A_d) Q$$

叫作是这个结合方案的 *第二特征阵*（second eigenmatrix）. 不难看出 $PQ = |X| I$.

给定一个有限 Abel 群 X，其运算为加法. 若存在它的一个划分 $S_0 = \{0\}, S_1, \cdots, S_d$ 使得

$$R_i = \{(x, x+y) |\, x \in X, y \in S_i\},$$

则称结合方案 $(X, \{R_i\}_{i=0}^d)$ 是一个 translation 结合方案或 Schur 环. 为了简便，我们一般就直接说 $(X, \{S_i\}_{i=0}^d)$ 是一个结合方案.

设 $(X, \{S_i\}_{i=0}^d)$ 是一个 Schur 环. 如下在 X 的特征群 $\hat{X}$ 上定义一个等价关系：对任一 $0 \le i \le d$，$\chi \sim \chi'$ 当且仅当 $\chi(S_i) = \chi'(S_i)$. 这里 $\chi(S) = \sum_{g \in S} \chi(g)$，其中 $\chi \in \hat{X}$，$S \subseteq X$. 将所有的等价类记为 $D_0, D_1, \cdots, D_d$，其中 D_0 只包含平凡的特征. 则 $(\hat{X}, \{D_i\}_{i=0}^d)$ 构成了一个 Schur 环，称作是 $(X, \{S_i\}_{i=0}^d)$ 的对偶方案. 不难验证对偶方案的第一特征阵等于原先方案的第二特征阵. 有关这方面的更多知识，请参考文献[10,18].

下面我们叙述著名的 Bannai-Muzychuk 判别法则[9,76]：给定一个结合方案 $(X, \{R_i\}_{0 \le i \le d})$. 令 P 为它的第一特征阵，$\Lambda_0 := \{0\}, \Lambda_1, \ldots, \Lambda_{d'}$ 为 $\{0, 1, \ldots, d\}$ 的一个划分. 则 $(X, \{R_{\Lambda_i}\}_{0 \le i \le d'})$ 构成一个结合方案当且仅当存在 $\{0, 1, 2, \ldots, d\}$ 的一个划分 $\{\Delta_i\}_{0 \le i \le d'} (\Delta_0 = \{0\})$ 使得 P 的任一 (Δ_i, Λ_j)-区块都具有相同的行和. 特别地，(Δ_i, Λ_j)-区块的行和就是 fusion 方案的第一特征阵 (i, j)-处的值.

4.2.2 Galois 环

令 $\mu : \mathbb{Z}_4 \to \mathbb{Z}_2$ 代表模 2 的映射. 我们将 μ 的定义自然地推广到 $\mathbb{Z}_4[x]$ 上. 首 1 多项式 $g(x) \in \mathbb{Z}_4[x]$ 叫作是基本不可约（basic irreducible）的若 $\mu(g(x))$ 是 $\mathbb{Z}_2[x]$ 中首 1 不可约多项式. 给定一个正整数 m. 特征为 4 且具有 4^m 个元素的 Galois 环 $R = GR(4, m)$ 可以通过商环 $\mathbb{Z}_4[x]/(f(x))$ 来定义，其中 $f(x)$ 是一个次数为 m 的首 1 基本不可约多项式. 所有 R 中的不可逆元形成了唯一的极大理想 $2R$，于是 R 是一个局部环. 不难看出，映射 μ 可以自然地被推广到 $R[x]$ 上，且 $\mu(R) = R/2R$ 与大小为 $q = 2^m$ 的有限域 $\mathbb{F}_q$ 同构.

Galois 环 R 的单位群 R^* 包含一个阶为 $2^m - 1$ 的循环子群，我们将它的一个生成元记为 β. 规定 $\mathcal{T} = \{0, 1, \beta, \ldots, \beta^{2^m-2}\}$. 任一 R 中的元素 z 均可以唯一表示为

$$z = A + 2B, \qquad A, B \in \mathcal{T}. \tag{4.1}$$

记 $\mu(\beta) = \alpha$. 则 α 为 $\mathbb{F}_q$ 中的一个本原元，且 $\mu(\mathcal{T}) = \mathbb{F}_q$.

Galois 环 R 具有一个阶为 m 的循环 Galois 群，它是由下面的 Frobenius 映射 σ

生成的：

$$\sigma(z) = \sigma(A + 2B) = A^2 + 2B^2.$$

元素 z 的从 R 到 $\mathbb{Z}_4$ 上的迹（trace）$\mathrm{T}(z)$ 定义为

$$\mathrm{T}(z) = \sum_{i=0}^{m-1} \sigma^i(z),$$

而 $\mathrm{tr}(x)$ 代表普通的从 $\mathbb{F}_q$ 到 $\mathbb{Z}_2$ 的迹函数.

对于任意的 $x \in R$，记 $\sqrt{x} = x^{2^{n-1}}$. 若我们在 $\mathcal{T}$ 上如下定义加法运算：

$$x \oplus y = x + y + 2\sqrt{xy},$$

则 $(\mathcal{T}, \oplus, \cdot)$ 构成了一个大小为 2^n 的有限域. 对于任意的 $a \in R$，如下定义映射 $\chi_a : R \to \mathbb{C}$:

$$\chi_a(x) = i^{\mathrm{T}(ax)}, \quad \forall\, x \in R.$$

不难验证特征群 $\widehat{R} = \{\chi_a \mid a \in R\}$. 有关 Galois 环的更多信息，请参见文献[44,58,90].

4.2.3 四元码

Goethals 码 $\mathcal{G}$ 是一类长度为 $q = 2^m$ 的 $\mathbb{Z}_4$ 线性码，它的校验阵（parity-check matrix）定义如下：

$$H_{\mathcal{G}} = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{2^m-2} \\ 0 & 2 & 2\beta^3 & 2\beta^6 & \cdots & 2\beta^{3(2^m-2)} \end{bmatrix}.$$

根据定理 25[44] 可知：当 m 为奇数时，Goethals 码 $\mathcal{G}$ 的极小 Lee 重量等于 8. 我们把 $\mathcal{G}$ 在 $\mathbb{Z}_4$ 上的对偶码叫作 Delsarte-Goethals 码，简记为 $\mathcal{DG}$. 于是它的生成矩阵也就是 $H_{\mathcal{G}}$.

另一方面，Delsarte-Goethals 码有下述的迹描述. 给定 $\mathbb{Z}_4^q$ 中的一个向量 $\mathbf{c}(u, a, b)$，其中 $u \in \mathbb{Z}_4, a \in R, b \in \mathcal{T}$，并且它的坐标由 $\mathcal{T}$ 中元素标记，且在 $x \in \mathcal{T}$ 处的值定义为 $\mathbf{c}(u, a, b)_x = u + \mathrm{T}(ax + 2bx^3)$. 则

$$\mathcal{DG} = \{\mathbf{c}(u, a, b) \mid u \in \mathbb{Z}_4, a \in R, b \in \mathcal{T}\}.$$

不难验证码字 $\mathbf{c}(u, a, b)$ 的 Lee 重量可以表示成

$$w_L(\mathbf{c}(u, a, b)) = q - \Re\left(i^u \sum_{x \in \mathcal{T}} i^{\mathrm{T}(ax+2bx^3)}\right), \tag{4.2}$$

其中 $\Re$ 代表一个复数的实数部分.

引理 4.1 (定理 1[47]): 给定奇数 $m \geq 3$，$q = 2^m$. 则 Delsarte-Goethals 码 $\mathcal{DG}$ 的 Lee 重量分布为

$$B_j = \begin{cases} 1, & \text{若 } j = 0 \text{ 或 } 2q; \\ (q-1)q(2q-1)/6, & \text{若 } j = q \pm \sqrt{2q}; \\ (q-1)2q(q+4)/3, & \text{若 } j = q \pm \sqrt{q/2}; \\ (2q-1)(q^2-q+2), & \text{若 } j = q. \end{cases}$$

长度为 $q = 2^m$ 的四元 Kerdock 码 $\mathcal{K}$ 是 $\mathcal{DG}$ 一个子码，它的生成矩阵为

$$H_{\mathcal{K}} = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{2^m-2} \end{bmatrix}.$$

所以

$$\mathcal{K} = \{\mathbf{c}(u, a, 0) \mid u \in \mathbb{Z}_4, a \in R\}.$$

四元 Preparata 码 $\mathcal{P}$ 的校验矩阵为 $H_{\mathcal{K}}$. 若 m 为奇数，则它的极小 Lee 重量等于 6.

引理 4.2 (引理 1[47]): 给定奇数 $m \geq 3$，$q = 2^m$. 则 Kerdock 码 $\mathcal{K}$ 的 Lee 重量分布为

$$B_j = \begin{cases} 1, & \text{若 } j = 0 \text{ 或 } 2q; \\ 2q(q-1), & \text{若 } j = q \pm \sqrt{q/2}; \\ 4q-2, & \text{若 } j = q. \end{cases}$$

以下在 Kerdock 码 $\mathcal{K}$ 上定义的关系给出了一个交换的 4 类结合方案：

$$(x, y) \in \begin{cases} R_0, & \text{若 } w_L(x-y) = 0; \\ R_1, & \text{若 } w_L(x-y) = q - \sqrt{q/2}; \\ R_2, & \text{若 } w_L(x-y) = q; \\ R_3, & \text{若 } w_L(x-y) = q + \sqrt{q/2}; \\ R_4, & \text{若 } w_L(x-y) = 2q. \end{cases} \tag{4.3}$$

定理 4.1: 给定奇数 $m \geq 3$，$q = 2^m$. 则 (4.3) 中给出的关系在四元 Kerdock 码上构成一个交换的 4 类的结合方案.

上面的结合方案恰是命题 6[13] 中构造的结合方案的对偶方案.

4.3 码 $\mathcal{DG}$ 上的结合方案

我们很自然要问关系 (4.3) 在 Delsarte-Goethals 码 $\mathcal{DG}$ 上的自然推广会否给出一个结合方案？答案是否定的. 为了能够构成一个结合方案，我们需要对关系稍加改

动：

$$(x,y)\in\begin{cases} S_0, & \text{若 } w_L(x-y)=0;\\ S_1, & \text{若 } w_L(x-y)=q-\sqrt{2q};\\ S_2, & \text{若 } w_L(x-y)=q-\sqrt{q/2};\\ S_3, & \text{若 } w_L(x-y)=q \text{ 且 } x-y\in\mathcal{K};\\ S_4, & \text{若 } w_L(x-y)=q \text{ 且 } x-y\notin\mathcal{K};\\ S_5, & \text{若 } w_L(x-y)=q+\sqrt{q/2};\\ S_6, & \text{若 } w_L(x-y)=q+\sqrt{2q};\\ S_7, & \text{若 } w_L(x-y)=2q. \end{cases} \tag{4.4}$$

定理 4.2：给定奇数 $m\geq 3$，$q=2^m$. 在四元 Delsarte-Goethals 码上定义的关系 (4.4) 构成一个 7 类的交换结合方案 $\mathfrak{A}$. 我们在附录 A 中列出了它的第一特征阵与第二特征阵.

事实上，我们可以对关系 (4.4) 再做细分，从而得到一个 9 类的交换结合方案：

$$(x,y)\in\begin{cases} S_0, & \text{若 } w_L(x-y)=0;\\ S_1, & \text{若 } w_L(x-y)=q-\sqrt{2q};\\ S_{21}, & \text{若 } w_L(x-y)=q-\sqrt{q/2} \text{ 且 } x-y\in\mathcal{K};\\ S_{22}, & \text{若 } w_L(x-y)=q-\sqrt{q/2} \text{ 且 } x-y\notin\mathcal{K};\\ S_3, & \text{若 } w_L(x-y)=q \text{ 且 } x-y\in\mathcal{K};\\ S_4, & \text{若 } w_L(x-y)=q \text{ 且 } x-y\notin\mathcal{K};\\ S_{51}, & \text{若 } w_L(x-y)=q+\sqrt{q/2} \text{ 且 } x-y\notin\mathcal{K};\\ S_{52}, & \text{若 } w_L(x-y)=q+\sqrt{q/2} \text{ 且 } x-y\in\mathcal{K};\\ S_6, & \text{若 } w_L(x-y)=q+\sqrt{2q};\\ S_7, & \text{若 } w_L(x-y)=2q. \end{cases} \tag{4.5}$$

定理 4.3：给定奇数 $m\geq 3$，$q=2^m$. 在四元 Delsarte-Goethals 码上定义的关系 (4.5) 构成一个 9 类的交换结合方案 $\mathfrak{B}$. 我们在附录 A 中列出了它的第一特征阵与第二特征阵.

我们将把上面两个定理的证明留到本节的最后. 它们都是定理 4.4 的直接推论. 根据 Delsarte-Goethals 码 $\mathcal{DG}$ 的迹描述，可知存在如下的 $\mathcal{DG}$ 的所有码字与集合 $\mathbb{Z}_4\times R\times\mathcal{T}$ 之间的一一对应：$(u,a,b)\longleftrightarrow\mathbf{c}(u,a,b)$. 因为 $\mu(\mathcal{T})=\mathbb{F}_q$，所以存在 $G=\mathbb{Z}_4\times R\times\mathbb{F}_q$ 与 $\mathcal{DG}$ 之间的群同构. 对 $(u,a,b)\in G$，我们引进一个新的指数和：

$$S(u,a,b)=\sum_{X\in\mathcal{T}} i^{u+\mathrm{T}(aX+2bX^3)}+\sum_{X\in\mathcal{T}} i^{-u-\mathrm{T}(aX+2bX^3)},$$

这里我们将元素 $b\in\mathbb{F}_q$ 与它的原象 $\mu^{-1}(b)\in\mathcal{T}$ 等同起来. 于是等式 (4.2) 化为

$$w_L(\mathbf{c}(u,a,b))=q-S(u,a,b)/2. \tag{4.6}$$

从 Delsarte-Goethals 码的重量分布可知

$$S(u,a,b) \in \{\pm 2q, \pm 2\sqrt{2q}, \pm\sqrt{2q}, 0\}.$$

最后我们依据 $S(u,a,b)$ 的取值给出 G 的如下划分：

$$\begin{aligned}
\mathcal{R}_0 &= \{(u,a,b) \in G \mid S(u,a,b) = 2q\} = \{(0,0,0)\},\\
\mathcal{R}_1 &= \{(u,a,b) \in G \mid S(u,a,b) = 2\sqrt{2q}\},\\
\mathcal{R}_2 &= \{(u,a,b) \in G \mid S(u,a,b) = \sqrt{2q}, b = 0\},\\
\mathcal{R}_3 &= \{(u,a,b) \in G \mid S(u,a,b) = \sqrt{2q}, b \neq 0\},\\
\mathcal{R}_4 &= \{(u,a,b) \in G \mid S(u,a,b) = 0, b = 0\},\\
\mathcal{R}_5 &= \{(u,a,b) \in G \mid S(u,a,b) = 0, b \neq 0\},\\
\mathcal{R}_6 &= \{(u,a,b) \in G \mid S(u,a,b) = -\sqrt{2q}, b \neq 0\},\\
\mathcal{R}_7 &= \{(u,a,b) \in G \mid S(u,a,b) = -\sqrt{2q}, b = 0\},\\
\mathcal{R}_8 &= \{(u,a,b) \in G \mid S(u,a,b) = -2\sqrt{2q}\},\\
\mathcal{R}_9 &= \{(u,a,b) \in G \mid S(u,a,b) = -2q\} = \{(2,0,0)\}.
\end{aligned}$$

由于群 G 是交换群，所以它的特征群 $\widehat{G} \cong G$. 于是我们可以将元素 $g = (v,c,d) \in G$ 和特征 $\chi_g \in \widehat{G}$ 看成是一样的，这里 $\chi_g((u,a,b)) = i^{uv+\mathrm{T}(ac+2bd)}, (u,a,b) \in G$. 为了描述对偶的结合方案，我们首先给出群 $\widehat{G} = G$ 的一个划分. 为了方便，我们用大写字母 X, Y 来代表 $\mathcal{T}$ 中的元素，对应的小写字母则代表这个元素模 2 后在 $\mathbb{F}_q$ 中的象. 令 $f_a(x) = x^3 + x + a \in \mathbb{F}_q[x]$. 定义

$$M_i = \left\{a \in \mathbb{F}_q, a \neq 0 \mid f_a(x) = 0 \text{ 在 } \mathbb{F}_q \text{ 中恰有 } i \text{ 个根}\right\}$$

其中 $i=0,1,3$. 下面我们给出对偶的划分：

$$
\begin{aligned}
\mathcal{E}_0 &= \{(0,0,0)\},\\
\mathcal{E}_1 &= \left\{(0,0,r) \mid r \in \mathbb{F}_q^*\right\},\\
\mathcal{E}_2 &= \left\{(1,X,x^3) \mid X \in \mathcal{T}\right\} \cup \left\{(3,-X,x^3) \mid X \in \mathcal{T}\right\},\\
\mathcal{E}_3 &= (\{(1,X,r) \mid X \in \mathcal{T}, r \in \mathbb{F}_q\} \cup \{(3,-X,r) \mid X \in \mathcal{T}, r \in \mathbb{F}_q\}) \backslash \mathcal{E}_2,\\
\mathcal{E}_4 &= \quad \{(0,-X+Y,x^3+y^3) \mid X,Y \in \mathcal{T}, X \neq Y\}\\
&\quad \cup \{(2,X+Y,x^3+y^3) \mid X,Y \in \mathcal{T}\}\\
&\quad \cup \{(2,-X-Y,x^3+y^3) \mid X,Y \in \mathcal{T}\},\\
\mathcal{E}_5 &= (\{(0,S,r) \mid S \in R \backslash 2R, r \in \mathbb{F}_q\} \cup \{(2,S,r) \mid S \in R, r \in \mathbb{F}_q\}) \backslash \mathcal{E}_4,\\
\mathcal{E}_6 &= \quad \{(1,X+2Y,x^3+y^3e) \mid X,Y \in \mathcal{T}, Y \neq 0, e \in \mathbb{F}_q \backslash M_0\}\\
&\quad \cup \{(3,-X+2Y,x^3+y^3e) \mid X,Y \in \mathcal{T}, Y \neq 0, e \in \mathbb{F}_q \backslash M_0\},\\
\mathcal{E}_7 &= \quad \{(1,X+2Y,x^3+y^3e) \mid X,Y \in \mathcal{T}, Y \neq 0, e \in M_0\}\\
&\quad \cup \{(3,-X+2Y,x^3+y^3e) \mid X,Y \in \mathcal{T}, Y \neq 0, e \in M_0\},\\
\mathcal{E}_8 &= \{(0,2X,\sum_{i=1}^{4} y_i^3) | X \in \mathcal{T}^*, Y_i \in \mathcal{T}, 2X = \sum_{i=1}^{4} Y_i \text{ or } 2X = Y_1+Y_2-Y_3-Y_4\},\\
\mathcal{E}_9 &= \{(0,2X,r) \mid X \in \mathcal{T}^*, r \in \mathbb{F}_q\} \backslash \mathcal{E}_8.
\end{aligned}
$$

我们将在引理 4.3 中证明集合 $\mathcal{E}_0, \mathcal{E}_1, \ldots, \mathcal{E}_9$ 构成群 G 的一个划分.

定理 4.4：给定奇数 $m \geq 3$ 和 $q = 2^m$. 令 $G = \mathbb{Z}_4 \times R \times \mathbb{F}_q$，且定义二元关系集 $R_i = \{(g,h) \mid g-h \in \mathcal{R}_i\}, i = 0, \ldots, 9$. 则 $\mathfrak{B}' = (G; R_i, 0 \leq i \leq 9)$ 是一个 9 类的结合方案. 它的第一与第二特征阵 P 和 Q 如附录 A 中所示. 二元关系集 $R_i' = \{(g,h) \mid g-h \in \mathcal{E}_i\}, i = 0, \ldots, 9$ 则定义了 $\mathfrak{B}'$ 的对偶方案，于是它的第一和第二特征阵为：$P' = Q, Q' = P$.

证明. 记 $s = \sqrt{2q}$. 群环 $\mathbb{C}G$ 中的元素均可表示成 $\sum_{(u,a,b) \in G} c(u,a,b)[(u,a,b)]$ 的形

式，其中 $c(u,a,b)\in\mathbb{C}$. 令

$$\begin{aligned}\mathcal{N}_{2i} &= \sum_{(u,a,b)\in G} S(u,a,b)^i[(u,a,b)],\\ \mathcal{N}_{2i+1} &= \sum_{\substack{(u,a,b)\in G\\ b=0}} S(u,a,b)^i[(u,a,b)],\end{aligned}$$

其中 $i=0,1,\ldots,4$. 于是上面的变换可以写成如下的矩阵形式：

$$(\mathcal{N}_0,\mathcal{N}_1,\ldots,\mathcal{N}_9)=(\mathcal{R}_0,\mathcal{R}_1,\ldots,\mathcal{R}_9)\,T,$$

这里

$$T=\begin{pmatrix}
1 & 1 & s^2 & s^2 & s^4 & s^4 & s^6 & s^6 & s^8 & s^8\\
1 & 0 & 2\,s & 0 & 4\,s^2 & 0 & 8\,s^3 & 0 & 16\,s^4 & 0\\
1 & 1 & s & s & s^2 & s^2 & s^3 & s^3 & s^4 & s^4\\
1 & 0 & s & 0 & s^2 & 0 & s^3 & 0 & s^4 & 0\\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & -s & 0 & s^2 & 0 & -s^3 & 0 & s^4 & 0\\
1 & 1 & -s & -s & s^2 & s^2 & -s^3 & -s^3 & s^4 & s^4\\
1 & 0 & -2\,s & 0 & 4\,s^2 & 0 & -8\,s^3 & 0 & 16\,s^4 & 0\\
1 & 1 & -s^2 & -s^2 & s^4 & s^4 & -s^6 & -s^6 & s^8 & s^8
\end{pmatrix}.$$

通过 Maple 计算得到 $\det(T)=-1152\,s^{23}\,(s-1)^2\,(s+1)^2$, 所以 T 是可逆的. 在我们的证明中，最关键的是完整地计算下面的特征表 $\mathfrak{T}$:

$$\begin{array}{c}
\\ \varepsilon_0\\ \varepsilon_1\\ \varepsilon_2\\ \varepsilon_3\\ \varepsilon_4\\ \varepsilon_5\\ \varepsilon_6\\ \varepsilon_7\\ \varepsilon_8\\ \varepsilon_9
\end{array}
\begin{array}{c}
\begin{array}{cccccccccc}
\mathcal{N}_0 & \mathcal{N}_1 & \mathcal{N}_2 & \mathcal{N}_3 & \mathcal{N}_4 & \mathcal{N}_5 & \mathcal{N}_6 & \mathcal{N}_7 & \mathcal{N}_8 & \mathcal{N}_9
\end{array}\\
\begin{pmatrix}
4\,q^3 & 4\,q^2 & 0 & 0 & 8\,q^4 & 8\,q^3 & 0 & 0 & 16\,q^4\,(3\,q-1) & 16\,q^3\,(3\,q-1)\\
0 & 4\,q^2 & 0 & 0 & 0 & 8\,q^3 & 0 & 0 & 0 & 16\,q^3\,(3\,q-1)\\
0 & 0 & 4\,q^3 & 4\,q^2 & 0 & 0 & 8\,q^3\,(3\,q-1) & 8\,q^2\,(3\,q-1) & 0 & 0\\
0 & 0 & 0 & 4\,q^2 & 0 & 0 & 0 & 8\,q^2\,(3\,q-1) & 0 & 0\\
0 & 0 & 0 & 0 & 8\,q^3 & 8\,q^2 & 0 & 0 & 32\,q^3\,(3\,q-2) & 32\,q^4\\
0 & 0 & 0 & 0 & 0 & 8\,q^2 & 0 & 0 & 32\,q^3\,(q-2) & 32\,q^4\\
0 & 0 & 0 & 0 & 0 & 0 & 24\,q^3 & 8\,q^2\,(2\,q-1) & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 8\,q^2\,(2\,q-1) & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 48\,q^4 & 16\,q^3\,(2\,q-1)\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16\,q^3\,(2\,q-1)
\end{pmatrix}
\end{array}.$$

下一节将专门用来计算这个表. 我们从列 $\mathcal{N}_6$ 中可以读出

$$g(\mathcal{N}_6) = \begin{cases} 8\,q^3\,(3\,q-1), & \text{若 } g\in\mathcal{E}_2;\\ 24\,q^3, & \text{若 } g\in\mathcal{E}_6;\\ 0, & \text{其他情形.}\end{cases}$$

所以特征表 P 可以通过对特征表 $\mathfrak{T}$ 左乘矩阵 T^{-1} 得到. 最后从 Bannai-Muzychuk 判别法立即可知 $\mathfrak{B}'=(G;R_i,0\le i\le 9)$ 构成一个 9 类的结合方案. □

定理 4.2-4.3 的证明. 从这一节开头的叙述，我们可以得到定理 4.3. 而定理 4.2 可以从结合方案 $\mathfrak{B}$ 的特征阵和 Bannai-Muzychuk 判别法直接得出. 结合方案 $\mathfrak{A}$ 这是方案 $\mathfrak{B}$ 的 fusion 方案. □

推论 4.1: *在商群 $G/\langle(2,0,0)\rangle$ 上存在一个 5 类的结合方案 $\mathcal{C}$，并且存在 $\mathcal{C}$ 的一个 4 类的 fusion 方案. 我们在附录 A 中列出了它们的第一和第二特征阵.*

证明. 通过结合方案 $\mathcal{B}'$ 的特征阵和 Bannai-Muzychuk 判别法直接验证. □

4.4 特征表 $\mathfrak{T}$ 的计算

4.4.1 列 $\mathcal{N}_0, \mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3$

特征表 $\mathfrak{T}$ 的前四列可以通过直接计算得到. 这里我们只计算列 $\mathcal{N}_2$，剩下的其它列可以类似地得到.

