分类号：O157.2　　单位代码：10335
密　级：　　学　　号：11835006

浙江大学

博士学位论文

中文论文题目：若干有限几何构型和码类的构造研究

英文论文题目：**On the constructions of certain finite geometric structures and codes**

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

论文提交日期：二〇二一年四月

若干有限几何构型和码类的构造研究

论文作者签名：王野

指导教师签名：冯淮

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：谈之奕 教授 浙江大学

委员 2：李松 教授 浙江大学

委员 3：蔺宏伟 教授 浙江大学

委员 4：李吉有 教授 上海交通大学

委员 5：王军 教授 上海师范大学

答辩日期：二〇二一年五月

On the constructions of certain finite geometric structures and codes

Author's signature: Ye Wang

Supervisor's signature: Tao Feng

External Reviewers: _____

_____

_____

_____

_____

Examining Committe Chairperson:

Prof. Jun Wang, Shanghai Normal University

Examining Committe Members:

Prof. Zhiyi Tan, Zhejiang University

Prof. Song Li, Zhejiang University

Prof. Hongwei Lin, Zhejiang University

Prof. Jiyou Li, Shanghai Jiao Tong University

Prof. Jun Wang, Shanghai Normal University

Date of oral defence: May, 2021

浙江大学研究生学位论文独创性声明

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

学位论文作者签名：王野　　签字日期：2021 年 6 月 25 日

学位论文版权使用授权书

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

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：王野　　导师签名：冯涛

签字日期：2021 年 6 月 25 日　　签字日期：2021 年 6 月 25 日

致　谢

首先, 我要感谢我的导师冯涛老师. 在五年间, 冯老师耐心的指导使我获益良多, 他的自律和严格深刻地影响着我. 冯老师对我们倾注了大量心血, 他教授我们知识, 为我们答疑. 在研究问题时, 冯老师给了我很多建议, 并且为我的论文提供了重要的指导. 此外, 冯老师邀请很多学者来我校交流并鼓励我们参加学术会议, 让我们受益匪浅.

其次我要感谢南方科技大学的向青教授, 他和冯老师与我合作了完成了我的第一个题目, 在论文撰写及修改时, 向老师为我提供了切实的帮助与指导.

接着我要感谢在我研究问题时给我启发的师长: 首都师范大学的葛根年教授和张韬师兄. 同时我也要感谢与我在学术上进行深度探讨及合作的陶然.

感谢和我一起学习交流的各位同门: 李伟聪师兄、钱昺辰师兄、林灯师兄、戚立波师兄、Jerod Michel 师兄、李抒行师兄、张一炜师兄、汪馨师兄、丁报昆师兄、马景学师兄、奚元宵、徐子翔、兰昭君、何智文、周靖坤、孙秀芳、陆建兵、狄文帝、林培贤等. 感谢他们的陪伴与帮助, 他们让我在漫长的研究生生活中不再孤单.

感谢我的朋友们: 徐纯逸、白雪彤、喻杉、杨贝、柳莹、庄文秀等人. 感谢她们听我倾诉, 给我建议, 与我分享快乐, 陪我走出困境.

感谢我的父母和亲人, 感谢他们在我读博期间给与我的支持与鼓励, 他们让我毫无后顾之忧, 得以专心投入科研.

感谢浙江大学的培养, 感谢学校提供的广阔平台.

感谢所有曾给与我帮助的人.

由于作者的水平有限, 文章难免有谬误和不足之处, 敬请各位专家学者批评指正!

摘　要

组合数学是一门十分有魅力的学科, 它的研究对象是离散的. 组合数学有很多分支, 例如图论、组合设计、有限几何等等, 它与编码理论、密码学等实用性较强的数学分支也有相当高的重合度. 组合数学中有很多具有良好性质的代数结构, 这些结构在信息科学、通信、存储等方面得到了广泛应用, 因此, 组合数学中的构造问题是有趣并且有意义的. 本论文涉及组合数学中的一类几何结构的构造以及几类在信息领域具有应用价值的码的构造. 本文的主旨是利用有限域、代数数论、群、特征等数学工具完成组合数学中的构造问题.

在第 1 章中, 我们介绍了本文研究的几何结构以及码的研究背景和本文的主要贡献.

在第 2 章中, 我们确定了在特定的条件下辛极空间 $\mathrm{W}(2r-1,p^e)$ 中强正则图和 m-ovoids 之间的等价关系, 并利用已知的强正则图构造出辛极空间上一些具有新参数的 m-ovoids.

在第 3 章中, 我们利用无定形的结合方案构造了 LCD 码以及 hull 维数为 1 的线性码. 此外, 在小参数的情况下, 我们利用计算机找到了一些性质较好的 LCD 码以及 hull 维数为 1 的线性码.

在第 4 章中, 我们利用一定条件的循环子空间码与 Sidon 空间之间的转换关系, 用已知的 Sidon 空间以及其变式构造了规模较大的循环子空间码. 此外, 我们构造了新的 Sidon 空间, 我们的构造解决了部分关于满足一定条件的循环子空间码的存在性问题.

最后, 我们将介绍我们的研究方向后续可以做的工作.

关键词: 辛极空间, 强正则图, m-ovoid, Hull, 结合方案, LCD 码, Sidon 空间, 循环子空间码.

Abstract

Combinatorics is a very attractive subject. Its research objects are discrete. Combinatorial mathematics has many branches, such as graph theory, combinatorial design, finite geometry and so on. It also has a high degree of coincidence with practical branches of mathematics such as coding theory and cryptography. There are many algebraic structures with great properties in combinatorics, which are widely used in information science, communication, storage and so on. Therefore, the construction problems in combinatorics is interesting and meaningful. This paper deals with the constructions of a class of geometric structures in combinatorial mathematics and several classes of useful codes in the field of information. The purpose of this paper is to deal with the construction problems by finite fields, algebraic number theory, groups, characters and other mathematical tools.

In Chapter 1, we introduce the research background of the geometric structures and codes we concerned and the main contributions of this paper.

In Chapter 2, we determine the equivalence between strong regular graphs and m-ovoids in the symplectic polar space $\mathrm{W}(2r-1, p^e)$ under certain conditions, and we give the construction of m-ovoids in the symplectic polar space by using the known strong regular graphs.

In Chapter 3, we construct LCD codes and linear codes with 1-dimensional hull by using some amorphic association schemes. Furthermore, we find some optimal LCD codes and linear codes with 1-dimensional hull with computer when the parameters are small.

In Chapter 4, we construct large cyclic subspace codes from known Sidon spaces and their variants by using the conversion relationship between cyclic subspace codes with certain conditions and Sidon spaces, our construction solves part of the conjuecture of the existence of cyclic subspace codes satisfying certain conditions.

Finally, we will introduce our later work about our research.

Keywords: Symplectic polar space, Strongly regular graph, m-ovoid, Hull, Association scheme, LCD code, Sidon space, Cyclic subspace codes.

图 目 录

表 目 录

目　次

1 绪论

组合数学是一种研究离散对象的数学, 它有很多分支, 例如有限几何、图论、组合设计等等, 它与很多其他应用性领域比如编码理论、密码学高度重合. 随着计算机的发展, 组合数学的重要性日渐凸显, 它在编码密码等领域的应用吸引了大量学者的关注. 组合数学中的构造问题是组合数学的热点问题, 一些有意思的组合结构可以被用在编码密码等领域中, 构造具有良好性质的码或者密码函数, 并且被应用到信息及网络安全等学科中. 这篇文章涉及了有限几何中的一类组合结构的构造以及在信息科学中具有优良性质的几类码的构造. 接下来我们将介绍研究课题的背景意义以及本文的主要贡献.

1.1 极空间上的 intriguing sets

有限几何是组合数学的一个重要分支, 它与无限几何有密切的联系, 它们有很多相类似的定义和性质, 但不同的是, 有限几何只包含有限数量的点和线, 它可以与组合数学中很多有趣的问题相联系. 有限几何中有很多有意思的组合结构, 极空间上的 intriguing sets 就是一个非常有意义的研究对象.

我们首先介绍极空间, 具体可以参考文献[35]. 在此之前, 我们先给出射影空间的描述.

令 q 为一个素数幂, $\mathbb{F}_q$ 为包含 q 个元素的有限域. 令 V 为 $\mathbb{F}_q$ 上的一个 $(n+1)$-维向量空间. 射影空间PG(V) 是包含点、线、面、…、超平面 (分别对应 V 的 1-维 $\mathbb{F}_q$-子空间、2-维 $\mathbb{F}_q$-子空间、3-维 $\mathbb{F}_q$-子空间、…、n-维 $\mathbb{F}_q$-子空间) 的几何, 其各个结构之间的关联关系是包含关系.

下面关于半双线性型的定义可以参考文献[66].

一个σ-半双线性型 *(σ-sesquilinear form)* 是一个变换式 $f : V \times V \to \mathbb{F}_q$, 它满足以下条件:

(1) 对于任意的 $x_1, x_2, y_1, y_2 \in V$, 我们有

$$f(x_1 + x_2, y_1 + y_2) = f(x_1, y_1) + f(x_1, y_2) + f(x_2, y_1) + f(x_2, y_2).$$

(2) 对于任意的 $\lambda, \mu \in \mathbb{F}_q$ 以及 $x, y \in V$, 我们有

$$f(\lambda x, \mu y) = \lambda \mu^{\sigma} f(x, y).$$

一个 σ-半双线性型 $f : V \times V \to \mathbb{F}_q$ 如果满足对任意的 $0 \neq x \in V$, 存在 V 上的

一个向量 y 使得 $f(x,y)\neq 0$, 并且对任意的 $0\neq y'\in V$, 存在 V 上的一个向量 x' 使得 $f(x',y')\neq 0$, 那么它被称为非退化的 *(nondegenerate)*.

令 f 为 V 上的一个非退化的半双线性型. 令 U 为 V 的一个子空间. 那么当下面的公式成立时, U 是完全迷向的 *(totally isotropic)*:

$$f(x,y)=0,\forall x,y\in U.$$

对于任意的 $x\in V$, 我们定义

$$x^{\perp}=\{y\in V|f(x,y)=0\}.$$

一个与 f 相关联的极空间 $\mathcal{S}$ 是一个几何结构, 它是由被 f 确定的完全迷向子空间诱导出的 PG(V) 的子空间构成的. 这些子空间包括完全迷向点、线、面等. 极空间 $\mathcal{S}$ 的 generators 是其所包含的维数最大的完全迷向子空间. 我们把 generators 的向量维数称为 $\mathcal{S}$ 的秩.

有限经典极空间分为三种类型: 正交极空间 (orthogonal polar space)、辛极空间 (symplectic polar space) 以及 Hermitian 极空间. 我们将有限经典极空间依次序总结在表格 1.1中, 表中的 g 是 $\mathbb{F}_q$ 上的不可约同态二次多项式.

表 1.1　有限经典极空间

极空间	秩	半双线性型 f
$Q(2n,q)$	n	$x_0^2+x_1x_2+\cdots+x_{2n-1}x_{2n}$
$Q^+(2n-1,q)$	n	$x_0x_1+x_2x_3+\cdots+x_{2n-2}x_{2n-1}$
$Q^-(2n+1,q)$	n	$g(x_0,x_1)+x_2x_3+\cdots+x_{2n}x_{2n+1}$
$\mathrm{W}(2n-1,q)$	n	$x_0y_1-y_0x_1+\cdots+x_{2n-2}y_{2n-1}-x_{2n-1}y_{2n-2}$
$H(2n,q^2)$	n	$x_0^{q+1}+\cdots+x_{2n}^{q+1}$
$H(2n-1,q^2)$	n	$x_0^{q+1}+\cdots+x_{2n-1}^{q+1}$

Tight sets 和 m-ovoids 都是有限经典极空间中极其重要的几何结构. 在 1987 年, 广义四边形上 tight sets 的概念首先由 Payne 在文献[54] 中提出, 而后 tight sets 的概念又被 Drudge[24] 于 1998 年推广到有限经典极空间中. 广义四边形中的 m-ovoids 最初是由 Thas 在文献[64] 中定义的, 然后 Shult 和 Thas[59] 又将 m-ovoids 的概念推广到了有限经典极空间中. 在文献[5] 中, Bamberg 等学者将广义四边形中的 tight sets 和 m-ovoids 的概念统一为 intriguing sets, 在此之后, intriguing sets 的概念在文献[3] 中又被推广了到有限经典极空间中. 接下来, 我们将给出极空间中 intriguing sets 的具体定义.

定义 1.1[5] 极空间 $\mathcal{S}$ 中的点集 $\mathcal{I}$ 如果对于某两个常数 h_1 及 h_2 满足下面的条件, 我

们就把它称为 intriguing sets:

$$|P^{\perp}\cap\mathcal{I}|=\begin{cases}h_1, & \text{当}P\in\mathcal{I}\text{时},\\ h_2, & \text{当}P\notin\mathcal{I}\text{时}.\end{cases}$$

这里, P 总是 $\mathcal{S}$ 中的点.

可以证明得到, 极空间中的 intriguing sets 只能是 tight sets 或者 m-ovoids. 对于极空间中的 tight sets 和 m-ovoids, 上述定义中的参数 h_1 和 h_2 分别如下面的引理所示.

引理 1.1 [5] 对于 $\mathbb{F}_q$ 上定义的秩为 $r(r\geq 2)$ 的极空间 $\mathcal{S}$. 我们有

(1) 极空间 $\mathcal{S}$ 的一个 i-tight set 是 h_1 和 h_2 如下的 intriguing set:

$$h_1=i\frac{q^{r-1}-1}{q-1}+q^{r-1},$$
$$h_2=i\frac{q^{r-1}-1}{q-1}.$$

(2) 极空间 $\mathcal{S}$ 中的一个 m-ovoid 是 h_1 和 h_2 如下的 intriguing set:

$$h_1=m\theta_{r-1}-\theta_{r-1}+1,$$
$$h_2=m\theta_{r-1}.$$

上述引理中所涉及到的 θ_{r-1} 是秩为 $r-1$ 的极空间的一个 ovoid 中点的个数. θ_r 在有限经典极空间中的取值如表 1.2所示.

表 1.2 $\mathbb{F}_q$ 上秩为 r 的极空间中的 1-ovoid 所含点的个数

极空间	$Q(2r,q)$	$Q^+(2r-1,q)$	$Q^-(2r+1)$	$\mathrm{W}(2r-1,q)$	$H(2r,q^2)$	$H(2r-1,q^2)$
θ_r	q^r+1	$q^{r-1}+1$	$q^{r+1}+1$	q^r+1	$q^{2r+1}+1$	$q^{2r-1}+1$

构造不同参数的 intriguing sets 是一个前沿的课题. 目前, 有限经典极空间中 intriguing sets 的构造已经有不少研究成果了. 然而对于辛极空间而言, 由于其结构的复杂性, 该空间上的 intriguing sets, 尤其是 m-ovoids 的构造还很稀缺. 在第 2 章中, 我们提供了一种构造辛极空间 $\mathrm{W}(2r-1,p^e)$ 中 m-ovoids 的方法, 该方法利用了文献[7] 中构造的一些强正则凯莱图 (strongly regular Cayley graph). 用这种方法, 我们得到了很多新的 m-ovoids, 并且这些 m-ovoids 无法由 field reduction 方法得到, 如果读者需要了解 field reduction 方法, 具体可以参考文献[38]. 这部分工作已经发表在《Journal of Combinatorial Theory, Series A》.

1.2 LCD 码及 hull 维数为 1 的码

线性码由于其代数结构简单, 与其他非线性的码相比, 更易于被刻画, 编码以及译码, 因此成为所有类型的码中被研究与应用得最多的码. 另一方面, 线性码是一种重要的纠错码, 由于它在通信、存储等领域都得到了普遍应用, 因此被视为一个很重要的研究对象.

以下是关于线性码的一些基本概念, 具体可以参考文献[47]:

设 q 是一个素数幂, $\mathbb{F}_q$ 是包含 q 个元素的有限域, 用 $\mathbb{F}_q^n$ 表示 $\mathbb{F}_q$ 上的 n 维向量空间. $\mathbb{F}_q$ 上的一个 $[n,k]$ 线性码 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 的一个 k 维子空间, 因此它的一组基中包含 k 个向量. 对于线性码 $\mathcal{C}$ 中任意一个元素 (即码字) $x=(x_1,x_2,...,x_n)$, 其汉明重量 *(Hamming weight)* 是指集合 $\{1\leq i\leq n : x_i\neq 0\}$ 的大小, 记为 $\mathrm{wt}(x)$. 线性码 $\mathcal{C}$ 的最小汉明距离 *(minimum Hamming weight)* 定义为

$$d(\mathcal{C})=\min\{\mathrm{wt}(x) : x\in\mathcal{C}\}.$$

线性码 $\mathcal{C}$ 的一个生成矩阵 *(generator matrix)* G 是一个由 $\mathcal{C}$ 的一组基作为行的矩阵.

线性码与其对偶的交集称为该码的 hull. 线性码的 hull 具有丰富的代数结构并且可以被广泛运用到信息科学领域, 因此, 线性码的 hull 被大量学者广泛研究. Hull 维数很小的线性码具有很好的性质. 一般情况下, 对于 hull 很小的线性码, 决定检查两个线性码的置换等价性和计算线性码的自同构群的算法复杂度是非常高效的. 特别地, 如果一个码的 hull 维数为 0, 则它是一个线性互补对偶 (linear complementary dual, 简称为 LCD) 码.

LCD 码具有良好的性质, 是一类很重要的线性码. 近年来, LCD 码被大量应用到数据存储, 通信系统和消费类电子产品以及密码学中, 是编码理论中的一个热点问题. LCD 码最初是由 Massey[50] 引入的, 他证明了生成矩阵为 G 的线性码 $\mathcal{C}$ 是 LCD 码当且仅当 GG^T 是非奇异的, 即 GG^T 是可逆的. 后面我们会利用该结论进行 LCD 码的构造.

在第 3 章中, 我们给出了一种通过结合方案 (association scheme) 来构造 LCD 码以及 hull 维数为 1 的线性码的方法. 该章中的其中一个构造推广了文献[19] 中给出的结合了高斯周期 (Gauss period) 的线性码. 此外, 我们提供了线性码的一种广义构造, 通过该构造我们可以得到更多类型的 LCD 码以及 hull 维数为 1 的线性码. 我们还利用 Magma 程序得到了一些小参数的 LCD (almost) MDS 码以及 hull 维数为 1 的 (almost) MDS 码的例子. 这意味着我们的构造是可以得到性质较好的线性码的. 这部分的工作已经被《Advances in Mathematics of Communications》接收.

1.3 循环子空间码

在 2000 年, Ahlswede 等人在文献[1] 中首次引入了随机网络编码, 这是一种可以在具有多个信源和信宿的非相关网络中使信息流达到最大化的非常高效的工具. 这种网络编码在整个网络中传播信息的高效性也意味着它对错误的传播具有高度敏感性. 由于子空间码特别是常维数码在随机网络编码的纠错方面的应用越来越普遍[41], 子空间码尤其是循环子空间码受到了更多的关注. 循环子空间码在编码及译码算法中十分高效, 寻找系统性的方法去构造码字尽量多, 最小距离尽可能大的循环子空间码是目前非常受关注的一个问题.

另外, 关于循环子空间码有一个非常著名的猜想[33,65]: 对于任意素数幂 q 和正整数 k 以及 $n > 2k$, 存在一个循环子空间码 $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, 其满足 $|\mathcal{C}| = \frac{q^n-1}{q-1}$ 和 $d(\mathcal{C}) = 2k-2$. (这里, $\mathcal{G}_q(n,k)$ 为域 $\mathbb{F}_{q^n}$ 的所有 k-维 $\mathbb{F}_q$-子空间的集合, 而 $d(\mathcal{C})$ 是码 $\mathcal{C}$ 的最小距离.)

在第 4 章中, 我们构造了 $\mathcal{G}_q(n,k)$ 中最小距离为 $2k-2$, 码字个数为 $(\lceil \frac{n}{2k} \rceil - 1) \cdot \frac{(q^n-1)q^k}{q-1}$ 的循环子空间码. 当 $n = 3k$, 并且 k 趋近于无穷大时, 它们的大小渐近地接近子空间码的著名的 sphere-packing 上界的 $\frac{1}{q-1}$. 我们的构造使用了 Roth 等人在文献[58] 中构造的 Sidon 空间的变体, 并且得到的结果和他在 $n = 2k$ 条件下得到的结果类似. 此外, 我们还明确了 $\mathcal{G}_q(7k,2k)$ 中 Sidon 空间的存在性, 并因此解决了部分关于 $\mathcal{G}_q(n,k)$ 中最小距离为 $2k-2$, 码字个数为 $\frac{q^n-1}{q-1}$ 的循环子空间码的存在性猜想. 这部分的工作已经发表在《Discrete Mathematics》.

2 辛极空间上的 m-ovoids

2.1 背景

给定整数 $e \geq 1, r \geq 2$, 设 p 是一个素数, $\mathbb{F}_{p^e}$ 是包含 p^e 个元素的有限域. 设 V 是 $\mathbb{F}_{p^e}$ 上一个 $2r$-维的向量空间, 令 f 为定义在 V 上的一个非退化的交错型 (alternating form). 被赋予交错型 f 的辛极空间 $\mathrm{W}(2r-1, p^e)$ 是由关于 f 的完全迷向子空间诱导出的 $\mathrm{PG}(V)$ 的子空间构成的几何结构. 辛极空间 $\mathrm{W}(2r-1, p^e)$ 包含完全迷向 (totally isotropic) 点、线、面等几何结构. 因为 f 是交错型, $\mathrm{PG}(V)$ 中的每个点是完全迷向的. 因此, $\mathrm{W}(2r-1, p^e)$ 中点的集合等同于 $\mathrm{PG}(V)$ 中点的集合. 维数最大的 (完全迷向) 子空间称为 $\mathrm{W}(2r-1, p^e)$ 中的 *maximals*(或者 *generators*). $\mathrm{W}(2r-1, p^e)$ 的秩 *(rank)* 是它的 maximals 的向量空间维数, 即 r.

在这一节里, 我们主要研究了 $\mathrm{W}(2r-1, p^e)$ 中 m-ovoids 的构造. $\mathrm{W}(2r-1, p^e)$ 中的一个*m-ovoid* 是一个点集 $\mathcal{M}$, 它使得 $\mathrm{W}(2r-1, p^e)$ 中的每个 maximal 和 $\mathcal{M}$ 的交集恰好有 m 个点. $\mathrm{W}(2r-1, p^e)$ 中的一个 1-ovoid 可以简称为一个 *ovoid*. $\mathrm{W}(2r-1, p^e)$(更一般的情况下任何经典极空间) 中的 ovoids 首先由 Thas[63] 在 1981 年定义. $\mathrm{W}(2r-1, p^e)$ 中 ovoids 的存在性问题已经被完全解决了: $\mathrm{W}(3, p^e)$ 中有 ovoids 当且仅当 $p = 2$; 当 $r > 2$ 时, $\mathrm{W}(2r-1, p^e)$ 中没有 ovoids. m-ovoids 的概念首先由 Thas[64] 在广义四边形中给出, 后又被 Shult 和 Thas[59] 推广到经典极空间中. 被称为 i-tight sets 的另一种结构也是极空间中备受关注的几何结构, 其与 m-ovoids 联系紧密并且经常相伴出现. 辛极空间 $\mathrm{W}(2r-1, p^e)$ 中的 m-ovoids 和 i-tight sets 被统一称为 intriguing sets. 在本章中, 我们只考虑 m-ovoids 的构造.

经典极空间中的 intriguing sets, 特别是 m-ovoids, 和其他几何和组合结构比如强正则图和射影 2-重量码有密切的联系, 参考[3–5,15]. 例如, $\mathrm{W}(2r-1, p^e)$ 中的 m-ovoids 同时也是 $\mathrm{PG}(2r-1, p^e)$ 中的二交集 (two-intersection set), 于是它可以生成一个强正则图, 参考文献[3]. 射影二交集和 2-重量码之间也有显著的联系[15]. 文献[4] 中给出了一个通过强正则凯莱图构造 $\mathrm{Q}^-(5, p^e)$ 中 m-ovoids 的方法.

关于 $\mathrm{W}(2r-1, p^e)$ 中 m-ovoids 的主要问题是: 对于满足怎样条件的 $m \geq 1$, 存在 $\mathrm{W}(2r-1, p^e)$ 中的一个 m-ovoid? 如上面提到的, 当 $m = 1$ 时, 这个问题已经被完全解决了. 与之形成鲜明对比的是, 当 $m \geq 2$ 时, m-ovoids 的存在性问题仍然留下了很大的研究空间. 我们接下来对已知的结论做一个简短的总结. 我们从 $\mathrm{W}(3, p^e)$ 开始: 当 p 是一个奇素数时, $\mathrm{W}(3, p^e)$ 中不存在 ovoids, 参考[55]; 但 $\mathrm{W}(3, p^e)$ 中存在一个划分, 其将 $\mathrm{W}(3, p^e)$ 划分成一些 2-ovoids, 于是对于每一个正偶数 m, 存在 $\mathrm{W}(3, p^e)$ 中的一个

m-ovoid, 参考[5]; 此外, Cossidente 等学者在[14] 中给出了一个 W$(3,p^e)$ 中 $\frac{(p^e+1)}{2}$-ovoids 的构造, 这里 p 是一个奇素数. 当 $p=2$ 时, 对于所有可能的 m, Cossidente 等人给出了 W$(3,p^e)$ 中 m-ovoids 的构造[14]. 接下来, 考虑 W$(5,p^e)$ 的情况: 首先, 在 W$(5,p^e)$ 中存在零星的几个例子[3]; 当 $p=2$ 时, Cossidente 和 Pavese[16] 提供了 W$(5,p^e)$ 中非典型 (p^e+1)-ovoids 的两个构造, 这两个构造利用了 relative hemisystems 以及埃尔米特面 (Hermitian surface) 中嵌入的 Suzuki-Tits ovoids. 对于一般性的 W$(2r-1,p^e)$, 在必要的条件下, 文献[3] 中证实, 对于 $r>2$, 如果 W$(2r-1,p^e)$ 中存在一个 m-ovoid, 那么就有 $m\geq\frac{(-3+\sqrt{9+4p^{er}})}{2p^e-2}$; 至于构造的详细情况, Cossidente 和 Pavese[17] 在 p^e 是偶数的情况下将辛极空间 W$(4n-1,p^e)$ 划分成一个 $\frac{(p^{e(2n-2)}-1)}{p^e-1}$-ovoid, 一个 $p^{e(2n-2)}$-ovoid 以及一些 $2p^{e(2n-2)}$-ovoids. Shult 和 Thas[59] 介绍了有限经典极空间中 m-systems 的概念, 并且证明了 $W(2r-1,p^e)$ 的一个 m-system 的子空间中的点构成了一个 $\frac{(p^{e(m+1)}-1)}{p^e-1}$-ovoid. 在文献[59] 的定理 14 中, 他们还证明了当 r 为奇数时, 如果 $H(r-1,p^{2e})$ 中包含一个 m-system, 那么可以由 field reduction 方法得到 $W(2r-1,p^e)$ 中的一个 $(2m+1)$-system. 因此, 当 $r=3$ 时, 存在 $W(5,p^e)$ 中的一个 1-system, 它由 $H(2,p^{2e})$ 中的一个 0-system 生成, 于是, 我们可以获得 $W(5,p^e)$ 中的一个 (p^e+1)-ovoid. 此外, 必须要提到一个重要的构造方法: 利用 field reduction, 一个低秩的经典极空间中的一个 m'-ovoid 可以生成一个高秩的经典极空间中的一个 m-ovoid. 特别地, 应用 field reduction 的方法, 如果 $r'\mid r$ 且 $re=r'e'$, 那么 $W(2r'-1,p^{e'})$ 中的一个 m'-ovoid 可以生成 $W(2r-1,p^e)$ 中的一个 m-ovoid, 具体可以参考文献[38]. 在本章的第三节中, 我们将会构造得到 $W(2r-1,p^e)$ 中的 m-ovoids, 这里 r 是一个素数, 记作 p_0; 由于 p_0 仅有两个素因子 1 和 p_0, 所以 $W(2p_0-1,p^e)$ 中的一个 m-ovoid 不能由秩小于 p_0 的辛极空间中的一个 m'-ovoid 通过 field reduction 构造得到.

从上面的总结可以看出, 直至今天, 我们对高秩辛极空间上的 m-ovoids 的构造及研究仍然很欠缺. 就构造而言, 当 q 是奇数的时候, 目前唯一已知的构造高秩辛极空间中的 m-ovoids 的方法是 field reduction, 参考[38]. 在本章中, 我们给出了一个新的构造方法, 该方法使我们可以构造出高秩辛极空间上大量的 m-ovoids. 特别地, 我们证明了 $W(2r-1,p^e)$ 中存在很多利用偏差集通过下文中的定理 2.3生成的具有新参数的 m-ovoids. 为了方便叙述我们的方法, 我们给出了下面 W$(2r-1,p^e)$ 中 m-ovoids 的等价定义.

引理 2.1 令 $\mathcal{M}$ 为 W$(2r-1,p^e)$ 中的一个点集. 那么 $\mathcal{M}$ 是一个 m-ovoid 当且仅当

$$|P^{\perp}\cap\mathcal{M}|=\begin{cases}m(p^{e(r-1)}+1)-p^{e(r-1)}, & \text{如果}P\in\mathcal{M},\\ m(p^{e(r-1)}+1), & \text{其他情形.}\end{cases}\tag{2.1}$$

对于引理 2.1的证明, 读者可以参考文献[3]. 我们构造 m-ovoids 的基本思路是利用文献[3] 中定理 11 的部分逆向结论. 关于辛极空间 $\mathrm{W}(2r-1,p^e)$, 文献[3] 中的定理 11 证实了一个 m-ovoid 可以生成 $(\mathbb{F}_{p^e}^{2r},+)$ 上的一个负拉丁方类型的强正则凯莱图. 这个论断的部分逆向结果是正确的, 即 $(\mathbb{F}_{p^e}^{2r},+)$ 上的一个具有特定性质的负拉丁方类型的强正则凯莱图可以生成 $\mathrm{W}(2r-1,p^e)$ 中的一个 m-ovoid (该特定的性质即“自对偶”的性质; 这部分将在下面的定理 2.2中得到明确解释). 为了实现这一个方法, 首先介绍文献[7] 中的一些强正则凯莱图 $\mathrm{Cay}(\mathbb{F}_q,D)$, 并且赋予有限域 $\mathbb{F}_q$ (现在视作一个子域 $\mathbb{F}_{p^e}$ 上的向量空间) 一个合适的非退化的交错型 f, 我们要证明相对于 f 来说, D 是“自对偶的”, 于是由 D 得到的射影点的集合 $\mathcal{M}$ 可以满足公式 (2.1), 于是可以生成秩为 r 的辛极空间 $\mathrm{W}(2r-1,p^e)$ 上的一个 m-ovoid. 本章的结构如下. 在第 2.2节中, 我们介绍了强正则图的一些基本知识, 并叙述了利用文献[7] 中有限域中的分圆类构造强正则图的方法. 在第 2.3节中, 我们首先详细介绍了我们的构造方法, 接着我们详细叙述了我们构造 $\mathrm{W}(2r-1,p^e)$ 上 m-ovoids 的具体细节. 最后, 我们在第 2.4节中对这一章做了总结.

2.2 准备工作

一个强正则图 $\mathrm{srg}(v,k,\lambda,\mu)$ 是一个有边的非完全图, 并且它是具有以下性质的简单无向图:

(1) 它是阶为 v(即总顶点个数为 v) 且每个顶点具有 k 条边的正则图.

(2) 对于任何一对相邻的顶点 x,y, 恰好有 λ 个顶点同时和 x 以及 y 相邻.

(3) 对于任何一对不相邻的顶点 x,y, 恰好有 μ 个顶点同时与 x 及 y 相邻.

例如, 一个五角形是一个 $\mathrm{srg}(5,2,0,1)$, 以及 Petersen 图 (见下方的图 2.1) 是一个 $\mathrm{srg}(10,3,0,1)$.

一个强正则图 $\mathrm{srg}(v,k,\lambda,\mu)$ 的参数满足下面引理 2.2所述的关系.

引理 2.2 (第 10.1 节, Godsil 和 Royle[31]) 设 Γ 是一个 $\mathrm{srg}(v,k,\lambda,\mu)$. 于是

$$k(k-\lambda-1)=\mu(v-k-1).$$

设 Γ 是一个简单无向图. Γ 的邻接矩阵 (adjacency matrix) 是 $(0,1)$-矩阵 A, 其行和列是以 Γ 中的顶点元素作为索引的, 当 x 和 y 在图 Γ 中相邻时, $A_{xy}=1$, 否则, $A_{xy}=0$. Γ 的特征值定义为其邻接矩阵 A 的特征值. 为方便起见, 如果 Γ 有一个非全一向量 $\mathbf{1}$ 的倍数的特征向量, 则称它的特征值是限制的 *(restricted)*. (对于一个 k-正则连通图, 其限制特征值即不同于 k 的特征值).

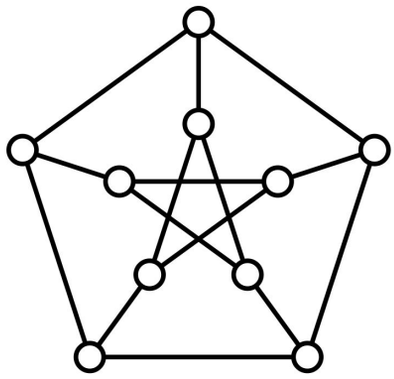

图 2.1　Petersen 图

定理 2.1 对于一个既非完全图也不是无边的 v 阶简单图 Γ, 记它的邻接矩阵为 A, 下列结论是等价的:

1. Γ 是参数为 (v,k,λ,μ) 的强正则图, 其中 k,λ,μ 是给定的整数,
2. 给定实数 k, λ, μ, 令 I, J 分别表示单位矩阵和全一矩阵, 则 $A^2=(\lambda-\mu)A+(k-\mu)I+\mu J$,
3. A 恰好有两个不同的限制特征值 α_1 和 α_2.

对于定理2.1的证明, 可以参考文献[6]. 为了方便后续调用, 我们给出如下 srg(v,k,λ,μ) 的参数和其限制特征值 α_1,α_2 之间的关系.

引理 2.3 (第 10.2 节, Godsil 和 Royle[31]) 令 Γ 为一个限制特征值为 α_1 和 α_2 的强正则图 srg(v,k,λ,μ), 其中 $\alpha_1>\alpha_2$. 于是

$$\begin{aligned}\alpha_1&=\frac{(\lambda-\mu)+\sqrt{(\lambda-\mu)^2+4(k-\mu)}}{2},\\ \alpha_2&=\frac{(\lambda-\mu)-\sqrt{(\lambda-\mu)^2+4(k-\mu)}}{2},\end{aligned}\tag{2.2}$$

它们的重数分别是

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

构造强正则图的一个有效方法是利用凯莱图 (Cayley graph). 令 G 是一个阶为 v 的加法交换群, 并且令 D 是群 G 的一个子集, 它满足条件 $0\notin D$ 以及 $-D=D$, 其中

$-D=\{-d|d\in D\}$. 群 G 上连接集为 D 的凯莱图 (这里用 Cay(G,D) 来表示) 是以 G 中的元素为顶点的图, 其顶点是相邻的当且仅当它们的差包含于 D. 令 $\hat{G}$ 为 G 的 (复) 特征群. 凯莱图 Cay(G,D) 的所有特征值可以表示为: $\psi(D):=\sum_{d\in D}\psi(d), \psi\in\hat{G}$. 注意到 $\psi_0(D)=|D|$, 这里 ψ_0 是 G 的平凡特征 (principal character). 由定理 2.1可知, 凯莱图 Cay(G,D) 是强正则图当且仅当 D 是 G 的生成集, 并且 $\{\psi(D):\psi\in\hat{G}\setminus\{\psi_0\}\}=\{\alpha_1,\alpha_2\}$, 这里 $\alpha_1\neq\alpha_2$. 在这种情况下, 相应的连接集 D 称为一个偏差集 *(partial difference set)*, 并且 D 的 *Delsarte* 对偶定义为 $\{\psi\in\hat{G}:\psi(D)=\alpha_i\}$ $(i=1,2)$ 中的任意一个.

一个强正则图 srg(v,k,λ,μ) 的参数如果满足 $(v,k,\lambda,\mu)=(n^2,a(n-\epsilon),\epsilon n+a^2-3\epsilon a,a^2-\epsilon a)$ 且 $\epsilon=1$ (相对应的, $\epsilon=-1$) , 我们称之为拉丁方类型 (相对应的, 负拉丁方类型).

令 G 和 D 分别为如上所述的群和集合, 假定相对应的凯莱图 Cay(G,D) 是一个强正则图 srg(v,k,λ,μ). 那么根据引理 2.3, D 的其中一个对偶和 D 含有相同数量的元素当且仅当

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

它们等价于

$$\frac{(2k+(v-1)(\lambda-\mu))^2}{(\lambda-\mu)^2+4(k-\mu)}=(v-1-2k)^2. \tag{2.3}$$

经过一些冗长的计算, 可以得到当 (2.3) 成立时, v 必定是一个平方元, 并且可以推出 $\mu=(\frac{k}{\sqrt{v}-1})^2-\frac{k}{\sqrt{v}-1}$ 或者 $\mu=(\frac{k}{\sqrt{v}+1})^2+\frac{k}{\sqrt{v}+1}$. 由引理 2.2可知, $\lambda=k-1+(1-\frac{v-1}{k})\mu$. 由此可知, 若 D 的一个对偶和 D 有相同数量的元素, 则强正则图 Cay(G,D) 一定是拉丁方类型的或者负拉丁方类型的.

反之, 当 $(v,k,\lambda,\mu)=(n^2,a(n-1),n+a^2-3a,a^2-a)$ 时, 由引理 2.3可知, $\alpha_1=n-a$, 其重数为 $f=a(n-1)$, 以及 $\alpha_2=-a$, 其重数为 $g=(n+1-a)(n-1)$. 因此, 对偶 $\{\psi\in\hat{G}:\psi(D)=\alpha_1\}$ 和 D 的元素个数相同. 当 $(v,k,\lambda,\mu)=(n^2,a(n+1),-n+a^2+3a,a^2+a)$ 时, 由引理 2.3可知, $\alpha_1=a$, 其重数为 $f=(n-1-a)(n+1)$, 以及 $\alpha_2=a-n$, 其重数为 $g=a(n+1)$. 因此, 对偶 $\{\psi\in\hat{G}:\psi(D)=\alpha_2\}$ 和 D 的元素个数相同.

我们要用凯莱图 Cay$(\mathbb{F}_q,D)$ 来构造辛极空间中的 m-ovoids, 这里 Cay$(\mathbb{F}_q,D)$ 的连接集 D 是一些分圆类的并. 在本节的最后, 我们给出有限域中分圆类的定义. 设 $q=p^s$ 是一个素数幂, 并且令 γ 为 $\mathbb{F}_q$ 中的一个给定的本原元. 设 $N>1$ 是 $q-1$ 的一

个因子. 定义 $\mathbb{F}_q$ 中 N 次分圆类$C_i^{(N,q)}$ 如下

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

其中, $0 \le i \le N-1$. 也就是说, $C_0^{(N,q)}$ 是由 $\mathbb{F}_q$ 中所有非零 N 次幂组成的 $\mathbb{F}_q^*$ 的子群, 并且对于所有的 $1 \le i \le N-1$, $C_i^{(N,q)} = \gamma^i C_0^{(N,q)}$ 成立. 在后文中, 如果 N, q 在行文中是明确的, 那么就把 $C_i^{(N,q)}$ 简写成 C_i.

假定 $q = p^s$, 其中 p 是一个素数, 设 e 是 s 的任意一个正因子. 令 $\mathrm{Tr}_{q/p^e} : \mathbb{F}_q \to \mathbb{F}_{p^e}$ 是 $\mathbb{F}_q$ 到 $\mathbb{F}_{p^e}$ 的迹函数, 即

$$\mathrm{Tr}_{q/p^e}(x) = x + x^{p^e} + \cdots + x^{p^{e(s/e-1)}},\ \forall x \in \mathbb{F}_q.$$

记 $\omega_p := \exp\left(\frac{2\pi\sqrt{-1}}{p}\right)$. 定义 $\psi_{\mathbb{F}_q} : \mathbb{F}_q \to \mathbb{C}^*$ 如下:

$$\psi_{\mathbb{F}_q}(x) = \omega_p^{\mathrm{Tr}_{q/p}(x)},\ \forall x \in \mathbb{F}_q.$$

映射 $\psi_{\mathbb{F}_q}$ 是 $\mathbb{F}_q$ 上加法群的特征, 它被称为 $\mathbb{F}_q$ 的标准加法特征 *(canonical additive character)*. 对于任意 $y \in \mathbb{F}_q$, 定义 $\psi_{\mathbb{F}_q,y} : \mathbb{F}_q \to \mathbb{C}^*$ 如下:

$$\psi_{\mathbb{F}_q,y}(x) = \psi_{\mathbb{F}_q}(xy),\ \forall x \in \mathbb{F}_q.$$

众所周知, 我们有 $\{\psi_{\mathbb{F}_q,y} \mid y \in \mathbb{F}_q\} = \widehat{(\mathbb{F}_q, +)}$.

接下来回顾由文献[7] 给出的关于强正则凯莱图的构造, 该构造也可以在文献[6] 的 9.8.5 节中找到. 假定 $q = p^s$, 其中 p 是一个素数, 令 N 为 $q-1$ 的一个真因子, 并且对某个正整数 ℓ, 它满足 $p^\ell \equiv -1 \pmod N$. 令 ℓ 取满足上述条件的最小值, 并且记 $s = 2\ell t$. 取大小为 u 的真子集 $J \subset \mathbb{Z}_N$. 若 q 是偶数, 那么 J 的取法是任意的; 若 q 是奇数, 那么就需要额外的条件, 即 $N \mid \frac{q-1}{2}$ 以及 $J + \frac{q-1}{2} = J$. 设 $D_J = \cup_{i\in J} C_i$. 那么图 $\mathrm{Cay}(\mathbb{F}_q, D_J)$ 是强正则图, 其特征值如下

$$\begin{aligned} k &= \frac{q-1}{N}u, \quad \text{重数为 } 1, \\ \alpha_1 &= \frac{u}{N}(-1 + (-1)^t\sqrt{q}), \quad \text{重数为 } q-1-k, \\ \alpha_2 &= \frac{u}{N}(-1 + (-1)^t\sqrt{q}) + (-1)^{t+1}\sqrt{q}, \quad \text{重数为 } k. \end{aligned} \tag{2.4}$$

具体地说, 对于 $i = 0, 1, ..., N-1$, 有

$$\psi_{\mathbb{F}_q}(\gamma^i D_J) = \begin{cases} \alpha_2, & \text{如果 } \varepsilon^s = 1 \text{ 以及 } i \in -J \pmod N \\ & \quad \text{或者 } \varepsilon^s = -1 \text{ 以及 } i \in -J + N/2 \pmod N, \\ \alpha_1, & \text{其他情形}, \end{cases} \tag{2.5}$$

其中, $\varepsilon = \begin{cases} -1, & \text{如果 } N \text{ 是偶数且 } \frac{p^\ell+1}{N} \text{ 是奇数,} \\ 1, & \text{其他情形.} \end{cases}$

若 t 是奇数 (相应的, 偶数), 则图 Cay($\mathbb{F}_q$, D_J) 是拉丁方类型 (相应的, 负拉丁方类型) 的.

2.3 用强正则凯莱图构造 $\mathbf{W}(2r-1, p^e)$ 中的 m-ovoids

在这一章的剩余部分中, 固定下面一些符号. 令 $q = p^s$, 其中 p 是一个奇素数, $s = 2er$, 其中 e 和 $r > 2$ 均为正整数. 将 $\mathbb{F}_q$ 看作 $\mathbb{F}_{p^e}$ ($\mathbb{F}_q$ 的一个子域) 上的一个 $2r$-维向量空间, 用 V 来表示这样的 $\mathbb{F}_{p^e}$-向量空间. 照例, 对于一个非零元 $v \in V$, 记 $\langle v \rangle$ 为由 v 张成的 1-维 $\mathbb{F}_{p^e}$-子空间在射影空间 PG(V) 中对应的射影点. 赋予 V 一个双线性型如下. 令 $L(X) = \sum_{i=0}^{2r-1} c_i X^{p^{ie}} \in \mathbb{F}_q[X]$ 是一个线性化多项式. 定义 $f : V \times V \to \mathbb{F}_{p^e}$ 如下

$$f(x,y) = \mathrm{Tr}_{q/p^e}(xL(y)), \forall (x,y) \in V \times V.$$

那么 f 是 V 上的一个 $\mathbb{F}_{p^e}$-双线性型.

引理 2.4 *沿用上面的符号, V 上的 $\mathbb{F}_{p^e}$-双线性型 f 是交错的当且仅当 $c_0 = 0$, 并且对于 $1 \le i \le 2r-1$, $c_{2r-i}^{p^{ie}} = -c_i$. 此外, f 是非退化的当且仅当 $x \mapsto L(x)$ 是将 $\mathbb{F}_q$ 映射到它自己的一个双线性型.*

证明. 可知双线性型 f 是一个交错型当且仅当 $f(x,x) = 0$ 对所有的 $x \in V$ 都成立. 我们有

$$\begin{aligned} f(x,x) &= \sum_{i=0}^{2r-1} \mathrm{Tr}_{q/p^e}\left(c_i x^{1+p^{ie}}\right) \\ &= \sum_{i,j=0}^{2r-1} c_i^{p^{je}} x^{p^{je}+p^{(i+j)e}} \\ &= \sum_{0 \le i < k \le 2r-1} (c_{k-i}^{p^{ie}} + c_{2r-k+i}^{p^{ke}}) x^{p^{ie}+p^{ke}} + \sum_{j=0}^{2r-1} c_0^{p^{je}} x^{2p^{je}}. \end{aligned}$$

将 $f(x,x)$ 视为关于 x 的多项式, 其系数是 $\mathbb{F}_q$ 中的元素. 从上面的表达式中, 可以观察得到多项式 $f(x,x)$ 的次数是小于等于 $q-1$ 的. $\mathbb{F}_q$ 中的每个元素代入到多项式 $f(x,x)$ 中都为 0 当且仅当多项式 $f(x,x)$ 是一个零多项式. 于是, 通过比较多项式 $f(x,x)$ 的系数, 我们可以证明引理的第一个结论.

假定 f 是非退化的. 假设对于所有的 $x \in \mathbb{F}_q$, $f(x,y) = \mathrm{Tr}_{q/p^e}(xL(y)) = 0$ 都成立. 因为 Tr_{q/p^e} 是 V 上的一个非平凡的线性型, 所以我们有 $L(y) = 0$. 根据假设, f 是非

退化的, 于是我们有 $y=0$. 又因为 L 是线性化的, 所以 $x \mapsto L(x)$ 是一个双射. 反之, 结果是显而易见的. 于是第二个结论的证明就完成了. □

令 $L(X)=\sum_{i=1}^{2r-1} c_i X^{p^{ie}} \in \mathbb{F}_q[X]$ 为一个线性化的置换多项式, 它使得 $f(x,y)=\mathrm{Tr}_{q/p^e}(xL(y))$ 是一个非退化的交错型. 赋予 $V=(\mathbb{F}_q,+)$ 上述交错型 f, 它将成为我们在辛极空间 $\mathrm{W}(2r-1,p^e)$ 上秩为 r 的模型. 对于任意非零 $y \in V$, 定义

$$\langle y\rangle^{\perp}=\{\langle x\rangle : f(x,y)=0,\ x \in V \setminus \{0\}\}.$$

同时, 对于任意 $y \in V$, 另外定义 $\Psi_y \in \widehat{(\mathbb{F}_q,+)}$ 如下:

$$\Psi_y(x)=\psi_{\mathbb{F}_q}(xL(y))=\psi_{\mathbb{F}_{p^e}}(f(x,y)).$$

众所周知, 我们有 $\{\Psi_y \mid y \in V\}=\widehat{(\mathbb{F}_q,+)}$. 我们现在给出 $(\mathbb{F}_q,+)$ 中自对偶偏差集的定义 (根据上一节中的讨论, 我们注意到这样的一个自对偶偏差集一定是拉丁方类型或者负拉丁方类型的). 令 D 为 $\mathbb{F}_q^*$ 中的一个 $\mathbb{F}_{p^e}^*$-不变子集, 即 D 为 $\mathbb{F}_{p^e}^*$ 在 $\mathbb{F}_q^*$ 中的某些陪集的并. 假定相应的凯莱图 $\mathrm{Cay}(\mathbb{F}_q,D)$ 为一个负拉丁方类型的强正则图, 其参数为

$$\left(q,|D|,-\sqrt{q}+(\frac{|D|}{\sqrt{q}+1})^2+\frac{3|D|}{\sqrt{q}+1},(\frac{|D|}{\sqrt{q}+1})^2+\frac{|D|}{\sqrt{q}+1}\right).$$

令 $D^* \subset \mathbb{F}_q \setminus \{0\}$ 为一个集合, 它使得 $\{\Psi_y \in \widehat{(\mathbb{F}_q,+)} \mid y \in D^*\}$ 是 D 的某一个 Delsarte 对偶. 如果 $D^*=D$, 就称 D 是自对偶的. 接下来我们将详细阐述 $\mathrm{W}(2r-1,p^e)$ 中的 m-ovoids 和 $(\mathbb{F}_q,+)$ 中的自对偶偏差集之间的关系.