对 $g = (v, c, d) \in G$，我们有

$$
\begin{aligned}
g(\mathcal{N}_2) &= \sum_{(u,a,b)\in G} S(u,a,b) i^{uv+\mathrm{T}(ac+2bd)} \\
&= \sum_{(u,a,b)\in G} \sum_{X\in\mathcal{T}} i^{u(v+1)+\mathrm{T}(a(c+X))+2\mathrm{T}(b(d+X^3))} + \\
&\quad \sum_{(u,a,b)\in G} \sum_{X\in\mathcal{T}} i^{u(v-1)+\mathrm{T}(a(c-X))+2\mathrm{T}(b(d-X^3))} \\
&= \sum_{X\in\mathcal{T}} \sum_{u\in\mathbb{Z}_4} i^{u(v+1)} \sum_{a\in R} i^{\mathrm{T}(a(c+X))} \sum_{b\in\mathcal{T}} i^{2\mathrm{T}(b(d+X^3))} + \\
&\quad \sum_{X\in\mathcal{T}} \sum_{u\in\mathbb{Z}_4} i^{u(v-1)} \sum_{a\in R} i^{\mathrm{T}(a(c-X))} \sum_{b\in\mathcal{T}} i^{2\mathrm{T}(b(d-X^3))} \\
&= \begin{cases} 4q^3, & \text{若 } g \in \mathcal{E}_2; \\ 0, & \text{其他情况.} \end{cases}
\end{aligned}
$$

4.4.2 列 $\mathcal{N}_4, \mathcal{N}_5, \mathcal{N}_6, \mathcal{N}_7, \mathcal{N}_9$

首先直接计算可得

$$\begin{aligned} g(\mathcal{N}_4) &= \sum_{(u,a,b)\in G} S(u,a,b)^2 i^{uv+\mathrm{T}(ac+2bd)} \\ &= \sum_{u\in\mathbb{Z}_4} i^{u(v+2)} \sum_{X,Y\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c+X+Y))} \sum_{b\in\mathbb{F}_q} i^{\mathrm{T}(2b(d+X^3+Y^3))} + \\ &\quad \sum_{u\in\mathbb{Z}_4} i^{u(v-2)} \sum_{X,Y\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c-X-Y))} \sum_{b\in\mathbb{F}_q} i^{\mathrm{T}(2b(d-X^3-Y^3))} + \\ &\quad 2\sum_{u\in\mathbb{Z}_4} i^{uv} \sum_{X,Y\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c+X-Y))} \sum_{b\in\mathbb{F}_q} i^{\mathrm{T}(2b(d+X^3-Y^3))} \end{aligned}$$

这里 $g=(v,c,d)\in G$.

设 $v=0$，$c=-Z+W$ 其中 $Z,W\in\mathcal{T}, Z\neq W$. 于是上面的和式中只有最后一项才有可能不等于 0. 利用引理 4.4 中的结论 (b)，可知最后一项的值等于 $8q^3$ 若 $d=z^3+w^3$，如若不然则等于 0. 直接的计算可得：

$$g(\mathcal{N}_4) = \begin{cases} 8\,q^4, & \text{若 } g\in\mathcal{E}_0; \\ 8\,q^3, & \text{若 } g\in\mathcal{E}_4; \\ 0, & \text{其他情况,} \end{cases}$$

从而我们也就得到了列 $\mathcal{N}_4$.

列 $\mathcal{N}_5$ 可以类似地得到.

下面我们来计算列 $\mathcal{N}_6$:

$$\begin{aligned} g(\mathcal{N}_6) &= \sum_{(u,a,b)\in G} S(u,a,b)^3 i^{uv+\mathrm{T}(ac+2bd)} \\ &= \sum_{u\in\mathbb{Z}_4} i^{u(v+3))} \sum_{X,Y,Z\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c+X+Y+Z))} \sum_{b\in\mathbb{F}_q} i^{\mathrm{T}(2b(d+X^3+Y^3+Z^3))} + \\ &\quad \sum_{u\in\mathbb{Z}_4} i^{u(v-3))} \sum_{X,Y,Z\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c-X-Y-Z))} \sum_{b\in\mathbb{F}_q} i^{\mathrm{T}(2b(d-X^3-Y^3-Z^3))} + \\ &\quad 3\sum_{u\in\mathbb{Z}_4} i^{u(v+1)} \sum_{X,Y,Z\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c+X+Y-Z))} \sum_{b\in\mathbb{F}_q} i^{\mathrm{T}(2b(d+X^3+Y^3-Z^3))} + \\ &\quad 3\sum_{u\in\mathbb{Z}_4} i^{u(v-1)} \sum_{X,Y,Z\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c-X-Y+Z))} \sum_{b\in\mathbb{F}_q} i^{\mathrm{T}(2b(d-X^3-Y^3+Z^3))} \end{aligned}$$

这里 $g=(v,c,d)\in G$.

从集合 $\mathcal{E}_0,\mathcal{E}_1,\ldots,\mathcal{E}_9$ 的定义可以看出 $g(\mathcal{N}_6)$ 等于 0 若 $g\notin\mathcal{E}_2\cup\mathcal{E}_6$. 所以我们只需处理当 $g\in\mathcal{E}_2\cup\mathcal{E}_6$ 的情形. 首先，设 $g=(v,c,d)=(1,W,w^3)\in\mathcal{E}_2$ 其中 $W\in\mathcal{T}$. 于是上面的和式中只有首项和最后一项有可能不等于 0. 根据引理 4.4 中结论 (d) 可知首项等于 $4\,q^3$ 若 $d=w^3$，如若不然则为 0. 类似地根据引理 4.4 中结论 (c) 可知最后一项等于 $12\,q^3(2q-1)$ 若 $d=w^3$，如若不然则等于 0. 对 $g=(3,-W,w^3)\in\mathcal{E}_2$ 情形的分析是类似地. 所以对 $g\in\mathcal{E}_2$ 我们有 $g(\mathcal{N}_6)=8q^3(3q-1)$. 现在设 $g=(v,c,d)\in\mathcal{E}_6$. 利用引理 4.9-4.10 可以类似地证明结论.

下面我们来处理列 $\mathcal{N}_7$:

$$
\begin{aligned}
g(\mathcal{N}_7) &= \sum_{\substack{(u,a,b)\in G\\ b=0}} S(u,a,b)^3 i^{uv+\mathrm{T}(ac+2bd)}\\
&= \sum_{u\in\mathbb{Z}_4} i^{u(v+3))} \sum_{X,Y,Z\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c+X+Y+Z))} +\\
&\quad \sum_{u\in\mathbb{Z}_4} i^{u(v-3))} \sum_{X,Y,Z\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c-X-Y-Z))} +\\
&\quad 3\sum_{u\in\mathbb{Z}_4} i^{u(v+1)} \sum_{X,Y,Z\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c+X+Y-Z))} +\\
&\quad 3\sum_{u\in\mathbb{Z}_4} i^{u(v-1)} \sum_{X,Y,Z\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c-X-Y+Z))}
\end{aligned}
$$

其中 $g=(v,c,d)\in G$. 利用引理 4.5 可以类似地证明结论.

最后我们来处理列 $\mathcal{N}_9$:

$$\begin{aligned} g(\mathcal{N}_9) &= \sum_{\substack{(u,a,b)\in G\\ b=0}} S(u,a,b)^4 i^{uv+\mathrm{T}(ac+2bd)} \\ &= \sum_{u\in\mathbb{Z}_4} i^{uv} \sum_{X,Y,Z,W\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c+X+Y+Z+W))} + \\ &\quad \sum_{u\in\mathbb{Z}_4} i^{uv} \sum_{X,Y,Z,W\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c-X-Y-Z-W))} + \\ &\quad 4\sum_{u\in\mathbb{Z}_4} i^{u(v+2)} \sum_{X,Y,Z,W\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c+X+Y+Z-W))} + \\ &\quad 4\sum_{u\in\mathbb{Z}_4} i^{u(v-2)} \sum_{X,Y,Z,W\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c-X-Y-Z+W))} + \\ &\quad 3\sum_{u\in\mathbb{Z}_4} i^{uv} \sum_{X,Y,Z,W\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c+X+Y-Z-W))} + \\ &\quad 3\sum_{u\in\mathbb{Z}_4} i^{uv} \sum_{X,Y,Z,W\in\mathcal{T}} \sum_{a\in R} i^{\mathrm{T}(a(c-X-Y+Z+W))} \end{aligned}$$

其中 $g=(v,c,d)\in G$. 利用推论 4.2 可以类似地证明.

4.4.3 列 $\mathcal{N}_8$

列 $\mathcal{N}_8$ 的计算是最困难的. 对 $g=(0,0,0)$，我们可以直接验证等式 $g(\mathcal{N}_8)=16q^4(3q-1)$. 当 $g\in\mathcal{E}_8$ 时，利用推论 4.4-4.5 可以证明 $g(\mathcal{N}_8)=48q^4$. 令特征和 $\xi(a,b)=\sum_{X\in\mathcal{T}} i^{\mathrm{T}(aX+2bX^3)}$. 它与特征和 $S(u,a,b)$ 有着紧密的联系. 我们还需要引进另外两个特征和：

$$\mathbf{E}(c,d) := \sum_{a\in R}\sum_{b\in\mathbb{F}_q} \left(\xi^4(a,b)+\overline{\xi^4(a,b)}+6\,\xi^2(a,b)\overline{\xi^2(a,b)}\right) i^{\mathrm{T}(ac+2bd)}$$

与

$$\mathbf{F}(c,d) := \sum_{a\in R}\sum_{b\in\mathbb{F}_q} \left(\xi^3(a,b)\overline{\xi(a,b)}+\xi(a,b)\overline{\xi^3(a,b)}\right) i^{uv+\mathrm{T}(ac+2bd)}.$$

则

$$g(\mathcal{N}_8)=\sum_{(u,a,b)\in G} S(u,a,b)^4 i^{uv+\mathrm{T}(ac+2bd)} = \sum_{u\in\mathbb{Z}_4} i^{uv}\mathbf{E}(c,d) + 4\sum_{u\in\mathbb{Z}_4} i^{u(v+2)}\mathbf{F}(c,d).$$

所以我们只需要去决定特征和 $\mathbf{E}(c,d)$ 与 $\mathbf{F}(c,d)$ 的确切值分布. 鉴于计算的过程过于繁琐，我们把相应的计算安排在了附录 B 中. 根据引理 4.12-4.14，我们可以直接

验证

$$g(\mathcal{N}_8) = \begin{cases} 2^{3m+6}(3\cdot 2^{m-1}-1), & \text{若 } g\in\mathcal{E}_4; \\ 2^{3m+6}(2^{m-1}-1), & \text{若 } g\in\mathcal{E}_5. \end{cases}$$

4.5 总结

在本章中，我们在 $\mathcal{DG}$ 码关于 Lee 重量划分的基础上构造了一族 9 类结合方案，并且我们利用复杂的指数和计算显式地决定出了这个结合方案的对偶方案的划分. 我们原先的结合方案的划分是基于 $\mathcal{DG}$ 码的 Lee 重量，然而我们目前还无法给它的对偶方案的划分一个合理的解释. 如果我们能够弄清楚这个对偶划分反映了 $\mathcal{DG}$ 码的什么特性，那将会是非常有意思的.

4.6 附录 A

给定奇数 $m\geq 3$ 和 $q=2^m$. 令 $s=\sqrt{2q}$.
结合方案 $\mathfrak{A}$ 的第一和第二特征阵分别为:

$$P = \begin{array}{c} \\ \mathcal{E}_0 \\ \mathcal{E}_1\cup\mathcal{E}_9 \\ \mathcal{E}_2 \\ \mathcal{E}_3\cup\mathcal{E}_7 \\ \mathcal{E}_4 \\ \mathcal{E}_5 \\ \mathcal{E}_6 \\ \mathcal{E}_8 \end{array} \begin{array}{c} \begin{array}{cccc} \mathcal{R}_0 & \mathcal{R}_1 & \mathcal{R}_2\cup\mathcal{R}_3 & \mathcal{R}_4 \end{array} \\ \begin{pmatrix} 1 & 1/24\,s^6-1/8\,s^4+1/12\,s^2 & 1/2\,s^4-4/3\,s^2+1/12\,s^6 & -2+2\,s^2 \\ 1 & -1/12\,s^4+1/12\,s^2 & 1/3\,s^4-4/3\,s^2 & -2+2\,s^2 \\ 1 & 1/12\,s^5-1/4\,s^3+1/6\,s & 1/2\,s^3-4/3\,s+1/12\,s^5 & 0 \\ 1 & -1/6\,s^3+1/6\,s & 1/3\,s^3-4/3\,s & 0 \\ 1 & 1/8\,s^4-1/4\,s^2 & 0 & -2 \\ 1 & -1/4\,s^2 & 0 & -2 \\ 1 & 1/12\,s^3+1/6\,s & -4/3\,s-1/6\,s^3 & 0 \\ 1 & 1/24\,s^4+1/12\,s^2 & -4/3\,s^2-1/6\,s^4 & -2+2\,s^2 \end{pmatrix} \end{array}$$

$$\begin{array}{cccc} \mathcal{R}_5 & \mathcal{R}_6\cup\mathcal{R}_7 & \mathcal{R}_8 & \mathcal{R}_9 \\ \hline 1/4\,s^6-3/4\,s^4+1/2\,s^2 & 1/2\,s^4-4/3\,s^2+1/12\,s^6 & 1/24\,s^6-1/8\,s^4+1/12\,s^2 & 1 \\ -1/2\,s^4+1/2\,s^2 & 1/3\,s^4-4/3\,s^2 & -1/12\,s^4+1/12\,s^2 & 1 \\ 0 & -1/12\,s^5+4/3\,s-1/2\,s^3 & -1/12\,s^5+1/4\,s^3-1/6\,s & -1 \\ 0 & -1/3\,s^3+4/3\,s & 1/6\,s^3-1/6\,s & -1 \\ -1/4\,s^4+1/2\,s^2 & 0 & 1/8\,s^4-1/4\,s^2 & 1 \\ 1/2\,s^2 & 0 & -1/4\,s^2 & 1 \\ 0 & 1/6\,s^3+4/3\,s & -1/12\,s^3-1/6\,s & -1 \\ 1/4\,s^4+1/2\,s^2 & -4/3\,s^2-1/6\,s^4 & 1/24\,s^4+1/12\,s^2 & 1 \end{array},$$

$$Q = \begin{pmatrix} 1 & 1/2\,s^2-1 & s^2 & 1/2\,\left(s^2-2\right)s^2 & 1/2\,s^2\left(s^2-1\right) \\ 1 & -1 & 2\,s & -2\,s & 3/2\,s^2 \\ 1 & 1/2\,s^2-1 & s & 1/2\,\left(s^2-2\right)s & 0 \\ 1 & -1 & s & -s & 0 \\ 1 & 1/2\,s^2-1 & 0 & 0 & -1/2\,s^2 \\ 1 & -1 & 0 & 0 & -1/2\,s^2 \\ 1 & -1 & -s & s & 0 \\ 1 & 1/2\,s^2-1 & -s & -1/2\,\left(s^2-2\right)s & 0 \end{pmatrix}$$

$$\begin{pmatrix}
1/4\,s^2\left(s^4-3\,s^2+2\right) & 1/6\,s^2\left(s^4-3\,s^2+2\right) & 1/6\,s^4-1/2\,s^2+1/3\\
-3/2\,s^2 & 1/3\,s\left(s^2+2\right) & 1/6\,s^2+1/3\\
0 & -1/3\,s\left(s^2-1\right) & 1/3-1/3\,s^2\\
-1/4\,\left(s^2-2\right)s^2 & 0 & 1/6\,s^4-1/2\,s^2+1/3\\
1/2\,s^2 & 0 & 1/6\,s^2+1/3\\
0 & 1/3\,s\left(s^2-1\right) & 1/3-1/3\,s^2\\
-3/2\,s^2 & -1/3\,s\left(s^2+2\right) & 1/6\,s^2+1/3\\
1/4\,s^2\left(s^4-3\,s^2+2\right) & -1/6\,s^2\left(s^4-3\,s^2+2\right) & 1/6\,s^4-1/2\,s^2+1/3
\end{pmatrix}.$$

结合方案 $\mathfrak{B}$ 的第一和第二特征阵分别为:

$$P=\begin{array}{c}\\ \mathcal{E}_0\\ \mathcal{E}_1\\ \mathcal{E}_2\\ \mathcal{E}_3\\ \mathcal{E}_4\\ \mathcal{E}_5\\ \mathcal{E}_6\\ \mathcal{E}_7\\ \mathcal{E}_8\\ \mathcal{E}_9\end{array}\begin{array}{c}\begin{array}{ccccc}\mathcal{R}_0 & \mathcal{R}_1 & \mathcal{R}_2 & \mathcal{R}_3 & \mathcal{R}_4\end{array}\\
\begin{pmatrix}
1 & 1/24\,s^6-1/8\,s^4+1/12\,s^2 & 1/2\,s^4-s^2 & 1/12\,s^6-1/3\,s^2 & -2+2\,s^2\\
1 & -1/12\,s^4+1/12\,s^2 & 1/2\,s^4-s^2 & -1/6\,s^4-1/3\,s^2 & -2+2\,s^2\\
1 & 1/12\,s^5-1/4\,s^3+1/6\,s & 1/2\,s^3-s & 1/12\,s^5-1/3\,s & 0\\
1 & -1/6\,s^3+1/6\,s & 1/2\,s^3-s & -1/6\,s^3-1/3\,s & 0\\
1 & 1/8\,s^4-1/4\,s^2 & 0 & 0 & -2\\
1 & -1/4\,s^2 & 0 & 0 & -2\\
1 & 1/12\,s^3+1/6\,s & -s & -1/6\,s^3-1/3\,s & 0\\
1 & -1/6\,s^3+1/6\,s & -s & -1/3\,s+1/3\,s^3 & 0\\
1 & 1/24\,s^4+1/12\,s^2 & -s^2 & -1/6\,s^4-1/3\,s^2 & -2+2\,s^2\\
1 & -1/12\,s^4+1/12\,s^2 & -s^2 & -1/3\,s^2+1/3\,s^4 & -2+2\,s^2
\end{pmatrix}\end{array}$$

$$\begin{array}{c}\begin{array}{ccccc}\mathcal{R}_5 & \mathcal{R}_6 & \mathcal{R}_7 & \mathcal{R}_8 & \mathcal{R}_9\end{array}\\
\begin{pmatrix}
1/4\,s^6-3/4\,s^4+1/2\,s^2 & 1/12\,s^6-1/3\,s^2 & 1/2\,s^4-s^2 & 1/24\,s^6-1/8\,s^4+1/12\,s^2 & 1\\
-1/2\,s^4+1/2\,s^2 & -1/6\,s^4-1/3\,s^2 & 1/2\,s^4-s^2 & -1/12\,s^4+1/12\,s^2 & 1\\
0 & -1/12\,s^5+1/3\,s & -1/2\,s^3+s & -1/12\,s^5+1/4\,s^3-1/6\,s & -1\\
0 & 1/6\,s^3+1/3\,s & -1/2\,s^3+s & 1/6\,s^3-1/6\,s & -1\\
-1/4\,s^4+1/2\,s^2 & 0 & 0 & 1/8\,s^4-1/4\,s^2 & 1\\
1/2\,s^2 & 0 & 0 & -1/4\,s^2 & 1\\
0 & 1/6\,s^3+1/3\,s & s & -1/12\,s^3-1/6\,s & -1\\
0 & 1/3\,s-1/3\,s^3 & s & 1/6\,s^3-1/6\,s & -1\\
1/4\,s^4+1/2\,s^2 & -1/6\,s^4-1/3\,s^2 & -s^2 & 1/24\,s^4+1/12\,s^2 & 1\\
-1/2\,s^4+1/2\,s^2 & -1/3\,s^2+1/3\,s^4 & -s^2 & -1/12\,s^4+1/12\,s^2 & 1
\end{pmatrix}\end{array},$$

$$Q=\begin{pmatrix}
1 & 1/2\,s^2-1 & s^2 & 1/2\,\left(s^2-2\right)s^2 & 1/2\,s^2\left(s^2-1\right) & 1/4\,s^2\left(s^4-3\,s^2+2\right)\\
1 & -1 & 2\,s & -2\,s & 3/2\,s^2 & -3/2\,s^2\\
1 & 1/2\,s^2-1 & s & 1/2\,\left(s^2-2\right)s & 0 & 0\\
1 & -1 & s & -s & 0 & 0\\
1 & 1/2\,s^2-1 & 0 & 0 & -1/2\,s^2 & -1/4\,\left(s^2-2\right)s^2\\
1 & -1 & 0 & 0 & -1/2\,s^2 & 1/2\,s^2\\
1 & -1 & -s & s & 0 & 0\\
1 & 1/2\,s^2-1 & -s & -1/2\,\left(s^2-2\right)s & 0 & 0\\
1 & -1 & -2\,s & 2\,s & 3/2\,s^2 & -3/2\,s^2\\
1 & 1/2\,s^2-1 & -s^2 & -1/2\,\left(s^2-2\right)s^2 & 1/2\,s^2\left(s^2-1\right) & 1/4\,s^2\left(s^4-3\,s^2+2\right)
\end{pmatrix}$$

$$\begin{pmatrix}
1/6\,s^2\left(s^4-3\,s^2+2\right) & 1/12\,s^2\left(s^4-4\right) & 1/6\,s^4-1/2\,s^2+1/3 & 1/12\,s^4-1/3\\
1/3\,s\left(s^2+2\right) & -1/3\,s\left(s^2+2\right) & 1/6\,s^2+1/3 & -1/6\,s^2-1/3\\
-1/3\,s\left(s^2-1\right) & -1/6\,s\left(s^2+2\right) & 1/3-1/3\,s^2 & -1/6\,s^2-1/3\\
-1/3\,s\left(s^2-1\right) & 1/3\,s\left(s^2-1\right) & 1/3-1/3\,s^2 & -1/3+1/3\,s^2\\
0 & 0 & 1/6\,s^4-1/2\,s^2+1/3 & 1/12\,s^4-1/3\\
0 & 0 & 1/6\,s^2+1/3 & -1/6\,s^2-1/3\\
1/3\,s\left(s^2-1\right) & -1/3\,s\left(s^2-1\right) & 1/3-1/3\,s^2 & -1/3+1/3\,s^2\\
1/3\,s\left(s^2-1\right) & 1/6\,s\left(s^2+2\right) & 1/3-1/3\,s^2 & -1/6\,s^2-1/3\\
-1/3\,s\left(s^2+2\right) & 1/3\,s\left(s^2+2\right) & 1/6\,s^2+1/3 & -1/6\,s^2-1/3\\
-1/6\,s^2\left(s^4-3\,s^2+2\right) & -1/12\,s^2\left(s^4-4\right) & 1/6\,s^4-1/2\,s^2+1/3 & 1/12\,s^4-1/3
\end{pmatrix}.$$