定理 2.2 沿用上面的符号, 令 D 为 $\mathbb{F}_q^*$ 的一个 $\mathbb{F}_{p^e}^*$-不变子集, 它满足

$$|D| \equiv 0 \pmod{(\sqrt{q}+1)(p^e-1)}.$$

那么集合 $\mathcal{M}=\{\langle v\rangle : v \in D\}$ 是 $\mathrm{W}(2r-1,p^e)$ 中的一个 $\frac{|D|}{(p^e-1)(\sqrt{q}+1)}$-ovoid 当且仅当 D 是一个自对偶偏差集, 且它的参数为

$$(q,|D|,-\sqrt{q}+(\frac{|D|}{\sqrt{q}+1})^2+\frac{3|D|}{\sqrt{q}+1},(\frac{|D|}{\sqrt{q}+1})^2+\frac{|D|}{\sqrt{q}+1}).$$

证明. 假定 D 是一个具有该定理中所述参数的自对偶偏差集. 那么根据引理 2.3, 凯莱图 $\mathrm{Cay}(\mathbb{F}_q, D)$ 有两个特征值 $\alpha_1=\frac{|D|}{\sqrt{q}+1}$ (其重数为 $m_1=q-1-|D|$), 以及 $\alpha_2=\frac{|D|}{\sqrt{q}+1}-\sqrt{q}$ (其重数为 $m_2=|D|$); 此外, 由于 D 是自对偶的, 所以当 $y \in D^*=D$, 我们有 $\Psi_y(D)=\alpha_2$, 当 $y \in \mathbb{F}_q^* \setminus D$ 时, 我们有 $\Psi_y(D)=\alpha_1$.

记 $\mathcal{M} := \{\langle v_i\rangle : 1 \le i \le M\}$, 这里 $M = |D|/(p^e-1)$. 那么 $D = \{\theta v_i : 1 \le i \le M, \theta \in \mathbb{F}_{p^e}^*\}$. 对于任意非零 $y \in V$, 可以计算得到

$$\begin{aligned}\Psi_y(D) &= \sum_{i=1}^{M}\sum_{\theta\in\mathbb{F}_{p^e}^*}\Psi_y(\theta v_i)\\ &= \sum_{i=1}^{M}\sum_{\theta\in\mathbb{F}_{p^e}^*}\psi_{\mathbb{F}_{p^e}}(\theta f(v_i,y))\\ &= -M + \sum_{i=1}^{M}\sum_{\theta\in\mathbb{F}_{p^e}}\psi_{\mathbb{F}_{p^e}}(\theta f(v_i,y))\\ &= -M + p^e\cdot|\{1\le i\le M:\ f(v_i,y)=0\}|\\ &= p^e\cdot|\langle y\rangle^\perp\cap\mathcal{M}| - |\mathcal{M}|.\end{aligned}$$

已知如果 $y \in D$, 则 $\Psi_y(D) = \alpha_2$, 可以推出, 如果 $\langle y\rangle \in \mathcal{M}$, 则

$$|\langle y\rangle^\perp\cap\mathcal{M}| = \frac{|D|}{(p^e-1)(\sqrt{q}+1)}\cdot(p^{e(r-1)}+1) - p^{e(r-1)};$$

进一步, 如果 $y \in \mathbb{F}_q^* \setminus D$, 则 $\Psi_y(D) = \alpha_1$, 可以推出, 如果 $\langle y\rangle \notin \mathcal{M}$, 则

$$|\langle y\rangle^\perp\cap\mathcal{M}| = \frac{|D|}{(p^e-1)(\sqrt{q}+1)}\cdot(p^{e(r-1)}+1).$$

因此由引理 2.1可知, 集合 $\mathcal{M}$ 是辛极空间 $\mathrm{W}(2r-1,p^e)$ 中的一个 $\frac{|D|}{(p^e-1)(\sqrt{q}+1)}$-ovoid. 反之, 我们可以简单地利用上述推导的反向推导得到结论. 所以, 定理的证明到这里就完成了. □

我们接下来会对自对偶性进行一些说明. 令 D 为 $\mathbb{F}_q^*$ 上的一个 $\mathbb{F}_{p^e}^*$-不变子集. 假定 $\mathrm{Cay}(\mathbb{F}_q, D)$ 是一个负拉丁方类型的强正则图, 其参数为

$$\left(q, |D|, -\sqrt{q} + (\frac{|D|}{\sqrt{q}+1})^2 + \frac{3|D|}{\sqrt{q}+1}, (\frac{|D|}{\sqrt{q}+1})^2 + \frac{|D|}{\sqrt{q}+1}\right).$$

定义

$$D' = \{y \in \mathbb{F}_q : \psi_{\mathbb{F}_q,y}(D) = \alpha_2\}. \tag{2.6}$$

注意到 $\Psi_y(D) = \psi_{\mathbb{F}_q,L(y)}(D)$, 于是可以知道 D 是自对偶的当且仅当 $L(D) = D'$.

我们将会利用定理 2.2来构造 $\mathrm{W}(2r-1,p^e)$ 中的 m-ovoids. 第一步, 我们将会通过仔细选择上面提到的 $L(X)$ 来赋予 V 一个具体的非退化交错型. 令 γ 为 $\mathbb{F}_q$ 中的一个本原元 (回顾上文, $q = p^s$ 为一个奇素数幂, 且 $s = 2er$), 并且设 $\delta = \gamma^{\frac{\sqrt{q}+1}{2}} \in \mathbb{F}_q$. 那么就有 $\delta^{\sqrt{q}} = -\delta$. 令 $L(X) = \delta X^{\sqrt{q}}$. 根据引理 2.4, $f(x,y) := \mathrm{Tr}_{q/p^e}(xL(y))$ 是一个定

义在 V 上的非退化交错型. 在本章的剩余部分, 我们将会选择伴随着 f 的 V 作为我们在辛极空间 $\mathrm{W}(2r-1,p^e)$ 中的模型.

我们进一步假定 $q=p^s$, 这里 $s=2\ell t$ 并且 t 是偶数. 选取 $N=p^\ell+1$, 并且令 $C_0,\ldots,C_{N-1}$ 为 $\mathbb{F}_q$ 中的 N 阶分圆类. 在这种情况下, 很容易验证 $N\mid\frac{q-1}{2}$. 令 J 为 $\mathbb{Z}_N$ 中大小为 u 的真子集, 并且设 $D_J=\cup_{i\in J}C_i$. 根据文献[7](参考第二节结尾部分的讨论), 图 $\mathrm{Cay}(\mathbb{F}_q,D_J)$ 是一个负拉丁方类型的强正则图, 其参数为

$$\left(q,\frac{u(\sqrt{q}-1)}{N}(\sqrt{q}+1),-\sqrt{q}+(\frac{u(\sqrt{q}-1)}{N})^2+\frac{3u(\sqrt{q}-1)}{N},\right.$$
$$\left.(\frac{u(\sqrt{q}-1)}{N})^2+\frac{u(\sqrt{q}-1)}{N}\right).$$

此外, 它的特征值为

$$\psi_{\mathbb{F}_q}(\gamma^iD_J)=\begin{cases}\frac{u}{N}(\sqrt{q}-1)-\sqrt{q}, & \text{如果 } -i\ (\mathrm{mod}\ N)\in J,\\ \frac{u}{N}(\sqrt{q}-1), & \text{其他情形.}\end{cases}\tag{2.7}$$

于是我们得到 $D'_J=\cup_{-i\in J}C_i$, 这里 D'_J 如 (2.6) 中所定义. 为了利用定理 2.2构造 $\mathrm{W}(2r-1,p^e)$ 中的 m-ovoids, 我们需要令 D_J 为自对偶的. 为了避免生成的结果可以同时由 field reduction 方法得到, 我们进一步假设 r 是奇数.

引理 2.5 沿用上述符号, 则 D_J 是自对偶的当且仅当 J 是 σ-不变的, 这里 $\sigma:i\mapsto -1-i\ (\mathrm{mod}\ N)$.

证明. 我们有 $L(C_i)=\gamma^{\frac{\sqrt{q}+1}{2}+\sqrt{q}i}C_0$, 即 L 将 C_i 映射到 $C_{\tau(i)}$, 这里 $\tau(i):=\frac{\sqrt{q}+1}{2}+\sqrt{q}i\ (\mathrm{mod}\ N)$. 注意到 $\sqrt{q}\equiv 1\ (\mathrm{mod}\ N)$, 且由假设, t 是偶数, 那么就有 $\frac{\sqrt{q}-1}{2}=\frac{(p^{\ell t}-1)}{(p^{2\ell}-1)}\cdot\frac{(p^\ell-1)}{2}\cdot N\equiv 0\ (\mathrm{mod}\ N)$. 因此 $\tau(i)\equiv i+1\ (\mathrm{mod}\ N)$. 偏差集 D_J 是自对偶的当且仅当 $L(D_J)=D'_J$, 这等价于 $\{i+1\ (\mathrm{mod}\ N):i\in J\}=\{-i\ (\mathrm{mod}\ N):i\in J\}$, 即 $-J-1=J$. 引理的证明到此完成. □

引理 2.6 沿用上面的符号, D_J 是 $\mathbb{F}_{p^e}^*$-不变的当且仅当 J 在映射 $\rho:i\mapsto i+2d_0\ (\mathrm{mod}\ N)$ 下是不变的, 这里 d_0 是一个奇数, 其定义如下

$$d_0:=\gcd\left(\frac{N}{2},\frac{\sqrt{q}-1}{p^e-1}\right).\tag{2.8}$$

证明. 注意到 $\mathbb{F}_{p^e}^*=\langle\gamma^{(q-1)/(p^e-1)}\rangle$. 所以 D_J 是 $\mathbb{F}_{p^e}^*$-不变的当且仅当 J 在映射 $i\mapsto i+\frac{q-1}{p^e-1}\ (\mathrm{mod}\ N)$ 下是不变的. 根据假设, t 是偶数, 那么就有有 $\sqrt{q}+1\equiv 2\ (\mathrm{mod}\ N)$. 于是可以推导出 $\gcd(N,\frac{q-1}{p^e-1})=\gcd(N,\frac{2(\sqrt{q}-1)}{p^e-1})=2d_0$, 这里 d_0 如(2.8)中所定义. 引理得证. □

定理 2.3 令 p 为一个奇素数, 并且令 $q = p^s$, 其中 $s = 2er = 2\ell t$ 对某些正整数 e, r, ℓ, t 成立, 这里 r 是奇数且 t 是偶数. 设 $N = p^\ell + 1$, 并且令 d_0 如(2.8)中所定义. 如果 $d_0 > 1$, 那么对于每个整数 $1 \leq b \leq d_0 - 1$, 都存在 $\mathrm{W}(2r-1, p^e)$ 中的一个 $\frac{b(\sqrt{q}-1)}{d_0(p^e-1)}$-ovoid.

证明. 我们继续沿用上面所有的符号. 根据引理 2.5以及引理 2.6, 集合 D_J 是 $\mathbb{F}_{p^e}^*$-不变的并且满足 $L(D_J) = D_J'$ 当且仅当 J 在映射 $\rho : i \mapsto i + 2d_0 \pmod N$ 和映射 $\sigma : i \mapsto -1 - i \pmod N$ 下是不变的. 根据 $\langle \rho, \sigma \rangle$ 是一个二面体群 $D_{\frac{N}{d_0}}$ 这个事实 (参考文献[57] 中的 2.24), 我们断定 $\langle \rho, \sigma \rangle = \{1, \rho, \rho^2, ..., \rho^{\frac{N}{2d_0}-1}, \sigma, \rho\sigma, \rho^2\sigma, ..., \rho^{\frac{N}{2d_0}-1}\sigma\}$. 因此, $\mathbb{Z}_N$ 上的每个 $\langle \rho, \sigma \rangle$-轨道 $\mathcal{O}$ 有相同的长度 $\frac{N}{d_0}$, 并且相应分圆类的并 $D_\mathcal{O} = \cup_{i \in \mathcal{O}} C_i$ 大小为 $|C_0| \cdot \frac{N}{d_0} = \frac{q-1}{d_0}$. 这个大小可以被 $(\sqrt{q}+1)(p^e-1)$ 整除, 因为由(2.8)可知, d_0 整除 $\frac{\sqrt{q}-1}{p^e-1}$. 因此, $D_\mathcal{O}$ 是 $\mathrm{W}(2r-1, p^e)$ 中的一个 m-ovoid, 这里 $m = \frac{\sqrt{q}-1}{d_0(p^e-1)}$. 对于每一个 $1 \leq b \leq d_0 - 1$, 通过合并 b 个不同的 $D_\mathcal{O}$, 就可以得到 $\mathrm{W}(2r-1, p^e)$ 上的 bm-ovoids. □

引理 2.7 定义映射 $g_1 : x \mapsto \eta x$, 这里 $\eta^{\frac{(\sqrt{q}+1)(p^e-1)}{2}} = 1$, 以及 $g_2 : x \mapsto x^{\sqrt{q}}$, 这两个映射是 $\mathrm{W}(2r-1, p^e)$ 上的自同构, 注意到 $f(x, y) = \mathrm{Tr}_{q/p^e}(\delta x y^{\sqrt{q}})$, 这里 $\delta = \gamma^{\frac{\sqrt{q}+1}{2}}$, 那么这两个自同构满足下面的条件:

(1) 对于任意的 $x, y \in \mathbb{F}_q$, 有 $f(g_1(x), g_1(y)) = \eta^{\sqrt{q}+1} f(x, y)$, 且 $g_1(D_\mathcal{O}) = D_\mathcal{O}$, 这里 $\mathcal{O}$ 如定理 2.3中所定义;

(2) 对于任意的 $x, y \in \mathbb{F}_q$, 有 $f(g_2(x), g_2(y)) = -f(x, y)$, 且 $g_2(D_\mathcal{O}) = D_\mathcal{O}$, 这里 $\mathcal{O}$ 如定理 2.3中所定义.

证明. 首先注意到 $\mathcal{O}$ 是 $\mathbb{Z}$ 上的一个 $\langle \rho, \sigma \rangle$-轨道, 这里, 我们有 $\rho : i \mapsto i + 2d_0 \pmod N$, $\sigma : i \mapsto -1 - i \pmod N$ 以及 $D_\mathcal{O} = \cup_{i \in \mathcal{O}} C_i$. 接着我们将提供该引理中 (1) 和 (2) 的证明.

(1) 对于任意的 $x, y \in \mathbb{F}_q$, 可以推出

$$\begin{aligned} f(g_1(x), g_1(y)) &= \mathrm{Tr}_{q/p^e}(\delta \eta^{\sqrt{q}+1} x y^{\sqrt{q}}) \\ &= \eta^{\sqrt{q}+1} \mathrm{Tr}_{q/p^e}(\delta x y^{\sqrt{q}}) \\ &= \eta^{\sqrt{q}+1} f(x, y). \end{aligned}$$

上述推导的第二个等号来自于结论 $\eta^{(\sqrt{q}+1)(p^e-1)} = (\eta^{\frac{(\sqrt{q}+1)(p^e-1)}{2}})^2 = 1$.

对于每一个 $z \in D_\mathcal{O}$, 存在一个 $j_0 \in \mathcal{O}$ 使得 $\eta^{\frac{(\sqrt{q}+1)(p^e-1)}{2}} = 1$ 成立, 也就是说, $\frac{h(\sqrt{q}+1)(p^e-1))}{2} \equiv 0 \pmod{q-1}$. 因此, 可以推出 $h \equiv 0 \pmod{\frac{2(\sqrt{q}-1)}{p^e-1}}$. 因为 $d_0 =$

$\gcd(\frac{N}{2}, \frac{\sqrt{q}-1}{p^e-1})$, 于是就有 $2d_0 = \gcd(N, \frac{2(\sqrt{q}-1)}{p^e-1})$, 因此, 对于某个整数 h', 有 $h \equiv 2d_0h' \pmod N$ 成立. 所以可以推导得到

$$g_1(z) = \eta z \in \gamma^{2d_0h'} C_{j_0} = C_{\rho^{h'}(j_0)}.$$

于是 $g_1(z) \in D_{\mathcal{O}}$. 注意到 g_1 是一个双射, 所以有 $g_1(D_{\mathcal{O}}) = D_{\mathcal{O}}$ 成立.

(2) 对于任意的 $x, y \in F_q$, 可以推出

$$\begin{aligned} f(g_2(x), g_2(y)) &= \mathrm{Tr}_{q/p^e}(\delta x^{\sqrt{q}} y) \\ &= \mathrm{Tr}_{q/p^e}(\delta^{1-\sqrt{q}} (\delta x y^{\sqrt{q}})^{\sqrt{q}}) \\ &= -\mathrm{Tr}_{q/p^e}(\delta x y^{\sqrt{q}}) \\ &= -f(x, y). \end{aligned}$$

上述推导的第三个等号由结论 $\delta^{1-\sqrt{q}} = \gamma^{-\frac{q-1}{2}} = -1$ 以及

$$\begin{aligned} \mathrm{Tr}_{q/p^e}((\delta x y^{\sqrt{q}})^{\sqrt{q}}) &= \mathrm{Tr}_{\sqrt{q}/p^e}(\mathrm{Tr}_{q/\sqrt{q}}(\delta x y^{\sqrt{q}})^{\sqrt{q}}) \\ &= \mathrm{Tr}_{\sqrt{q}/p^e}(\mathrm{Tr}_{q/\sqrt{q}}(\delta x y^{\sqrt{q}})) \\ &= \mathrm{Tr}_{q/p^e}(\delta x y^{\sqrt{q}}) \end{aligned}$$

得到.

对于每一个 $z \in D_{\mathcal{O}}$, 存在一个 $j_0 \in \mathcal{O}$ 使得 $z \in C_{j_0}$ 成立. 因为 $N = p^l + 1$ 以及 $\sqrt{q} - 1 = p^{lt} - 1$, 这里 t 是一个偶数, 我们有 $j_0\sqrt{q} \equiv j_0 \pmod N$. 因此, 可以推导得到

$$g_2(z) = z^{\sqrt{q}} \in C_{j_0}.$$

对于 $z, z' \in \mathcal{O}$, 当 $g_2(z) = g_2(z')$ 时, 很容易证明得到 $z = z'$. 所以, 有 $g_2(D_{\mathcal{O}}) = D_{\mathcal{O}}$ 成立.

□

注 2.1 由定理 2.3得到的 $W(2r-1, p^e)$ 中的 m-ovoids 有下面的自同构:$g_1 : x \mapsto \eta x$, 这里 $\eta \in \mathbb{F}_q^*$ 的乘法阶为 $\frac{(\sqrt{q}+1)(p^e-1)}{2}$, 以及 $g_2 : x \mapsto x^{\sqrt{q}}$, 它们共同构成了一个亚循环群. 该亚循环群同时也是相应的强正则凯莱图 $\mathrm{Cay}(\mathbb{F}_q, D_{\mathcal{O}})$ 的自同构群. 确定定理 2.3中生成的 m-ovoids 的全自同构群以及探究我们构造的 m-ovoids 的自同构群和其相应的强正则凯莱图之间的联系也是个相当有意义的问题.

在以下讨论中, 我们选取 r 为奇素数 p_0, 并且给出使得 $d_0 > 1$ 的具体条件, 这里 d_0 如(2.8)中所定义. 这种情况下, 我们可以排除由定理 2.3得到的 m-ovoids 可以同时

由 field reduction 方法得到的可能性. 回顾上文, 我们有 $s = 2ep_0 = 2\ell t$, 这里 t 是偶数. 考虑如下两种可能.

(A) 首先考虑 $p_0 \mid t$ 的情况. 记 $t = p_0 t_0$. 由于 t 是偶数, p_0 是奇素数, 所以 t_0 为偶数, 且 $e = \ell t_0$, 于是

$$\frac{\sqrt{q}-1}{p^e-1} = \sum_{i=0}^{p_0-1} p^{ie} = \sum_{i=0}^{p_0-1} p^{i\ell t_0} \equiv p_0 \pmod{p^\ell+1}.$$

因此 $d_0 = \gcd(N/2, p_0) = \gcd(N, p_0)$. 在这种情况下, $d_0 > 1$ 当且仅当 $p_0 \mid (p^\ell+1)$, 这也等同于 $d_0 = p_0$. 在表格 2.1中, 我们给出利用定理 2.3, 在这种情况下构造出的一些 m-ovoids 的例子.

(B) 接下来, 考虑 p_0 不整除 t 的情况. 在这种情况下, 由 $p_0 e = \ell t$, 可以推出 $p_0 \mid \ell$. 记 $\ell = \ell_0 p_0$, 于是 $e = \ell_0 t$. 我们断定 $d_0 = \gcd(N/2, \frac{\sqrt{q}-1}{p^e-1})$ 总是大于 1 的. 由于 t 是偶数, 则我们有

$$\sqrt{q} - 1 = p^{\ell t} - 1 \equiv (-1)^t - 1 = 0 \pmod{N},$$

所以 $N/2$ 整除 $\sqrt{q}-1$. 另一方面, 由于 $p_0 \nmid t$, 我们有

$$\gcd(p^e-1, N/2) \mid \gcd(p^e-1, p^{2\ell}-1) = p^{\gcd(e,2\ell)} - 1 = p^{2\ell_0} - 1.$$

因为 $p^{2\ell_0} - 1 < N/2 = (p^{\ell_0 p_0}+1)/2$, 可以知道 $N/2$ 不整除 $p^e - 1$. 综上所述, 总是有 $d_0 > 1$. 在表格 4.1中, 我们给出了通过定理 2.3在这种情况下构造得到的一些 m-ovoids 的例子.

文献[2] 中提出了一种猜想: 如果辛极空间 $\mathrm{W}(2r-1, p^e)$ 中存在一个 m-ovoid, 这里 $r > 2$, 那么对于某个常数 $c > 0$, 有 $m \geq cp^{e(r-2)}$ 成立.

根据定理 2.3, 我们可以知道, 当 $d_0 > 1$ 时, $\mathrm{W}(2r-1, p^e)$ 中存在 m-ovoids, 这里 $m = \frac{b(\sqrt{q}-1)}{d_0(p^e-1)}$. 可以计算得到

$$\frac{m}{p^{e(r-2)}} = \frac{b(\sqrt{q}-1)}{d_0(p^e-1)p^{e(r-2)}} = \frac{b(p^{er}-1)}{d_0(p^{e(r-1)} - p^{e(r-2)})}.$$

接下来我们将给出一些例子作为上述猜想的反例.

例子 2.1 在情况 (B) 中, 当 $p = 3, r = p_0 = 5, t = 2$ 时, 我们有

$$d_0 = \gcd\left(\frac{3^{5\ell_0}+1}{2}, \frac{3^{10\ell_0}-1}{3^{2\ell_0}-1}\right).$$

表 2.1　当 $r = p_0$ 为奇素数, $p_0 \mid t$ 时, 定理 2.3构造得到的 m-ovoids

p_0	p	ℓ	t	d_0	$W(2p_0-1, p^e)$	m
3	p odd	1	$6k, k \in \mathbb{Z}^+$	3	$W(5, p^{2k})$	$\frac{b}{3}(p^{4k}+p^{2k}+1), b \in \{1,2\}$
5	3	2	$10k, k \in \mathbb{Z}^+$	5	$W(9, 3^{4k})$	$\frac{b(3^{20k}-1)}{5(3^{4k}-1)}, 1 \le b \le 4$
5	7	2	$10k, k \in \mathbb{Z}^+$	5	$W(9, 7^{4k})$	$\frac{b(7^{20k-1})}{5(7^{4k}-1)}, 1 \le b \le 4$
5	13	2	$10k, k \in \mathbb{Z}^+$	5	$W(9, 13^{4k})$	$\frac{b(13^{20k}-1)}{5(13^{4k}-1)}, 1 \le b \le 4$
5	17	2	$10k, k \in \mathbb{Z}^+$	5	$W(9, 17^{4k})$	$\frac{b(17^{20k}-1)}{5(17^{4k}-1)}, 1 \le b \le 4$
5	19	1	$10k, k \in \mathbb{Z}^+$	5	$W(9, 19^{2k})$	$\frac{b(19^{10k}-1)}{5(19^{2k}-1)}, 1 \le b \le 4$
7	3	3	$14k, k \in \mathbb{Z}^+$	7	$W(13, 3^{6k})$	$\frac{b(3^{42k}-1)}{7(3^{6k}-1)}, 1 \le b \le 6$
7	5	3	$14k, k \in \mathbb{Z}^+$	7	$W(13, 5^{6k})$	$\frac{b(5^{42k}-1)}{7(5^{6k}-1)}, 1 \le b \le 6$
7	13	3	$14k, k \in \mathbb{Z}^+$	7	$W(13, 13^{6k})$	$\frac{b(13^{42k}-1)}{7(13^{6k}-1)}, 1 \le b \le 6$
11	7	5	$22k, k \in \mathbb{Z}^+$	11	$W(21, 7^{10k})$	$\frac{b(7^{110k}-1)}{11(7^{10k}-1)}, 1 \le b \le 10$
11	13	5	$22k, k \in \mathbb{Z}^+$	11	$W(21, 13^{10k})$	$\frac{b(13^{110k}-1)}{11(13^{10k}-1)}, 1 \le b \le 10$
11	17	5	$22k, k \in \mathbb{Z}^+$	11	$W(21, 17^{10k})$	$\frac{b(17^{110k}-1)}{11(17^{10k}-1)}, 1 \le b \le 10$
11	19	5	$22k, k \in \mathbb{Z}^+$	11	$W(21, 19^{10k})$	$\frac{b(19^{110k}-1)}{11(19^{10k}-1)}, 1 \le b \le 10$
13	5	2	$26k, k \in \mathbb{Z}^+$	13	$W(25, 5^{4k})$	$\frac{b(5^{52k}-1)}{13(5^{4k}-1)}, 1 \le b \le 12$
13	7	6	$26k, k \in \mathbb{Z}^+$	13	$W(25, 7^{12k})$	$\frac{b(5^{156k}-1)}{13(5^{12k}-1)}, 1 \le b \le 12$

表 2.2　当 $r = p_0$ 为奇素数, $p_0 \nmid t$ 时, 定理 2.3构造得到的 m-ovoids

p_0	p	ℓ	t	d_0	$W(2p_0-1, p^e)$	m
3	3	3	$2k, 3 \nmid k$	7	$W(5, 3^{2k})$	$\frac{b(3^{6k}-1)}{7(3^{2k}-1)}, 1 \le b \le 6$
3	5	3	$2k, 3 \nmid k$	21	$W(5, 5^{2k})$	$\frac{b(5^{6k}-1)}{21(5^{2k}-1)}, 1 \le b \le 20$
3	7	3	$2k, 3 \nmid k$	43	$W(5, 7^{2k})$	$\frac{b(7^{6k}-1)}{43(7^{2k}-1)}, 1 \le b \le 42$
5	3	5	$2k, 5 \nmid k$	61	$W(9, 3^{2k})$	$\frac{b(3^{10k}-1)}{61(3^{2k}-1)}, 1 \le b \le 60$
5	5	5	$2k, 5 \nmid k$	521	$W(9, 5^{2k})$	$\frac{b(5^{10k}-1)}{521(5^{2k}-1)}, 1 \le b \le 520$
7	3	7	$2k, 7 \nmid k$	547	$W(13, 3^{2k})$	$\frac{b(3^{14k}-1)}{547(3^{2k}-1)}, 1 \le b \le 546$
7	5	7	$2k, 7 \nmid k$	13021	$W(13, 5^{2k})$	$\frac{b(5^{14k}-1)}{13021(5^{2k}-1)}, 1 \le b \le 13020$
11	3	11	$2k, 11 \nmid k$	44287	$W(21, 3^{2k})$	$\frac{b(3^{22k}-1)}{44287(3^{2k}-1)}, 1 \le b \le 44286$

于是, 可以得到 $\frac{3^{5\ell_0}+1}{3^{\ell_0}+1} \mid d_0$; 因此, 对于某个给定的元素 b, 可以推导得到

$$\frac{m}{p^{e(p_0-2)}} \leq \frac{b(3^{4\ell_0}+3^{3\ell_0}+3^{2\ell_0}+3^{\ell_0}+1)}{3^{6\ell_0}},$$

于是 $\lim_{\ell_0\to\infty} \frac{m}{p^{e(p_0-2)}} = 0$.

例子 2.2 在情况 (B) 中, 当 $p = 5, r = p_0 = 7, t = 2$ 时, 我们有

$$d_0 = \gcd\left(\frac{5^{7\ell_0}+1}{2}, \frac{5^{14\ell_0}-1}{5^{2\ell_0}-1}\right).$$

于是, 可以得到 $\frac{5^{7\ell_0}+1}{5^{\ell_0}+1} \mid d_0$; 因此, 对于某个给定的元素 b, 可以推导得到

$$\frac{m}{p^{e(p_0-2)}} \leq \frac{b(5^{7\ell_0}-1)}{(5^{\ell_0}-1)5^{10\ell_0}},$$

于是 $\lim_{\ell_0\to\infty} \frac{m}{p^{e(p_0-2)}} = 0$.

例子 2.3 在情况 (B) 中, 当 $p = 5, r = p_0 = 11, t = 2$ 时, 我们有

$$d_0 = \gcd\left(\frac{5^{11\ell_0}+1}{2}, \frac{5^{22\ell_0}-1}{5^{2\ell_0}-1}\right).$$

于是, 可以得到 $\frac{5^{11\ell_0}+1}{5^{\ell_0}+1} \mid d_0$; 因此, 对于某个给定的元素 b, 可以推导得到

$$\frac{m}{p^{e(p_0-2)}} \leq \frac{b(5^{11\ell_0}-1)}{(5^{\ell_0}-1)5^{18\ell_0}},$$

于是 $\lim_{\ell_0\to\infty} \frac{m}{p^{e(p_0-2)}} = 0$.

2.4 本章小结

在本章中, 我们给出了一种有限辛极空间中 m-ovoids 的具有创新性的构造方法. 我们利用了一些从文献[7] 中的分圆方法得到的特殊的强正则凯莱图 $\mathrm{Cay}(\mathbb{F}_q, D)$, 并且对有限域 $\mathbb{F}_q$ 赋予一个非退化的交错型 f 以使连接集合 D 给出辛空间 $(\mathbb{F}_q, f)$ 中的一个 m-ovoid. 通过这种方法可以得到高秩辛空间中大量的 m-ovoids, 并且我们所得的 m-ovoids 无法通过 field reduction 的方法得到. 我们注意到近年来学者在利用分圆的方法构造强正则凯莱图方面取得了显著的成果, 具体可以参考文献[27,28,48,49], 确定是否可以利用这些强正则图来通过定理 2.2构造新的 m-ovoids 将是个很有意义的工作.

需要指出的是, 在此章中我们只考虑了由负拉丁方类型的强正则凯莱图构造的辛极空间中的 m-ovoids, 但没有涉及类似的由拉丁方类型的强正则凯莱图构造的辛极空间中的 i-tight sets. 理由如下所述: $\mathrm{W}(2r-1, p^e)$ 中的一个 spread 的每个元素都是一个 1-tight set, 于是对于每一个 i, $\mathrm{W}(2r-1, p^e)$ 中都存在 i-tight sets.

本章的结论证明了有限辛极空间中存在的 m-ovoids 比预想中多了很多. 此外, 在辛极空间 $\mathrm{W}(2r-1,p^e)$ 中寻找更多具有新参数的 m-ovoids 仍旧是一个十分有意义的问题.

3 用结合方案构造 hull 维数很小的线性码

3.1 引言

设 q 为素数幂, $\mathbb{F}_q$ 表示包含 q 个元素的有限域. $\mathbb{F}_q$ 上的一个 $[n,k,d]$ 线性码$\mathcal{C}$ 是 $\mathbb{F}_q^n$ 的最小汉明距离 (我们简称其为最小距离) 为 d 的 k-维子空间. $\mathcal{C}$ 在 $\mathbb{F}_q$ 上的对偶码 *(dual code)* $\mathcal{C}^\perp$ 定义为

$$\mathcal{C}^\perp = \{\mathbf{b} \in \mathbb{F}_q^n : \mathbf{b}\cdot\mathbf{c}^T = 0\,, \forall \mathbf{c} \in \mathcal{C}\},$$

其中 $\mathbf{b}\cdot\mathbf{c}^T$ 是向量 **b** 和 **c** 的标准内积. 线性码 $\mathcal{C}$ 的 hull 定义为

$$\text{Hull}(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^\perp.$$

线性码的 hull 在确定用于检查两个线性码的置换等价性算法复杂性和计算线性码的自同构群的算法复杂性时起到了关键性的作用[60,61], 特别地, 在 hull 的维数很小的时候, 这些算法通常会非常高效. 如果一个线性码 $\mathcal{C}$ 满足 Hull($\mathcal{C}$) 的维数为 0, 即 Hull($\mathcal{C}$) $= \{0\}$ 时, 则它被称为线性互补对偶 *(linear complementary dual,* 简称为 *LCD)* 码.

对于一个线性码 $\mathcal{C}$, 其最小汉明距离 d 被 Singleton 界所限制

$$d \le n - k + 1.$$

如果 $d = n - k + 1$, 则码 $\mathcal{C}$ 是一个极大距离可分 (maximum distance separable, 简称为 MDS) 码, 更进一步地, 若它满足 Hull($\mathcal{C}$) $= \{0\}$, 则它是一个 LCD MDS 码. 如果 $d = n - k$, 则码 $\mathcal{C}$ 是一个 almost MDS 码, 若此外有 Hull($\mathcal{C}$) $= \{0\}$, 则它是一个 LCD almost MDS 码.

LCD 码被广泛地应用于数据存储, 通信系统和消费类电子产品等. 最近, 它们已经被运用于密码学中. LCD 码最初是由 Massey[50] 引入的.Carlet 和 Gailley[18] 介绍了二进制 LCD 码在对抗边信道攻击 (SCA) 和故障注入攻击 (FIA) 上的应用. 除了它们的实际应用, LCD 码在代数编码领域也是一个令人感兴趣的对象. 很多类型的码和 LCD 码的等价性已经或正在被广泛研究. Carlet 等研究者[20] 表明任何 MDS 码都和某个 LCD 码是等价的, Jin 等学者[37] 表明 $\mathbb{F}_{2^m}(m \ge 7)$ 上的一个代数几何码等价于一个 LCD 码. 在此之后, 文献[22] 给出了一个著名的结果, 它证明了 $\mathbb{F}_q(q > 3)$ 上任何一个线性码都等价于一个 LCD 码. LCD 码的研究于是变得更加有趣. 大量的研究被投入到 LCD 码的构造中. Liu 等学者[45] 给出了一个结合准正交矩阵的 LCD 矩阵

乘积码的构造. Li 等学者在文献[42] 中给出了几类有限域上 LCD 循环码的构造. 在文献[51] 中, Mesnager 等研究者构造了可以有效抵抗 SCA 的代数几何 LCD 码. 如需了解更多关于 LCD 码的研究, 请参考文献[21,22,44,56,62]. 需要强调的是, Carlet 等学者[19] 利用了半本元情况下的特征构造了 LCD 码以及 hull 维数为 1 的线性码. 受该方法的启发, 我们注意到, 结合方案和 LCD 码之间有非常紧密的联系. 我们接下来会在这章中给出利用结合方案来构造 LCD 码以及 hull 维数为 1 的线性码的方法, 其中一个构造是对文献[19] 中结合了高斯周期的构造的推广, 我们将会在第 3.3小节中给出具体细节.

这一章的结构如下, 在第 3.2节中, 我们回顾了有关代数数论, 结合方案和特征的一些基本知识. 在第 3.3节中, 我们给出了利用结合方案的 LCD 码和 hull 维数为 1 的线性码的几种构造. 在第 3.4节中, 我们提供了一个一般性的构造, 利用结合方案以及矩阵的扩展得到更多的 LCD 码以及 hull 维数为 1 的线性码. 最后, 第 3.5节是对这一章内容的总结.

3.2 准备工作

3.2.1 代数数论

首先介绍涉及的代数数论中的一些基础知识和基本结论, 读者可以参考文献[36] 和文献[29].

设 $\mathbb{Q}$ 是一个有理数域, K 是 $\mathbb{Q}$ 上的一个 n 次有限扩张. 令 $\mathbb{Z}$ 表示整数环. 对一个元素 $\alpha \in K$, 如果存在一个多项式 $f(x) = x^n + r_1x^{n-1} + \cdots + r_n$, 其中 $r_1, ..., r_n \in \mathbb{Z}$, 满足 $f(\alpha) = 0$, 则称 α 为一个代数整数. 所有代数整数的集合构成一个环, 称为戴德金整环 *(Dedekind domain)*, 用 $\mathbb{O}_K$ 来表示. 我们称 $\mathbb{Z}$ 为有理整环, 而 $\mathbb{Z}$ 中的元素被称为有理整数, 显而易见, $\mathbb{Z} \subset \mathbb{O}_K$.

设 p 是一个素数. 于是 $p\mathbb{O}_K$ 是 p 在 $\mathbb{O}_K$ 中生成的主理想整环, 它可以唯一写作 $\mathbb{O}_K$ 中素理想的乘积. 设 $\mathcal{P}$ 是 $\mathbb{O}_K$ 中包含 $p\mathbb{O}_K$ 的素理想. 如果 $\mathbb{O}_K \subset \mathcal{P}^e$ 并且 $p\mathbb{O}_K \not\subset \mathcal{P}^{e+1}$, 那么就称 $e = \mathrm{ord}_{\mathcal{P}}(p)$ 为 $\mathcal{P}$ 的分歧指数 *(ramification index)*. 因为 $\mathbb{O}_K$ 是一个戴德金整环, 那么每一个素理想 $\mathcal{P}$ 都是极大的, 且 $\mathbb{O}_K/\mathcal{P}$ 是一个包含 $\mathbb{Z}/p\mathbb{Z}$ 的有限域. 因此 $\mathbb{O}_K/\mathcal{P}$ 中的元素个数是 p^f, 其中 $f := [\mathbb{O}_K/\mathcal{P} : \mathbb{Z}/p\mathbb{Z}]$. 这里 f 被称为 $\mathcal{P}$ 的次数.

设 $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_g$ 是 $\mathbb{O}_K$ 中所有包含 $p\mathbb{O}_K$ 的素理想. 对于每一个 $i = 1, 2, ..., g$, 设 e_i 和 f_i 分别是 $\mathcal{P}_i$ 的分歧指数和次数. 于是

$$p\mathbb{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2} \cdots \mathcal{P}_g^{e_g}.$$

可知 $f_i, e_i (i = 1, 2, ..., g)$ 和 n 之间满足关系式

$$\sum_{i=1}^{g} e_i f_i = n.$$

设 m 是一个满足 $m \geq 3$ 以及 $m \not\equiv 2 \pmod 4$ 的整数. 设 $\zeta_m = e^{\frac{2\pi i}{m}}$ 是 m-次本元单位根. 设 $K = \mathbb{Q}(\zeta_m)$ 是由 m-次本元单位根所构成的分圆域. 那么, 就有 $\mathbb{O}_K = \mathbb{Z}[\zeta_m]$. 对于一个有理素数 p, 下面的引理给出了 $p\mathbb{O}_K$ 在 $\mathbb{O}_K$ 中的分解式.

引理 3.1 (定理 2.14, Feng[29]) 令 $K = \mathbb{Q}(\zeta_m)$ 为如上定义的分圆域. 对于每一个素数 $p \in \mathbb{Z}$, 设 $m = p^l m'$ $(l \geq 0)$ 以及 $p \nmid m'$. 设 f 是满足 $p^f \equiv 1 \pmod{m'}$ 的最小有理整数. 于是

$$p\mathbb{O}_K = (\mathcal{P}_1 \mathcal{P}_2 \cdots \mathcal{P}_g)^e,$$

其中, $e = \varphi(p^l)$, 且对于每一个 $i = 1, 2, ..., g$, $\mathcal{P}_i$ 的次数都为 f, 并且有 $g = \frac{\varphi(m')}{f}$. 此处 φ 是欧拉函数.

3.2.2 结合方案

定义 3.1 设 X 是一个有限集合, 令 R_i $(i = 0, 1, \ldots, d)$ 为 $X \times X$ 的满足下列性质的子集

(1) $R_0 = \{(x, x) | \, x \in X\}$;

(2) $X \times X = R_0 \cup \ldots \cup R_d$, 且当 $i \neq j$ 时, 有 $R_i \cap R_j = \emptyset$;

(3) 对某个 $i' \in \{0, 1, \ldots, d\}$, 有 $R_i^t = R_{i'}$, 这里 $R_i^t := \{(x, y) : (y, x) \in R_i\}$. 若 $i' = i$, 那么就称 R_i 是对称的;

(4) 对于 $\{0, 1, 2, \ldots, d\}$ 中的任意 i, j, k, 存在一个整数 p_{ij}^k 满足对所有的 $(x, y) \in R_k$, 有

$$|\{z \in X | (x, z) \in R_i \text{ 且 } (z, y) \in R_j\}| = p_{ij}^k.$$

这样的结构 $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ 被称为 X 上的 d 类结合方案. 此外, 若对所有的 $0 \leq i \leq d$, R_i 都是对称的, 那么该结合方案就是对称的, 若对所有的 i, j, k, 都有 $p_{ij}^k = p_{ji}^k$, 那么该结合方案是交换的.

定义 3.2 设 $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ 是一个 d 类结合方案. 对于所有的 $i \in \{0, 1, \ldots, d\}$, A_i 定义为关系 R_i 的邻接矩阵, 其行和列以 X 中的元素为索引, 并且有

$$(A_i)_{xy} = \begin{cases} 1, & \text{如果} (x, y) \in R_i, \\ 0, & \text{其他情形}. \end{cases}$$

因此, 上述定义 3.1中所列的关于结合方案 $\mathcal{X}$ 的性质 (1)-(4) 分别和下列性质等价:

(1) $A_0 = I$;

(2) $A_0 + A_1 + \ldots + A_d = J$, 其中 J 为全 1 矩阵;

(3) 对任意 $i \in \{0, 1, ..., d\}$, 存在一个 $i' \in \{0, 1, ..., d\}$ 使得 $A_i^T = A_{i'}$, 这里 A_i^T 表示 A_i 的转置;

(4) 对于所有的 $i, j \in \{0, 1, ..., d\}$, 有 $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$.

因此, 向量空间 $\langle A_0, A_1, \ldots, A_d\rangle_{\mathbb{C}}$ 构成了一个代数 $\mathcal{M}$, 它被称为 *Bose-Mesner* 代数. 对于一个交换结合方案, 它的 Bose-Mesner 代数也是交换的. 在此章余下的部分中, 我们只考虑交换结合方案, 并且该章第三小节里涉及的所有结合方案都是交换的.

设 $\mathcal{X} = (X, \{R_i\}_{0\le i\le d})$ 是一个交换的结合方案, 这里 $X = \{x_1, x_2, \ldots, x_n\}$, 并且 $\mathcal{M} = \langle A_0, A_1, \ldots, A_d\rangle_{\mathbb{C}}$ 是相应的交换代数. 注意到 $\mathcal{M}$ 是交换的, 则 $A_i^T A_i = A_i A_i^T$, 因此 A_i 是一个正规矩阵. 所以邻接矩阵 $A_0, A_1, \ldots, A_d$ 是两两交换的正规矩阵. 由线性代数理论, 它们可以被 $\mathbb{C}$ 上的一个酉矩阵同时对角化. $V = \mathbb{C}^{|X|} = \mathbb{C}^n$ 有一个分解

$$V = V_0 \oplus V_1 \oplus \ldots \oplus V_r,$$

这里每一个 V_i 都是 $A_0, A_1, \ldots, A_d$ 的一个共同特征空间. 考虑使 r 取得最小值的分解. 则对于任意的 $i \neq j$, 存在一个整数 k 使得 A_k 在 V_i 和 V_j 上有不同的特征值. 由于 $J = \sum_{i=0}^{d} A_i$ 的对应于特征值 n 的特征空间是由 $(1, 1, ..., 1)$ 张成的子空间, 对某个 i,1-维子空间 $\langle(1, 1, ..., 1)\rangle$ 恰好是 V_i. 那么不失一般性, 可以取 $i = 0$ 使得 $\dim V_0 = 1$. 设 $p_i(j)$ 是 A_i 在 V_j 上的特征值. 在这一小节的剩余部分, 我们分别用 v^c 表示 v 的共轭, 用 v^T 表示 v 的转置, 用 v^H 表示 v 的共轭转置, 用 $p_i(j)^c$ 表示 $p_i(j)$ 的共轭. 如果 $A_i^T = A_{i'}$, 选取 $v \in V_j$ 使得 $v \neq 0$. 则由 $vA_i = p_i(j)v$ 可以推出 $vA_iv^H = p_i(j)vv^H$. 对其取转置和共轭, 可以得到 $vA_{i'}v^H = p_i(j)^c vv^H$. 类似地, 由 $vA_{i'} = p_{i'}(j)v$ 可以得到 $vA_{i'}v^H = p_{i'}(j)vv^H$. 于是, 可以推断出 $p_{i'}(j) = p_i(j)^c$.

显而易见, $A_0, A_1, \ldots, A_d$ 是代数 $\mathcal{M}$ 的一组基. 我们接下来将介绍 $\mathcal{M}$ 的另外一组基. 对于每一个 $i = 1, 2, \ldots, r$, 令 E_i 为表示成矩阵形式的关于基 $\{e_x : x \in X\}$ 的正交投影 $V \to V_i$, 其中 $e_x = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{C}^n$, 这里 1 位于使得 $x = x_i \in X$ 的第 i 个位置. 由正交投影的性质, 我们有

(1) $E_0 + E_1 + \ldots + E_r = I$,

(2) $E_0 = \frac{1}{|X|}J$,

(3) $E_iE_j = \delta_{ij}E_i$,

其中, $\delta_{ij} = \begin{cases} 1, & \text{如果} i = j, \\ 0, & \text{其他情形.} \end{cases}$

接着我们研究对于所有的 $i \in \{1, 2, \ldots, r\}$ 以及 $j \in \{1, 2, \ldots, d\}$, E_i 和 A_j 之间的相互关系. 回顾上文, 可以知道 $p_i(j)$ 是 A_i 在 V_j 上的特征值. 于是, 可以推导出 $E_jA_i = p_i(j)E_j$, 因此, 我们有

$$A_i = (\sum_{j=0}^{r} E_j)A_i = \sum_{j=0}^{r} p_i(j)E_j.$$

可以证明 $r = d$, 读者可以参考文献[8] 中的定理 3.1. 因此, 幂等元 $E_0, E_1, \ldots, E_d$ 的集合也构成代数 $\mathcal{M}$ 的一组基. 令 P 为阶是 $d+1$ 的矩阵, 其 (j, i) 位置上的元素为 $p_i(j)$. 为了保持本章中代表元的一致性, 我们用索引集 $\{1, 2, \ldots, d\}$ 标记矩阵 P 的行和列. 于是, 我们有

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

上述 $d+1$ 阶矩阵 P 被称为 $\mathcal{X}$ 的第一特征矩阵 ***(first eigenmatrix)*** .