结合方案 $\mathcal{C}$ 的第一和第二特征阵分别为:

$$P=\begin{pmatrix}
1 & 1/24\,s^6-1/8\,s^4+1/12\,s^2 & 1/2\,s^4-s^2 & 1/12\,s^6-1/3\,s^2 & s^2-1 & 1/8\,s^6-3/8\,s^4+1/4\,s^2\\
1 & -1/12\,s^4+1/12\,s^2 & 1/2\,s^4-s^2 & -1/6\,s^4-1/3\,s^2 & s^2-1 & -1/4\,s^4+1/4\,s^2\\
1 & 1/8\,s^4-1/4\,s^2 & 0 & 0 & -1 & -1/8\,s^4+1/4\,s^2\\
1 & -1/4\,s^2 & 0 & 0 & -1 & 1/4\,s^2\\
1 & 1/24\,s^4+1/12\,s^2 & -s^2 & -1/6\,s^4-1/3\,s^2 & s^2-1 & 1/8\,s^4+1/4\,s^2\\
1 & -1/12\,s^4+1/12\,s^2 & -s^2 & -1/3\,s^2+1/3\,s^4 & s^2-1 & -1/4\,s^4+1/4\,s^2
\end{pmatrix},$$

$$Q=\begin{pmatrix}
1 & 1/2\,s^2-1 & 1/2\,s^2\left(s^2-1\right) & 1/4\,s^2\left(s^4-3\,s^2+2\right) & 1/6\,s^4-1/2\,s^2+1/3 & 1/12\,s^4-1/3\\
1 & -1 & 3/2\,s^2 & -3/2\,s^2 & 1/6\,s^2+1/3 & -1/6\,s^2-1/3\\
1 & 1/2\,s^2-1 & 0 & 0 & 1/3-1/3\,s^2 & -1/6\,s^2-1/3\\
1 & -1 & 0 & 0 & 1/3-1/3\,s^2 & -1/3+1/3\,s^2\\
1 & 1/2\,s^2-1 & -1/2\,s^2 & -1/4\left(s^2-2\right)s^2 & 1/6\,s^4-1/2\,s^2+1/3 & 1/12\,s^4-1/3\\
1 & -1 & -1/2\,s^2 & 1/2\,s^2 & 1/6\,s^2+1/3 & -1/6\,s^2-1/3
\end{pmatrix}.$$

结合方案 $\mathcal{D}$ 的第一和第二特征阵分别为:

$$P=\begin{pmatrix}
1 & 1/24\,s^6-1/8\,s^4+1/12\,s^2 & 1/2\,s^4-4/3\,s^2+1/12\,s^6 & s^2-1 & 1/8\,s^6-3/8\,s^4+1/4\,s^2\\
1 & -1/12\,s^4+1/12\,s^2 & 1/3\,s^4-4/3\,s^2 & s^2-1 & -1/4\,s^4+1/4\,s^2\\
1 & 1/8\,s^4-1/4\,s^2 & 0 & -1 & -1/8\,s^4+1/4\,s^2\\
1 & -1/4\,s^2 & 0 & -1 & 1/4\,s^2\\
1 & 1/24\,s^4+1/12\,s^2 & -4/3\,s^2-1/6\,s^4 & s^2-1 & 1/8\,s^4+1/4\,s^2
\end{pmatrix},$$

$$Q=\begin{pmatrix}
1 & 1/2\,s^2-4/3+1/12\,s^4 & 1/2\,s^2\left(s^2-1\right) & 1/4\,s^2\left(s^4-3\,s^2+2\right) & 1/6\,s^4-1/2\,s^2+1/3\\
1 & -4/3-1/6\,s^2 & 3/2\,s^2 & -3/2\,s^2 & 1/6\,s^2+1/3\\
1 & 1/3\,s^2-4/3 & 0 & 0 & 1/3-1/3\,s^2\\
1 & 1/2\,s^2-4/3+1/12\,s^4 & -1/2\,s^2 & -1/4\left(s^2-2\right)s^2 & 1/6\,s^4-1/2\,s^2+1/3\\
1 & -4/3-1/6\,s^2 & -1/2\,s^2 & 1/2\,s^2 & 1/6\,s^2+1/3
\end{pmatrix}.$$

4.7 附录 B

给定集合 $\mathcal{T}$ 上的任一序关系 $<$.

引理 4.3: [46]令 $\mathbf{e}=(e_X)_{X\in\mathcal{T}}$ 和 $E_j=\{X\mid e_X=j\}$ 其中 $j=0,1,2,3$. 则方程

$$\sum_{X\in\mathcal{T}} e_X X=A+2B,\quad A,B\in\mathcal{T},e_X\in\mathbb{Z}_4$$

等价于以下的两个方程

$$a = \sum_{X \in E_1 \cup E_3} x$$

和

$$b^2 = \sum_{X \in E_2 \cup E_3} x^2 + \sum_{\substack{X,Y \in E_1 \cup E_3 \\ X<Y}} xy.$$

记 $2R = \{2x \mid x \in R\}$ 和 $-\mathcal{T} = \{-X \mid X \in \mathcal{T}\}$.

引理 4.4: [13]令 $R = GR(4, m), m > 0$，集合 $\mathcal{T}$ 为它的 Teichmuller 集.

(a) 多重集 $\mathcal{T} + 2\mathcal{T} = \{X + 2Y \mid X, Y \in \mathcal{T}\}$ 恰包含 R 中每个元素一次.

(b) 多重集 $\mathcal{T} - \mathcal{T} = \{X - Y \mid X, Y \in \mathcal{T}\}$ 包含元素 0 的次数为 2^m 次，不包含 $2R$ 中的任一元素，恰包含 $R\backslash 2R$ 中每个元素一次.

(c) 多重集 $\mathcal{T} + \mathcal{T} = \{X + Y \mid X, Y \in \mathcal{T}\}$ 恰包含 $2R$ 中每个元素一次，包含 $R\backslash 2R$ 中一半的元素恰两次.

(d) 当 m 为偶数时，多重集 $\mathcal{T} + \mathcal{T}$ 和 $-(\mathcal{T} + \mathcal{T})$ 相等. 当 m 为奇数时，它们的交集等于 $2R$. 特别地，只有当 m 为偶数时，$-\mathcal{T}$ 中的元素才会出现在 $\mathcal{T} + \mathcal{T}$ 中.

下面两个结果是引理 4.4 的自然推广.

引理 4.5: 给定奇数 $m > 0$ 和 $R = GR(4, m)$. 记 $\mathcal{T}$ 为它的 Teichmuller 集. 则

(a) 多重集 $\mathcal{T} + \mathcal{T} + \mathcal{T} = \{X + Y + Z \mid X, Y, Z \in \mathcal{T}\}$ 恰包含集合 $-\mathcal{T}$ 中每个元素一次，恰包含剩下的每个元素 $2^m + 1$ 次；

(b) 多重集 $\mathcal{T} + \mathcal{T} - \mathcal{T} = \{X + Y - Z \mid X, Y, Z \in \mathcal{T}\}$ 恰包含集合 $\mathcal{T}$ 中每个元素 $2^{m+1} - 1$ 次，恰包含剩下的每个元素 $2^m - 1$ 次.

证明. 下面我们只给出结论 (a) 的证明。结论 (b) 的证明是完全类似的. 我们需要考察方程

$$X + Y + Z = C,$$

在 $X,Y,Z \in \mathcal{T}$，$C \in R$ 条件下解的个数. 这里元素 C 可以唯一地表示成 $C = A + 2B$，其中 $A, B \in \mathcal{T}$.

首先设 $C \in -\mathcal{T}$，即 $A = B$. 则 $X + Y + Z + A = 0$. 由此推出 $X = Y = Z = A$. 也就是说多重集 $\mathcal{T} + \mathcal{T} + \mathcal{T}$ 恰包含集合 $-\mathcal{T}$ 中任一元素一次.

接着设 $C \notin -\mathcal{T}$，即 $A \neq B$. 我们分以下两种情形：$A = 0$ 和 $A \neq 0$ 来进行讨论.

当 $A = 0$ 时，通过变量替换，我们只需考虑方程

$$X + Y + Z = 2. \tag{4.7}$$

根据引理 4.3 它等价于

$$\begin{cases} x + y + z = 0, \\ xy + xz + yz = 1, \end{cases} \tag{4.8}$$

容易看出

$$x^2 + y^2 + xy + 1 = 0.$$

若 $x = 0$，则方程只有一个解

$$(x, y, z) = (0, 1, 1).$$

若 $x \neq 0$，则设 $y = tx$，其中 $t \in \mathbb{F}_{2^m}$. 于是

$$(t^2 + t + 1)x^2 + 1 = 0.$$

整理可得

$$(x, y, z) = \left(\frac{1}{\sqrt{t^2 + t + 1}}, \frac{t}{\sqrt{t^2 + t + 1}}, \frac{t+1}{\sqrt{t^2 + t + 1}} \right).$$

不难验证此时方程 (4.7) 共有 $2^m + 1$ 个解.

当 $A \neq 0$ 时，我们只需考虑方程

$$X + Y + Z = 1 + 2B, \tag{4.9}$$

其中 $B \in \mathcal{T}$，$B \neq 1$. 根据引理 4.3，方程 (4.9) 等价于

$$\begin{cases} x + y + z = 1, \\ xy + xz + yz = b^2. \end{cases} \tag{4.10}$$

容易看出

$$x^2 + xy + y^2 + x + y + b^2 = 0. \tag{4.11}$$

令 $x = (1+b)u + b$，$y = (1+b)v + b$. 则上述方程化为

$$u^2 + uv + v^2 + u + v = 0.$$

不失一般性，可以在方程 (4.11) 中设 $b = 0$.

若 $x = 0$，则可得两个解 $(x, y, z) = (0, 0, 1)$ 与 $(x, y, z) = (0, 1, 0)$.

若 $x \neq 0$，则设 $y = tx$，其中 $t \in \mathbb{F}_{2^m}$. 于是

$$(t^2 + t + 1)x^2 + (t + 1)x = 0.$$

整理可得

$$(x, y, z) = \left(\frac{t+1}{t^2+t+1}, \frac{t^2+t}{t^2+t+1}, \frac{t}{t^2+t+1} \right).$$

若 $t = 1$，则只有一个解 $(x, y, z) = (0, 0, 1)$. 不难验证方程 (4.11) 一共有 $2^m + 1$ 个解. □

由上面的引理我们有以下的直接推论.

推论 4.2：给定奇数 m 和 $R = GR(4, m)$. 记 $\mathcal{T}$ 为它的 Teichmuller 集.

(a) 多重集 $\mathcal{T} + \mathcal{T} + \mathcal{T} + \mathcal{T} = \{X + Y + Z + W : X, Y, Z, W \in \mathcal{T}\}$ 包含元素 0 的次数为 2^m 次，恰包含集合 $2R\backslash\{0\}$ 中每个元素 $2^m(2^m + 1)$ 次，包含剩下的每个元素 2^{2m} 次.

(b) 多重集 $\mathcal{T} + \mathcal{T} - \mathcal{T} - \mathcal{T} = \{X + Y - Z - W : X, Y, Z, W \in \mathcal{T}\}$ 包含元素 0 的次数为 $(2^{m+1} - 1)2^m$ 次，恰包含集合 $2R\backslash\{0\}$ 中每个元素 $(2^m - 1)2^m$ 次，包含剩下的每个元素 2^{2m} 次.

(c) 多重集 $\mathcal{T} + \mathcal{T} + \mathcal{T} - \mathcal{T} = \{X + Y + Z - W : X, Y, Z, W \in \mathcal{T}\}$ 恰包含集合 $2R$ 中每个元素 2^{2m} 次，恰包含集合 $(\mathcal{T} + \mathcal{T})\backslash 2R$ 中每个元素 $(2^m + 1)2^m$ 次，包含剩下的每个元素 $(2^m - 1)2^m$ 次.

回忆一下我们在第 4.3 节中给出的集合 $\mathcal{E}_0, \ldots, \mathcal{E}_9$ 的定义.

推论 4.3：给定奇数 $m \geq 3$. 令 $q = 2^m$，$G = \mathbb{Z}_4 \times R \times \mathbb{F}_q$. 则集合 $\mathcal{E}_0, \ldots, \mathcal{E}_9$ 构成 G 的一个划分.

证明. 利用引理 4.4 中结论 (b)，我们不难验证集合 $\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_4, \mathcal{E}_5, \mathcal{E}_8, \mathcal{E}_9$ 中所有第一坐标等于 0 的元素恰构成 $\{0\} \times R \times \mathbb{F}_q$ 的一个划分. 利用引理 4.4 中结论 (c)，我们可以验证第一坐标等于 2 的情形. 剩下的元素第一坐标等于 1 或 3 的情形可以利用引理 4.4 中结论 (a) 来验证. □

令 $\mathrm{tr}(x)$ 表示从 $\mathbb{F}_{2^m}$ 到 $\mathbb{F}_2$ 的迹函数. 下面的结论是我们所熟知的[73].

引理 4.6：给定正整数 m. 设二次方程 $f_a(x) = x^2 + x + a = 0, a \in \mathbb{F}_{2^m}$. 若 $\mathrm{tr}(a) = 0$，则它在 $\mathbb{F}_{2^m}$ 中有两个解；若 $\mathrm{tr}(a) = 1$，则它在 $\mathbb{F}_{2^m}$ 中无解.

令 $f_a(x) = x^3 + x + a$. 记

$$M_i = \left\{ a \in \mathbb{F}_{2^m}, a \neq 0 \mid f_a(x) = 0 \text{ 在 } \mathbb{F}_{2^m} \text{ 中恰有 } i \text{ 个解} \right\}$$

其中 $i = 0, 1, 3$. 它们的大小 $|M_0|, |M_1|, |M_3|$ 可以在文献[52] 的附录中找到：

$$\begin{aligned} |M_0| &= \frac{q+1}{3}, \\ |M_1| &= \frac{q}{2} - 1, \\ |M_3| &= \frac{q-2}{6}. \end{aligned}$$

引理 4.7：给定正整数 m 和三次方程 $f_a(x) = x^3 + x + a, a \in \mathbb{F}_{2^m}$.

(a) 若 $a = 0$，则 $f_a(x)$ 在 $\mathbb{F}_{2^m}$ 中有两个根 $x = 0, 1$.

(b) 若 $a = b + b^{-1}$ 对某一 $b \in \mathbb{F}_{2^m} \backslash \{0, 1\}$ 成立，则 $f_a(x)$ 在 $\mathbb{F}_{2^m}$ 有且仅有一个根.

(c) 若 $a = b^{-1} + b^{-3}$ 对某一 $b \in \mathbb{F}_{2^m} \backslash \{0, 1\}$ 成立且 $\mathrm{tr}(b) = 1$，则 $f_a(x)$ 在 $\mathbb{F}_{2^m}$ 中有三个不同的根.

(d) 若 a 不满足上述任一条件，则 $f_a(x)$ 在 $\mathbb{F}_{2^m}$ 上不可约.

证明. 结论 (a) 可以直接验证. 文献[11]（p.169） 中已经证明 $f_a(x)=0$ 在 $\mathbb{F}_{2^m}$ 中恰有一个根当且仅当 $\mathrm{tr}(1/a)=0$ 成立. 若 $a=b+b^{-1}$ 对某一 $b\in\mathbb{F}_{2^m}\backslash\{0,1\}$ 成立，则

$$\mathrm{tr}\left(\frac{1}{b+b^{-1}}\right)=\mathrm{tr}\left(\frac{b}{b^2+1}\right)=\mathrm{tr}\left(\frac{b}{b+1}+\left(\frac{b}{b+1}\right)^2\right)=0.$$

容易验证集合 $\{b+b^{-1}\mid b\in\mathbb{F}_{2^m}\backslash\{0,1\}\}$ 的大小与 $|M_1|$ 相等. 于是我们证明了结论 (b).

若 $a=b^{-1}+b^{-3}$ 对某一 $b\in\mathbb{F}_{2^m}\backslash\{0,1\}$ 且 $\mathrm{tr}(b)=1$ 成立，则

$$\mathrm{tr}\left(\frac{1}{b^{-1}+b^{-3}}\right)=\mathrm{tr}\left(b+\frac{b}{b^2+1}\right)=\mathrm{tr}(b)=1.$$

因为 b^{-1} 已经是 $f_a(x)$ 的一个根，所以 $f_a(x)$ 在 $\mathbb{F}_{2^m}$ 中必有三个不同的根. 下面我们来验证集合 $\{b^{-1}+b^{-3}\mid b\in\mathbb{F}_{2^m}\backslash\{0,1\},\mathrm{tr}(b)=1\}$ 的大小等于 $|M_3|$. 设 $b^{-1}+b^{-3}=c^{-1}+c^{-3}$，其中 $b\in\mathbb{F}_{2^m}\backslash\{0,1\}$ 且 $\mathrm{tr}(b)=1$，$c\in\mathbb{F}_{2^m}\backslash\{0,1\}$. 于是

$$\begin{aligned}
& b^{-1}+b^{-3}=c^{-1}+c^{-3}\\
\Longleftrightarrow\quad & (b+c)(b^2c^2+b^2+bc+c^2)=0\\
\Longleftrightarrow\quad & c=b \text{ or } c^2+(b/(b^2+1))c+b^2/(b^2+1)=0.
\end{aligned}$$

由于

$$\mathrm{tr}\left(\frac{b^2/(b^2+1)}{b^2/(b^2+1)^2}\right)=\mathrm{tr}(b^2+1)=0,$$

根据引理 4.6 可知方程 $c^2+(b/(b^2+1))c+b^2/(b^2+1)=0$ 在 $\mathbb{F}_{2^m}$ 中有两个不同的根. 从方程 $b^2c^2+b^2+bc+c^2=0$ 的对称性可知 $\mathrm{tr}(c)$ 必等于 1. 由此可以看出集合 $\{b^{-1}+b^{-3}\mid b\in\mathbb{F}_{2^m}\backslash\{0,1\},\mathrm{tr}(b)=1\}$ 的大小就是 $(q-2)/6=|M_3|$，于是我们也就证明了结论 (c). 然后可以立即推出结论 (d). □

下面我们总是假设 $q=2^m$，其中 $m\geq 3$ 为奇数.

引理 4.8：给定 $W\in\mathcal{T}$. 则方程组

$$\begin{cases} X+Y-Z=W+2;\\ x^3+y^3+z^3=w^3+e, \end{cases}$$

的解的个数为 (a) 1，若 $e=0$；(b) 2，若 $e\in M_1$；(c) 0，若 $e\in M_0\cup M_3$.

证明. 根据 $X+Y=(\sqrt{X}+\sqrt{Y})^2+2\sqrt{XY}$ 可知第一个方程 $X+Y=2+Z+W$ 等价于 $\mathbb{F}_{2^m}$ 上的方程组：

$$x+y=z+w,\quad xy=zw+1.$$

于是

$$\begin{aligned}e&=x^3+y^3+z^3+w^3\\&=(x+y)^3+xy(x+y)+z^3+w^3\\&=(z+w)^3+(zw+1)(z+w)+z^3+w^3\\&=z+w.\end{aligned}$$

整理得 $z=e+w, y=e+x$. 将它们代入 $xy=zw+1$，我们有 $(x+z)^2+e(x+z)+1=0$. 若 $e=0$，则 $x=1+z=e+w+1$，这个方程组只有 1 个解. 若 $e\neq 0$，则 $(x+z)^2/e^2+(x+z)/e+1/e^2=0$. 这个方程有 0 或 2 个解分别对应于 $\mathrm{tr}(1/e)=1$ 成立或不成立. □

引理 4.9：给定 $A,B\in\mathcal{T}$ 且 $B\neq 0$. 则方程组

$$\begin{cases}X+Y+Z=A+2B;\\x^3+y^3+z^3=a^3+b^3e,\end{cases}$$

解的个数为 (a) 1，若 $e=0$；(b) 2，若 $e\in M_1$；(c) 0，若 $e\in M_0\cup M_3$.

类似地，我们有下面的几个结论.

引理 4.10：给定 $A,B\in\mathcal{T}$ 且 $B\neq 0$. 则方程组

$$\begin{cases}X+Y+Z=-A+2B,\\x^3+y^3+z^3=a^3+b^3e,\end{cases}$$

解的个数为 (a) 3，若 $e=0$；(b) 0，若 $e\in M_0\cup M_1$；(c) 6，若 $e\in M_3$.

推论 4.4：给定 $0\neq B\in\mathcal{T}$. 则方程组

$$\begin{cases}X+Y+Z-W=2B;\\x^3+y^3+z^3+w^3=b^3e,\end{cases}$$

解的个数为(a) 2^m，若 $e=0$；(b) 2^{m+1}，若 $e\in M_1$；(c) 0，若 $e\in M_0\cup M_3$.

推论 4.5：给定 $0 \neq B \in \mathcal{T}$. 则方程组

$$\begin{cases} X & + & Y & + & Z & + & W & = & 2B; \\ x^3 & + & y^3 & + & z^3 & + & w^3 & = & b^3 e, \end{cases}$$

解的个数为 (a) $3 \cdot 2^m$，若 $e = 0$；(b) 0，若 $e \in M_0 \cup M_1$；(c) $6 \cdot 2^m$，若 $e \in M_3$.

4.8 附录 C

在这一节中，我们总是假定 $q = 2^m$ 其中 $m \geq 3$ 为奇数. 对 $(a, b) \in G \times \mathbb{F}_q$，指数和 $\xi(a, b)$ 具有下面的性质：

(a) 若 $b \neq 0$，则 $\xi(a, b) = \xi(aB^{-1/3}, 1)$；

(b) 若 $U, V \in \mathcal{T}, W \in \mathcal{T}^*$，则 $\xi(U + 2V, b) = \xi(UW + 2VW, bw^3)$.

我们需要引进一些记号. 给定 R 中元素 a 和 c. 则它们可以表示成 $a = U + 2V$ 和 $c = S + 2T$，其中 $U, V, S, T \in \mathcal{T}$. 为了方便，记 $\eta_a = \xi(a, 1)$. 令 u 为 a 模 2 后在 $\mathbb{F}_q$ 中的投影. 记

$$f_u(z) = z^2 + u^2 z + \sqrt{z} + u$$

和 F_u 为 $f_u(z)$ 在 $\mathbb{F}_q$ 中的零点. 又记

$$h_u(z) = f_u(z) - u = z^2 + u^2 z + \sqrt{z}$$

和 H_u 为 $h_u(z)$ 在 $\mathbb{F}_q$ 中的零点. 不难验证 $u^2 \in F_u$，

$$F_u = \{x + u^2 \mid x \in H_u\}.$$

所以 $|F_u| = |H_u|$. 对任一 $x \in H_u$，都有 $\mathrm{tr}(ux) = \mathrm{tr}(u^2 x^2) = \mathrm{tr}(x^3 + x^{3/2}) = 0$. 于是 $\mathrm{tr}(uy) = \mathrm{tr}(u^3)$ 对任一 $y \in F_u$ 均成立. 对 $X, Y \in \mathcal{T}$，我们有

$$X + Y = (\sqrt{X} + \sqrt{Y})^2 + 2\sqrt{XY}.$$

我们将把元素 $(\sqrt{X} + \sqrt{Y})^2 \in \mathcal{T}$ 记作 $X \oplus Y$.

引理 4.11：给定 $a \in R$ 且令 u 为 a 模 2 后在 $\mathbb{F}_q$ 中的象. 则指数和 η_a 具有下述性质：

$$\eta_a^2 = 2^m \sum_{\substack{Z \in \mathcal{T} \\ f_u(z) = 0}} i^{\mathrm{T}(aZ + 2Z^3)}, \qquad \eta_a \overline{\eta_a} = 2^m \sum_{\substack{Z \in \mathcal{T} \\ h_u(z) = 0}} i^{\mathrm{T}(aZ + 2Z^3)},$$

$$\eta_a^4 = 2^m (-1)^{\mathrm{tr}(u^3)} |F_u| \eta_a \overline{\eta_a}, \qquad (\eta_a \overline{\eta_a})^2 = 2^m |F_u| \eta_a \overline{\eta_a}, \qquad \eta_a^3 \overline{\eta_a} = 2^m |F_u| \eta_a^2.$$

证明. 我们首先计算

$$\begin{aligned}\eta_a^2 &= \sum_{X\in\mathcal{T}}\sum_{Y\in\mathcal{T}} i^{\mathrm{T}(a(X+Y)+2(X^3+Y^3))} = \sum_{Y\in\mathcal{T}}\sum_{Z\in\mathcal{T}} i^{\mathrm{T}(a(Y\oplus Z+Y)+2((Y\oplus Z)^3+Y^3))}\\ &= \sum_{Y\in\mathcal{T}}\sum_{Z\in\mathcal{T}} i^{T(aZ+2Z^3+2(aY+a\sqrt{YZ}+Y^2Z+Z^2Y+Z^3))}\\ &= \sum_{Z\in\mathcal{T}} i^{\mathrm{T}(aZ+2Z^3)}\sum_{y\in\mathbb{F}_q}(-1)^{\mathrm{tr}(y(z^2+u^2z+\sqrt{z}+u))}\\ &= 2^m\sum_{\substack{Z\in\mathcal{T}\\ f_u(z)=0}} i^{\mathrm{T}(aZ+2Z^3)}.\end{aligned}$$

类似的计算可以得到

$$\eta_a\overline{\eta_a} = 2^m\sum_{\substack{Z\in\mathcal{T}\\ h_u(z)=0}} i^{\mathrm{T}(aZ+2Z^3)}.$$

于是

$$\begin{aligned}\eta_a^4 &= 2^{2m}\sum_{\substack{Z\in\mathcal{T}\\ f_u(z)=0}}\sum_{\substack{W\in\mathcal{T}\\ f_u(w)=0}} i^{\mathrm{T}(a(Z+W)+2(Z^3+W^3))}\\ &= 2^{2m}\sum_{\substack{Z\in\mathcal{T}\\ f_u(z)=0}}\sum_{\substack{W\in\mathcal{T}\\ h_u(w)=0}} i^{\mathrm{T}(a(Z+Z\oplus W)+2(Z^3+(Z\oplus W)^3))}\\ &= 2^{2m}\sum_{\substack{W\in\mathcal{T}\\ h_u(w)=0}} i^{\mathrm{T}(aW+2W^3)}\sum_{\substack{Z\in\mathcal{T}\\ f_u(z)=0}}(-1)^{\mathrm{tr}(uz+w(z^2+u^2z+\sqrt{z}))}\\ &= 2^{2m}\sum_{\substack{W\in\mathcal{T}\\ h_u(w)=0}} i^{\mathrm{T}(aW+2W^3)}\sum_{\substack{Z\in\mathcal{T}\\ f_u(z)=0}}(-1)^{\mathrm{tr}(u(z+w))}\\ &= 2^m(-1)^{\mathrm{tr}(u^3)}|F_u|\eta_a\overline{\eta_a}.\end{aligned}$$

类似地，我们可以证明余下的结论. □

引理 4.12: 给定 $c\in R\backslash 2R$ 和 $d\in\mathbb{F}_q$. 则 c 可以唯一地表示成 $c=F-G$，其中 $F,G\in\mathcal{T}$. 我们有

$$\mathbf{E}(c,d) = \begin{cases} 2^{3m+4}(3\cdot 2^{m-1}-1), & \text{若 } d=f^3+g^3;\\ 2^{3m+4}(2^{m-1}-1), & \text{若 } d\neq f^3+g^3,\end{cases}$$

其中 f,g 为 F,G 模 2 后在 $\mathbb{F}_q$ 中的象.

证明. 通过直接验证可知

$$st^2+s^{-1}t^4+s^3 = f^3+g^3$$

和

$$\mathrm{tr}(s^{-3}(f^3+g^3))=1.$$

令 $X\in\mathcal{T}$ 和 $B\in\mathcal{T}^*$. 计算

$$\begin{aligned}\mathcal{U} &:= i^{\mathrm{T}(Xc)}\sum_{Y\in\mathcal{T}}\eta_{(X+2Y)B^{-1/3}}\overline{\eta_{(X+2Y)B^{-1/3}}}(-1)^{\mathrm{tr}(ys)}\\ &= 2^m i^{\mathrm{T}(Xc)}\sum_{Y\in\mathcal{T}}\sum_{\substack{Z\in\mathcal{T}\\ h_{x'}(z)=0}} i^{\mathrm{T}((X+2Y)B^{-1/3})Z+2Z^3)}(-1)^{\mathrm{tr}(ys)}\\ &= 2^m i^{\mathrm{T}(Xc)}\sum_{\substack{Z\in\mathcal{T}\\ h_{x'}(z)=0}} i^{\mathrm{T}(XB^{-1/3}Z+2Z^3)}\sum_{Y\in\mathcal{T}}(-1)^{\mathrm{tr}(y(b^{-1/3}z+s))}\\ &= \begin{cases}2^{2m}(-1)^{\mathrm{tr}(b(f^3+g^3))}, & \text{若 } X=B^{\frac12}S^{\frac12}\oplus B^{\frac14}S^{-\frac14};\\ 0, & \text{其他情况,}\end{cases}\end{aligned}$$

其中 $x'=xb^{-1/3}$. 注意到：若 $b=s^{-3}$，则 $B^{\frac12}S^{\frac12}\oplus B^{\frac14}S^{-\frac14}=0$.

设 $x,s\in\mathbb{F}_q^*$ 和 $b\in\mathbb{F}_q^*\backslash\{s^{-3}\}$. 我们来考查集合 H_x. 显然 0 为 $h_x(z)$ 的一个根. 方程 $h_x(z)=0$ 等价于

$$(h_x(z))^2=z(z^3+x^4z+1)=0.$$

用 x^2w 来替代 z，则方程 $z^3+x^4z+1=0$ 化为 $w^3+w+x^{-6}=0$.

若

$$x=(bs)^{1/2}+(bs^{-1})^{1/4},$$

则

$$x^6=b^{1/2}s^{3/2}+bs^3+b^{-1/2}s^{-3/2}+1$$

且

$$x^{-6}=(1+b^{-1/2}s^{-3/2})^{-1}+(1+b^{-1/2}s^{-3/2})^{-3}.$$

利用引理 4.7，可知若

$$\mathrm{tr}(1+b^{-1/2}s^{-3/2})=0,$$

则

$$\mathrm{tr}(x^6)=\mathrm{tr}(1+b^{-1}s^{-3})=0,$$

因而

$$|F_{b^{\frac16}s^{\frac12}+b^{-\frac{1}{12}}s^{-\frac14}}|=|H_{b^{\frac16}s^{\frac12}+b^{-\frac{1}{12}}s^{-\frac14}}|=2;$$

如若不然，则我们有

$$|F_{b^{\frac{1}{6}}s^{\frac{1}{2}}+b^{-\frac{1}{12}}s^{-\frac{1}{4}}}| = |H_{b^{\frac{1}{6}}s^{\frac{1}{2}}+b^{-\frac{1}{12}}s^{-\frac{1}{4}}}| = 4.$$

所以式子

$$(2(-1)^{\mathrm{tr}(1+b^{-1}s^{-3})}+6)|F_{b^{\frac{1}{6}}s^{\frac{1}{2}}+b^{-\frac{1}{12}}s^{-\frac{1}{4}}}|$$

总是等于 16.

指数和 $\mathbf{E}(c,d)$ 将会被拆分成四个部分来进行计算。我们应用的主要工具是引理 4.11. 首先我们计算

$$\begin{aligned}
\mathbf{E}(c,d)_1 &= \sum_{a\in R^*}\sum_{b\in\mathbb{F}_q^*}\left(\xi^4(a,b)+\overline{\xi^4(a,b)}+6\,\xi^2(a,b)\overline{\xi^2(a,b)}\right)i^{\mathrm{T}(ac+2bd)}\\
&= \sum_{X\in\mathcal{T}^*}\sum_{Y\in\mathcal{T}}\sum_{b\in\mathbb{F}_q^*}\Big(\xi^4(X+2Y,b)+\overline{\xi^4(X+2Y,b)}\\
&\qquad +6\xi^2(X+2Y,b)\overline{\xi^2(X+2Y,b)}\Big)i^{\mathrm{T}((X+2Y)c+2bd)}\\
&= \sum_{X\in\mathcal{T}^*}\sum_{Y\in\mathcal{T}}\sum_{b\in\mathbb{F}_q^*}\left(\eta^4_{(X+2Y)B^{-\frac{1}{3}}}+\overline{\eta^4_{(X+2Y)B^{-\frac{1}{3}}}}\right.\\
&\qquad \left.+6\eta^2_{(X+2Y)B^{-\frac{1}{3}}}\overline{\eta^2_{(X+2Y)B^{-\frac{1}{3}}}}\right)i^{\mathrm{T}((X+2Y)c+2bd)}\\
&= 2^m\sum_{X\in\mathcal{T}^*}\sum_{b\in\mathbb{F}_q^*}(-1)^{\mathrm{tr}(bd)}\left(2(-1)^{\mathrm{tr}(x^3b^{-1})}+6\right)|F_{xb^{-\frac{1}{3}}}|\mathcal{U}\\
&= 2^{3m}\sum_{b\in\mathbb{F}_q^*\setminus\{s^{-3}\}}\left[\left(2(-1)^{\mathrm{tr}(1+b^{-1}s^{-3})}+6\right)|F_{b^{\frac{1}{6}}s^{\frac{1}{2}}+b^{-\frac{1}{12}}s^{-\frac{1}{4}}}|\right](-1)^{\mathrm{tr}(b(f^3+g^3+d))}\\
&= 2^{3m+4}\sum_{b\in\mathbb{F}_q^*\setminus\{s^{-3}\}}(-1)^{\mathrm{tr}(b(f^3+g^3+d))}.
\end{aligned}$$

然后，

$$\begin{aligned}
\mathbf{E}(c,d)_2 &= \sum_{X\in\mathcal{T}^*}\sum_{Y\in\mathcal{T}}\Big(\xi^4(X+2Y,0)+\overline{\xi^4(X+2Y,0)}\\
&\qquad +6\xi^2(X+2Y,0)\overline{\xi^2(X+2Y,0)}\Big)i^{\mathrm{T}((X+2Y)c)}\\
&= \sum_{X\in\mathcal{T}^*}\sum_{Y\in\mathcal{T}}\left(2^{2m}i^{\mathrm{T}(2)}+2^{2m}i^{-\mathrm{T}(2)}+6\cdot 2^{2m}\right)i^{\mathrm{T}((X+2Y)c)}\\
&= 2^{2m+2}\sum_{X\in\mathcal{T}^*}i^{\mathrm{T}(Xc)}\sum_{Y\in\mathcal{T}}(-1)^{\mathrm{tr}(ys)}\\
&= 0.
\end{aligned}$$

接着是

$$\begin{aligned}\mathbf{E}(c,d)_3 &= \sum_{Y\in\mathcal{T}}\sum_{b\in\mathbb{F}_q^*}\left(\xi^4(2Y,b)+\overline{\xi^4(2Y,b)}+6\xi^2(2Y,b)\overline{\xi^2(2Y,b)}\right)i^{\mathrm{T}(2Yc+2bd)}\\ &= \sum_{Y\in\mathcal{T}}\sum_{b\in\mathbb{F}_q^*}\left(2^{2m+4}(1+(-1)^{\mathrm{tr}(yb^{-1/3}+1)}\right)(-1)^{\mathrm{tr}(ys+bd)}\\ &= 2^{2m+4}\sum_{b\in\mathbb{F}_q^*}(-1)^{\mathrm{tr}(bd+1)}\sum_{Y\in\mathcal{T}}(-1)^{\mathrm{tr}(y(b^{-1/3}+s))}\\ &= 2^{3m+4}(-1)^{\mathrm{tr}(s^{-3}d+1)}.\end{aligned}$$

最后我们计算

$$\mathbf{E}(c,d)_4 = \xi^4(0,0)+\overline{\xi^4(0,0)}+6\xi^2(0,0)\overline{\xi^2(0,0)}=2^{4m+3}.$$

将式子 $\mathbf{E}(c,d)_1,\mathbf{E}(c,d)_2,\mathbf{E}(c,d)_3$ 和 $\mathbf{E}(c,d)_4$ 加起来便证明了我们的结论. □

引理 4.13: 给定 $c\in R\backslash 2R$ 和 $d\in\mathbb{F}_q$. 存在 $F,G\in\mathcal{T}$ 使得 $c=F+G, F\neq G$. 我们有

$$\mathbf{F}(c,d) = \begin{cases} 2^{3m+2}(3\cdot 2^{m-1}-1), & \text{若 } d=f^3+g^3;\\ 2^{3m+2}(2^{m-1}-1), & \text{若 } d\neq f^3+g^3,\end{cases}$$

其中 f,g 分别是 F,G 模 2 后在 $\mathbb{F}_q$ 中得到的象.

证明. 不难验证

$$st^2+s^3=f^3+g^3.$$

令 $X\in\mathcal{T}$ 和 $B\in\mathcal{T}^*$. 我们有

$$\begin{aligned}\mathcal{V} &:= i^{\mathrm{T}(X)}\sum_{Y\in\mathcal{T}}\Big(\eta^3_{(X+2Y)B^{-1/3}}\overline{\eta_{(X+2Y)B^{-1/3}}}\\ &\qquad +\eta_{(X+2Y)B^{-1/3}}\overline{\eta^3_{(X+2Y)B^{-1/3}})}\Big)(-1)^{\mathrm{tr}(y)}\\ &= 2^{2m}|K_{xb^{-1/3}}|i^{\mathrm{T}(X)}\sum_{\substack{Z\in\mathcal{T}\\ f_{x'}(z)=0}}\Big(i^{\mathrm{T}(XB^{-1/3}Z+2Z^3)}\\ &\qquad +i^{-\mathrm{T}(XB^{-1/3}Z+2Z^3)}\Big)\sum_{Y\in\mathcal{T}}(-1)^{\mathrm{tr}(v(b^{-1/3}z+1))}\\ &= \begin{cases} 2^{3m}|K_{b^{1/6}}|(1+(-1)^{\mathrm{tr}(b)}), & \text{若 } U=B^{1/2};\\ 2^{3m}|K_{b^{1/6}+b^{-1/3}}|(-1+(-1)^{\mathrm{tr}(b)}), & \text{若 } U=1\oplus B^{1/2};\\ 0, & \text{其他情况,}\end{cases}\end{aligned}$$

其中 $x'=xb^{-1/3}$.

首先我们计算

$$\begin{aligned}
\mathbf{F}(c,d)_1 &= \sum_{X\in\mathcal{T}^*}\sum_{Y\in\mathcal{T}}\sum_{b\in\mathbb{F}_q^*}\Big(\xi^3(X+2Y,b)\overline{\xi(X+2Y,b)} \\
&\qquad +\xi(X+2Y,b)\overline{\xi^3(X+2Y,b)}\Big)\, i^{\mathrm{T}((X+2Y)c+2bd)} \\
&= \sum_{X\in\mathcal{T}^*}\sum_{Y\in\mathcal{T}}\sum_{b\in\mathbb{F}_q^*}\Big(\xi^3((X+2Y)S,bs^3)\overline{\xi((X+2Y)S,bs^3)} \\
&\qquad +\xi((X+2Y)S,bs^3)\overline{\xi^3((X+2Y)S,bs^3)}\Big)\, i^{\mathrm{T}((X+2Y)S(1+2S^{-1}T)+2bd)} \\
&= \sum_{X\in\mathcal{T}^*}\sum_{Y\in\mathcal{T}}\sum_{b\in\mathbb{F}_q^*}\Big(\xi^3(X+2Y,b)\overline{\xi(X+2Y,b)} \\
&\qquad +\xi(X+2Y,b)\overline{\xi^3(X+2Y,b)}\Big)\, i^{\mathrm{T}((X+2Y)(1+2S^{-1}T)+2bs^{-3}d)} \\
&= \sum_{X\in\mathcal{T}^*}\sum_{b\in\mathbb{F}_q^*} i^{\mathrm{T}(2XS^{-1}T+2bs^{-3}d)}\,\mathcal{V} \\
&= 2^{3m}\sum_{b\in\mathbb{F}_q^*}|K_{b^{1/6}}|(-1)^{\mathrm{tr}(b^{1/2}s^{-1}t+bs^{-3}d)}(1+(-1)^{\mathrm{tr}(b)}) \\
&\quad +2^{3m}\sum_{b\in\mathbb{F}_q\setminus\{0,1\}}|K_{b^{1/6}+b^{-1/3}}|(-1)^{\mathrm{tr}(b^{1/2}s^{-1}t+s^{-1}t+bs^{-3}d)}(-1+(-1)^{\mathrm{tr}(b)}) \\
&= 2^{3m+2}\left(\sum_{\substack{b\in\mathbb{F}_q^*\\ \mathrm{tr}(b)=0}}(-1)^{\mathrm{tr}(b(s^{-2}t^2+s^{-3}d))}+\sum_{\substack{b\in\mathbb{F}_q\setminus\{0,1\}\\ \mathrm{tr}(b)=1}}(-1)^{\mathrm{tr}(s^{-1}t+b(s^{-2}t^2+s^{-3}d))}\right) \\
&= 2^{3m+2}(1+(-1)^{\mathrm{tr}(s^{-3}d+1)})\sum_{\substack{b\in\mathbb{F}_q^*\\ \mathrm{tr}(b)=0}}(-1)^{\mathrm{tr}(b(s^{-2}t^2+s^{-3}d))} \\
&= \begin{cases} 2^{3m+3}(2^{m-1}-1), & \text{若 } d=f^3+g^3; \\ -2^{3m+2}(1+(-1)^{\mathrm{tr}(s^{-3}d+1)}), & \text{其他情况.}\end{cases}
\end{aligned}$$

然后

$$\begin{aligned}
\mathbf{F}(c,d)_2 &= \sum_{X\in\mathcal{T}^*}\sum_{Y\in\mathcal{T}}\Big(\xi^3(X+2Y,0)\overline{\xi(X+2Y,0)} \\
&\qquad +\xi(X+2Y,0)\overline{\xi^3(X+2Y,0)}\Big)\, i^{\mathrm{T}((X+2Y)c)} \\
&= 2^{2m}\sum_{X\in\mathcal{T}^*}\sum_{Y\in\mathcal{T}}\left(i^{\mathrm{T}(1+2X^{-1}Y+(X+2Y)c)}+i^{\mathrm{T}(-1-2X^{-1}Y+(X+2Y)c)}\right) \\
&= 2^{2m}\left(\sum_{X\in\mathcal{T}^*}i^{\mathrm{T}(1+Xc)}+\sum_{X\in\mathcal{T}^*}i^{\mathrm{T}(-1+Xc)}\right)\sum_{Y\in\mathcal{T}}(-1)^{\mathrm{tr}(y(x^{-1}+s))} \\
&= 2^{3m}\left(i^{\mathrm{T}(2+2s^{-1}t)}+i^{\mathrm{T}(2s^{-1}t)}\right) \\
&= 0.
\end{aligned}$$

接着是

$$\begin{aligned}
\mathbf{F}(c,d)_3 &= \sum_{Y\in\mathcal{T}}\sum_{b\in\mathbb{F}_q^*}(\xi^3(2Y,b)\overline{\xi(2Y,b)}+\xi(2Y,b)\overline{\xi^3(2Y,b)})i^{\mathrm{T}(2Yc+2bd)}\\
&= 2^{2m+2}\sum_{Y\in\mathcal{T}}\sum_{b\in\mathbb{F}_q^*}(1+(-1)^{\mathrm{tr}(yb^{-1/3}+1)})(-1)^{\mathrm{tr}(ys+bd)}\\
&= 2^{2m+2}\sum_{b\in\mathbb{F}_q^*}(-1)^{\mathrm{tr}(bd+1)}\sum_{Y\in\mathcal{T}}(-1)^{\mathrm{tr}(y(b^{-1/3}+s))}\\
&= 2^{3m+2}(-1)^{\mathrm{tr}(s^{-3}d+1)}
\end{aligned}$$

最后我们计算

$$\mathbf{F}(c,d)_4 = \xi^3(0,0)\overline{\xi(0,0)}+\xi(0,0)\overline{\xi^3(0,0)} = 2^{4m+1}.$$

将式子 $\mathbf{F}(c,d)_1, \mathbf{F}(c,d)_2, \mathbf{F}(c,d)_3$ 和 $\mathbf{F}(c,d)_4$ 加起来证明了我们的结论. □

类似地，我们可以证明下面的结果.