3.2.3 特征

阶为 $|G|$ 的有限交换群 $(G, +)$ 的一个特征ϕ 是一个同态映射 $\phi : G \to \mathbb{C}^\times$, 其中 $\mathbb{C}^\times$ 代表非零复数构成的乘法群, 也就是说, 对于所有的 $g_1, g_2 \in G$, 有 $\phi(g_1 + g_2) = \phi(g_1)\phi(g_2)$ 成立. 显然, 我们有 $\phi(0) = 1$ 以及 $\phi(g)^{|G|} = \phi(|G|g) = \phi(0) = 1$ 对于所有的 $g \in G$ 都成立. 由此可知, 对于任意的 $g \in G$, $\phi(g)$ 是一个复 $|G|$-次单位根. 如果对于任意的 $g \in G$, 都有 $\phi_0(g) = 1$, 那么特征 ϕ_0 就被称为 G 的平凡特征 ***(trivial character)*** .

令 $\mathbb{F}_q$ 为 q 元有限域, 这里 $q = p^h$, p 是一个素数, h 是一个正整数. 有限域 $\mathbb{F}_q$ 的加法特征ϕ 是加法群 $(\mathbb{F}_q, +)$ 的一个特征. 对于这样的特征 ϕ, 我们有

$$\phi(a + b) = \phi(a)\phi(b)$$

对任意 $a, b \in \mathbb{F}_q$ 成立, 并且 $\phi(0) = 1$. 令 $\mathrm{Tr}_{q/p}$ 表示 $\mathbb{F}_q$ 到 $\mathbb{F}_p$ 上的迹函数, 其定义如下

$$\mathrm{Tr}_{q/p}(x) = x + x^p + \ldots + x^{p^{h-1}}, \text{ 对任意 } x \in \mathbb{F}_q \text{成立.}$$

由于 $\mathrm{Tr}_{q/p}(\cdot)$ 是一个 $\mathbb{F}_p$-线性函数, 那么对于任意 $a \in \mathbb{F}_q$, 可以得到一个加法特征 $\phi_a : (\mathbb{F}_q, +) \to \mathbb{C}^\times$, 定义如下

$$\phi_a(x) = \zeta_p^{\mathrm{Tr}_{q/p}(ax)},$$

其中 $\zeta_p = e^{\frac{2\pi i}{p}}$ 是一个 p-次本元单位根. 特别地, 特征 ϕ_1 被称为标准特征 *(canonical character)*.

3.3 由结合方案构造的线性码

下面的两个引理分别给出了 LCD 码的一个完全刻画以及 hull 维数为 1 的线性码的一个充分条件.

引理 3.2 [50] 令 $\mathcal{C}$ 为 $\mathbb{F}_q$ 上的一个 $[n,k]$ 线性码, 其生成矩阵为 $G=[I_k,Q]$. 那么码 $\mathcal{C}$ 是 LCD 的当且仅当 I_k+QQ^T 是非奇异的, 即-1 不是矩阵 QQ^T 的特征, 这里 Q^T 表示 Q 的转置.

引理 3.3 [43] 令 $\mathcal{C}$ 为 $\mathbb{F}_q$ 上的一个 $[n,k]$ 线性码, 其生成矩阵为 $G=[I_k,Q]$. 那么如果-1 是矩阵 QQ^T 的特征值, 并且其 (代数) 重数为 1, 那么码 $\mathcal{C}$ 的 hull 维数为 1, 这里 Q^T 表示 Q 的转置.

本小节的主要工作是利用交换 Bose-Mesner 代数分别构造满足引理 3.2和引理 3.2中条件的矩阵 Q. 此外, 我们可以分别得到 LCD 码和 hull 维数为 1 的线性码. 为了展示我们的主要结果, 现在将统一这一小节所使用的符号. 令 $\mathcal{X}=(X,\{R_i\}_{0\le i\le d})$ 为一个交换的 d 类结合方案, 其满足 $|X|=n$, 并且 $\mathcal{M}=\langle A_0,A_1,\ldots,A_d\rangle_{\mathbb{C}}$ 是相对应的交换代数. 那么就有分解式 $V=V_0\oplus V_1\oplus\ldots\oplus V_d$. 以下引理提出了 Bose-Mesner 代数 $\mathcal{M}$ 中矩阵特征值的一个重要性质.

引理 3.4 令 $\chi_t(B)$ 表示 B 在 V_t 上的特征值, 这里 $B=\sum_{i=0}^d b_iA_i\in\mathcal{M}$ 且 $t\in\{0,1,\ldots,d\}$. 对于每一个 t, 对任意的 $B=\sum_{i=0}^d b_iA_i\in\mathcal{M}$ 以及 $C=\sum_{i=0}^d c_iA_i\in\mathcal{M}$, 都有 $\chi_t(B)=\sum_{i=0}^d b_ip_i(t)$ 以及 $\chi_t(BC)=\chi_t(B)\chi_t(C)$ 成立.

证明. 对于任意的 $t\in\{0,1,\ldots,d\}$, 选择任意的 $0\neq v\in V_t$, 可以推出 $vB=\sum_{i=0}^d b_ivA_i=\sum_{i=0}^d b_ip_i(t)v$, 所以可以推导出 $\chi_t(B)=\sum_{i=0}^d b_ip_i(t)$. 根据 $B,C,\chi_t(B)$ 和 $\chi_t(C)$ 的表达式, 我们只需要证明对于任意的 $i,j\in\{0,1,\ldots,d\}$, 都有 $\chi_t(A_iA_j)=\chi_t(A_i)\chi_t(A_j)$ 成立即可. 对于任意的 $0\neq v\in V_t$, 总有

$$v\chi_t(A_iA_j)=v(A_iA_j)=(vA_i)A_j=\chi_t(A_i)(vA_j)=v\chi_t(A_i)\chi_t(A_j).$$

因此, 证明完成. □

在这章的余下部分, 我们始终将 p_0 设置为一个素数, 将 u 设置成一个正整数, 那么 $\mathbb{F}_{p_0^u}$ 是一个含有 p_0^u 个元素的有限域. 对于任意的 $n_0\in\mathbb{Z}$, 定义 $\overline{n_0}=n_0 \pmod{p_0}$,

那么就有 $\overline{n_0} \in \mathbb{F}_{p_0}$. 令 $M_n(\mathbb{Z})$ 表示 $\mathbb{Z}$ 上阶为 n 的方阵. 取

$$Q = \sum_{i=0}^{d} c_i A_i \in \mathcal{M}, \text{这里 } c_i \in \mathbb{Z}, 0 \leq i \leq d. \tag{3.1}$$

对于这样的矩阵 $Q = (q_{ij}) \in \mathcal{M} \cap M_n(\mathbb{Z})$, 定义

$$\overline{Q} = (\overline{q}_{ij}) \in M_n(\mathbb{F}_{p_0}), \text{这里 } \overline{q}_{ij} = q_{ij} (\text{mod } p_0). \tag{3.2}$$

对于任意的 $t \in \{0, 1, \ldots, d\}$, 定义 $T'_t = \chi_t(QQ^T)$ 为矩阵 QQ^T 在 V_t 上的特征值. 由 QQ^T 的定义以及引理 3.4, 可以推出

$$T'_t = \left(\sum_{i=0}^{d} c_i p_i(t) \right) \left(\sum_{i=0}^{d} c_i p_{i'}(t) \right), \tag{3.3}$$

这里, 对某个 $i' \in \{0, 1, \ldots, d\}$, 有 $A_i^T = A_{i'}$ 成立. 特别地, 如果该结合方案是对称的, 那么就有

$$T'_t = \left(\sum_{i=0}^{d} c_i p_i(t) \right)^2 \tag{3.4}$$

对每个 $t \in \{0, 1, \ldots, d\}$ 成立.

沿用上面提到的符号, 下面我们将给出这章的主要结论.

定理 3.1 令 $\mathcal{C}$ 为 $\mathbb{F}_{p_0^u}$ 上的一个 $[2n, n]$ 线性码, 其生成矩阵为 $G = [I_n, \overline{Q}]$, 这里 Q 是由公式 (3.1) 给出的. 对于每一个 $t \in \{0, 1, \ldots, d\}$, 令 T'_t 为公式 (3.3) 所定义的矩阵 QQ^T 在 V_t 上的特征值, 并且令 $T_t = T'_t + 1$. 如果所有的 T'_t 都是有理数, 那么就有以下结论

(1) 码 $\mathcal{C}$ 是 LCD 的当且仅当 $\Pi_{t=0}^{d} T_t \not\equiv 0 \pmod{p_0}$;

(2) 当 $T_0 \equiv 0 \pmod{p_0}$ 以及 $T_t \not\equiv 0 \pmod{p_0}$ 对所有 $t = 1, 2, ..., d$ 成立时, 码 $\mathcal{C}$ 的 hull 维数为 1.

证明. 由于 $Q \in M_n(\mathbb{Z})$, 那么矩阵 QQ^T 所有的特征值 T'_t $(0 \leq t \leq d)$ 都是代数整数. 因此, 所有 T'_t 都是有理数当且仅当所有 T'_t 都是整数, 所以, 对于 $t \in \{0, 1, \ldots, d\}$, 可以定义 $\overline{T'_t} = T'_t \pmod{p_0}$. 我们断定 $\overline{T'_t}$ 是 $\overline{QQ^T}$ 的一个特征值当且仅当对所的有 $t = 0, 1, ..., d$, T'_t 是 QQ^T 的一个特征值. 可知 T'_t 是 QQ^T 的一个特征值当且仅当 T'_t 是下列多项式的一个根

$$g(x) = \det(xI - QQ^T) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x],$$

其等价于 $\overline{T_t'}$ 是下列多项式的一个根

$$\overline{g}(x) = x^n + \overline{a}_{n-1}x^{n-1} + \cdots + \overline{a}_1 x + \overline{a}_0 \in \mathbb{Z}_{p_0}[x].$$

所以, 可知上述论断成立.

(1) 根据引理 3.2以及上述讨论, 可以知道码 $\mathcal{C}$ 是 LCD 的当且仅当 $\Pi_{t=0}^{d} T_t \neq 0 \pmod{p_0}$;

(2) 如果对于 $t = 1, 2, ..., d$, 有 $T_0 \equiv 0 \pmod{p_0}$ 以及 $T_t \neq 0 \pmod{p_0}$ 成立. 则 -1 是 QQ^T 在 V_0 上的一个特征值, 但是对于任意的 $i \neq 0$, 根据上面的讨论, -1 不是 QQ^T 在 V_i 上的特征值. 回想第 3.2节提到的内容, V_0 是由 $(1, 1, \ldots, 1)$ 生成的 1-维子空间, 因此 $-1 = \chi_0(QQ^T)$ 的重数是 1. 第二个结论由引理 3.3和引理 3.4得到.

□

根据定理 3.1, 我们用几种不同类型的结合方案给出 LCD 码和 hull 维数为 1 的线性码的构造.

3.3.1 与分圆结合方案相关的线性码

对于一个 d 类结合方案 $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$, 如果 $S_0 = R_0$, 并且对于任意的 $i = 1, 2, ..., d_1$, S_i 均为某些 R_j 的并, 那么就称 $(X, \{S_i\}_{0 \leq i \leq d_1})$ 是结合方案 $(X, \{R_i\}_{0 \leq i \leq d})$ 的融合. 如果一个结合方案的任意融合都仍然是一个结合方案, 那么称该结合方案为无定形的 *(amorphic)* . 如果需要了解更多关于无定形的结合方案的知识, 请读者参考文献[67]. 无定形的结合方案的一个经典例子是半本元情况下有限域上的分圆结合方案, 我们将会在下面对这部分内容进行详细的介绍.

令 $q = p^h$, 这里 p 是一个素数, h 是一个正整数. 令 α 为 $\mathbb{F}_q$ 上一个给定的本原元, 并且令整数 N 满足 $N \mid (q-1)$ 和 $N > 1$. 令 $C_0 = \langle \alpha^N \rangle$, 以及

$$C_i = \alpha^i C_0, 1 \leq i \leq N-1. \tag{3.5}$$

假定 $-1 \in C_0$. 定义 $R_0 = \{(x, x) | \, x \in \mathbb{F}_q\}$, 并且对于任意的 $i \in \{1, 2, \ldots, N\}$, 定义 $R_i = \{(x, y) | \, x, y \in \mathbb{F}_q, \, x - y \in C_{i-1}\}$. 那么 $(\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})$ 是一个结合方案, 它被称为 $\mathbb{F}_q$ 上的一个 N 类分圆结合方案. 如果存在一个整数 j_0 使得 $p^{j_0} \equiv -1 (\mathrm{mod}\, N)$, 那么称该分圆结合方案是在半本元情况下的. 对于 $N > 2$, 一个分圆结合方案是无定形的当且仅当它是在半本元情况下的. 这个结论在文献[9] 中可以看到具体证明.

N 类分圆结合方案的第一特征矩阵 P 如下所示

$$P=\begin{pmatrix} 1 & \frac{q-1}{N} & \frac{q-1}{N} & \frac{q-1}{N} & \cdots & \frac{q-1}{N} \\ 1 & \eta_0 & \eta_1 & \eta_2 & \cdots & \eta_{N-1} \\ 1 & \eta_1 & \eta_2 & \eta_3 & \cdots & \eta_0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \eta_{N-1} & \eta_0 & \eta_1 & \cdots & \eta_{N-2} \end{pmatrix}, \tag{3.6}$$

其中, $\eta_i(0 \le i \le N-1)$ 是阶为 N 的高斯周期, 它定义如下

$$\eta_i = \sum_{x \in C_i} \phi_1(x).$$

这里, ϕ_1 是第 3.2节介绍的 $\mathbb{F}_q$ 上的标准加法特征. 下面的引理给出了半本元情况下的高斯周期.

引理 3.5[25] 令 $N \ge 3$ 是一个整数. 假定存在一个最小的正整数 j_0 使得 $p^{j_0} \equiv -1 \pmod N$. 对于某个正整数 γ, 令 $q = p^{2j_0\gamma}$.

(1) 如果 p, γ 和 $\frac{p^{j_0}+1}{N}$ 都是奇数, 那么

$$\eta_i = \begin{cases} \frac{(N-1)\sqrt{q}-1}{N}, & \text{如果} i = N/2, \\ -\frac{\sqrt{q}+1}{N}, & \text{其他情形;} \end{cases} \tag{3.7}$$

(2) 在其他情况下,

$$\eta_i = \begin{cases} \frac{(-1)^{\gamma+1}(N-1)\sqrt{q}-1}{N}, & \text{如果} i = 0, \\ \frac{(-1)^{\gamma}\sqrt{q}-1}{N}, & \text{其他情形.} \end{cases} \tag{3.8}$$

定理 3.2 令 $\mathcal{X} = (\mathbb{F}_q, \{R_i\}_{0 \le i \le N})$ 为 N 类结合方案, 且 $A_0, A_1, \ldots, A_N$ 是相应的邻接矩阵. 沿用定理 3.1中的符号, 设 Q 和 $\overline{Q}$ 由公式 (3.1) 和 (3.2) 给出. 令 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个 $[2q, q]$ 线性码, 其生成矩阵为 $[I_q, \overline{Q}]$.

(1) 如果 p, γ 以及 $\frac{p^{j_0}+1}{N}$ 都是奇数, 我们设 $L_0 = (c_0 + \frac{q-1}{N}\sum_{i=1}^{N} c_i)^2 + 1$, 对于 $j = 1, 2, ..., N$, 设 $L_j = (c_0 + c_j\eta_{N/2} + \eta_0 \sum_{i=1, i\ne j}^{N} c_i)^2 + 1$. 那么码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个 $[2q, q]$ LCD 码当且仅当

$$\prod_{j=0}^{N} L_j \not\equiv 0 \pmod{p_0}.$$

并且当满足下面条件时, 码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[2q, q]$ 线性码:

$$L_0 \equiv 0 \pmod{p_0},\ L_j \not\equiv 0 \pmod{p_0} \text{ 对} j = 1, 2, ..., N \text{都成立.}$$

(2) 在其他情况下, 对于 $j = 1, 2, ..., N$, 我们设 $L_0 = (c_0 + \frac{q-1}{N}\sum_{i=1}^{N} c_i)^2 + 1$, 对于 $j = 1, 2, ..., N$, 设 $L_j = (c_0 + c_j\eta_0 + \eta_1 \sum_{i=1, i\neq j}^{N} c_i)^2 + 1$. 那么码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个 $[2q, q]$ LCD 码当且仅当

$$\prod_{j=0}^{N} L_j \not\equiv 0 \pmod{p_0}.$$

并且当满足下面条件时, 码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[2q, q]$ 线性码:

$$L_0 \equiv 0 \pmod{p_0},\ L_j \not\equiv 0 \pmod{p_0} 对 j = 1, 2, ..., N 都成立.$$

证明. 因为 $-1 \in C_0$, 很容易验证该分圆结合方案是对称的, 于是, 对于 $Q = \sum_{i=0}^{N} c_i A_i$ ($c_i \in \mathbb{Z}$), 有 $Q^T = Q$ 成立. 根据公式 (3.3) 以及 Q 的对称性, 可以得到矩阵 QQ^T 的所有特征值

$$T_t' = \left(\sum_{i=0}^{N} c_i p_i(t)\right)^2, \tag{3.9}$$

这里 $t = 0, 1, \ldots, N$. 利用引理 3.5, 可以计算并且总结如下:

(1) 如果 p, γ 以及 $\frac{p^{j_0}+1}{N}$ 都是奇数, 那么对于任意的 $i \in \{0, 1, \ldots, N-1\} \setminus \{N/2\}$, 都有 $\eta_i = \eta_0$. 这意味着, 除了 P 的第一行外, 在 P 的其余所有行中, $\eta_{N/2}$ 出现了一次, 而 η_0 出现了 $N-1$ 次. 于是, 可以很容易地计算得到, $L_j - 1 (0 \leq j \leq d)$ 是矩阵 QQ^T 的所有特征值, 并且由公式 (3.9), 可以推出 $L_0 = T_0' + 1$. 由于所有的 η_i 都是有理数, 应用定理 3.1, 由此得到第一个论断成立.

(2) 在其他情况下, 对于任意的 $i \in \{1, \ldots, N-1\}$, 都有 $\eta_i = \eta_1$. 用和第一种情况相同的论述, 可以计算得到 $L_j - 1 (0 \leq j \leq d)$ 是矩阵 QQ^T 全部的特征值, 在这种情况下, 公式 (3.9) 可以推出 $L_0 = T_0' + 1$. 根据定理 3.1, 第二个论断也可以得到证明.

□

注 3.1 我们注意到文献[19] 中的定理 3 和定理 4 是本章中定理 3.2的特殊情况. 特别地, 如果在定理 3.2中取定 $Q = A_1$, 那么可以分别得到和文献[19] 中的定理 3 和定理 4 相同的结论. 因此, 利用分圆结合方案的方法, 通过改变矩阵 Q 的系数 c_i, 我们可以得到更多 LCD 码和 hull 维数为 1 的线性码的构造.

下面给出定理 3.2的两个例子.

例子 3.1 令 $p=3,\gamma=1,N=4$. 那么根据引理 3.5中的假设, 我们有 $j_0=1$ 以及 $q=9$. 根据公式 (3.6) 和引理 3.5, 第一特征矩阵 P 如下所示

$$P=\begin{pmatrix}1&2&2&2&2\\1&-1&-1&2&-1\\1&-1&2&-1&-1\\1&2&-1&-1&-1\\1&-1&-1&-1&2\end{pmatrix}. \tag{3.10}$$

令码 $\mathcal{C}$ 为 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵为 $[I_q,\overline{Q}]$, 这里记 $Q=3A_0+A_1+4A_2+2A_3+5A_4$. 因为 p,γ 和 $\frac{p^{j_0+1}}{N}$ 都是奇数, 应用定理 3.2中的第一个结论, 就可以计算得到 $L_0=730,L_1=10,L_2=10,L_3=37,L_4=37$, 于是我们有 $\prod_{j=0}^{4}L_j=2^3\cdot5^3\cdot37^2\cdot73$. 如果 $p_0\neq2,5,37,73$, 那么码 $\mathcal{C}$ 是一个 $[18,9]$ LCD 码. 特别地, 用 Magma 搜索, 可以得到, 当 $p_0=19,43,47,53,61,71,79,83,89,97$ 时, 码 $\mathcal{C}$ 是一个 $[18,9,9]$ LCD almost MDS 码; 如果 $p_0=73$, 那么码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[18,9,9]$ almost MDS 线性码.

例子 3.2 令 $p=2,\gamma=1,N=3$. 那么根据引理 3.5中的假设, 我们有 $j_0=1$ 以及 $q=4$. 根据公式 (3.6) 和引理 3.5, 第一特征矩阵 P 如下所示

$$P=\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&-1&1\\1&-1&1&-1\end{pmatrix}. \tag{3.11}$$

令码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵为 $[I_q,\overline{Q}]$, 这里 $Q=8A_0+A_1+7A_2+6A_3$. 因为 γ 和 $\frac{p^{j_0+1}}{N}$ 都不是奇数, 应用定理 3.2中的第二个结论, 可以计算得到 $L_0=485$, $L_1=17$, $L_2=65$, $L_3=37$, 于是我们有 $\prod_{j=0}^{3}L_j=5^2\cdot13\cdot17\cdot37\cdot97$. 如果 $p_0\neq5,13,17,37,97$ 那么码 $\mathcal{C}$ 是一个 $[8,4]$ LCD 码; 特别地, 用 Magma 搜索, 可以得到, 如果 $p_0=19,29,31,43,47,53,59,61,71,73,79,83,101,103,107,109,113,127,137$, 那么码 $\mathcal{C}$ 是一个 $[8,4,5]$ LCD MDS 码. 如果 $p_0=97$, 那么码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[8,4,5]$ MDS 线性码.

3.3.2 与三类结合方案相关的线性码

三类结合方案是一类很重要的结合方案. 在文献[30] 中, 作者给出了几种作为分圆结合方案的融合形式的对称三类结合方案的构造. 现在我们利用这些三类结合方案中的一种来给出定理 3.1中的 LCD 码以及 hull 维数为 1 的线性码的构造.

令 s 为一个正整数, 用 $E=\mathbb{F}_{2^s}$ 和 $F=\mathbb{F}_{2^{3s}}$ 分别表示元素个数为 2^s 和 2^{3s} 的有限域. 设 ω 是 F 中的一个本原元. 令 $N=\frac{2^{3s}-1}{2^s-1}$, 并且对于所有的 $0\leq i\leq N-1$, 令 $C_i=\omega^i\langle\omega^N\rangle$ 为 F 中阶为 N 的分圆类. 显然 C_0 等同于 E^*, 这里 E^* 表示 E 的乘法群.

令 $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$. 由文献[30] 第 1206 页的构造, 对于一个整数 $a \in \mathbb{Z}_N$, 定义

$$S_a := \{u \in F^* : \mathrm{Tr}_{F/E}(u^{1+2^s}) = 0, \mathrm{Tr}_{F/E}(\omega^a u) = 0)\}.$$

那么 S_a 所有可能包含的元素个数是 $0, 2^s-1, 2(2^s-1)$. 基于这个事实, 进一步定义 $\mathbb{Z}_N$ 的三个子集如下

$$\begin{aligned} H_1 &:= \{a \in \mathbb{Z}_N : |S_a| = 2^s - 1\}, \\ H_2 &:= \{a \in \mathbb{Z}_N : |S_a| = 2(2^s - 1)\}, \\ H_3 &:= \{a \in \mathbb{Z}_N : |S_a| = 0\}. \end{aligned}$$

因此, 集合 H_1, H_2 以及 H_3 是 $\mathbb{Z}_N$ 的一个划分. 下面给出的引理提供了有限域 F 上一个对称的三类结合方案.