引理 4.14: 令 $c \in 2R$ 和 $d \in \mathbb{F}_q$. 我们有

$$\mathbf{F}(c,d) = \begin{cases} 2^{3m+2}(3\cdot 2^{m-1}-1), & \text{若 } d=0;\\ 2^{3m+2}(2^{m-1}-1), & \text{若 } d\neq 0. \end{cases}$$

5 偶特征的伪平面二项式函数及其相关的结合方案

5.1 引言

给定奇素数 p 和正整数 n. 令 $q = p^n$. 给定函数 $f : \mathbb{F}_q \to \mathbb{F}_q$. 若对任一 $\epsilon \in \mathbb{F}_q^*$, 映射

$$x \to f(x+\epsilon) - f(x) \tag{5.1}$$

都是 $\mathbb{F}_q$ 上的置换，则称 f 是一个 *平面函数*（planar function）. 为了构造奇特征有限域上的射影平面，Dembowski 和 Ostrom[28] 引进了平面函数的概念. 在密码学中，平面函数也被称作 *完全非线性函数*（perfect nonlinear functions）[72]. 基于其对差分攻击的最优抵抗性，人们将它们用于构造类似 DES 的迭代密码系统. Carlet、Ding 和 Yuan[21,29,95] 等研究者则利用平面函数构造纠错码，然后将其用于设计秘密分享方案. 平面函数还被用于构造验证码[30]、常重复合码[34] 和信号集[33]. 它们还被用于构造一些组合结构，比如斜 Hadamard 差集和 Paley 型的部分差集[93].

对于 $p = 2$ 的情形，不存在有限域 $\mathbb{F}_{2^n}$ 上的平面函数：因为若 x 满足 $f(x+\epsilon) - f(x) = d$，则 $x + \epsilon$ 亦满足. 此时我们称一个函数 $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ 是 *几乎完全非线性的*（almost perfect nonlinear），若对任一 $\epsilon \in \mathbb{F}_{2^n}^*$ 映射 (5.1) 都是 2-到-1 的. 遗憾的是，几乎完全非线性函数和有限射影平面没有多少直接的联系. 直到最近，Zhou[97] 在偶特征的有限域上提出了一个新的“平面函数”的定义，由它我们可以得到有限射影平面. 从现在开始，我们将称一个函数 $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ 是 *伪平面的*（pseudo-planar），若对任一 $\epsilon \in \mathbb{F}_{2^n}^*$，

$$x \to f(x+\epsilon) + f(x) + \epsilon x$$

均为 $\mathbb{F}_{2^n}$ 上的置换. 需要注意的是，Zhou[97] 起先称这样的函数为“平面函数”，“伪平面函数”这个叫法最早是 Abdukhalikov[1] 提出的，以示与奇特征的平面函数有所区别.

Schmidt 和 Zhou[80] 及 Scherr 和 Zieve[79] 已经考察过伪平面单项式函数. 我们将他们得到的结果列在表 5.1 中，这里 $\mathrm{T}_{n/2}$ 表示从 $\mathbb{F}_{2^{n/2}}$ 到 $\mathbb{F}_2$ 的迹函数. 在这一章中

表 5.1　已知的 $\mathbb{F}_{2^n}$ 上的伪平面函数

函数	条件	出处
ax^{2^k}	$a \in \mathbb{F}_{2^n}^*$	平凡的
ax^{2^k+1}	$n=2k, a \in \mathbb{F}_{2^{n/2}}^*, \mathrm{T}_{n/2}(a)=0$	定理 6[80]
$ax^{4^k(4^k+1)}$	$n=6k$, $a \in \mathbb{F}_{2^n}^*$, a 是 (4^k-1) 次幂但不是 $3(4^k-1)$ 次幂	定理 1.1[79]

我们将构造三类新的伪平面二项式函数，其中的两类是无穷类. 另外我们发现任一伪平面函数都将给出一个定义在 Galois 环上的 5-类结合方案. 我们的结果可以看作是 Liebler 和 Mena[58] 及 Bonnecaze 和 Duursma[13] 等人结果的推广. Abdukhalikov、Bannai 和 Suda[2] 及 LeCompte、Martin 和 Owens[55] 也构造过类似的 4 类结合方案.

本章的结构安排如下：在第 5.2 中我们介绍相关的预备知识. 在第 5.3 节中我们将构造三类新的伪平面二项式函数. 在第 5.4 中我们来考察与伪平面函数相关的结合方案. 在第 5.5 节中给一个总结.

5.2　预备知识

给定一个有限 Abel 群 G 和它的子群 N. 一个 G 的子集 D 称作是 G 中相对于 N 的 $(|G|/|N|, |N|, |D|, \lambda)$ **相对差集**，如果每个元素 $g \in G\backslash N$ 都能够表示成 $g_1 g_2^{-1}, (g_1, g_2 \in D, g_1 \neq g_2)$ 的形式恰好 λ 次. 利用群环的语言可知： D 是 G 中相对于子集 N 的差集当且仅当

$$DD^{(-1)} = |D|1_G + \lambda(G - N),$$

其中 1_G 是 G 的单位元.

对于群环 $\mathbb{Z}[G]$ 中的任一元素 $A = \sum d_g g$，在这一章中我们将用 $[A]_0$ 来代表 d_{1_G}. 下面我们再回顾一下我们在第 3 章中给出的反演公式.

引理 5.1: 给定一个有限 Abel 群 G. 若 $A = \sum_{g\in G} d_g g \in \mathbb{Z}[G]$，则

$$d_h = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(A)\chi(h^{-1}),$$

其中 $h \in G$. 特别地，我们有

$$[A]_0 = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(A).$$

有关 Galois 环的相关知识，请参加第 4.2.2 节中的内容.

5.3 伪平面二项式函数

不难验证每个从 $\mathbb{F}_{2^n}$ 到自身的函数都可以唯一地表示成一个次数至多为 $2^n - 1$ 的多项式函数. 单项式函数 $x \mapsto cx^t$ ($c \in \mathbb{F}_{2^n}, t \in \mathbb{Z}$) 则是最简单的非平凡多项式函数. 若存在 $c \in \mathbb{F}_{2^n}^*$ 使得函数 $x \mapsto cx^t$ 在 $\mathbb{F}_{2^n}$ 上是伪平面的，则称整数 $t(1 \leq t \leq 2^n - 1)$ 是一个 伪平面指数 (pseudo-planar exponent). Schmidt 和 Zhou[80] 猜想 所有的伪平面指数就只是表 5.1 中所列的那三类.

除却伪平面单项式函数之外，第二简单的函数就是伪平面二项式函数. 接下来，我们将在 $\mathbb{F}_{2^{3m}}$ 上构造三类伪平面二项式函数. 下面的结论将是我们的主要的证明工具.

引理 5.2 (p. 362[59]): 给定素数幂 q. 令 $\mathbb{F}_{q^r}$ 为 $\mathbb{F}_q$ 的扩域. 则线性多项式

$$L(x) = \sum_{i=0}^{r-1} c_i x^{q^i} \in \mathbb{F}_{q^r}[x]$$

是 $\mathbb{F}_{q^r}$ 上的置换当且仅当

$$\det \begin{pmatrix} c_0 & c_{r-1}^q & c_{r-2}^{q^2} & \cdots & c_1^{q^{r-1}} \\ c_1 & c_0^q & c_{r-1}^{q^2} & \cdots & c_2^{q^{r-1}} \\ c_2 & c_1^q & c_0^{q^2} & \cdots & c_3^{q^{r-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{r-1} & c_{r-2}^q & c_{r-3}^{q^2} & \cdots & c_0^{q^{r-1}} \end{pmatrix} \neq 0.$$

给定任一正整数 m. 我们记从 $\mathbb{F}_{2^{3m}}$ 到 $\mathbb{F}_{2^m}$ 的相对迹（范数）为 T_3（N_3）.

命题 5.1: 给定任一偶数 $m > 0$. 则函数

$$f(x) = a^{2^{2m}+1} x^{2^{2m}+1} + a^{-(2^m+1)} x^{2^m+1}$$

在 $\mathbb{F}_{2^{3m}}$ 上是伪平面的当且仅当

$$\mathrm{T}_3((a^{2^{2m}+2^m}+a^{-2^{2m}-2^m-2})(a^{2^m+1}+\epsilon^{2^m-1})\epsilon^{2^m+2}+a^{2^m-2^{2m}}\epsilon^3+\epsilon)\neq 0$$

对任一 $\epsilon\in\mathbb{F}_{2^{3m}}^*$ 都成立.

证明. 令 $t=2^m$. 对任一 $\epsilon\in\mathbb{F}_{2^{3m}}^*$，我们有

$$f(x+\epsilon)+f(x)+\epsilon x=a^{t^2+1}\epsilon x^{t^2}+a^{-(t+1)}\epsilon x^t+(a^{t^2+1}\epsilon^{t^2}+a^{-(t+1)}\epsilon^t+\epsilon)x+(a\epsilon)^{t^2+1}+(a^{-1}\epsilon)^{t+1}.$$

于是我们只需证明：对任一 $\epsilon\in\mathbb{F}_{2^{3m}}^*$，

$$G_\epsilon(x):=a^{t^2+1}\epsilon x^{t^2}+a^{-(t+1)}\epsilon x^t+(a^{t^2+1}\epsilon^{t^2}+a^{-(t+1)}\epsilon^t+\epsilon)x$$

都是 $\mathbb{F}_{2^{3m}}$ 上的置换. 根据引理 5.2，可知 $G_\epsilon(x)$ 是一个置换当且仅当

$$\begin{aligned}
&\det\begin{pmatrix} a^{t^2+1}\epsilon^{t^2}+a^{-(t+1)}\epsilon^t+\epsilon & a^{t+1}\epsilon^t & a^{-(t^2+1)}\epsilon^{t^2} \\ a^{-(t+1)}\epsilon & a^{t+1}\epsilon+a^{-(t^2+t)}\epsilon^{t^2}+\epsilon^t & a^{t^2+t}\epsilon^{t^2} \\ a^{t^2+1}\epsilon & a^{-(t^2+t)}\epsilon^t & a^{t^2+t}\epsilon^t+a^{-(t^2+1)}\epsilon+\epsilon^{t^2} \end{pmatrix} \\
=&\mathrm{T}_3((a^{t^2+t}+a^{-t^2-t-2})(a^{t+1}+\epsilon^{t-1})\epsilon^{t+2}+a^{t-t^2}\epsilon^3+\epsilon) \\
=&\mathrm{T}_3((a^{2^{2m}+2^m}+a^{-2^{2m}-2^m-2})(a^{2^m+1}+\epsilon^{2^m-1})\epsilon^{2^m+2}+a^{2^m-2^{2m}}\epsilon^3+\epsilon) \\
\neq&0.
\end{aligned}$$

由此我们证明了结论. □

注：我们目前还不能简化命题 5.1 中的充要条件. 我们也无法判断这个构造是否会给出无穷多的伪平面二项式函数.

下面我们举两个例子. 对任一 $a\in\mathbb{F}_{2^n}^*$，记 $\mathrm{ord}\,(a)$ 为元素 a 的乘法阶.

例 5.1：令 $m=2$. 通过计算机验证可知

$$f(x)=a^{17}x^{17}+a^{-5}x^5$$

在 $\mathbb{F}_{2^{3m}}$ 上是伪平面的当且仅当 $\mathrm{ord}\,(a)\in\{9,63\}$.

例 5.2：令 $m=4$. 通过计算机验证可知

$$f(x)=a^{257}x^{257}+a^{-17}x^{17}$$

在 $\mathbb{F}_{2^{3m}}$ 上是伪平面的当且仅当 $\mathrm{ord}\,(a)\in\{9,63,117,819\}$.

接下来，我们将构造两个无穷类的伪平面二项式函数.

给定任一正整数 m. 设 $\epsilon \in \mathbb{F}_{2^{3m}}^* \backslash \mathbb{F}_{2^m}$ 且它在 $\mathbb{F}_{2^m}$ 上的极小多项式为

$$C_\epsilon(x) = x^3 + B_1 x^2 + B_2 x + B_3 \in \mathbb{F}_{2^m}[x] \quad (B_3 \neq 0).$$

记 $C_\epsilon(x)$ 的三个根为 $x_1(=\epsilon)$、$x_2(=\epsilon^{2^m})$ 和 $x_3(=\epsilon^{2^{2m}})$. 于是

$$\begin{aligned} B_1 =& x_1 + x_2 + x_3 = \mathrm{T}_3(\epsilon), \\ B_2 =& x_1x_2 + x_1x_3 + x_2x_3, \\ B_3 =& x_1x_2x_3 = \mathrm{N}_3(\epsilon). \end{aligned}$$

直接计算

$$\begin{aligned} \mathrm{T}_3(\epsilon^3) =& x_1^3 + x_2^3 + x_3^3 \\ =& (x_1 + x_2 + x_3)^3 + x_1x_2x_3 + (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) \\ =& B_1^3 + B_3 + B_1B_2, \\ \mathrm{T}_3(\epsilon^{1+2^{m+1}}) =& \mathrm{T}_3(x_1x_2^2) = x_1x_2^2 + x_2x_3^2 + x_3x_1^2. \end{aligned}$$

记 $u_1 = \mathrm{T}_3(x_1x_3^2)$ 和 $u_2 = \mathrm{T}_3(x_1x_2^2)$. 则我们有

$$u_1 + u_2 = B_3 + B_1B_2, \tag{5.2}$$

$$u_1u_2 = B_1^3B_3 + B_2^3 + B_3^2. \tag{5.3}$$

命题 5.2：给定任一正整数 m. 设 $m \not\equiv 2 \pmod 3$. 则

$$f(x) = x^{2^m+1} + x^{2^{2m}+2^m}$$

在 $\mathbb{F}_{2^{3m}}$ 上是伪平面的.

证明. 与命题 5.1 中的分析类似，我们不难验证 f 是伪平面的当且仅当对任一 $\epsilon \in \mathbb{F}_{2^{3m}}^*$，都成立

$$\mathrm{N}_3(\epsilon) + \mathrm{T}_3(\epsilon^3 + \epsilon^{1+2^{m+1}}) \neq 0.$$

为了方便，我们记 $M_\epsilon = \mathrm{N}_3(\epsilon) + \mathrm{T}_3(\epsilon^3 + \epsilon^{1+2^{m+1}})$.

首先设 $\epsilon \in \mathbb{F}_{2^m}^*$. 于是 $M_\epsilon = \mathbf{N}_3(\epsilon) + \mathbf{T}_3(\epsilon^3 + \epsilon^3) = \mathbf{N}_3(\epsilon) \neq 0$.

现在设 $\epsilon \in \mathbb{F}_{2^{3m}}^* \backslash \mathbb{F}_{2^m}$. 容易验证

$$M_\epsilon = B_1^3 + B_1 B_2 + u_2.$$

下面我们将根据 B_1 是否等于 0 分成两种情形来进行讨论.

设 $B_1 = 0$. 则 $M_\epsilon = u_2$. 若 $M_\epsilon = 0$，则根据 (5.3) 可知 $B_3 = B_2^{3/2}$. 因此 $B_2 \neq 0$，如若不然则 $B_1 = B_2 = B_3 = 0$，而这是不可能的. 将式子 $B_3 = B_2^{3/2}$ 代入 $C_\epsilon(x)$ 中，我们得到

$$\left(\frac{\epsilon}{B_2^{1/2}}\right)^3 + \frac{\epsilon}{B_2^{1/2}} + 1 = 0.$$

由此推出

$$\frac{\epsilon}{B_2^{1/2}} \in \mathbb{F}_{2^3}.$$

也就是说 $\epsilon = b\beta$，其中 $\beta := B_2^{1/2} \in \mathbb{F}_{2^m}^*$，$b := \epsilon / B_2^{1/2} \in \mathbb{F}_{2^3}^*$. 若 $m \equiv 0 \pmod 3$，则 $b \in \mathbb{F}_{2^3}^* \subseteq \mathbb{F}_{2^m}$，故 $\epsilon \in \mathbb{F}_{2^m}$，而这是不可能的. 若 $m \equiv 1 \pmod 3$，则 $2^m \equiv 2 \pmod 7$，$2^{m+1} \equiv 2^{2m} \equiv 4 \pmod 7$. 于是

$$\begin{aligned}\mathbf{T}_3(\epsilon^3) =& \mathbf{T}_3((b\beta)^3) = \beta^3 \mathbf{T}_3(b^3),\\ \mathbf{T}_3(\epsilon^{1+2^{m+1}}) =& \mathbf{T}_3(b^{1+2^{m+1}} \beta^{1+2^{m+1}}) = \beta^3 \mathbf{T}_3(b^5) = \beta^3 \mathbf{T}_3(b^3).\end{aligned}$$

所以

$$M_\epsilon = \mathbf{N}_3(\epsilon) + \mathbf{T}_3((b\beta)^3 + (b\beta)^{1+2^{m+1}}) = \mathbf{N}_3(\epsilon) \neq 0$$

而这与我们的假设矛盾.

现在设 $B_1 \neq 0$. 不失一般性，令 $B_1 = 1$. 假设 $M_\epsilon = 1 + B_2 + u_2 = 0$，则 $u_2 = B_2 + 1$. 将其代入 (5.2) 和 (5.3) 中得到 $u_1 = B_3 + 1$ 和

$$B_2^3 + B_3^2 + B_2 B_3 + B_2 + 1 = 0. \tag{5.4}$$

若 $B_2 = 0$，则 $B_3 = 1$，

$$\epsilon^3 + \epsilon^2 + 1 = 0.$$

与前面类似，我们可以得到 $M_\epsilon = \mathbf{N}_3(\epsilon) \neq 0$，而这也与我们的假设 $M_\epsilon = 0$ 矛盾. 若 $B_2 \neq 0$，我们记 $w = (B_3+1)/B_2$. 则 (5.4) 化为 $B_2 = w^2 + w$. 所以 $B_3 = B_2 w + 1 = w^3 + w^2 + 1$. 此时 $C_\epsilon(x)$ 可以写成

$$x^3 + x^2 + (w^2+w)x + (w^3+w^2+1) = 0. \tag{5.5}$$

记多项式 x^3+x+1 在 $\mathbb{F}_{2^m}$ 中的三个根分别为 τ_1、$\tau_2(=\tau_1^2)$、$\tau_3(=\tau_1^4)$. 直接计算

$$\begin{aligned}
&(\tau_2+\tau_1 w+1)^3 + (\tau_2+\tau_1 w+1)^2 + B_2(\tau_2+\tau_1 w+1) + B_3\\
=&(\tau_1^3+\tau_1+1)w^3 + (\tau_2\tau_1^2+\tau_2+\tau_1)w^2 + (\tau_2^2\tau_1+\tau_2+\tau_1+1)w + \tau_2^3+\tau_2+1\\
=&0.
\end{aligned}$$

因此元素 $\tau_2+\tau_1 w+1$ 是 $C_\epsilon(x)$ 的一个根. 若 $m \equiv 0 \pmod 3$，则 $\tau_i\,(1 \le i \le 3) \in \mathbb{F}_{2^3} \subseteq \mathbb{F}_{2^m}$. 从而 $\tau_2+\tau_1 w+1 \in \mathbb{F}_{2^m}$. 而这与 $C_\epsilon(x)$ 在 $\mathbb{F}_{2^m}$ 上不可约矛盾. 若 $m \equiv 1 \pmod 3$，则

$$\begin{aligned}
\mathbf{T}_3(\epsilon^3) =&\mathbf{T}_3((\tau_2+\tau_1 w+1)^3)\\
=&(\tau_2+\tau_1 w+1)^3 + (\tau_2+\tau_1 w+1)^{3\cdot 2^m} + (\tau_2+\tau_1 w+1)^{3\cdot 2^{2m}}\\
=&(\tau_2+\tau_1 w+1)^3 + (\tau_3+\tau_2 w+1)^3 + (\tau_1+\tau_3 w+1)^3\\
=&(\tau_1^3+\tau_2^3+\tau_3^3)w^3 + (\tau_1^2\tau_2+\tau_2^2\tau_3+\tau_3^2\tau_1+\tau_1^2+\tau_2^2+\tau_3^2)w^2\\
&+(\tau_1\tau_2^2+\tau_2\tau_3^2+\tau_3^2\tau_1^2+\tau_1+\tau_2+\tau_3)w\\
&+(\tau_1^3+\tau_2^3+\tau_3^3+\tau_1^2+\tau_2^2+\tau_3^2+\tau_1+\tau_2+\tau_3+1)\\
=&w^3+w^2,\\
\mathbf{T}_3(\epsilon^{1+2^{m+1}}) =&\mathbf{T}_3((\tau_2+\tau_1 w+1)^{1+2^{m+1}})\\
=&\mathbf{T}_3((\tau_2+\tau_1 w+1)(\tau_1+\tau_3 w^2+1))\\
=&(\tau_1\tau_2+\tau_2\tau_3+\tau_3\tau_1)w^3 + (\tau_1\tau_2+\tau_2\tau_3+\tau_3\tau_1+\tau_1+\tau_2+\tau_3)w^2\\
&+(\tau_1^2+\tau_2^2+\tau_3^2+\tau_1+\tau_2+\tau_3)w + (\tau_1\tau_2+\tau_2\tau_3+\tau_3\tau_1+1)\\
=&w^3+w^2.
\end{aligned}$$

所以

$$M_\epsilon = \mathbf{N}_3(\epsilon) + \mathbf{T}_3(\epsilon^3+\epsilon^{1+2^{m+1}}) = \mathbf{N}_3(\epsilon) \neq 0,$$

而这也与我们的假设矛盾. 由此我们证明了 M_ϵ 总是不等于 0. □

注：在命题 5.2 中令 $m \equiv 2 \pmod 3$. 设 $\epsilon \in \mathbb{F}_{2^{3m}}$ 且满足 $\epsilon^3 + \epsilon^2 + 1 = 0$. 直接计算 $M_\epsilon = N_3(\epsilon) + \mathrm{T}_3(\epsilon^3 + \epsilon^{1+2^{m+1}}) = \sum_{i=0}^{6} \epsilon^i = 0$. 所以 $f(x) = x^{2^m+1} + x^{2^{2m}+2^m}$ 在 $\mathbb{F}_{2^{3m}}$ 上不是伪平面的.

命题 5.3：给定任一正整数 m. 设 $m \not\equiv 1 \pmod 3$. 则

$$f(x) = x^{2^{2m}+1} + x^{2^{2m}+2^m}$$

在 $\mathbb{F}_{2^{3m}}$ 上是伪平面的.

证明. 通过与命题 5.1 类似的分析可知 f 是伪平面的当且仅当

$$\mathrm{N}_3(\epsilon) + \mathrm{T}_3(\epsilon^3 + \epsilon^{2+2^m}) \neq 0$$

对任一 $\epsilon \in \mathbb{F}_{2^{3m}}^*$ 都成立. 剩下的讨论则与命题 5.2 一样. □

5.4 5 类结合方案的构造

令 $R = GR(4, n)$ 为一个 Galois 环. 对任一 R 中集合 A（A 可以是多重集），我们将把 A 与群环元素 $\sum_{g \in A} d_g g \in \mathbb{Z}[R]$ 等同起来，其中 d_g 是 $g \in A$ 的重数. 众所周知，Teichmüller 系 $\mathcal{T}$ 是 R 中相对于 Z 的一个 $(2^n, 2^n, 2^n, 1)$-RDS，其中

$$Z = \{2x \mid x \in R\}.$$

Bonnecaze 和 Duursma[13] 证明了 $\mathcal{T}$ 将给出一个结合方案. 具体来说，当 $n \geq 3$ 时，我们有四个不相交的集合

$$\Omega_0 = \{0\},\ \Omega_1 = \mathcal{T}^*,\ \Omega_2 = \{-x \mid x \in \Omega_1\},\ \Omega_3 = Z \setminus \{0\},$$

其中 $\mathcal{T}^* := \mathcal{T} \setminus \{0\}$. R 中的剩余元素将被分成两个集合. 令 Ω_4 包含那些在多重集 $\mathcal{T}^2$ 中出现的剩余元素，而 Ω_5 则包含那些不在多重集 $\mathcal{T}^2$ 中出现的剩余元素. 则划分 $\{\Omega_i \mid 0 \leq i \leq 5\}$ 形成 R 上的一个 Schur 环，从而也就导出一个 5 类结合方案. 对任一伪平面函数 f，集合

$$D_f = \{x + 2\sqrt{f(x)} \mid x \in \mathcal{T}\}$$

同样也是一个 R 中相对于 Z 的 $(2^n, 2^n, 2^n, 1)$-RDS[80]. 所以我们自然要问是否能从 D_f 中得到类似的结合方案. 在这一节中，我们将证明任一从伪平面函数 f 中导出的相对差集 D_f 都会给出一个结合方案. 事实上，我们可以得到 R 的类似划分. 首先我们有四个互不相交的集合

$$\mathcal{S}_0 = \{0\},\ \mathcal{S}_1 = D_f \setminus \{0\},\ \mathcal{S}_2 = \{-x \mid x \in \mathcal{S}_1\} = \mathcal{S}_1^{(-1)},\ \mathcal{S}_3 = Z \setminus \{0\}.$$

然后令 $\mathcal{S}_4$ 那些包含在多重集 D_f^2 中出现的剩余元素而 $\mathcal{S}_5$ 包含那些不出现的剩余元素.

利用引理 4.4 我们可以直接验证 $\{\mathcal{S}_i \mid 0 \le i \le 5\}$ 确实构成 R 的一个划分. 接下来我们考虑 $\{\mathcal{S}_i \mid 0 \le i \le 5\}$ 在特征群 $\widehat{R}$ 上的对偶划分. 根据定理 3[80]，若 f 是伪平面的，则当 χ 遍历 $\widehat{R}$ 中所有特征时，$\chi(D_f)$ 恰取六个值. 具体来说：
当 n 为奇数时，

$$\chi_a(D_f) = \begin{cases} 2^n & \text{若 } a = 0\,, \\ 0 & \text{若 } a \in Z \setminus \{0\}, \\ \pm 2^{(n-1)/2} \pm 2^{(n-1)/2} i & \text{若 } a \in R \setminus Z; \end{cases}$$

当 n 为偶数时，

$$\chi_a(D_f) = \begin{cases} 2^n & \text{若 } a = 0\,, \\ 0 & \text{若 } a \in Z \setminus \{0\}, \\ \pm 2^{n/2} \text{ 或 } \pm 2^{n/2} i & \text{若 } a \in R \setminus Z. \end{cases}$$

定义 5.1：*我们称多重集*

$$\{\chi(D_f) \mid \chi \in \widehat{R}\}.$$

为伪平面函数 f 的 Fourier *谱*（Fourier spectrum）.

作为下面的定理 5.1 的一个直接推论，我们可以看出所有的伪平面函数的 Fourier 谱都是相同的.

易知 $\chi(\mathcal{S}_1) = \chi(D_f) - 1$. 下面我们给出在特征群 $\widehat{R}$ 上的划分：

当 n 为奇数时，

$$\begin{array}{rcl}\mathcal{E}_0 &=& \{\chi_0\},\\ \mathcal{E}_1 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1\}=\{\chi_a\mid a\in Z\setminus\{0\}\},\\ \mathcal{E}_2 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1+2^{(n-1)/2}+2^{(n-1)/2}i\},\\ \mathcal{E}_3 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1+2^{(n-1)/2}-2^{(n-1)/2}i\},\\ \mathcal{E}_4 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1-2^{(n-1)/2}+2^{(n-1)/2}i\},\\ \mathcal{E}_5 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1-2^{(n-1)/2}-2^{(n-1)/2}i\};\end{array} \tag{5.6}$$

当 n 为偶数时，

$$\begin{array}{rcl}\mathcal{E}_0 &=& \{\chi_0\},\\ \mathcal{E}_1 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1\}=\{\chi_a\mid a\in Z\setminus\{0\}\},\\ \mathcal{E}_2 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1+2^{n/2}\},\\ \mathcal{E}_3 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1-2^{n/2}\},\\ \mathcal{E}_4 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1+2^{n/2}i\},\\ \mathcal{E}_5 &=& \{\chi\in\widehat{R}\mid \chi(\mathcal{S}_1)=-1-2^{n/2}i\}.\end{array} \tag{5.7}$$

下面我们证明 $(R,\{\mathcal{S}_i\}_{i=0}^5)$ 是一个 Schur 环，且它的对偶是 $(\widehat{R},\{\mathcal{E}_i\}_{i=0}^5)$. 首先我们将利用引理 5.3 和引理 5.4 证明 $\mathcal{S}_4$ 可以表示成 $\mathcal{S}_1^2,\mathcal{S}_2,\mathcal{S}_3$ 的线性组合. 于是 $\chi(\mathcal{S}_4)$ 与 $\chi(\mathcal{S}_5)$ 的取值情况可以被完全确定. 最后结合 Bannai-Muzychuk 判别方法，我们可以得到结论.

引理 5.3：给定 $R=GR(4,n)$ 和 $\mathbb{F}_{2^n}$ 上的伪平面函数 f，并将其看作是从 $\mathcal{T}$ 到 $\mathcal{T}$ 的函数. 令 $D_f=\{x+2\sqrt{f(x)}\mid x\in\mathcal{T}\}$，$\mathcal{S}_1=D_f\setminus\{0\}$. 则

(i) 多重集 $\mathcal{S}_1\mathcal{S}_1^{(-1)}$ 包含元素 0 的次数为 2^n-1 次，包含集合 $\mathcal{S}_4\cup\mathcal{S}_5$ 中的元素恰一次，且不包含其他的元素；

(ii) 多重集 $\mathcal{S}_1^2$ 包含 $\mathcal{S}_3$ 中元素恰 1 次，包含其他的元素的次数为 0 次或 2 次.

证明. (i) 从 f 是伪平面的，可知集合 D_f 为一个 RDS：$D_fD_f^{(-1)}=2^n\mathcal{S}_0+(R-Z)$. 不难验证 $\mathcal{S}_1\mathcal{S}_1^{(-1)}=(2^n-1)\mathcal{S}_0+(R-Z-\mathcal{S}_1-\mathcal{S}_2)=(2^n-1)\mathcal{S}_0+\mathcal{S}_4+\mathcal{S}_5$.

(ii) 给定任意的 $x,y,z\in\mathcal{T}^*$. 设 $x+2\sqrt{f(x)}+y+2\sqrt{f(y)}=2z$. 则 $x+2\sqrt{f(x)}=y+2(\sqrt{f(y)}\oplus z\oplus y)$. 根据表示的唯一性 (4.1)，可知 $x=y=z$. 所以 $\mathcal{S}_1^2$ 包含 $\mathcal{S}_3$ 中元素的次数为 1 次. 设 $\mathcal{S}_1^2=\mathcal{S}_3+2U_f$，其中 $U_f=\sum_{g\in R\setminus\mathcal{S}_3}d_gg$. 我们只需证明 $d_g=0$ 或 1. 由于 $\mathcal{S}_1^2=\mathcal{S}_3+2U_f$，对这个式子应用平凡的特征可知

$$\sum_{g\in R\setminus\mathcal{S}_3}d_g=(2^n-1)(2^{n-1}-1). \tag{5.8}$$

下面我们考察元素 0 在 $\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2$ 中的系数. 一方面，$\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2 = (\mathcal{S}_1\mathcal{S}_1^{(-1)})^2 = ((2^n-1)\mathcal{S}_0 + \mathcal{S}_4 + \mathcal{S}_5)^2 = (2^n-1)^2\mathcal{S}_0 + 2(2^n-1)(\mathcal{S}_4+\mathcal{S}_5) + (\mathcal{S}_4+\mathcal{S}_5)^2$. 因为 $\mathcal{S}_4 + \mathcal{S}_5 = \mathcal{S}_4^{(-1)} + \mathcal{S}_5^{(-1)}$，$|\mathcal{S}_4 \cup \mathcal{S}_5| = (2^n-1)(2^n-2)$，我们有 $[(\mathcal{S}_4+\mathcal{S}_5)^2]_0 = (2^n-1)(2^n-2)$. 因此 $[\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2]_0 = (2^n-1)(2^{n+1}-3)$. 另一方面，$\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2 = (\mathcal{S}_3 + 2U_f)(\mathcal{S}_3 + 2U_f^{(-1)}) = \mathcal{S}_3^2 + 2\mathcal{S}_3U_f + 2\mathcal{S}_3U_f^{(-1)} + 4U_fU_f^{(-1)}$. 不难验证 $[\mathcal{S}_1^2(\mathcal{S}_1^{(-1)})^2]_0 = 2^n - 1 + 4\sum_{g\in R\setminus\mathcal{S}_3} d_g^2$. 于是有

$$\sum_{g\in R\setminus\mathcal{S}_3} d_g^2 = (2^n-1)(2^{n-1}-1). \tag{5.9}$$

根据 (5.8)-(5.9)，我们有

$$\sum_{g\in R\setminus\mathcal{S}_3} d_g = \sum_{g\in R\setminus\mathcal{S}_3} d_g^2,$$

也就推出 $d_g = 0$ 或 1.

□

现在我们来决定引理 5.3 中的 U_f.

引理 5.4: 给定 $R = GR(4,n)$ 和 $\mathbb{F}_{2^n}$ 上的伪平面函数 f. 令 $\mathcal{S}_i, 0 \le i \le 5$ 如上所定义. 则

(i) 当 n 为奇数时，$\mathcal{S}_1^2 = \mathcal{S}_3 + 2\mathcal{S}_4$;

(ii) 当 n 为偶数时，$\mathcal{S}_1^2 = \mathcal{S}_3 + 2\mathcal{S}_2 + 2\mathcal{S}_4$.

证明. 我们将只给出结论 (ii) 的证明，因为类似的方法同样适用于结论 (i). 此时的划分 $\{\mathcal{E}_i \mid 0 \le i \le 5\}$ 由 (5.7) 中所定义. 记 $m_i = |\mathcal{E}_i|$，$0 \le i \le 5$. 则 $m_0 = 1$，$m_1 = 2^n - 1$. 我们首先来考察 m_2, m_3, m_4, m_5 之间的关系. 通过直接计算可以看出 $\sum_{a\in R}\chi_a(D_f) = 2^{2n}$. 另一方面，

$$\begin{aligned}\sum_{a\in R}\chi_a(D_f) &= m_0\cdot 2^n + m_1\cdot 0 + m_2\cdot 2^{n/2} + m_3\cdot(-2^{n/2}) + m_4\cdot 2^{n/2}i + m_5\cdot(-2^{n/2}i)\\ &= 2^n + 2^{n/2}(m_2-m_3) + 2^{n/2}(m_4-m_5)i.\end{aligned}$$

整理可得

$$m_2 - m_3 = 2^{3n/2} - 2^{n/2},$$

$$m_4 - m_5 = 0.$$

根据引理 5.3，可知 $\mathcal{S}_1^2 = \mathcal{S}_3 + 2U_f$. 对任一 $x, y \in \mathcal{T}$，若 $x+2\sqrt{f(x)}+y+2\sqrt{f(y)} = 0$，则 $x = y + 2(\sqrt{f(x)} \oplus \sqrt{f(y)} \oplus y)$. 由此推出 $x = y = 0$. 所以元素 0 不出现在 $\mathcal{S}_1^2$ 中，即 $U_f \cap \mathcal{S}_0 = \emptyset$. 根据定义可以看出 $\mathcal{S}_4 \subset U_f$，$\mathcal{S}_5 \cap U_f = \emptyset$. 最后我们来考察 $\mathcal{S}_1, \mathcal{S}_2, U_f$ 之间的关系.

先来考察 $\mathcal{S}_1$. 通过反演公式可知

$$\begin{aligned}
[D_f^2 D_f^{(-1)}]_0 &= \frac{1}{|R|}\sum_{a\in R}\chi_a(D_f^2 D_f^{(-1)}) \\
&= \frac{1}{|R|}\sum_{a\in R}|\chi_a(D_f)|^2\chi_a(D_f) \\
&= \frac{1}{|R|}(2^{3n} + 2^{3n/2}(m_2 - m_3) + 2^{3n/2}(m_4 - m_5)i) \\
&= 2^{n+1} - 1.
\end{aligned}$$

注意到

$$D_f^2 D_f^{(-1)} = \mathcal{S}_1^2\mathcal{S}_1^{(-1)} + 2\mathcal{S}_1\mathcal{S}_1^{(-1)} + \mathcal{S}_1^2 + 2\mathcal{S}_1 + \mathcal{S}_2 + \mathcal{S}_0,$$

$[\mathcal{S}_1\mathcal{S}_1^{(-1)}]_0 = 2^n - 1$，$[\mathcal{S}_0]_0 = 1$. 由此推出 $[\mathcal{S}_1^2\mathcal{S}_1^{(-1)}]_0 = 0$. 所以 $\mathcal{S}_1^2$ 不包含 $\mathcal{S}_1$ 中任一元素，即 $\mathcal{S}_1 \cap U_f = \emptyset$.

再来考察 $\mathcal{S}_2$. 根据反演公式可知

$$\begin{aligned}
[D_f^3]_0 &= \frac{1}{|R|}\sum_{a\in R}\chi_a(D_f)^3 \\
&= \frac{1}{|R|}(2^{3n} + 2^{3n/2}(m_2 - m_3) - 2^{3n/2}(m_4 - m_5)i) \\
&= 2^{n+1} - 1.
\end{aligned}$$

根据

$$D_f^3 = (\mathcal{S}_0 + \mathcal{S}_1)^3 = \mathcal{S}_0 + 3\mathcal{S}_1 + 3\mathcal{S}_1^2 + \mathcal{S}_1^3,$$

$[\mathcal{S}_0]_0 = 1$，$[\mathcal{S}_1]_0 = [\mathcal{S}_1^2]_0 = 0$，可知 $[\mathcal{S}_1^2\mathcal{S}_2^{(-1)}]_0 = [\mathcal{S}_1^3]_0 = 2^{n+1} - 2$. 应用引理 5.3 推出 $\mathcal{S}_1^2$ 包含 $\mathcal{S}_2$ 中任一元素的次数至多为两次. 另一方面，$[\mathcal{S}_1^2\mathcal{S}_2^{(-1)}]_0 = 2|\mathcal{S}_2|$. 所以 $\mathcal{S}_2$ 中任一元素都恰在 $\mathcal{S}_1^2$ 中出现两次. 也就证明了：当 n 为偶数时，$\mathcal{S}_1^2 = \mathcal{S}_3 + 2\mathcal{S}_2 + 2\mathcal{S}_4$. □

环 R 上的划分 $\{\mathcal{S}_i \mid 0 \le i \le 5\}$ 自然地诱导了 $R\times R$ 上的划分 $\{\mathcal{R}_i \mid 0 \le i \le 5\}$：

$$\mathcal{R}_i = \{(x, y) \in R \times R \mid x - y \in \mathcal{S}_i\} \quad (0 \le i \le 5).$$

现在我们来证明 $(R, \{\mathcal{R}_i\}_{i=0}^5)$ 确实构成了一个结合方案.

定理 5.1: 给定 $R = GR(4, n)$ 和 $\mathcal{S}_i, 0 \le i \le 5$ 如上所定义. 则 $(R, \{\mathcal{S}_i\}_{i=0}^5)$ 是一个 Schur 环，且它的对偶是 $(\widehat{R}, \{\mathcal{E}_i\}_{i=0}^5)$. 若 $n \ge 3$，则 $(R, \{\mathcal{R}_i\}_{i=0}^5)$ 构成一个 5 类结合方案. 下面我们列出它的第一特征阵：当 n 是奇数时，记 $b = 2^{(n-1)/2}$，则

$$P = \begin{bmatrix} 1 & 2b^2-1 & 2b^2-1 & 2b^2-1 & 2b^4-3b^2+1 & 2b^4-3b^2+1 \\ 1 & -1 & -1 & 2b^2-1 & -b^2+1 & -b^2+1 \\ 1 & -1+b+bi & -1+b-bi & -1 & (1-b)(1-bi) & (1-b)(1+bi) \\ 1 & -1+b-bi & -1+b+bi & -1 & (1-b)(1+bi) & (1-b)(1-bi) \\ 1 & -1-b+bi & -1-b-bi & -1 & (1+b)(1-bi) & (1+b)(1+bi) \\ 1 & -1-b-bi & -1-b+bi & -1 & (1+b)(1+bi) & (1+b)(1-bi) \end{bmatrix}. \tag{5.10}$$

当 n 是偶数时，记 $b = 2^{(n-2)/2}$，则

$$P = \begin{bmatrix} 1 & 4b^2-1 & 4b^2-1 & 4b^2-1 & 8b^4-10b^2+2 & 8b^4-2b^2 \\ 1 & -1 & -1 & 4b^2-1 & -2b^2+2 & -2b^2 \\ 1 & 2b-1 & 2b-1 & -1 & 2b^2-4b+2 & -2b^2 \\ 1 & -2b-1 & -2b-1 & -1 & 2b^2+4b+2 & -2b^2 \\ 1 & -1+2bi & -1-2bi & -1 & -2b^2+2 & 2b^2 \\ 1 & -1-2bi & -1+2bi & -1 & -2b^2+2 & 2b^2 \end{bmatrix}. \tag{5.11}$$

第二特征阵可以在附录 5.6 中找到.

证明. 依据 Bannai-Muzychuk 判别法，只需证明对任意的 $\chi_j \in \mathcal{E}_j$，$\chi_j(\mathcal{S}_i)$ 都等于常数，其中 $0 \le i, j \le 5$. 容易直接验证 $0 \le j \le 5, 0 \le i \le 3$ 的情形. 再根据引理 5.4，我们可以对 $0 \le j \le 5$ 计算出 $\chi_j(\mathcal{S}_4)$ 的值. 于是也就得到了 $\chi_j(\mathcal{S}_5)$ 的值，从而完成了证明. □

注： (i) 当 $n = 1$ 时，$\mathcal{S}_4 = \mathcal{S}_5 = \emptyset$. 此时 $(R, \{\mathcal{R}_i\}_{i=0}^5)$ 是一个 3 类结合方案. 当 $n = 2$ 时，我们有 $\mathcal{S}_4 = \emptyset$. 此时 $(R, \{\mathcal{R}_i\}_{i=0}^5)$ 是一个 4 类结合方案.

(ii) Bonnecaze 和 Duursma[13] 得到的 5 类结合方案可以看作是我们的构造的特殊情况，其中取 $f = 0$.

推论 5.1: 给定 $\mathbb{F}_{2^n}$ 上的一个伪平面函数 f. 则它的 Fourier 谱 $\{\chi(D_f) \mid \chi \in \widehat{R}\}$ 如表 5.2 和表 5.3 中所示.

表 5.2　Fourier 谱，n 为奇数，$b = 2^{(n-1)/2}$

值	重数
$2b^2$	1
0	$2b^2-1$
$b+bi$	$\frac{b(2b^3+2b^2-b-1)}{2}$
$b-bi$	$\frac{b(2b^3+2b^2-b-1)}{2}$
$-b+bi$	$\frac{b(2b^3-2b^2-b+1)}{2}$
$-b-bi$	$\frac{b(2b^3-2b^2-b+1)}{2}$

表 5.3　Fourier 谱，n 为偶数，$b = 2^{(n-2)/2}$

值	重数
$4b^2$	1
0	$4b^2-1$
$2b$	$b(4b^3+4b^2-b-1)$
$-2b$	$b(4b^3-4b^2-b+1)$
$2bi$	$b^2(4b^2-1)$
$-2bi$	$b^2(4b^2-1)$

证明. 根据附录 5.6 中的第二特征阵可以直接看出. □

5.5　总结

在本章中，我们构造了三类新的伪平面二项式函数. 另外，我们给出了一个从伪平面二项式函数构造 5 类结合方案的方法. 我们的构造方法推广了 Bonnecaze 和 Duursma[13] 的构造.

下面是一些我们没有解决的问题.