引理 3.6 (定理 5, Feng 和 Momihara[30]) 沿用上面的符号, 选取 F 的划分如下:

$$R_0 = \{0\}, R_1 = \bigcup_{i \in H_1} C_i, R_2 = \bigcup_{i \in H_2} C_i, R_3 = \bigcup_{i \in H_3} C_i.$$

那么 $(F, \{R_i\}_{i=0}^3)$ 是一个三类结合方案, 其第一特征矩阵是

$$P = \begin{pmatrix} 1 & 2^{2s}-1 & 2^{s-1}(2^{2s}-1) & 2^{s-1}(2^s-1)^2 \\ 1 & 2^{2s}-1 & -2^{s-1}(2^s+1) & -2^{s-1}(2^s-1) \\ 1 & -1 & 2^{s-1}(2^s-1) & -2^{s-1}(2^s-1) \\ 1 & -1 & -2^{s-1} & 2^{s-1} \end{pmatrix}.$$

令 $\mathcal{X} = (F, \{R_i\}_{i=0}^3)$ 为由引理 3.6 给出的一个三类结合方案, 并且对于 $i = 0, 1, 2, 3$, A_i 是关系 R_i 的邻接矩阵. 设 $Q = \sum_{i=0}^3 c_i A_i$, 这里 $c_i \in \mathbb{Z}$, $i = 0, 1, 2, 3$. 由于上面给出的三类结合方案是对称的, 那么在这种情况下, 定理 3.1中的 T_0, T_1, T_2 和 T_3 如下所示

$$\begin{aligned} T_0 &= [c_0 + (2^{2s}-1)c_1 + 2^{s-1}(2^{2s}-1)c_2 + 2^{s-1}(2^s-1)^2 c_3]^2 + 1, \\ T_1 &= [c_0 + (2^{2s}-1)c_1 - 2^{s-1}(2^s+1)c_2 - 2^{s-1}(2^s-1)c_3]^2 + 1, \\ T_2 &= [c_0 - c_1 + 2^{s-1}(2^s-1)c_2 - 2^{s-1}(2^s-1)c_3]^2 + 1, \\ T_3 &= [c_0 - c_1 - 2^{s-1}c_2 + 2^{s-1}c_3]^2 + 1. \end{aligned} \tag{3.12}$$

注意到所有的 T_i 都是整数. 由定理 3.1, 我们得到下面的定理.

定理 3.3 令码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵是 $[I_{2^{3s}}, \overline{Q}]$, 令 $T_j, j = 0, 1, 2, 3$ 如 (3.12) 所定义. 那么码 $\mathcal{C}$ 是一个 $[2^{3s+1}, 2^{3s}]$LCD 码当且仅当 $\prod_{j=0}^3 T_j \not\equiv 0 \pmod{p_0}$, 而

当以下条件成立时, 码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[2^{3s+1}, 2^{3s}]$ 线性码:

$$T_0 \equiv 0 \pmod{p_0},\ T_j \not\equiv 0 \pmod{p_0} \text{ 对} j = 1, 2, 3 \text{都成立.}$$

例子 3.3 沿用引理 3.6和定理 4.1中的符号, 设 $s = 2$, 那么相应的第一特征矩阵如下所示

$$P = \begin{pmatrix} 1 & 15 & 30 & 18 \\ 1 & 15 & -10 & -6 \\ 1 & -1 & 6 & -6 \\ 1 & -1 & -2 & 2 \end{pmatrix}.$$

令码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵是 $[I_{64}, \overline{Q}]$, 这里 $Q = A_0 + 2A_1 + 2A_2 + A_3$. 根据公式 (3.12), 我们有 $T_0 = 11882 = 2 \cdot 13 \cdot 457$, $T_1 = 26$, $T_2 = 26$, $T_3 = 10$, 于是 $\prod_{j=0}^{3} T_j = 2^4 \cdot 5 \cdot 13^3 \cdot 457$. 如果 $p_0 \neq 2, 5, 13, 457$, 那么码 $\mathcal{C}$ 是一个 $[128, 64]$ LCD 码. 如果 $p_0 = 457$, 那么码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[128, 64]$ 线性码.

3.3.3 与四类结合方案相关的线性码

在本小节中, 我们将会介绍不是由分圆类得到的四类结合方案. 下面给出的来自文献[39] 的引理就提供了这样的结合方案.

引理 3.7 令 $p = 3, q = 3^s$, 令 $X = \mathbb{F}_q \times \mathbb{F}_q$ 为一个有限集合. 定义

$$\begin{aligned} R_0 &= \{(x, x) : x \in X\}, \\ R_i &= \{(x, y) : x = (x_1, x_2), y = (y_1, y_2) \in X, x_1 \neq y_1, \mathrm{Tr}((-x_1 + y_1)(-x_2 + y_2)) = i\}, \\ R_4 &= \{(x, y) : x = (x_1, x_2), y = (y_1, y_2) \in X, x_1 = y_1, x_2 \neq y_2\}, \end{aligned}$$

这里 $i = 1, 2, 3$, Tr 是由 $\mathbb{F}_q$ 到 $\mathbb{F}_p$ 的迹函数. 那么结合方案 $(X, \{R_i\}_{i=0}^4)$ 是一个对称的结合方案, 其第一特征矩阵为

$$P = \begin{pmatrix} 1 & 3^{s-1}(3^s - 1) & 3^{s-1}(3^s - 1) & 3^{s-1}(3^s - 1) & 3^s - 1 \\ 1 & 2 \cdot 3^{s-1} & -3^{s-1} & -3^{s-1} & -1 \\ 1 & -3^{s-1} & 2 \cdot 3^{s-1} & -3^{s-1} & -1 \\ 1 & -3^{s-1} & -3^{s-1} & 2 \cdot 3^{s-1} & -1 \\ 1 & -3^{s-1} & -3^{s-1} & -3^{s-1} & 3^s - 1 \end{pmatrix}.$$

令 $\mathcal{X} = (X, \{R_i\}_{i=0}^4)$ 为引理 3.7中给出的四类结合方案, 这里 $|X| = q^2$, 对于 $i = 0, 1, 2, 3, 4$, A_i 是关系 R_i 的邻接矩阵. 设 $Q = \sum_{i=0}^4 c_i A_i$, 其中 $c_i \in \mathbb{Z}$ 对 $i = 0, 1, 2, 3, 4$

都成立. 由于上述四类结合方案是对称的, 那么由定理 3.1得到的 T_0, T_1, T_2, T_3, T_4 为

$$\begin{aligned}
T_0 &= [c_0 + 3^{s-1}(3^s-1)c_1 + 3^{s-1}(3^s-1)c_2 + 3^{s-1}(3^s-1)c_3 + (3^s-1)c_4]^2 + 1,\\
T_1 &= [c_0 + 2\cdot 3^{s-1}c_1 - 3^{s-1}c_2 - 3^{s-1}c_3 - c_4]^2 + 1,\\
T_2 &= [c_0 - 3^{s-1}c_1 + 2\cdot 3^{s-1}c_2 - 3^{s-1}c_3 - c_4]^2 + 1,\\
T_3 &= [c_0 - 3^{s-1}c_1 - 3^{s-1}c_2 + 2\cdot 3^{s-1}c_3 - c_4]^2 + 1,\\
T_4 &= [c_0 - 3^{s-1}c_1 - 3^{s-1}c_2 - 3^{s-1}c_3 + (3^s-1)c_4]^2 + 1.
\end{aligned} \tag{3.13}$$

注意到所有的 T_i 都是整数. 根据定理 3.1, 我们得到以下定理.

定理 3.4 令码 $\mathcal{C}$ 为 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵为 $[I_{3^{2s}}, \overline{Q}]$, 并且对于 $j = 0, 1, \ldots, 4$, T_j 由公式 (3.13) 得到. 那么码 $\mathcal{C}$ 是一个 $[2\cdot 3^{2s}, 3^{2s}]$ LCD 码当且仅当 $\prod_{j=0}^{4} T_j \not\equiv 0 \pmod{p_0}$, 而如果满足如下条件, 那么码 $\mathcal{C}$ 就是一个 hull 维数为 1 的 $[2\cdot 3^{2s}, 3^{2s}]$ 线性码:

$$T_0 \equiv 0 \pmod{p_0},\ T_j \not\equiv 0 \pmod{p_0} \text{ 对} j = 1, 2, 3, 4 \text{都成立.}$$

例子 3.4 沿用引理 3.7和定理 3.4的符号, 设 $s = 2$. 那么相应的第一特征矩阵是

$$P = \begin{pmatrix} 1 & 24 & 24 & 24 & 8 \\ 1 & 6 & -3 & -3 & -1 \\ 1 & -3 & 6 & -3 & -1 \\ 1 & -3 & -3 & 6 & -1 \\ 1 & -3 & -3 & -3 & 8 \end{pmatrix}.$$

令码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵为 $[I_{81}, \overline{Q}]$, 这里 $Q = A_0 + 2A_1 + A_2$. 根据公式 (3.13), 我们有 $T_0 = 5330 = 2\cdot 5\cdot 13\cdot 41$, $T_1 = 101$, $T_2 = 2$, $T_3 = 65$, $T_4 = 65$, 于是 $\prod_{j=0}^{4} T_j = 2^2\cdot 5^3\cdot 13^3\cdot 41\cdot 101$. 如果 $p_0 \neq 2, 5, 13, 41, 101$, 那么码 $\mathcal{C}$ 是一个 $[162, 81]$ LCD 码. 如果 $p_0 = 41$, 则码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[162, 81]$ 线性码.

3.3.4 与具有无理第一特征矩阵的结合方案相关的线性码

观察到前三小节构造的结合方案的第一特征矩阵 P 都是属于 $M_{|X|}(\mathbb{Z})$ 的. 一个自然的问题就是是否存在一个结合方案, 其特征矩阵 $P \notin M_{|X|}(\mathbb{Z})$. 答案显然是肯定的. 在这一小节, 我们将会介绍一个这样的结合方案的例子, 对于其第一特征矩阵 P, 存在某个位置 (j, i) 使得 P 的第 (j, i) 位置上的数 (将其记为 $p_i(j)$) 是非有理数.

令 Γ 是 X 上的一个无向的连通图, 其中 $|X| = n$. 对于 $x, y \in X$, 一条从 x 到 y 的长度为 r 的路径为一个序列, 其顶点为 $x_0 = x, x_1, \ldots, x_{r-1}, x_r = y$, 使得对于每一

个 $i \in \{0,1,\ldots,r-1\}$, (x_i, x_{i+1}) 都是 Γ 的一条边. x 和 y 的距离是 x 到 y 的最短路径, 我们记它为 $\partial(x,y)$. 这里 $\partial(x,x)$ 定义为 0. 图 Γ 中两个顶点之间的最大距离被称为 Γ 的直径.

基于上面关于距离的定义, 可以定义 X 上的关系 R_i: 对于每一个 $i \in \{0,1,\ldots,d\}$, $(x,y) \in R_i$ 当且仅当 $\partial(x,y) = i$. 如果 $\mathcal{X} = (X, \{R_i\}_{0\le i\le d})$ 构成一个 d 类结合方案, 则 Γ 被称为一个距离正则图. 显而易见, $\mathcal{X}$ 总是对称的. 读者可以通过文献[8]和文献[10]获取更多关于距离正则图和结合方案的信息. 在这些文献中, 可以了解到, 存在一个广义六边形, 记作 $\mathcal{H}(6)$, 它是通过 $\mathbb{F}_{3^2}$ 上的 3 维 Hermitian 极空间的来定义点和线的. 我们在这里省略具体的构造细节. 该广义六边形 $\mathcal{H}(6)$ 是一个直径为 6, 顶点个数为 126 的距离正则图. 在这一小节的剩余部分, 我们设 $\mathcal{X} = (X, \{R_i\}_{0\le i\le 6})$ 为由 $\mathcal{H}(6)$ 定义的 6 类结合方案. 下面的矩阵是 $\mathcal{H}(6)$ 的第一特征矩阵 P, 具体可以参考文献[8] 第 71 页.

$$P = \begin{pmatrix} 1 & 3 & 6 & 12 & 24 & 48 & 32 \\ 1 & \sqrt{6} & 3 & \sqrt{6} & 0 & -2\sqrt{6} & -4 \\ 1 & \sqrt{2} & -1 & -3\sqrt{2} & -4 & 2\sqrt{2} & 4 \\ 1 & 0 & -3 & 0 & 6 & 0 & -4 \\ 1 & -\sqrt{2} & -1 & 3\sqrt{2} & -4 & -2\sqrt{2} & 4 \\ 1 & -\sqrt{6} & 3 & -\sqrt{6} & 0 & 2\sqrt{6} & -4 \\ 1 & -3 & 6 & -12 & 24 & -48 & 32 \end{pmatrix}. \tag{3.14}$$

令 $\mathcal{X} = (X, \{R_i\}_{i=0}^6)$(这里 $|X| = 126$) 为由距离正则图 $\mathcal{H}(6)$ 定义的 6 类结合方案, 对于 $i = 0,1,\ldots,6$, A_i 是关系 R_i 对应的邻接矩阵. 设 $Q = \sum_{i=0}^6 c_i A_i$, 这里对于所有 $i = 0,1,\ldots,6$, 都有 $c_i \in \mathbb{Z}$. 因为这个 6 类结合方案是对称的, 那么对于每一个 $t(0 \le t \le 6)$, 定理 3.1给出的 T_t 如下所示

$$T_t = \left(\sum_{i=0}^{6} c_i p_i(t) \right)^2 + 1, \tag{3.15}$$

这里 $p_i(t)$ 代表由 (3.14) 给出的矩阵 P 的 (t,i) 位置上的元素. 应用定理 3.1, 我们得到下面的定理.

定理 3.5 令码 $\mathcal{C}$ 为 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵为 $[I_{126}, \overline{Q}]$, 对于 $j = 0,1,\ldots,6$, T_j 是由公式 (3.15) 定义的. 如果所有的 T_i 都是有理数, 那么我们可以得到如下结论, 码 $\mathcal{C}$ 是一个 $[252,126]$ LCD 码当且仅当 $\prod_{j=0}^6 T_j \not\equiv 0 \pmod{p_0}$, 而当满足下面条件时, 码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[252,126]$ 线性码:

$$T_0 \equiv 0 \pmod{p_0},\ T_j \not\equiv 0 \pmod{p_0}, j = 1,\ldots,6.$$

例子 3.5 沿用定理 3.5的符号, 令码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵为 $[I_{126}, \overline{Q}]$, 这里 $Q = 2A_1$. 根据公式 (3.15), 我们有 $T_0 = (2\cdot 3)^2 + 1 = 37, T_1 = (2\sqrt{6})^2 + 1 = 25$, $T_2 = (2\sqrt{2})^2+1 = 9, T_3 = (0)^2+1 = 1, T_4 = (-2\sqrt{2})^2+1 = 9, T_5 = (-2\sqrt{6})^2+1 = 25$, $T_6 = (-6)^2+1 = 37$, 所以可以推出 $\prod_{j=0}^{6} T_j = 3^4\cdot 5^4\cdot 37^2$. 观察到所有的 $T_i(0 \le i \le 6)$ 都是整数. 根据定理 3.5, 如果 $p_0 \neq 3, 5, 37$, 那么码 $\mathcal{C}$ 是一个 $[252, 126]$ LCD 码.

事实上, 基于定理 3.1以及第 3.2节中给出的代数数论的基本结论, 可以推导出下面的定理.

定理 3.6 令 p_0 为一个素数, $K = \mathbb{Q}(\zeta_m)$ 为一个满足 $m = p_0^l m'$ $(l \ge 0, p_0 \nmid m')$ 的分圆域, 且令 $\mathbb{O}_K = \mathbb{Z}[\zeta_m]$. 令 $\mathcal{P}$ 为 $\mathbb{O}_K$ 中包含 $p_0\mathbb{O}_K$ 的素理想, f 是由引理 3.1给出的 $\mathcal{P}$ 的次数, u 是一个满足 $f \mid u$ 的正整数. 令码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个 $[2n, n]$ 线性码, 其生成矩阵为 $G = [I_n, \overline{Q}]$, 这里 Q 由公式 (3.1) 给出. 沿用定理 3.1中的符号. 如果对于所有的 $t \in \{0, 1, \ldots, d\}$, 都有 $T_t' \in \mathbb{O}_K$, 那么我们有以下结论.

(1) 码 $\mathcal{C}$ 是 LCD 的当且仅当 $\Pi_{t=0}^{d} T_t \not\equiv 0 \pmod{\mathcal{P}}$;

(2) 当 $T_0 \equiv 0 \pmod{\mathcal{P}}$ 且对于 $t = 1, 2, ..., d$, 有 $T_t \not\equiv 0 \pmod{\mathcal{P}}$ 成立时, 码 $\mathcal{C}$ 的 hull 维数为 1.

证明. 正如第 3.2节中提到的, 我们有 $[\mathbb{O}_K/\mathcal{P} : \mathbb{F}_{p_0}] = f$, 于是 $\mathbb{O}_K/\mathcal{P} = \mathbb{F}_{p_0^f}$, 它是 $\mathbb{F}_{p_0^u}$ 的一个子域. 由于 $T_t'(0 \le t \le d)$ 是矩阵 QQ^T 所有的特征值, 且 $\mathcal{P}$ 是包含 $p_0\mathbb{O}_K$ 的一个素理想, 于是通过和定理 3.1的证明类似的讨论可以推出结论. □

因为素理想相关的计算更为复杂, 所以我们仅仅给出一个基于定理 3.6和广义六边形的例子, 对其他更多的构造我们不做探究.

例子 3.6 令 p_0 是一个素数, $K = \mathbb{Q}(\zeta_m)$, 这里 $m = p_0^l m'$ $(l \ge 0, p_0 \nmid m')$, $\mathcal{P}$ 是 $\mathbb{O}_K$ 中包含 p_0 的一个素理想. $\mathcal{P}$ 的次数 f 由引理 3.1给出. 设 u 为满足 $f \mid u$ 的一个正整数. 令 $Q = A_1 + A_2$, 码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵是 $[I_{126}, \overline{Q}]$. 根据公式 (3.15), 我们有 $T_0 = (3+6)^2 + 1 = 82 = 2\cdot 41, T_1 = (\sqrt{6}+3)^2 + 1 = 16 + 6\sqrt{6}$, $T_2 = (\sqrt{2}-1)^2 + 1 = 4 - 2\sqrt{2}, T_3 = (-3)^2 + 1 = 10 = 2\cdot 5, T_4 = (-\sqrt{2}-1)^2 + 1 = 4 + 2\sqrt{2}, T_5 = (-\sqrt{6}+3)^2 + 1 = 16 - 6\sqrt{6}, T_6 = (-3+6)^2 + 1 = 10 = 2\cdot 5$, 于是可以得到 $\prod_{j=0}^{6} T_j = 2^9\cdot 5^3\cdot 41$. 注意到, 如果 $\mu \in \mathbb{Z}$, 那么 $\overline{\mu} = \mu (\mathrm{mod}\, \mathcal{P}) \in \mathbb{F}_{p_0}$. 因此, 若 $p_0 \neq 2, 5, 41$, 则码 $\mathcal{C}$ 是一个 $[252, 126]$ LCD 码.

取 $p_0 = 41$, 对于 $p_0 = 41$ 所对应的素理想 $\mathcal{P}$, 对于每一个 $i \in \{0, 1, \ldots, 6\}$, 设 $\overline{T_i} = T_i + \mathcal{P}$. 显然, 我们有 $\overline{T_0} = \overline{0}, \overline{T_3} \neq \overline{0}$ 以及 $\overline{T_6} \neq \overline{0}$. 由于 $\gcd(8, 41) = 1$, 那么

$\overline{T_2T_4}=\overline{8}\neq\overline{0}$, 于是 $\overline{T_2}\neq\overline{0}$, $\overline{T_4}\neq\overline{0}$. 根据相类似的讨论, 我们得到 $\overline{T_1}\neq\overline{0}$ 以及 $\overline{T_5}\neq\overline{0}$. 于是可以得到结论: 码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[252,126]$ 线性码.

3.4 线性码的一个广义构造

第 3.3节中我们构造的所有生成矩阵为 $[I_n,Q]$ 的线性码 $\mathcal{C}$ 都是 $[2n,n]$ 线性码. 这意味着生成矩阵中的矩阵 Q 是一个 n 阶方阵. 在这一节中, 我们将推广第 3.3节中的构造, 使得构造 LCD 码以及 hull 维数为 1 的线性码所涉及到的矩阵 Q 不一定为方阵.

沿用第 3.3节中的符号, 令 $\mathcal{X}=(X,\{R_i\}_{0\leq i\leq d})$ 为一个交换的 d 类结合方案, 其满足 $|X|=n$, 且令 $\mathcal{M}=\langle A_0,A_1,\ldots,A_d\rangle_{\mathbb{C}}$ 为相应的交换代数. 设 ℓ 是一个满足 $\ell\geq 1$ 的整数. 对于每一个满足 $1\leq j\leq\ell$ 的 j, 定义

$$Q_j=\sum_{i=0}^{d}c_{ij}A_i\in\mathcal{M}, \tag{3.16}$$

这里对于每一个 $0\leq i\leq d$, 都有 $c_{ij}\in\mathbb{Z}$. 对于每个矩阵 Q_j $(1\leq j\leq\ell)$, 由公式 (3.2), 我们可以定义 $\overline{Q_j}$, 令

$$\overline{Q}=[\overline{Q}_1,\overline{Q}_2,...,\overline{Q}_\ell]. \tag{3.17}$$

于是有 $QQ^T=\sum_{j=1}^{\ell}Q_jQ_j^T$ 成立. 对于每一个 $t\in\{0,1,\ldots,d\}$, 都可以得到 QQ^T 在 V_t 上的特征值

$$T_t'=\sum_{j=1}^{\ell}\left(\sum_{i=0}^{d}c_{ij}p_i(t)\right)\left(\sum_{i=0}^{d}c_{ij}p_{i'}(t)\right), \tag{3.18}$$

这里, 根据引理 3.4和公式 (3.3), 我们有 $A_i^T=A_{i'}$ 对某个 $i'\in\{0,1,\ldots,d\}$ 成立. 特别地, 如果该结合方案是对称的, 那么对于每一个 $t\in\{0,1,\ldots,d\}$, 都有

$$T_t'=\sum_{j=1}^{\ell}\left(\sum_{i=0}^{d}c_{ij}p_i(t)\right)^2. \tag{3.19}$$

注意到引理 3.2以及引理 3.3中涉及到的矩阵 Q 不一定是一个方阵. 沿用上面的符号, 通过和定理 3.1相同的讨论, 可以很容易推导出下面的定理.

定理 3.7 令码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的一个 $[(\ell+1)n,n]$ 线性码, 其生成矩阵为 $G=[I_n,\overline{Q}]$, 这里 $\overline{Q}$ 由公式 (3.17) 给出. 对于每一个 $t\in\{0,1,\ldots,d\}$, 令 T_t' 为由公式 (3.18) 给出的 QQ^T 在 V_t 上的特征值, 且设 $T_t=T_t'+1$. 如果所有的 T_t' 都是有理数, 那么码 $\mathcal{C}$ 是 LCD 的当且仅当 $\Pi_{t=0}^{d}T_t\not\equiv 0\pmod{p_0}$, 而当 $T_0\equiv 0\pmod{p_0}$, 且 $T_t\not\equiv 0\pmod{p_0}$ 对于所有 $t=1,2,...,d$ 都成立时, 码 $\mathcal{C}$ 的 hull 维数为 1.

注 3.2 定理3.7给出的构造可以看成是定理3.1的一个推广. 显然, 定理3.7中生成矩阵为 $[I_n, \overline{Q}]$ 的线性码 $\mathcal{C}$ 的最小距离大于或等于生成矩阵为 $[I_n, \overline{Q_1}]$ 的线性码 $\mathcal{C}'$ 的最小距离. 经过同样的讨论, 在第 3.3节中, 定理 3.2, 定理 4.1, 定理 3.4和定理 3.5的结论都可以通过使矩阵 $\overline{Q}$ 如公式 (3.17) 中所定义而得到推广. 因此, 我们可以应用第 3.3节和定理 3.7中给出的结合方案来构造 $[(\ell+1)n, n]$ LCD 码以及 hull 维数为 1 的线性码.