(i) 本章中我们构造的伪平面函数都具有形式

$$f(x) = ax^{2^i+2^j} + bx^{2^k+2^l},$$

其中 $i \neq j, k \neq l$ 且 $\{i,j\} \neq \{k,l\}$. 对于 $n \leq 9$，通过计算机穷举搜索，我们发现这种类型的伪平面二项式函数只可能在域 $\mathbb{F}_{2^n} = \mathbb{F}_{2^{3m}}$ 上存在. 因此我们想知道是否这种类型的伪平面二项式函数只可能在满足 $3|n$ 的域 $\mathbb{F}_{2^n}$ 上存在.

(ii) 简化命题 5.1 中的充要条件.

5.6 附录

当 n 是奇数时，结合方案的第二特征阵为：

$$Q=\begin{bmatrix}
1 & 2b^2-1 & \frac{b}{2}\left(2b^3+2b^2-b-1\right) & \frac{b}{2}\left(2b^3+2b^2-b-1\right) & \frac{b}{2}\left(2b^3-2b^2-b+1\right) & \frac{b}{2}\left(2b^3-2b^2-b+1\right)\\
1 & -1 & \frac{b}{2}\left(b^2-1-(b^2+b)i\right) & \frac{b}{2}\left(b^2-1+(b^2+b)i\right) & \frac{b}{2}\left(1-b^2-(b^2-b)i\right) & \frac{b}{2}\left(1-b^2+(b^2-b)i\right)\\
1 & -1 & \frac{b}{2}\left(b^2-1+(b^2+b)i\right) & \frac{b}{2}\left(b^2-1-(b^2+b)i\right) & \frac{b}{2}\left(1-b^2+(b^2-b)i\right) & \frac{b}{2}\left(1-b^2-(b^2-b)i\right)\\
1 & 2b^2-1 & -\frac{b}{2}(1+b) & -\frac{b}{2}(1+b) & \frac{b}{2}(1-b) & \frac{b}{2}(1-b)\\
1 & -1 & -\frac{b}{2}(1+bi) & \frac{b}{2}(-1+bi) & \frac{b}{2}(1+bi) & \frac{b}{2}(1-bi)\\
1 & -1 & \frac{b}{2}(-1+bi) & -\frac{b}{2}(1+bi) & \frac{b}{2}(1-bi) & \frac{b\left(b^2+1\right)}{2(1-bi)}
\end{bmatrix}.$$

当 n 是偶数时，结合方案的第二特征阵为：

$$Q=\begin{bmatrix}
1 & 4b^2-1 & b\left(4b^3-b+4b^2-1\right) & b\left(4b^3-4b^2-b+1\right) & b^2\left(4b^2-1\right) & b^2\left(4b^2-1\right)\\
1 & -1 & b\left(b+2b^2-1\right) & -\left(2b^2-b-1\right)b & -b^2(1+2bi) & b^2(-1+2bi)\\
1 & -1 & b\left(b+2b^2-1\right) & -\left(2b^2-b-1\right)b & b^2(-1+2bi) & -b^2(1+2bi)\\
1 & 4b^2-1 & -b(1+b) & -b(-1+b) & -b^2 & -b^2\\
1 & -1 & b(-1+b) & b(1+b) & -b^2 & -b^2\\
1 & -1 & -b(1+b) & -b(-1+b) & b^2 & b^2
\end{bmatrix}.$$

6 一类从 Hermitian 型图中导出的循环码的重量分布

6.1 引言

给定素数 p 和有限域 $\mathbb{F}_p$ 上长为 l 的循环码 $\mathcal{C}$. 令 A_i 表示 $\mathcal{C}$ 中汉明重量（Hamming weight）等于 i 的码字数目. 关于重量分布 $\{A_0, A_1, \ldots, A_l\}$ 的研究是编码理论中非常重要的课题. 令 $h(x)$ 为 $\mathcal{C}$ 的校验多项式. 我们称 $\mathcal{C}$ 是不可约的（可约的）若 $h(x)$ 在 $\mathbb{F}_p$ 上是不可约的（可约的）. 当 $h(x)$ 可以表示成 $h(x) = h_0(x)h_1(x)\cdots h_{s-1}(x)$，其中 $h_i(x)$ 为 $\mathbb{F}_p$ 上不可约多项式，则码 $\mathcal{C}$ 是一个具有 s 个零点的循环码的对偶码.

McEliece[68] 证明了不可约的循环码的重量分布可以由 Gauss 和表示出来. 因此我们可以利用数论中的技巧来决定循环码的重量分布[40,68,69,87,94]. 遗憾的是，通常情况下计算 Gauss 和是非常困难的. 对于只具有一种非零重量的不可约循环码，Ding 等[32,88,89] 已经给出了很好的刻画. 而只具有两种非零重量的不可约循环码也已经被人们所广泛研究. Schmidt 与 White[81] 给出了一个不可约循环码具有至多两个非零重量的充要条件，并且他们进一步猜测所有的只具有两种非零重量的不可约循环码是由两个无穷类和另外 11 个散在的例子组成. 更多的信息可以在文献[32] 中找到.

对于可约的循环码，它的重量分布的计算则牵涉到指数和的计算. 尽管在一些文献中[31,35,50,61–65,71,96] 可以得到简洁的计算结果，但是通常情况下这都是非常复杂的. 在已知的绝大部分文献中，这类循环码的对偶码都具有两个或三个零点.

在本章中，我们决定了一类可约循环码的重量分布. 特别地，它的对偶码可以具有任意多个零点. 我们的主要工作是建立了相关的指数和与 Hermitian 型图的谱之间的对应关系. 本章的结构安排如下：在第 6.2 节中我们详细地描述了我们将要考察的循环码. 在第 6.3 节中，我们介绍一些与 Cayley 图和 Hermitian 型图相关的预备知识. 在第 6.4 中我们将建立起指数和与 Hermitian 型图的谱之间的对应关系. 由此我们可以直接得到重量分布. 在最后一节中，我们简要地总结了我们的工作.

6.2 循环码 $\mathcal{C}_{(p,m)}$

给定素数 p 和奇数 $m>0$. 令 $n=2m$ 及 $q=p^n$. 记 $t=(m-1)/2$. 记 π 为 $\mathbb{F}_q$ 的一个本原元. 令 $h_0(x)$ 为 $\pi^{-(p^m+1)}$ 在 $\mathbb{F}_p$ 上的极小多项式. 不难看出 $\deg h_0(x)=m$. 再令 $h_i(x), 1\le i\le t$ 为 $\pi^{-(p^{2i-1}+1)}$ 在 $\mathbb{F}_p$ 上的极小多项式. 对任一整数 $l>1$ 且 $l|2m$，我们有 $\pi^{-(p^{2i-1}+1)(p^{2m/l}-1)}\neq 1, 1\le i\le t$. 于是 $\deg h_i(x)=n, 1\le i\le t$. 由于 $1\le i<j\le t$，所以不存在正整数 k 使得

$$p^k(p^{2i-1}+1)\equiv p^{2j-1}+1 \pmod{q-1},$$

也就是说元素 $\pi^{-(p^{2i-1}+1)}$ 和 $\pi^{-(p^{2j-1}+1)}$ 在 $\mathbb{F}_p$ 上的极小多项式是互不相同的，即多项式 $h_i(x), 0\le i\le t$ 互不相同.

令 $\mathcal{C}_{(p,m)}$ 为 $\mathbb{F}_p$ 上校验多项式为 $h_0(x)h_1(x)\cdots h_t(x)$ 的循环码. 于是码 $\mathcal{C}_{(p,m)}$ 是一个具有 $t+1$ 个零点的循环码的对偶码，并且 $\dim_{\mathbb{F}_p}\mathcal{C}_{(p,m)}=m^2$. 记 T_i^j 为从 $\mathbb{F}_{p^j}$ 到 $\mathbb{F}_{p^i}$ 的迹映射. 码 $\mathcal{C}_{(p,m)}$ 中的任一码字均可以表示成[27]

$$\mathbf{c}_{[\alpha_0,\alpha_1,\ldots,\alpha_t]}=(c_0,c_1,\ldots,c_{q-2}) \quad (\alpha_0\in\mathbb{F}_{p^m},\alpha_1,\ldots,\alpha_t\in\mathbb{F}_q)$$

其中

$$c_i=\mathrm{T}_1^m(\alpha_0\pi^{i(p^m+1)})+\sum_{j=1}^{t}\mathrm{T}_1^n(\alpha_j\pi^{i(p^{2j-1}+1)}) \ (0\le i\le q-2).$$

于是码字 $\mathbf{c}_{[\alpha_0,\alpha_1,\ldots,\alpha_t]}$ 的汉明重量等于

$$w_H(\mathbf{c})=p^{n-1}(p-1)-\frac{1}{p}\sum_{a\in\mathbb{F}_p^*}T(a\alpha_0,a\alpha_1,\ldots,a\alpha_t),$$

其中

$$T(\alpha_0,\alpha_1,\ldots,\alpha_t)=\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{T}_1^m(\alpha_0x^{p^m+1})+\sum_{j=1}^{t}\mathrm{T}_1^n(\alpha_jx^{p^{2j-1}+1})}.$$

通常情况下，要得到 $T(\alpha_0,\alpha_1,\ldots,\alpha_t), \alpha_0\in\mathbb{F}_{p^m},\alpha_1,\ldots,\alpha_t\in\mathbb{F}_q$ 的值分布是非常困难的，特别是当 t 值较大的时候. 在接下来的这一节中，我们将给出多重集 $\{T(\alpha_0,\alpha_1,\ldots,\alpha_t)\mid \alpha_0\in\mathbb{F}_{p^m},\alpha_1,\ldots,\alpha_t\in\mathbb{F}_q\}$ 和 Hermitian 型图（Hermitian forms graphs）的特征值之间的一个令人意外的联系，由此我们可以大大地简化 $T(\alpha_0,\alpha_1,\ldots,\alpha_t)$ 的计算.

6.3 Cayley 图与 Hermitian 型图

首先我们介绍一些关于 Cayley 图和 Hermitian 型图的结论.

6.3.1 Cayley 图

给定一个有限群 G 和它的一个子集 D. 在 G 上关于连通集（connection set）D 的 Cayley 图 $Cay(G,D)$ 就是顶点集为 G，边集为 $\{(g,h) \mid g,h \in G,\ hg^{-1} \in D\}$ 的有向图.

定义 $D^{(-1)} = \{d^{-1} \mid d \in D\}$. 若 $D = D^{(-1)}$，则 $Cay(G,D)$ 是无向的. 特别地，$Cay(G,D)$ 是 k-正则的（k-regular），这里 $k = |D|$. 若 G 是一个有限 Abel 群，我们容易计算 $Cay(G,D)$ 的特征谱. 对任一 G 的特征 χ，定义 $\chi(D) = \sum_{d\in D}\chi(d)$. 记群 G 的特征群为 $\widehat{G}$. 于是 $|\widehat{G}| = |G|$.

引理 6.1：*设 $\Gamma = Cay(G,D)$ 为有限群 G 上关于连通集 D 的 Cayley 图. 记 $A = A(\Gamma)$ 为图 Γ 的邻接矩阵. 则 G 的每个特征 χ 均给出 A 的一个具有特征值 $\chi(D)$ 的特征向量. 特别地，图 Γ 的谱就是多重集 $\{\chi(D) \mid \chi \in \widehat{G}\}$.*

证明. 设 χ 为 G 的一个特征. 令 e_χ 表示列向量 $(\chi(g))_{g\in G}$. 对任一 $h \in G$，我们有

$$(Ae_\chi)_h = \sum_{g\sim h}\chi(g) = \left(\sum_{d\in D}\chi(d)\right)\chi(h) = \chi(D)\chi(h).$$

所以 e_χ 是 A 的一个具有特征值 $\chi(D)$ 的特征向量. 特征群 $\widehat{G}$ 中所有的特征将给出 $|G|$ 个线性独立的特征向量，因此我们也就得到了 Cayley 图 Γ 的特征谱. □

6.3.2 Hermitian 型图

给定素数幂 r 和向量空间 $V = \mathbb{F}_{r^2}^d$. 对任一 $x \in \mathbb{F}_{r^2}$，它的*共轭元*（conjugate element）$\overline{x}$ 定义为 $\overline{x} = x^r$. 一个 $\mathbb{F}_{r^2}$ 上的矩阵 H 叫作 Hermitian 矩阵若 $H = H^*$ 成立，这里 H^* 是 H 的转置共轭矩阵. 令 $\mathcal{H}$ 代表由所有的 $d \times d$ Hermitian 矩阵在矩阵加法运算下构成的 Abel 群. 不难看出 $|\mathcal{H}| = r^{d^2}$. 向量空间 V 上的 Hermitian 型图（Hermitian forms graph）的顶点集为 $\mathcal{H}$ 中元素，并且点 $H_1, H_2 \in \mathcal{H}$ 是相邻的当且仅当 $rank(H_1 - H_2) = 1$. 等价地说，Hermitian 型图 就是关于 $\mathcal{D} = \{H \in \mathcal{H} \mid$

$rank(H)=1\}$ 的 Cayley 图 $Cay(\mathcal{H},\mathcal{D})$. 一个 $d\times d$ 的秩为 1 的 Hermitian 矩阵 H 可以表示成 $H=\mathbf{a}^T\overline{\mathbf{a}}$，其中 $\mathbf{a}=(a_1,\ldots,a_d)\in V$，$\overline{\mathbf{a}}=(\overline{a_1},\overline{a_2},\ldots,\overline{a_d})$. 因为对于任意的 $\mathbf{a},\mathbf{b}\in V$，$\mathbf{a}^T\overline{\mathbf{a}}=\mathbf{b}^T\overline{\mathbf{b}}$ 成立当且仅当 $\mathbf{a}=\gamma\mathbf{b}$，其中 γ 为某个 $(r+1)$-次单位根，所以我们有 $|\mathcal{D}|=(r^{2d}-1)/(r+1)$.

人们已经知道 V 上的 Hermitian 型图是一类具有经典参数 $(d,b,\alpha,\beta)=(d,-r,-r-1,-(-r)^d-1)$ 的距离正则图（表 6.1[18]）. Stanton[84] 第一个计算了 Hermitian 型图的特征值. 这里我们将应用由 Brower 等[18] 简化了的计算公式. 对任意的整数 $j\geq i\geq 0, b\neq 0,1$，以 b 为基的 Gaussian 二项式系数定义为

$$\begin{bmatrix} j \\ i \end{bmatrix}_b = \begin{cases} \prod_{l=0}^{i-1} \frac{b^j-b^l}{b^i-b^l} & \text{若 } i\geq 1, \\ 1 & \text{若 } i=0. \end{cases}$$

引理 6.2 (推论 8.4.4[18]): 给定素数幂 r 且令向量空间 $V=\mathbb{F}_{r^2}^d$. 则 V 上定义的 Hermitian 型图的特征值为

$$\theta_0=\frac{r^{2d}-1}{r+1},\quad \theta_j=\frac{r^{2d}-1}{r+1}+(-r)^{2d-j}\begin{bmatrix} j \\ 1 \end{bmatrix}_{(-r)},\ 1\leq j\leq d.$$

对应的特征值的重数为

$$f_0=1,\quad f_j=\begin{bmatrix} d \\ j \end{bmatrix}_{(-r)}\prod_{l=0}^{j-1}[(-1)^{d+1}r^d+(-1)^{l+1}r^l],\ 1\leq j\leq d.$$

6.4 码 $\mathcal{C}_{(p,m)}$ 的重量分布

在这一节中，符号 p,q,n,m,t 如第 6.2 中所定义. 我们来考察 Abel 群

$$\mathcal{G}=\mathbb{F}_{p^m}\times\underbrace{\mathbb{F}_q\times\mathbb{F}_q\times\cdots\times\mathbb{F}_q}_{t},$$

及它的子集

$$\mathcal{S}=\left\{(x^{p^m+1},x^{p+1},x^{p^3+1},\ldots,x^{p^{m-2}+1})\mid x\in\mathbb{F}_q^*\right\}.$$

不难看出 $|\mathcal{S}|=(q-1)/(p+1)$. 令 $W=\mathbb{F}_{p^2}^m$，$\mathcal{H}$ 为由 $\mathbb{F}_{p^2}$ 上所有的 $m\times m$ Hermitian 矩阵所组成的 Abel 群. 令 $\mathcal{D}=\{H\in\mathcal{H}\mid rank(H)=1\}$. 则 W 上的 Hermitian 型图就是 Cayley 图 $Cay(\mathcal{H},\mathcal{D})$. 下面的引理指出 Cayley 图 $Cay(\mathcal{G},\mathcal{S})$ 与 $Cay(\mathcal{H},\mathcal{D})$ 具有相同的谱.

引理 6.3: 给定奇数 m. 则 $W = \mathbb{F}_{p^2}^m$ 上的 Hermitian 型图 Γ_1 同构于 Cayley 图 $\Gamma_2 = Cay(\mathcal{G}, \mathcal{S})$. 特别地，$\Gamma_1$ 和 Γ_2 具有相同的谱.

证明. 由于 Γ_1 就是 Cayley 图 $Cay(\mathcal{H}, \mathcal{D})$，所以我们只需证明存在一个从 $\mathcal{H}$ 到 $\mathcal{G}$ 的群同构 φ 使得 $\varphi(\mathcal{D}) = \mathcal{S}$.

设 $e_1, \ldots, e_m$ 为 $\mathbb{F}_q$ 在 $\mathbb{F}_{p^2}$ 上的一组基，且记 $\mathbf{e} = (e_1, e_2, \ldots, e_m)$. 对于任意的 $H \in \mathcal{H}$ 和 $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^m$，定义 $f_H(\mathbf{x}, \mathbf{y}) = \mathbf{x}H\mathbf{y}^T$，其中 $\mathbf{y}^T$ 为 $\mathbf{y}$ 的转置. 现在我们来构造一个从 $\mathcal{H}$ 到 $\mathcal{G}$ 的映射 φ，其将 $H \in \mathcal{H}$ 映到

$$\varphi(H) = (f_H(\mathbf{e}, \mathbf{e}^{p^m}), f_H(\mathbf{e}, \mathbf{e}^p), f_H(\mathbf{e}, \mathbf{e}^{p^3}), \ldots, f_H(\mathbf{e}, \mathbf{e}^{p^{m-2}})).$$

这里我们规定对任意的整数 s，$\mathbf{e}^s := (e_1^s, e_2^s, \ldots, e_m^s)$. 直接验证可知 $\varphi(H) \in \mathcal{G}$ 且 φ 是一个群同态.

下面来证明 φ 事实上是一个群同构. 先来证明 φ 是一个单射. 对于任一矩阵 $H = (h_{ij})$ 和整数 s，记 $H^s = (h_{ij}^s)$. 设 $\varphi(H) = (0, 0, \ldots, 0)$，即 $\mathbf{e}H(\mathbf{e}^{p^m})^T = f_H(\mathbf{e}, \mathbf{e}^{p^m}) = 0$，$\mathbf{e}H(\mathbf{e}^{p^{2i-1}})^T = f_H(\mathbf{e}, \mathbf{e}^{p^{2i-1}}) = 0$，$1 \le i \le t$. 将 $\mathbf{e}H(\mathbf{e}^{p^{2i-1}})^T$ 中所有元素都提升到它的 $p^{2m-2i+1}$ 次幂，我们有

$$\mathbf{e}^{p^{2m-2i+1}} H^{p^{2m-2i+1}} \mathbf{e}^T = \mathbf{e}^{p^{2m-2i+1}} H^p \mathbf{e}^T = 0.$$

于是

$$\mathbf{e}H(\mathbf{e}^{p^{2m-2i+1}})^T = 0.$$

因此 $\mathbf{e}H\Psi = (0, 0, \ldots, 0)$，其中

$$\Psi = ((\mathbf{e}^p)^T, (\mathbf{e}^{p^3})^T, \cdots, (\mathbf{e}^{p^m})^T, \cdots, (\mathbf{e}^{p^{2m-3}})^T, (\mathbf{e}^{p^{2m-1}})^T).$$

从 $\mathbf{e}$ 的定义可知 Ψ 是一个非奇异的矩阵（见推论 2.38[59]）. 所以 $\mathbf{e}H = (0, 0, \ldots, 0)$，从而 H 是零矩阵. 也就是说 φ 是单的. 另一方面，直接验证可知 $|\mathcal{H}| = |\mathcal{G}| = p^{m^2}$. 所以 φ 是一个群同构.

对于任意的 $H \in \mathcal{D}$，我们有 $H = \mathbf{a}^T\mathbf{a}^p$ 对某一 $\mathbf{a} = (a_1, a_2, \ldots, a_m) \in W$ 成立，

其中 $\mathbf{a}^p = (a_1^p, a_2^p, \ldots, a_m^p)$. 因此

$$\begin{aligned}\varphi(H) &= (\mathbf{e}H(\mathbf{e}^{p^m})^T, \mathbf{e}H(\mathbf{e}^p)^T, \ldots, \mathbf{e}H(\mathbf{e}^{p^{m-2}})^T)\\ &= (\mathbf{e}\mathbf{a}^T\mathbf{a}^p(\mathbf{e}^{p^m})^T, \mathbf{e}\mathbf{a}^T\mathbf{a}^p(\mathbf{e}^p)^T, \ldots, \mathbf{e}\mathbf{a}^T\mathbf{a}^p(\mathbf{e}^{p^{m-2}})^T)\\ &= (x^{p^m+1}, x^{p+1}, \ldots, x^{p^{m-2}+1}),\end{aligned}$$

其中 $x = \mathbf{e}\mathbf{a}^T \in \mathbb{F}_q^*$. 于是 $\varphi(\mathcal{D}) \subset \mathcal{S}$. 又因为

$$|\mathcal{D}| = (p^{2m}-1)/(p+1) = (q-1)/(p+1) = |\mathcal{S}|,$$

所以 $\varphi(\mathcal{D}) = \mathcal{S}$. 也就证明了 φ 是一个从 $\mathcal{H}$ 到 $\mathcal{G}$ 的群同构并且将连通集 $\mathcal{D}$ 映到 $\mathcal{S}$. 所以 Γ_1 同构于 Γ_2，从而具有相同的谱. □

从引理 6.3 和引理 6.2 可以得到 Γ_2 特征值及其重数. 另一方面，Γ_2 的特征值可以应用引理 6.1 得到.