令 $\mathcal{X} = (\mathbb{F}_q, \{R_i\}_{0\le i\le N})$ 为 N 类分圆结合方案, $A_0, A_1, \ldots, A_N$ 是相对应的邻接矩阵. 我们现在通过定理 3.7给出两个例子作为定理 3.2中构造的推广.

例子 3.7 令 $p = 3, \gamma = 1, N = 4$. 那么根据引理 3.5中的假设, 我们有 $j_0 = 1$ 以及 $q = 9$. 在这种情况下, 第一特征矩阵由公式 (3.10) 给出. 令码 $\mathcal{C}$ 为 $\mathbb{F}_{p_0^u}$ 上的一个线性码, 其生成矩阵为 $[I_q, \overline{Q_1}, \overline{Q_2}]$, 这里 $Q_1 = A_1 + 2A_2 + 4A_3 + 3A_4$, $Q_2 = 2A_0 + 2A_1 + 3A_2 + 4A_3$. 由于该结合方案是对称的, 那么应用公式 (3.19) 可以计算得到 $T_0 = 801$, $T_1 = 51$, $T_2 = 21$, $T_3 = 30$, $T_4 = 51$, 于是可以得到 $\Pi_{t=0}^4 T_t = 2\cdot 3^6\cdot 5\cdot 7\cdot 17^2\cdot 89$. 如果 $p_0 \neq 2, 3, 5, 7, 17, 89$, 那么码 $\mathcal{C}$ 是一个 $[27, 9]$ LCD 码. 特别地, 如果 $p_0 = 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79$, 则码 $\mathcal{C}$ 是一个 $[27, 9, 16]$ LCD 码. 如果 $p_0 = 89$, 则码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[27, 9, 16]$ 线性码.

例子 3.8 令 $p = 2, \gamma = 1, N = 3$. 那么根据引理 3.5的假设, 我们有 $j_0 = 1$ 以及 $q = 4$. 在这种情况下, 第一特征矩阵由公式 (3.11) 给出. 令码 $\mathcal{C}$ 是 $\mathbb{F}_{p_0^u}$ 上的线性码, 其生成矩阵为 $[I_q, \overline{Q_1}, \overline{Q_2}]$, 这里 $Q_1 = 2A_0 + A_1 + 6A_2 + 4A_3$, $Q_2 = A_0 + 3A_1 + 5A_2 + 4A_3$. 由于该结合方案是对称的, 那么应用公式 (3.19) 可以计算得到 $T_0 = 339$, $T_1 = 75$, $T_2 = 11$, $T_3 = 11$, 于是可以得到 $\Pi_{t=0}^3 T_t = 3\cdot 5^2\cdot 11^2\cdot 113$. 如果 $p_0 \neq 3, 5, 11, 113$, 那么码 $\mathcal{C}$ 是一个 $[12, 4]$ LCD 码. 特别地, 如果 $p_0 = 37, 61, 67, 73, 83, 89, 97, 101, 103, 107, 109, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173$, ..., 那么码 $\mathcal{C}$ 是一个 $[12, 4, 9]$ LCD MDS 码. 如果 $p_0 = 113$, 那么码 $\mathcal{C}$ 是一个 hull 维数为 1 的 $[12, 4, 9]$ MDS 线性码.

3.5 本章小结

在本章中, 我们给出了一种用结合方案来构造 LCD 码和 hull 维数为 1 的线性码的方法. 基于无定形的结合方案, 一些 LCD 码的充分必要条件以及 hull 维数为 1 的线性码的充分条件都在本章中给出. 我们利用已知的结合方案, 通过找到满足这些条件的码, 构造了大量 LCD 码以及 hull 维数为 1 的线性码. 基于本章的构造, 我们利用 Magma 程序, 提供了 LCD (almost) MDS 码以及 hull 维数为 1 的 (almost) MDS 码的

例子.

4 大的循环子空间码和 Sidon 空间的新构造

4.1 背景

令 q 为一个素数幂, $\mathbb{F}_q$ 是包含元素个数为 q 的有限域. 令 $\mathbb{F}_{q^n}$ 为 $\mathbb{F}_q$ 的 n 次扩张, 它可以被视为 $\mathbb{F}_q$ 上的一个 n 维向量空间. 对于非负整数 $k \leq n$, 用 $\mathcal{G}_q(n,k)$ 表示域 $\mathbb{F}_{q^n}$ 的所有 k-维 $\mathbb{F}_q$-子空间的集合. 我们可以在 $\mathcal{G}_q(n,k)$ 上定义一个度量: 对于 $U,V \in \mathcal{G}_q(n,k)$,

$$d(U,V) = 2k - 2\dim(U \cap V).$$

对于某些正整数 n, k, $\mathcal{G}_q(n,k)$ 的任何一个非空子集称为一个常维数码 *(constant dimension code)*. 由于 $k=1$ 的情况是平凡的, 我们接下来默认考虑 $k \geq 2$ 的情况. 近年来, 常维数码因其在随机网络编码中的应用引起了广泛的关注[41]. 其中一个主要的研究问题是寻找系统性的方法构造最小距离尽可能大的以及码字个数尽可能多的常维数子空间码.

对于一个子空间 $U \in \mathcal{G}_q(n,k)$ 以及 $\alpha \in \mathbb{F}_{q^n}^*$, 子空间 U 相对于 α 的循环移位 *(cyclic shift)* 记作 $\alpha U = \{\alpha u : u \in U\}$. 显然, αU 是一个和 U 具有相同维数的子空间. U 的轨道是 $\mathrm{orb}(U) = \{\alpha U : \alpha \in \mathbb{F}_{q^n}^*\}$, 并且对于某个 $t \mid n$, 有 $|\mathrm{orb}(U)| = \frac{q^n-1}{q^t-1}$, 具体细节可以参考文献[33] 中的推论 3.13. 如果 $\mathrm{orb}(U)$ 中包含的元素个数为 $\frac{q^n-1}{q-1}$, 那么它被称为一个全长轨道码 *(full-length orbit code)*. 这样的码的最小距离不超过 $2k-2$, 如果达到这样的界, 则该码被称为最优的 *(optimal)*[32]. 一般地, 如果 $\mathcal{C} \in \mathcal{G}_q(n,k)$ 是一个子空间码, 使得如果 $U \in \mathcal{C}$, 则 U 轨道中的所有元素也都在子空间码 $\mathcal{C}$ 中, 那么就称子空间码 $\mathcal{C}$ 为一个循环子空间码 *(cyclic subspace code)*. 循环子空间码最初在文献[26] 中被引入是为了寻找性质较好的子空间码, 这样的子空间码具有非常高效的编码算法和译码算法[12,26,34,40].

对于一个至少含有 $\frac{q^n-1}{q-1}$ 个码字的循环子空间码 $\mathcal{C}$, 其最小距离不能超过 $2k-2$[23]. 正如在文献[33] 的结尾作者提到的那样, 找到系统性的方法去构造 $\mathcal{G}_q(n,k)$ 中最小距离为 $2k-2$ 且码字个数远大于 $\frac{q^n-1}{q-1}$ 的 k-维循环子空间码是很有意义的. 根据子空间码的球堆积 *(sphere-packing)* 界, 参考下面的引理 4.6, 最小距离为 $2k-2$ 的子空间码最多含有 $\frac{(q^n-1)(q^{n-1}-1)}{(q^k-1)(q^{k-1}-1)}$ 个码字. 这个上界通常在 $k < n/2$ 并且 k 与 $n/2$ 不相近时是远大于 $\frac{q^n-1}{q-1}$ 的. 这个结论指示了我们寻找这类码的方向. 继作者在文献[11] 中的杰出工作之后, 利用线性化多项式构造 $\mathcal{G}_q(n,k)$ 中最小距离为 $2k-2$ 且码字个数远大于 $\frac{q^n-1}{q-1}$ 的循环子空间码的方法得到了广泛的研究, 具体可以参考文献[23,53,68]. 他们将子空间表示成单项数较少的子空间多项式的根, 并且谨慎地选取最优全长循环

子空间码的并, 避免缩短新构造的子空间码的最小距离. 这样的构造生成了很大 (即码字个数很多) 的循环子空间码, 但是一般来说, 由于求解这种多项式的复杂性, 很难给出这种构造下子空间码的最大可能规模的明确估计.

一个 *Sidon* 空间是指一个子空间 $U \in \mathcal{G}_q(n,k)$, 它满足 U 中的任意两个非零元素的乘积在 U 中有唯一分解 (若一个分解中的一个元素可以表示成另一个分解中的一个元素与 $\mathbb{F}_q$ 中某一个非零元的乘积, 那么这两个分解被视作同一个分解), 也就是说, 对于元素 $a,b,c,d \in U \setminus \{0\}$, 如果 $ab = cd$, 那么可以推出 $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$. 这里, 对于 $x \in \mathbb{F}_{q^n}$, 记 $x \cdot \mathbb{F}_q = \{\lambda x : \lambda \in \mathbb{F}_q\}$. Sidon 空间最初是在文献[13] 中被定义并且被用来研究子空间的某些特定乘法性质的, 事实上, 它和最优全长轨道码有非常密切的联系.

引理 4.1 (引理 34, Roth, Raviv 和 Tamo[58]) 令子空间 $U \in \mathcal{G}_q(n,k)$. 集合 $\mathcal{C} = \{\alpha U : \alpha \in \mathbb{F}_{q^n}^*\}$ 是一个最优全长轨道码当且仅当 U 是一个 Sidon 空间.

引理 4.1中给出的关系令 Sidon 空间成为了解决下面猜想的一个主要工具.

猜想 4.1 [33,65] 对于任意素数幂 q 和正整数 k 以及 $n > 2k$, 存在一个循环子空间码 $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, 其满足 $|\mathcal{C}| = \frac{q^n-1}{q-1}$ 和 $d(\mathcal{C}) = 2k-2$.

通过引理 4.1给出的关系, Roth 等学者[58] 解决了猜想 4.1的一部分, 即在 n 为偶数, $n \geq 2k$ 且 $q \geq 3$ 的情况下猜想中满足条件的循环子空间码的存在性. 这极大地推动了对 Sidon 空间的研究.

注 4.1 文献[58] 中提到, 由于一个 Sidon 空间的子空间也是 Sidon 空间, 于是 $\mathcal{G}_q(n,k)$ 中一个 Sidon 空间的构造也意味着对于任何 $1 \leq t \leq k$, $\mathcal{G}_q(n,t)$ 中也存在一个 Sidon 空间.

我们将目前为止所有已知的构造总结在表格 4.1中.

表 4.1　已知的关于 $\mathcal{G}_q(n,k)$ 中 Sidon 空间的构造

	q	n	k	参考文献
I	$q \geq 3$	n 为偶数	$k \leq \frac{n}{2}$	[58] 定理 12
II	$q \geq 2$	$n = rt, r \geq 3$	$k \leq t$	[58] 定理 16
III	$q \geq 2$	$n \geq 6$	$k \leq \lfloor \frac{n-2}{4} \rfloor$	[58] 定理 19
IV	$q \geq 2$	$n = 7t$	$k \leq \frac{2n}{7}$	定理 4.3

在文献[58] 中, 作者也提供了当 $n = 2k$ 时, $\mathcal{G}_q(n,k)$ 中最小距离为 $2k-2$ 的规

模很大的循环子空间码的构造, 其构造思路是选取由 Sidon 空间生成的最优全长轨道码的并构成新的子空间码. 该构造生成的码的一个显著特点是: 当 k 趋向于无穷大时, 它们的规模渐近地趋向球堆积界 (参考下文的引理 4.6) 的 $\frac{1}{2}$. 通过结合子空间多项式的技巧和 Sidon 空间的方法, Niu 等人[52] 给出了一个新的构造方法, 该构造产生了与仅仅使用线性化多项式方法的构造相比具有更多码字的循环子空间码.

在本章中, 我们提供了一种在 $\mathcal{G}_q(n,k)$ 中构造最小距离为 $2k-2$, 包含码字个数为 $(\lceil\frac{n}{2k}\rceil-1)\cdot\frac{q^k(q^n-1)}{q-1}$ 的循环子空间码的方法, 这里 n 是 k 的一个倍数, 且满足 $n\geq 3k$. 该构造利用了文献[58] 中构造的 Sidon 空间以及它们的变体, 详细信息可以参考本章中的引理 4.4和定理 4.1. 特别地, 当 $n=3k$ 且 k 趋向于无穷大时, 我们构造的子空间码的规模渐近地趋向于子空间码的球堆积界的 $\frac{1}{q-1}$. 这个结果和文献[58] 中的构造在 $n=2k$ 情形下的结果是类似的. 我们同时也提供了 $\mathcal{G}_q(7k,2k)$ 中 Sidon 空间的一个构造, 该构造利用引理 4.1证实了猜想 4.1在一些新情况下是成立的.

本章结构如下, 在第 4.2节中, 我们给出了本章中用到的一些基础知识. 在第 4.3节中, 我们介绍了本章的主要结论, 即 $\mathcal{G}_q(3k,k)$ 中最小距离为 $2k-2$ 且码字个数远多于 $\frac{q^n-1}{q-1}$ 的循环子空间码的构造以及 $\mathcal{G}_q(7k,2k)$ 中 Sidon 空间的一个新构造.

4.2 基础知识

首先介绍一些这章中要使用的符号. 令 k 为一个正整数, n 是 k 的一个倍数并且满足 $n\geq 3k$. 设

$$e:=\left\lceil\frac{n}{2k}\right\rceil-1. \tag{4.1}$$

令 q 为一个素数幂, 并且令 ξ 为 $\mathbb{F}_{q^k}$ 中的一个本原元. 令 γ 为 $\mathbb{F}_{q^k}$ 上某个 $\frac{n}{k}$ 次不可约多项式的根, 它是属于 $\mathbb{F}_{q^n}$ 的. 定义

$$\gamma_{i,j}:=\xi^i\gamma^j,\quad 0\leq i\leq q^k-2, 1\leq j\leq e. \tag{4.2}$$

引理 4.2 沿用上面的符号, 那么 $\{1,\gamma,\cdots,\gamma^{n/k-1}\}$ 是 $\mathbb{F}_{q^k}$ 上一个线性无关的集合.

证明. 证明具体可以参考文献[46] 中的定理 1.86 (ii). □

引理 4.3 假定 l 是一个正整数并且满足 $\gcd(l,k)=1$, u,v,s,t 是 $\mathbb{F}_{q^k}$ 中使得 $uv=st$ 以及 $u^{q^l}v=s^{q^l}t$ 成立的非零元素. 那么 $\frac{u}{s}=\frac{t}{v}$ 是 $\mathbb{F}_q^*$ 中的元素.

证明. 我们有 $(us^{-1})^{q^l}=tv^{-1}=us^{-1}$, 所以 us^{-1} 是 $\mathbb{F}_{q^l}$ 中的元素. 由于 $d:=\gcd(l,k)=1$, 我们有 $\mathbb{F}_{q^k}\cap\mathbb{F}_{q^l}=\mathbb{F}_{q^d}=\mathbb{F}_q$. 于是结论成立. □

定理 4.1 令 i, j 为确定的整数, 满足 $0 \le i \le q^k - 2$, $1 \le j \le e$, 令 $\gamma_{i,j}$ 为(4.2)中定义的形式. 令 l 为一个满足 $\gcd(l,k) = 1$ 的整数. 则 $U = \{u + (u^{q^l} - u)\gamma_{i,j} : u \in \mathbb{F}_{q^k}\}$ 是 $\mathbb{F}_q$ 上的一个 k 维 Sidon 空间.

证明. 对于 $1 \le j \le e$, 由引理 4.2可知, 1 和 γ^j 在 $\mathbb{F}_{q^k}$ 上是线性无关的, 所以我们有 $\gamma_{i,j} \notin \mathbb{F}_{q^k}$. 于是可以推出 U 在 $\mathbb{F}_q$ 上维数为 k. 令 u, v, s, t 为 $\mathbb{F}_{q^k}$ 上的非零元素, 并且设

$$\overline{u} := u + (u^{q^l} - u)\gamma_{i,j},\ \overline{v} := v + (v^{q^l} - v)\gamma_{i,j},$$
$$\overline{s} := s + (s^{q^l} - s)\gamma_{i,j},\quad \overline{t} := t + (t^{q^l} - t)\gamma_{i,j}.$$

假定 $\overline{u} \cdot \overline{v} = \overline{s} \cdot \overline{t}$. 我们需要证明

$$\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}. \tag{4.3}$$

因为由(4.1)可知, $2e \le n/k - 1$, 于是根据引理 4.2, $1, \gamma, \ldots, \gamma^{2e}$ 在 $\mathbb{F}_{q^k}$ 上是线性无关的. 比较公式 $\overline{u} \cdot \overline{v} = \overline{s} \cdot \overline{t}$ 展开后 $1, \gamma, \ldots, \gamma^{2e}$ 在两边的系数, 可以推导出 $uv = st$ 以及 $\xi^i(uv^{q^l} + u^{q^l}v - 2uv) = \xi^i(st^{q^l} + s^{q^l}t - 2st)$. 对两个公式做化简处理, 就可以得到

$$uv = st, \tag{4.4}$$
$$uv^{q^l} + u^{q^l}v = st^{q^l} + s^{q^l}t. \tag{4.5}$$

特别地, 由上面两个公式, 可以得到 $uv^{q^l} + u^{q^l}v = st^{q^l} + s^{q^l}t$ 以及 $(uv^{q^l}) \cdot (u^{q^l}v) = (st^{q^l}) \cdot (s^{q^l}t)$, 根据韦达定理, 可以推出 $\{uv^{q^l}, u^{q^l}v\} = \{st^{q^l}, s^{q^l}t\}$. 我们考虑以下两种情况.

(1) 如果有 $uv^{q^l} = st^{q^l}$ 以及 $u^{q^l}v = s^{q^l}t$ 成立, 那么根据引理 4.3, 可以推出 $\frac{u}{s} = \frac{t}{v} \in \mathbb{F}_q^*$. 于是(4.3)在这种情况下成立.

(2) 如果有 $uv^{q^l} = s^{q^l}t$ 以及 $u^{q^l}v = st^{q^l}$ 成立, 那么同样根据引理 4.3, 可以推出 $\frac{s}{v} = \frac{u}{t} \in \mathbb{F}_q^*$. 因此(4.3)在这种情况下也是成立的.

综上所述, $U \in \mathcal{G}_q(n,k)$ 是一个 Sidon 空间. □

引理 4.4 令 i 为一个给定的整数, 满足 $1 \le i \le e$. 那么子空间 $U = \{u + u^{q^l}\gamma^i : u \in \mathbb{F}_{q^k}\}$ 是一个 Sidon 空间, 这里 l 是一个满足 $\gcd(l,k) = 1$ 的正整数.

证明. 这个证明和文献[58] 中的定理 12 以及本章中的定理 4.1的证明类似, 我们对此不做过多描述. □

注 4.2 对于引理 4.4, 如果设 $i=1$, 并且取 k 为 n 的小于 $\frac{n}{2}$ 的最大因子, 那么就可以得到文献[58] 中的注 18 的其中一个构造, 该构造是文献[58] 中的构造 11 的推广. 注意到, 当 k 仅仅为 n 的一个小于 $\frac{n}{2}$ 的因子, 而不需要是最大因子时, 文献[58] 中的定理 12 的证明也是成立的.

定理 4.1和引理 4.4的构造都是文献[58] 中定理 12 的变式, 但是它们并没有生成具有新参数的 Sidon 空间. 我们将选取定理 4.1和引理 4.4中构造得到的 Sidon 空间轨道的并, 以此构造第三节中最小距离为 $2k-2$ 的循环子空间码. 为此, 我们需要以下结论.

引理 4.5 (引理 36, Roth, Raviv 和 Tamo[58]) 令 U 和 V 为 $\mathcal{G}_q(n,k)$ 中的两个不同的元素. 那么下面两个结论是等价的.

(1) 对于任意的 $\alpha \in \mathbb{F}_{q^n}^*$, 都有 $\dim(U \cap \alpha V) \leq 1$.

(2) 对于任意非零 $a, c \in U$ 以及非零 $b, d \in V$, 等式 $ab = cd$ 意味着 $a\mathbb{F}_q = c\mathbb{F}_q$ 以及 $b\mathbb{F}_q = d\mathbb{F}_q$.

最后, 我们回顾下面关于常维数子空间码的球堆积界. 对于满足 $s \leq t$ 的非负整数 t, s, 设 $\begin{bmatrix} t \\ s \end{bmatrix}_q := \prod_{i=0}^{s-1} \frac{q^{t-i}-1}{q^{i+1}-1}$.

引理 4.6 (定理 2, Etzion 和 Vardy[26]) 一个最小距离为 d 的子空间码 $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ 满足

$$|\mathcal{C}| \leq \frac{\begin{bmatrix} n \\ k-\frac{d}{2}+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\frac{d}{2}+1 \end{bmatrix}_q}.$$

4.3 主要结论

4.3.1 一个关于大规模的循环子空间码的构造

定理 4.2 令 k 为一个满足 $k \geq 2$ 的正整数, n 是 k 的倍数并且满足 $n \geq 3k$, 设 $e = \lceil \frac{n}{2k} \rceil - 1$. 令 ξ, γ 和 $\gamma_{i,j}$ ($0 \leq i \leq q^k-2, 1 \leq j \leq e$) 如第 4.2节那样定义, 并且令 l 为一个给定的且满足 $\gcd(l,k)=1$ 的正整数. 对于 $0 \leq i \leq q^k-2, 1 \leq j \leq e$, 我们设

$$U_{i,j} = \{u + (u^{q^l} - u)\gamma_{i,j} : u \in \mathbb{F}_{q^k}\}.$$

同时, 对于 $r = 1, \cdots, e$, 我们设

$$U_{q^k-1,r} := \{u + u^{q^l}\gamma^r : u \in \mathbb{F}_{q^k}\}.$$

对于每一对 (i, j), 我们相应地定义

$$\mathcal{C}_{i,j} := \{\alpha U_{i,j} : \alpha \in \mathbb{F}_{q^n}^*\}.$$

那么集合 $\mathcal{C} := \cup_{j=1}^{e} \cup_{i=0}^{q^k-1} \mathcal{C}_{i,j} \subseteq \mathcal{G}_q(n, k)$ 是一个包含码字个数为 $\frac{eq^k(q^n-1)}{q-1}$, 且最小距离为 $2k-2$ 的循环子空间码.

证明. 根据定理 4.1和引理 4.4, 对于每一组 (i, j), $U_{i,j}$ 都是 Sidon 空间, 并且由引理 4.1可知, 每一个码 $\mathcal{C}_{i,j}$ 都是一个大小为 $|\mathcal{C}_{i,j}| = \frac{q^n-1}{q-1}$ 以及最小距离为 $d(\mathcal{C}_{i,j}) = 2k-2$ 的循环子空间码. 为了证明码 $\mathcal{C}$ 的最小距离为 $2k-2$, 只需证明对于任意的 $\alpha \in \mathbb{F}_{q^n}^*$ 以及 $(i, r_1) \neq (j, r_2)$, 都有

$$\dim(\alpha U_{i,r_1} \cap U_{j,r_2}) \leq 1.$$

下面我们将分四种不同的情况, 分别应用引理 4.5证明该定理的结论.

(A) 首先考虑 $0 \leq i < j \leq q^k - 2, r_1 = r_2 = r \leq e$ 的情况. 令

$$\overline{u}_{i,r} = u + (u^{q^l} - u)\gamma_{i,r}, \overline{s}_{i,r} = s + (s^{q^l} - s)\gamma_{i,r}$$

为 $U_{i,r}$ 中任意非零元素, 并且令

$$\overline{v}_{j,r} = v + (v^{q^l} - v)\gamma_{j,r}, \overline{t}_{j,r} = t + (t^{q^l} - t)\gamma_{j,r}$$

为 $U_{j,r}$ 中任意非零元素, 这里 u, v, s, t 都是 $\mathbb{F}_{q^k}$ 中的非零元素. 由引理 4.5可知, 我们只需要证明 $\overline{u}_{i,r} \cdot \overline{v}_{j,r} = \overline{s}_{i,r} \cdot \overline{t}_{j,r}$ 意味着 $\overline{u}_{i,r}\mathbb{F}_q = \overline{s}_{i,r}\mathbb{F}_q, \overline{v}_{j,r}\mathbb{F}_q = \overline{t}_{j,r}\mathbb{F}_q$ 即可.