注意到

$$\widehat{\mathcal{G}} = \{\chi_{(\alpha_0,\alpha_1,\ldots,\alpha_t)} \mid \alpha_0 \in \mathbb{F}_{p^m}, \alpha_1, \ldots, \alpha_t \in \mathbb{F}_q\},$$

其中

$$\chi_{(\alpha_0,\alpha_1,\ldots,\alpha_t)}(u) = \zeta_p^{\mathrm{T}_1^m(\alpha_0 u_0)+\sum_{j=1}^t \mathrm{T}_1^n(\alpha_j u_j)},\ u = (u_0, u_1, \ldots, u_t) \in \mathcal{G}.$$

根据引理 6.1 可知图 Γ_2 的特征值为

$$\begin{aligned}&\chi_{(\alpha_0,\alpha_1,\ldots,\alpha_t)}(\mathcal{S})\\ &= \sum_{u\in\mathcal{S}} \zeta_p^{\mathrm{T}_1^m(\alpha_0 u_0)+\sum_{j=1}^t \mathrm{T}_1^n(\alpha_j u_j)}\\ &= \frac{1}{p+1}\sum_{x\in\mathbb{F}_q^*} \zeta_p^{\mathrm{T}_1^m(\alpha_0 x^{p^m+1})+\sum_{j=1}^t \mathrm{T}_1^n(\alpha_j x^{p^{2j-1}+1})}\\ &= \frac{1}{p+1}\big(T(\alpha_0, \alpha_1, \ldots, \alpha_t) - 1\big),\end{aligned}$$

其中 $\alpha_0 \in \mathbb{F}_{p^m}, \alpha_1, \ldots, \alpha_t \in \mathbb{F}_q$. 于是我们有

$$T(\alpha_0, \alpha_1, \ldots, \alpha_t) = (p+1)\chi_{(\alpha_0,\alpha_1,\ldots,\alpha_t)}(\mathcal{S}) + 1.$$

再根据引理 6.2 可知 Γ_2 的特征值都是有理数. 所以 $T(\alpha_0,\alpha_1,\ldots,\alpha_t)\in\mathbb{Q}$. 对于任意的 $a\in\mathbb{F}_p^*$，都存在一个自同构 $\sigma_a\in\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ 满足 $\sigma_a(\zeta_p)=\zeta_p^a$. 于是

$$\begin{aligned}\sum_{a\in\mathbb{F}_p^*}T(a\alpha_0,a\alpha_1,\ldots,a\alpha_t) &= \sum_{a\in\mathbb{F}_p^*}\sigma_a\big(T(\alpha_0,\alpha_1,\ldots,\alpha_t)\big)\\ &= (p-1)T(\alpha_0,\alpha_1,\ldots,\alpha_t).\end{aligned}$$

因此 $\mathbf{c}_{[\alpha_0,\alpha_1,\ldots,\alpha_t]}$ 的汉明重量等于

$$\begin{aligned}w_H(\mathbf{c}) &= p^{n-1}(p-1)-\frac{1}{p}\sum_{a\in\mathbb{F}_q^*}T(a\alpha_0,a\alpha_1,\ldots,a\alpha_t)\\ &= p^{n-1}(p-1)-\frac{p-1}{p}T(\alpha_0,\alpha_1,\ldots,\alpha_t)\\ &= p^{n-1}(p-1)-\frac{p-1}{p}\big(1+(p+1)\chi_{(\alpha_0,\alpha_1,\ldots,\alpha_t)}(\mathcal{S})\big).\end{aligned}\tag{6.1}$$

现在我们根据 (6.1) 和引理 6.2 直接计算出码 $\mathcal{C}_{(p,m)}$ 的重量分布. 在下面的定理中，我们用记号 $[l,k,d]$ 码来表示一个 k-维的极小距离等于 d 的线性码.

定理 6.1：给定任一奇数 $m>0$. 码 $\mathcal{C}_{(p,m)}$ 的重量分布为：

$$A_i=\begin{cases}1 & \text{若 } i=0,\\ f_j & \text{若 } i=w_j,\\ 0 & \text{其他情况},\end{cases}$$

其中

$$w_j=(p^{2m}-p^{2m-1})\left(1-\frac{1}{(-p)^j}\right),$$

及

$$f_j=\begin{bmatrix}m\\ j\end{bmatrix}_{(-p)}\prod_{l=0}^{j-1}\big(p^m-(-p)^l\big),$$

$1\le j\le m$. 特别地，码 $\mathcal{C}_{(p,m)}$ 是一个 $[p^{2m}-1,m^2,(p^{2m}-p^{2m-1})(1-p^{-2})]$ 循环码.

对于任一重量分布为 $\{A_0,A_1,\ldots,A_l\}$ 的码 $\mathcal{C}$，定义它的重量计数子（weight enumerator）为

$$\sum_{i=0}^{l}A_ix^i.$$

例 6.1：给定 $p=3$ 和 $m=3$. 码 $\mathcal{C}_{(3,3)}$ 是 GF(3) 上的 $[728,9,432]$ 码，且它的重量计数子为

$$1+5460x^{432}+14040x^{504}+182x^{648}.$$

例 6.2: 给定 $p = 2$ 和 $m = 5$. 码 $\mathcal{C}_{(2,5)}$ 是 GF(2) 上的 $[1023, 25, 384]$ 码，且它的重量计数子为

$$1 + 57970x^{384} + 12985280x^{480} + 18887680x^{528} + 1623160x^{576} + 341x^{768}.$$

6.5 总结

在循环码的研究工作中，学者们已经建立了许多它的重量分布与其他数学结构之间的联系：例如 Gauss 和[36,70]，代数曲线[82,87,91]，二次型[35,61,62] 等等. 在本章中，我们找到了一类循环码的重量分布和一类距离正则图的谱之间的对应关系，并且由此成功地计算出了这类码的重量分布. 这类码的特别之处在于它的对偶码可以具有任意多个零点，而之前人们的结果都集中在两个或三个零点的情况.

参 考 文 献

[1] K. Abdukhalikov, Symplectic spreads, planar functions and mutually unbiased bases, 2013, arXiv:math.CO/1306.3478.

[2] K. Abdukhalikov, E. Bannai, and S. Suda, Association schemes related to universally optimal configurations, Kerdock codes and extremal Euclidean line-sets, *J. Combin. Theory Ser. A* **116** (2009), 434–448.

[3] R.J.R. Abel, I. Anderson, and N.J. Finizio, Necessary conditions for the existence of two classes of $\mathbb{Z}$CPS-Wh(v), *Discrete Appl. Math.* **159** (2011), 845–851.

[4] I. Anderson, A hundred years of whist tournaments, *J. Combin. Math. Combin. Comput.* **19** (1995), 129–150.

[5] I. Anderson, *Combinatorial Designs and Tournaments*, Oxford Univ. Press, Oxford, 1997.

[6] I. Anderson, N.J. Finizio, and P. Leonard, New product theorems for $\mathbb{Z}$-cyclic whist tournaments, *J. Combin. Theory Ser. A* **88** (1999), 162–166.

[7] R.D. Baker, Whist tournaments, *Proceedings of Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla.)*, *Congressus Numerantium* **XIV**, Utilitas Math., Winnipeg, Man., 1975, pp. 89–100.

[8] B. Ballinger, G. Blekherman, H. Cohn, N. Giansiracusa, E. Kelly, and A. Schürmann, Experimental study of energy-minimizing point configurations on spheres, *Experiment. Math.* **18** (2009), 257–283.

[9] E. Bannai, Subschemes of some association schemes, *J. Algebra* **144** (1991), 167–188.

[10] E. Bannai and T. Ito, *Algebraic combinatorics. I*, The Benjamin/Cummings Publishing Co. Inc., Menlo Park, CA, 1984.

[11] E. R. Berlekamp. *Algebraic coding theory*. McGraw-Hill Book Co., New York, 1968.

[12] T. Beth, D. Jungnickel, H. Lenz, *Design theory. Vol. I*, second edition, Cambridge University Press, Cambridge, 1999.

[13] A. Bonnecaze and I. M. Duursma. Translates of linear codes over Z_4. *IEEE Trans. Inform. Theory*, **43** (1997), 1218–1230.

[14] R.C. Bose and J.M. Cameron, The Bridge tournament problem and calibration designs for comparing pairs of objects, *J. Res. Bur. Standards* **69B** (1965), 323–332.

[15] W. G. Bridges and R. A. Mena, Multiplicative designs. I. The normal and reducible cases, *J. Combin. Theory Ser. A* **27** (1979), 69–84.

[16] W. G. Bridges and R. A. Mena, Multiplicative designs. II. Uniform normal and related structures, *J. Combin. Theory Ser. A* **27** (1979), 269–281.

[17] W. G. Bridges and R. A. Mena, Multiplicative cones–a family of three eigenvalue graphs, *Aequationes Math.* **22** (1981), 208–214.

[18] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-regular graphs*, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]* **18**, Springer-Verlag, Berlin, 1989.

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

[20] M. Buratti and A. Pasotti, Combinatorial designs and the theorem of Weil on multiplicative character sums, *Finite Fields Appl.* **15** (2009), 332–344.

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

[22] Y.Q. Chen, On the existence of abelian Hadamard difference sets and a new family of difference sets, *Finite Fields Appl.* **3** (1997), 234–256.

[23] C.J. Colbourn and W. De Launey, Difference matrices, in C.J. Colbourn and J.H. Dinitz, eds., *CRC Handbook of Combinatorial Designs,*, CRC Press, Boca Raton, FL, 1996, pp. 287–297.

[24] J.A. Davis and J. Jedwab, A unifying construction for difference sets, J. Combin. Theory Ser. A **80** (1987), 13–78.

[25] J.A. Davis and J. Polhill, Difference set constructions of DRADs and association schemes. J. Combin. Theory Ser. A **117** (2010), 598–605.

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

[27] P. Delsarte, On subfield subcodes of modified Reed-Solomon codes, *IEEE Trans. Inform. Theory* **21** (1975), 575–576.

[28] P. Dembowski and T. G. Ostrom, Planes of order n with collineation groups of order n^2, *Math. Z.* **103** (1968), 239–258.

[29] C. Ding, Cyclic codes from APN and planar functions, 2012, arxiv:cs.IT/1206.4687.

[30] C. Ding and H. Niederreiter, Systematic authentication codes from highly nonlinear functions, *IEEE Trans. Inform. Theory* **50** (2004), 2421–2428.

[31] C. Ding, Y. Liu, C. Ma, and L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, *IEEE Trans. Inform. Theory* **57** (2011), 8000–8006.

[32] C. Ding and J. Yang, Hamming weights in irreducible cyclic codes, *Discrete Math.* **313** (2013), 434–446.

[33] C. Ding and J. Yin, Signal sets from functions with optimum nonlinearity, *IEEE Trans. Commun.* **55** (2007), 936–940.

[34] C. Ding and J. Yuan, A family of optimal constant-composition codes, *IEEE Trans. Inform. Theory* **51** (2005), 3668–3671.

[35] K. Feng and J. Luo, Weight distribution of some reducible cyclic codes, *Finite Fields Appl.* **14** (2008), 390–409.

[36] T. Feng and K. Momihara, Evaluation of the weight distribution of a class of cyclic codes based on index 2 gauss sums, *IEEE Trans. Inform. Theory* **59** (2013), 5980–5984.

[37] N.J. Finizio, $\mathbb{Z}$-cyclic whist tournaments with a patterned starter initial round, *Discrete Appl. Math.* **52** (1994), 287–293.

[38] N.J. Finizio and P.A. Leonard, More $\mathbb{Z}$CPS-Wh(v) and several new infinite classes of $\mathbb{Z}$-cyclic whist tournaments, *Discrete Appl. Math.* **85** (1998), 193–202.

[39] S. Furino, Y. Miao and J. Yin, *Frames and Resolvable Designs: Uses, Constructions, and Existence*, CRC Press, Boca Raton, 1996.

[40] R. Fitzgerald and J. Yucas, Sums of Gauss sums and weights of irreducible codes, *Finite Fields Appl.* **11**(2005), 89–110.

[41] G. Ge, General frame constructions for Z-cyclic triplewhist tournaments, *J. Combin. Theory Ser. A* **114** (2007), 747–760.

[42] G. Ge and L. Zhu, Frame Constructions for Z-cyclic whist triplewhist tournaments, *Bull. Inst. Combin. Appl.* **32** (2001), 53–62.

[43] M. Hagita and B. Schmidt, Bijections between group rings preserving character sums, *Des. Codes Cryptogr.* **24** (2001), 243–254.

[44] A. Roger Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé, The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **40** (1994), 301–319.

[45] M. Harada, New 5-designs constructed from the lifted Golay code over Z_4, *J. Combin. Des.* **6** (1998), 225–229.

[46] T. Helleseth and P. Vijay Kumar, The algebraic decoding of the Z_4-linear Goethals codes, *IEEE Trans. Inform. Theory* **41** (1995), 2040–2048.

[47] T. Helleseth, P. Vijay Kumar, and A. Shanbhag, Codes with the same weight distributions as the Goethals codes and the Delsarte-Goethals codes, *Des. Codes Cryptogr.* **9** (1996), 257–266.

[48] T. Helleseth and V. Zinoviev, Codes with the same coset weight distributions as the Z_4-linear Goethals codes, *IEEE Trans. Inform. Theory* **47** (2001), 1589–1595.

[49] T. Helleseth and V. Zinoviev, On coset weight distributions of the Z_4-linear Goethals codes, *IEEE Trans. Inform. Theory* **47** (2001), 1758–1772.

[50] H. D. L. Hollmann and Q. Xiang, On binary cyclic codes with few weights, *Finite fields and applications (Augsburg, 1999)*, 251–275, Springer, Berlin, 2001.

[51] S. Hu and G. Ge, Necessary Conditions and Frame Constructions for $\mathbb{Z}$-cyclic Patterned Starter Whist Tournaments, *Discrete Appl. Math.* **160** (2012), 2188–2198.

[52] P. Vijay Kumar, Tor Helleseth, A. R. Calderbank, and A. Roger Hammons, Jr., Large families of quaternary sequences with low correlation, *IEEE Trans. Inform. Theory* **42** (1996), 579–592.

[53] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, *Graduate Texts in Mathematics* **84**, second edn, Springer-Verlag, New York, 1990.

[54] D. Jungnickel and B. Schmidt, Difference sets: an update, *London Math. Soc. Lecture Note Ser.* **245**, Cambridge Univ. Press, Cambridge, 1997, pp. 89–112.

[55] N. LeCompte, W. J. Martin, and W. Owens, On the equivalence between real mutually unbiased bases and a certain class of association schemes, *European J. Combin.* **31** (2010), 1499–1512.

[56] P.A. Leonard, Some new $\mathbb{Z}$-cyclic whist tournaments, *Util. Math.* **49** (1996), 223–232.

[57] P.A. Leonard and J.W. Jones, $\mathbb{Z}$-cyclic whist tournaments for q^2 players, *J. Combin. Math. Combin. Comput.* **66** (2008), 215–223.

[58] R. A. Liebler and R. A. Mena, Certain distance-regular digraphs and related rings of characteristic 4, *J. Combin. Theory Ser. A*, **47** (1988), 111–123.

[59] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, UK, 1997.

[60] Y. Lu and L. Zhu, On the existence of triplewhist tournaments TWh(v), *J. Combin. Des.* **5** (1997), 249–256.

[61] J. Luo and K. Feng, Cyclic codes and sequences from generalized Coulter-Matthews function, *IEEE Trans. Inform. Theory* **54** (2008), 5345–5353.

[62] J. Luo and K. Feng, On the weight distributions of two classes of cyclic codes, *IEEE Trans. Inform. Theory* **54** (2008), 5332–5344.

[63] J. Luo, Y. Tang, and H. Wang, On the weight distribution of a class of cyclic codes, *IEEE International symposium on information theory* (2009), 1726–1729.

[64] J. Luo, Y. Tang, and H. Wang, Cyclic codes and sequences: the generalized Kasami case, *IEEE Trans. Inform. Theory* **56** (2010), 2130–2142.

[65] C. Ma, L. Zeng, Y. Liu, D. Feng, and C. Ding, The weight enumerator of a class of cyclic codes, *IEEE Trans. Inform. Theory* **57** (2011), 397–402.

[66] S. L. Ma, Polynomial addition sets and polynomial digraphs, *Linear Algebra Appl.* **69** (1985), 213–230.

[67] S. L. Ma, On association schemes, Schur rings, strongly regular graphs and partial difference sets, *Ars Combin.* **27** (1989), 211–220.

[68] R. J. McEliece, Irreducible cyclic codes and Gauss sums, *Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of designs, finite geometry and coding theory*, *Math. Centre Tracts* **55**, Amsterdam: Math. Centrum, 1974, pp. 179–196.

[69] R. J. McEliece and J. H. Rumsey, Euler products, cyclotomy, and coding, *J. Number Theory* **4** (1972), 302–311.

[70] M. Moisio, Exponential sums, Gauss sums and cyclic codes, *Acta Univ. Oulu. Ser. A Sci. Rerum Natur.* **306**, dissertation, University of Oulu, Oulu, 1998.

[71] M. Moisio, Explicit evaluation of some exponential sums, *Finite Fields Appl.* **15** (2009), 644–651.

[72] K. Nyberg and L. R. Knudsen, Provable security against differential cryptanalysis, *Advances in cryptology—CRYPTO '92 (Santa Barbara, CA, 1992)*, *Lecture Notes in Comput. Sci.* **740**, Springer, Berlin, 1993, pp. 566–574.

[73] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, *North-Holland Mathematical Library* **16**, North-Holland Publishing Co., Amsterdam, 1977.

[74] P.K. Menon, On difference sets whose parameters satisfy a certain relation, *Proc. Amer. Math. Soc.* **13** (1962), 739–745.

[75] E.H. Moore, Tactical memoranda I–III, *Amer. J. Math.* **18** (1896), 264–303.

[76] M. E. Muzychuk, *V-rings of permutation groups with invariant metric*, PhD thesis, Kiev State University, 1987.

[77] A. Pasini and S. Yoshiara, New distance regular graphs arising from dimensional dual hyperovals, *European J. Combin.* **22** (2001), 547–560.

[78] A. Pott, *Finite geometry and character theory*, *Lecture Notes in Mathematics* **1601**, Springer-Verlag, Berlin, 1995.

[79] Z. Scherr and M. E. Zieve, Planar monomials in characteristic 2, 2013, arXiv:math.CO/1302.1244.

[80] K.-U. Schmidt and Y. Zhou, Planar functions over fields of characteristic two, to appear in *J. Algebraic Combin.*, 2014.

[81] B. Schmidt and C. White, All two-weight irreducible cyclic codes? *Finite Fields Appl.* **8** (2002), 1–17.

[82] R. Schoof, Families of curves and weight distributions of codes, *Bull. Amer. Math. Soc. (N.S.)* **32** (1995), 171–183.

[83] D.-J. Shin, P. Vijay Kumar, and T. Helleseth, An Assmus-Mattson-type approach for identifying 3-designs from linear codes over Z_4, *Des. Codes Cryptogr.* **31** (2004), 75–92.

[84] D. Stanton, Three addition theorems for some q-Krawtchouk polynomials, *Geom. Dedicata* **10** (1981), 403–425.

[85] P. Solé, Four applications of $\mathbb{Z}_4$-codes, *Fifth Conference on Discrete Mathematics and Computer Science (Spanish)*, *Ciencias (Valladolid)* **23**, Univ. Valladolid, Secr. Publ. Intercamb. Ed., Valladolid, 2006, pp. 37–40.

[86] D.R. Stinson, The equivalence of certain incomplete transversal designs and frames, *Ars Combin.* **22** (1986), 189–214.

[87] M. van der Vlugt, Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes, *J. Number Theory* **55** (1995), 145–159.

[88] G. Vega, Determining the number of one-weight cyclic codes when length and dimension are given, *Arithmetic of finite fields, Lecture Notes in Comput. Sci.* **4547**, Springer, Berlin, 2007, pp. 284–293.

[89] G. Vega and J. Wolfmann, New classes of 2-weight cyclic codes, *Des. Codes Cryptogr.*, **42** (2007), 327–334.

[90] Z. X. Wan, *Lectures on finite fields and Galois rings*, World Scientific Publishing Co. Inc., River Edge, NJ, 2003.

[91] B. Wang, C. Tang, Y. Qi, Y. Yang, and M. Xu, The weight distributions of cyclic codes and elliptic curves, *IEEE Trans. Inform. Theory* **58** (2012), 7253–7259.

[92] G.L. Watson, Bridge problem, *Math. Gazette* **38** (1954), 129–130.

[93] G. Weng, W. Qiu, Z. Wang, and Q. Xiang, Pseudo-Paley graphs and skew Hadamard difference sets from presemifields, *Des. Codes Cryptogr.* **44** (2007), 49–62.

[94] J. Wolfmann, Weight distributions of some binary primitive cyclic codes, *IEEE Trans. Inform. Theory* **40** (1994), 2068–2071.

[95] J. Yuan, C. Carlet, and C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, *IEEE Trans. Inform. Theory* **52** (2006), 712–717.

[96] X. Zeng, N. Li, and L. Hu, A class of nonbinary codes and sequence families, *Sequences and their applications—SETA 2008, Lecture Notes in Comput. Sci.* **5203**, Springer, Berlin, 2008, pp. 81–94.

[97] Y. Zhou, $(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations, *J. Combin. Designs.* **21** (2013), 563–584.

个人简介

- 胡思煌，男，浙江大学理学院数学系博士生，导师：葛根年、冯涛.
- 通信地址：中国浙江省杭州市浙江大学玉泉校区数学系，310027.
- 联系方式：18911518783，husihuang@zju.edu.cn

- 教育经历：

  2004.9–2008.6，北京航空航天大学理学院数学系，应用数学专业，理学学士.

  2009.9–今，浙江大学理学院数学系，应用数学专业，理学博士，研究方向：代数组合与代数编码.

- 研究兴趣：组合设计理论，代数组合学，编码理论，格，球填充.

攻读博士学位期间主要研究成果

[1] Sihuang Hu, Tao Feng, and Gennian Ge, Association schemes related to Delsarte-Goethals codes, to appear in *Journal of Algebraic Combinatorics*, arXiv:math.CO/1212.0347.

[2] Sihuang Hu, Shuxing Li, Tao Zhang, Tao Feng, and Gennian Ge, New pseudo-planar binomials in characteristic two and related schemes, to appear in *Designs, Codes and Cryptography*, arXiv:math.CO/1304.7044.

[3] Tao Feng, Sihuang Hu, Shuxing Li, and Gennian Ge, Difference sets with few character values, to appear in *Designs, Codes and Cryptography*, arXiv:math.CO/1303.1659.

[4] Gennian Ge, Sihuang Hu, Emre Kolotoğlu, and Hengjia Wei, A complete solution to spectrum problem for five-vertex graphs with application to traffic grooming in optical networks, to appear in *Journal of Combinatorial Designs*.

[5] Sihuang Hu and Gennian Ge, Some new results on Z-cyclic patterned starter whist tournaments and related frames, *Journal of Combinatorial Designs* **21** (2013), 181–203.

[6] Shuxing Li, Sihuang Hu, Tao Feng, and Gennian Ge, The weight distribution of a class of cyclic codes related to Hermitian forms graphs, *IEEE Transactions on Information Theory* **59** (2013), 3064–3067, arXiv:cs.IT/1212.6371.

[7] Sihuang Hu and Gennian Ge, Necessary conditions and frame constructions for Z-cyclic patterned starter whist tournaments, *Discrete Applied Mathematics* **160** (2012), 2188–2198.

[8] Tao Feng, Gennian Ge, Sihuang Hu, and Jianmin Ma, Some results on infinite families of strongly distance regular graphs, 2013, Submitted.