因为根据(4.1), 我们有 $2e \leq n/k - 1$, 于是由引理 4.2可知, $1, \gamma, \cdots, \gamma^{2e}$ 在 $\mathbb{F}_{q^k}$ 上是线性无关的. 比较 $1, \gamma^r, \gamma^{2r}$ 在 $\overline{u}_{i,r} \cdot \overline{v}_{j,r} = \overline{s}_{i,r} \cdot \overline{t}_{j,r}$ 展开式两边的系数, 可以推出 $uv = st$ 以及

$$(uv^{q^l} - uv)\xi^{j-i} + (u^{q^l}v - uv) = (st^{q^l} - st)\xi^{j-i} + (s^{q^l}t - st),$$
$$u^{q^l}v^{q^l} - (uv^{q^l} + u^{q^l}v) + uv = s^{q^l}t^{q^l} - (st^{q^l} + s^{q^l}t) + st.$$

由于 $uv = st$, 上面的两个等式可以化简为

$$uv^{q^l}\xi^{j-i} + u^{q^l}v = st^{q^l}\xi^{j-i} + s^{q^l}t,$$
$$uv^{q^l} + u^{q^l}v = st^{q^l} + s^{q^l}t.$$

将两个等式作差, 可以得到 $uv^{q^l}(\xi^{j-i}-1)=st^{q^l}(\xi^{j-i}-1)$. 由于 ξ 是 $\mathbb{F}_{q^k}^*$ 中的一个本原元, 并且 $0\leq i<j\leq q^k-2$, 可以推出 $\xi^{j-i}\neq 1$, 于是有 $uv^{q^l}=st^{q^l}$. 由引理 4.3, 可以推出 $\frac{u}{s}=\frac{t}{v}\in\mathbb{F}_q^*$. 因此可以得到 $\overline{u}_{i,r}\mathbb{F}_q=\overline{s}_{i,r}\mathbb{F}_q$ 和 $\overline{v}_{j,r}\mathbb{F}_q=\overline{t}_{j,r}\mathbb{F}_q$. 在这种情况下, 结论得到证明.

(B) 接着考虑 $i=q^k-1, 0\leq j\leq q^k-2, r_1=r_2=r\leq e$ 的情况. 和情况 (A) 做同样处理, 令

$$\overline{u}_{q^k-1,r}=u+u^{q^l}\gamma^r, \overline{s}_{q^k-1,r}=s+s^{q^l}\gamma^r$$

为 $U_{q^k-1,r}$ 中任意非零元素, 令

$$\overline{v}_{j,r}=v+(v^{q^l}-v)\gamma_{j,r}, \overline{t}_{j,r}=t+(t^{q^l}-t)\gamma_{j,r}$$

为 $U_{j,r}$ 中任意非零元素, 这里 u,s,v,t 是 $\mathbb{F}_{q^k}$ 中的非零元素. 我们只需要证明 $\overline{u}_{q^k-1,r}\cdot\overline{v}_{j,r}=\overline{s}_{q^k-1,r}\cdot\overline{t}_{j,r}$ 意味着 $\overline{u}_{q^k-1,r}\mathbb{F}_q=\overline{s}_{q^k-1,r}\mathbb{F}_q, \overline{v}_{j,r}\mathbb{F}_q=\overline{t}_{j,r}\mathbb{F}_q$ 即可.

比较 $1,\gamma^{2r}$ 在 $\overline{u}_{q^k-1,r}\cdot\overline{v}_{j,r}=\overline{s}_{q^k-1,r}\cdot\overline{t}_{j,r}$ 的展开式两端的系数, 可以得到 $uv=st$ 以及 $u^{q^l}v^{q^l}-u^{q^l}v=s^{q^l}t^{q^l}-s^{q^l}t$. 由于 $u^{q^l}v^{q^l}=s^{q^l}t^{q^l}$, 后者可以简化为 $u^{q^l}v=s^{q^l}t$. 由引理 4.3, 可以推出 $\frac{u}{s}=\frac{t}{v}\in\mathbb{F}_q^*$. 于是我们可以得到目标结论 $\overline{u}_{q^k-1,r}\mathbb{F}_q=\overline{s}_{q^k-1,r}\mathbb{F}_q$ 和 $\overline{v}_{j,r}\mathbb{F}_q=\overline{t}_{j,r}\mathbb{F}_q$.

(C) 考虑 $0\leq i,j\leq q^k-2$ 和 $1\leq r_1<r_2\leq e$ 的情况. 与前面两种情况一样, 我们令

$$\overline{u}_{i,r_1}=u+(u^{q^l}-u)\gamma_{i,r_1}, \overline{s}_{i,r_1}=s+(s^{q^l}-s)\gamma_{i,r_1}$$

为 U_{i,r_1} 中任意非零元素, 令

$$\overline{v}_{j,r_2}=v+(v^{q^l}-v)\gamma_{j,r_2}, \overline{t}_{j,r_2}=t+(t^{q^l}-t)\gamma_{j,r_2}$$

为 U_{j,r_2} 中任意非零元素, 这里 u,s,v,t 是 $\mathbb{F}_{q^k}^*$ 中的非零元素. 现在进一步假定 $\overline{u}_{i,r_1}\cdot\overline{v}_{j,r_2}=\overline{s}_{i,r_1}\cdot\overline{t}_{j,r_2}$. 比较 $1,\gamma^{r_2}$ 在其展开式两端的系数, 可以推出 $uv=st$ 和 $\xi^j u(v^{q^l}-v)=\xi^j s(t^{q^l}-t)$. 后者可以简化为 $uv^{q^l}=st^{q^l}$. 我们可以像前面的情况一样推导出 $\frac{t}{v}=\frac{u}{s}\in\mathbb{F}_q^*$. 所以, 我们可以得到目标结论 $\overline{u}_{i,r_1}\mathbb{F}_q=\overline{s}_{i,r_1}\mathbb{F}_q$ 以及 $\overline{v}_{j,r_2}\mathbb{F}_q=\overline{t}_{j,r_2}\mathbb{F}_q$. 因此我们完成了这种情况下的证明.

(D) 最后, 我们考虑情况 $i=q^k-1, 0\leq j\leq q^k-1, 1\leq r_1,r_2\leq e$, 其中 $r_1\neq r_2$. 令

$$\overline{u}_{q^k-1,r_1}=u+u^{q^l}\gamma^{r_1}, \overline{s}_{q^k-1,r_1}=s+s^{q^l}\gamma^{r_1}$$

为 U_{q^k-1,r_1} 中任意非零元素, 令

$$\overline{v}_{j,r_2}=v+g_j(v), \overline{t}_{j,r_2}=t+g_j(t)$$

为 U_{j,r_2} 中任意非零元素, 这里 u, v, s, t 是 $\mathbb{F}_{q^k}$ 中的非零元素, 并且

$$g_j(x) = \begin{cases} (x^{q^l} - x)\gamma_{j,r_2}, & \text{如果} 0 \le j \le q^k - 2, \\ x^{q^l}\gamma^{r_2}, & \text{如果} j = q^k - 1. \end{cases}$$

假定 $\overline{u}_{q^k-1,r_1} \cdot \overline{v}_{j,r_2} = \overline{s}_{q^k-1,r_1} \cdot \overline{t}_{j,r_2}$. 比较 $1, \gamma^{r_1}$ 在其展开式两端的系数, 我们有 $uv = st$ 以及 $u^{q^l}v = s^{q^l}t$. 根据引理 4.3, 可以推出 $\frac{u}{s} = \frac{t}{v} \in \mathbb{F}_q^*$, 于是我们得到 $\overline{u}_{i,r_1}\mathbb{F}_q = \overline{s}_{i,r_1}\mathbb{F}_q$ 以及 $\overline{v}_{j,r_2}\mathbb{F}_q = \overline{t}_{j,r_2}\mathbb{F}_q$.

综上所述, 我们证明了子空间码 $\mathcal{C}$ 的最小距离为 $2k-2$. 特别地, 我们证明了 $\mathcal{C}$ 中的这 $\frac{eq^k(q^n-1)}{q-1}$ 个元素是各不相同的, 所以 $|\mathcal{C}| = \frac{eq^k(q^n-1)}{q-1}$. 因此, 我们完成了对该定理的证明. □

注 4.3 当 $n = 2k$ 时, 文献[58] 中的构造 37 利用 Sidon 空间生成了 $\mathcal{G}_q(2k, k)$ 中最小距离为 $2k-2$ 的码字个数远多于 $\frac{q^n-1}{q-1}$ 的循环子空间码. 该构造中给出的子空间码的码字个数可以达到引理 4.6中球堆积界的 $\frac{1}{2} + o_k(1)$, 这里符号 $o_k(1)$ 意味着当 k 趋向于无穷大时, 其大小趋向于 0. 当 $n = 3k$ 时, 定理 4.2利用 Sidon 空间构造了 $\mathcal{G}_q(3k, k)$ 中一个最小距离为 $2k-2$, 包含码字个数为 $\frac{q^k(q^{3k}-1)}{q-1}$ 的循环子空间码. 根据引理 4.6, $\mathcal{G}_q(3k, k)$ 中最小距离为 $2k-2$ 的子空间码包含码字个数的上界为 $\frac{(q^{3k}-1)(q^{3k-1}-1)}{(q^k-1)(q^{k-1}-1)}$. 当 k 趋向于无穷大时, 上述构造的循环子空间码的码字个数可以达到引理 4.6中球堆积界的 $\frac{1}{q-1} + o_k(1)$. 特别地, 当 $q = 2$ 时, 码字个数可以渐近地达到这个上界.

4.3.2 $\mathcal{G}_q(7k, 2k)$ 中 Sidon 空间的构造

定理 4.3 令 $k > 1$ 为一个整数, n 是 k 的倍数, 并且满足 $\frac{n}{k} \ge 7$. 取 γ 为 $\mathbb{F}_{q^k}$ 上次数为 n/k 的一个不可约多项式的根. 设

$$U = \{u_1 + (u_1^{q^l} - u_1)\gamma + u_2\gamma^2 + u_2^{q^l}\gamma^3 : u_1, u_2 \in \mathbb{F}_{q^k}\},$$

这里 l 是一个满足 $\gcd(l, k) = 1$ 的整数. 那么 $U \in \mathcal{G}_q(n, 2k)$ 是一个 Sidon 空间.

证明. 假定 $\overline{u} \cdot \overline{v} = \overline{s} \cdot \overline{t}$, 这里 $\overline{u}, \overline{v}, \overline{s}, \overline{t}$ 是 U 中的非零元素. 记

$$\overline{u} = u_1 + (u_1^{q^l} - u_1)\gamma + u_2\gamma^2 + u_2^{q^l}\gamma^3, \ \ \overline{v} = v_1 + (v_1^{q^l} - v_1)\gamma + v_2\gamma^2 + v_2^{q^l}\gamma^3,$$
$$\overline{s} = s_1 + (s_1^{q^l} - s_1)\gamma + s_2\gamma^2 + s_2^{q^l}\gamma^3, \quad \overline{t} = t_1 + (t_1^{q^l} - t_1)\gamma + t_2\gamma^2 + t_2^{q^l}\gamma^3,$$

这里, 对于 $i = 1, 2$, u_i, v_i, s_i, t_i 都是 $\mathbb{F}_{q^k}$ 中的元素. 要证明 U 是一个 Sidon 空间, 我们只需要证明

$$\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$$

总是成立即可.

由于 $\frac{n}{k}-1\geq 6$, 根据引理 4.2, 元素 $1,\gamma,\ldots,\gamma^6$ 在 $\mathbb{F}_{q^k}$ 上是线性无关的. 比较它们在 $\overline{u}\cdot\overline{v}=\overline{s}\cdot\overline{t}$ 展开式两端的系数, 我们得到

$$u_1v_1=s_1t_1, \tag{4.6}$$

$$u_1(v_1^{q^l}-v_1)+(u_1^{q^l}-u_1)v_1=s_1(t_1^{q^l}-t_1)+(s_1^{q^l}-s_1)t_1, \tag{4.7}$$

$$u_1v_2+u_2v_1+(u_1^{q^l}-u_1)(v_1^{q^l}-v_1)=s_1t_2+s_2t_1+(t_1^{q^l}-t_1)(s_1^{q^l}-s_1), \tag{4.8}$$

$$u_1v_2^{q^l}+u_2^{q^l}v_1+(u_1^{q^l}-u_1)v_2+u_2(v_1^{q^l}-v_1)=s_1t_2^{q^l}+s_2^{q^l}t_1+(s_1^{q^l}-s_1)t_2+s_2(t_1^{q^l}-t_1), \tag{4.9}$$

$$(u_1^{q^l}-u_1)v_2^{q^l}+u_2^{q^l}(v_1^{q^l}-v_1)+u_2v_2=(s_1^{q^l}-s_1)t_2^{q^l}+s_2^{q^l}(t_1^{q^l}-t_1)+s_2t_2, \tag{4.10}$$

$$u_2v_2^{q^l}+u_2^{q^l}v_2=s_2t_2^{q^l}+s_2^{q^l}t_2, \tag{4.11}$$

$$u_2^{q^l}v_2^{q^l}=s_2^{q^l}t_2^{q^l}. \tag{4.12}$$

由于 $u_1v_1=s_1t_1$, (4.7)可以简化为

$$u_1v_1^{q^l}+u_1^{q^l}v_1=s_1t_1^{q^l}+s_1^{q^l}t_1. \tag{4.13}$$

结合(4.6), (4.8)以及(4.13), 我们推出

$$u_1v_2+u_2v_1=s_1t_2+s_2t_1. \tag{4.14}$$

于是(4.9)可以简化成

$$u_1v_2^{q^l}+u_2^{q^l}v_1+u_1^{q^l}v_2+u_2v_1^{q^l}=s_1t_2^{q^l}+s_2^{q^l}t_1+s_1^{q^l}t_2+s_2t_1^{q^l}. \tag{4.15}$$

结合(4.12)和(4.14), (4.10)可以简化成

$$u_1v_2^{q^l}+u_2^{q^l}v_1=s_1t_2^{q^l}+s_2^{q^l}t_1. \tag{4.16}$$

由(4.6)可知, 我们有 $(u_1v_1^{q^l})\cdot(u_1^{q^l}v_1)=(s_1t_1^{q^l})\cdot(s_1^{q^l}t_1)$. 结合(4.13), 由韦达定理, 可以推出

$$\{u_1v_1^{q^l},u_1^{q^l}v_1\}=\{s_1t_1^{q^l},s_1^{q^l}t_1\}. \tag{4.17}$$

类似地, 可以推出

$$\{u_1v_2,u_2v_1\}=\{s_1t_2,s_2t_1\}\ (\text{由(4.6), (4.14), (4.12)可得}), \tag{4.18}$$

$$\{u_1v_2^{q^l},u_2^{q^l}v_1\}=\{s_1t_2^{q^l},s_2^{q^l}t_1\}\ (\text{由(4.6), (4.16), (4.12)可得}), \tag{4.19}$$

$$\{u_2v_2^{q^l},u_2^{q^l}v_2\}=\{s_2t_2^{q^l},s_2^{q^l}t_2\}\ (\text{由(4.11), (4.12)可得}). \tag{4.20}$$

注意到由 $\overline{u}\cdot\overline{v}=\overline{s}\cdot\overline{t}$ 推导出的(4.6)-(4.12)这七个公式和简化后得到的七个公式(4.6), (4.13), (4.14), (4.15), (4.16), (4.11), (4.12)是等价的. 后面的七个公式具有高度对称性, 并且它们在由 (a), (b), (c), (d) 所示的在八个参数 $\{u_1,\cdots,t_2\}$ 之间的作用下是不变的:

(a) $(u_i,v_i,s_i,t_i)\mapsto(u_{3-i},v_{3-i},s_{3-i},t_{3-i}),\ i=1,2;$

(b) $(u_i,v_i,s_i,t_i)\mapsto(v_i,u_i,s_i,t_i),\ i=1,2;$

(c) $(u_i,v_i,s_i,t_i)\mapsto(u_i,v_i,t_i,s_i),\ i=1,2;$

(d) $(u_i,v_i,s_i,t_i)\mapsto(s_i,t_i,u_i,v_i),\ i=1,2.$

它们共同构成了阶为 16 的一个群 G, 这个群 G 作用在这八个参数之间是传递的. 我们将会在下面的证明中充分利用这种对称性.

情况 **1.** 假定 u_i, v_i, s_i, t_i $(i=1,2)$ 中至少有一个为 0. 根据上文提到的对称性, 不失一般性, 我们假定 $u_1=0$. 根据公式(4.6), 我们可以推出 $s_1t_1=0$. 可知 u_1 在 G 中的稳定子的阶为 2 (即 (c) 型作用), 其作用在 $\{s_1,t_1\}$ 上是传递的. 因此, 不失一般性, 我们假定 $s_1=0$. 因为 $\overline{u}$ 和 $\overline{s}$ 都是非零的, 所以我们必然有 $u_2s_2\neq0$. 于是公式(4.14)和(4.16)可以分别简化为 $u_2v_1=s_2t_1$ 以及 $u_2^{q^l}v_1=s_2^{q^l}t_1$. 特别地, 如果 $v_1=0$, 那么显然有 $t_1=0$.

(1.1) 假定 $v_1=0$ 以及 $t_1=0$. 由于 $\overline{v}$ 和 $\overline{t}$ 都是非零的, 我们有 $v_2\neq0$ 以及 $t_2\neq0$ 成立. 根据公式(4.20), 我们有 $u_2v_2^{q^l}=s_2t_2^{q^l}$ 或者 $u_2v_2^{q^l}=s_2^{q^l}t_2$ 成立. 根据引理 4.3以及(4.12)中的 $u_2v_2=s_2t_2$, 可以推出 $\frac{v_2}{t_2}=\frac{s_2}{u_2}\in\mathbb{F}_q^*$ 或者 $\frac{v_2}{s_2}=\frac{t_2}{u_2}\in\mathbb{F}_q^*$ 成立. 在任何一种可能性中, 都有 $\{\overline{u}\mathbb{F}_q,\overline{v}\mathbb{F}_q\}=\{\overline{s}\mathbb{F}_q,\overline{t}\mathbb{F}_q\}$.

(1.2) 假定 $v_1t_1\neq0$. 根据引理 4.3, 由 $u_2v_1=s_2t_1$ 和 $u_2^{q^l}v_1=s_2^{q^l}t_1$, 我们可以推出 $\frac{u_2}{s_2}=\frac{t_1}{v_1}\in\mathbb{F}_q^*$. 在这种情况下, 我们仍然可以证明 $\{\overline{u}\mathbb{F}_q,\overline{v}\mathbb{F}_q\}=\{\overline{s}\mathbb{F}_q,\overline{t}\mathbb{F}_q\}$.

因此, 我们完成了情况 1 的证明.

情况 **2.** 假定 u_i, v_i, s_i, t_i $(i=1,2)$ 中任何一个都不为 0. 回顾(4.17)中的等式

$$\{u_1v_1^{q^l},u_1^{q^l}v_1\}=\{s_1t_1^{q^l},s_1^{q^l}t_1\}.$$

根据 (a) 型对称和 (c) 型对称, 不失一般性, 我们假定 $u_1v_1^{q^l}=s_1t_1^{q^l}$ 以及 $u_1^{q^l}v_1=s_1^{q^l}t_1$. 由(4.6), 我们有 $s_1t_1=u_1v_1$. 应用引理 4.3, 我们可以推出 $u_1s_1^{-1}=t_1v_1^{-1}\in\mathbb{F}_q^*$. 我们可以推断由(4.18)-(4.20)给出的八种可能情况都直接导致 $\{\overline{u}\mathbb{F}_q,\overline{v}\mathbb{F}_q\}=\{\overline{s}\mathbb{F}_q,\overline{t}\mathbb{F}_q\}$ 成立. 我们分以下三种情况讨论.

(2.1) 如果 $(u_1v_2, u_2v_1) = (s_1t_2, s_2t_1)$, 那么 $\frac{u_2}{s_2} = \frac{t_1}{v_1} = \frac{u_1}{s_1} = \frac{t_2}{v_2} \in \mathbb{F}_q^*$. 于是我们有 $\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$ 成立.

(2.2) 如果 $(u_1v_2^{q^l}, u_2^{q^l}v_1) = (s_1t_2^{q^l}, s_2^{q^l}t_1)$, 那么 $(\frac{t_2}{v_2})^{q^l} = \frac{u_1}{s_1} = \frac{t_1}{v_1} = (\frac{u_2}{s_2})^{q^l} \in \mathbb{F}_q$, 也同时有 $\frac{t_2}{v_2} = \frac{u_2}{s_2}$. 于是我们有 $\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$ 成立.

(2.3) 如果以上两种情况都不成立, 那么我们有

$$(u_1v_2, u_2v_1) = (s_2t_1, s_1t_2),$$
$$(u_1v_2^{q^l}, u_2^{q^l}v_1) = (s_2^{q^l}t_1, s_1t_2^{q^l})$$

同时成立. 于是, $\frac{s_2}{v_2} = \frac{u_1}{t_1} = (\frac{s_2}{v_2})^{q^l} \in \mathbb{F}_q^*$, 所以 $\frac{u_2}{t_2} = \frac{s_2}{v_2} = \frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q^*$. 于是我们有 $\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$ 成立.

情况 2 同样得到证明.

综上所述, 我们证明了 $U \in \mathcal{G}_q(n, 2k)$ 是一个 Sidon 空间.

□

注 4.4 根据定理 4.3, 对于任意的 $1 \leq t \leq 2k$, 存在 $\mathcal{G}_q(7k, t)$ 中的 Sidon 空间. 与文献[58] 中已知的构造相比较, 这个定理生成了具有新参数的 Sidon 空间. 例如, 如果 n 的最小素因子是 7, 那么对于满足 $t \leq \frac{2n}{7}$ 的整数 t, 我们的构造给出了 $\mathcal{G}_q(n, t)$ 中的 Sidon 空间, 并且当 $t > \lfloor \frac{n-2}{4} \rfloor$ 时, 这些 Sidon 空间并不能由文献[58] 中的构造生成, 具体可以参考表格 4.1.

接下来我们给出另一个构造, 虽然新构造的参数可以被定理 4.3中构造的参数所涵盖, 但是我们得到了不同的 Sidon 空间.

定理 4.4 令 $k > 1$ 为一个整数, n 是 k 的倍数且 n 是一个奇数, 并且满足 $\frac{n}{k} \geq 7$. 取 γ 为 $\mathbb{F}_{q^k}$ 上次数为 n/k 的一个不可约多项式的根. 设

$$U = \{u_1 + u_1^{q^l}\gamma + u_2^{q^l}\gamma^2 + u_2\gamma^3 : u_1, u_2 \in \mathbb{F}_{q^k}\},$$

这里 l 是一个满足 $\gcd(l, k) = 1$ 的整数. 那么 $U \in \mathcal{G}_q(n, 2k)$ 是一个 Sidon 空间.

证明. 假定 $\overline{u} \cdot \overline{v} = \overline{s} \cdot \overline{t}$, 这里 $\overline{u}, \overline{v}, \overline{s}, \overline{t}$ 是 U 中的非零元素. 我们记

$$\overline{u} = u_1 + u_1^{q^l}\gamma + u_2^{q^l}\gamma^2 + u_2\gamma^3, \quad \overline{v} = v_1 + v_1^{q^l}\gamma + v_2^{q^l}\gamma^2 + v_2\gamma^3,$$
$$\overline{s} = s_1 + s_1^{q^l}\gamma + s_2^{q^l}\gamma^2 + s_2\gamma^3, \quad \overline{t} = t_1 + t_1^{q^l}\gamma + t_2^{q^l}\gamma^2 + t_2\gamma^3,$$

这里, 对于 $i=1,2$, u_i, v_i, s_i, t_i 都是 $\mathbb{F}_{q^k}$ 中的元素. 要证明 U 是一个 Sidon 空间, 我们只需要证明

$$\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$$

总是成立即可.

由于 $\frac{n}{k}-1 \geq 6$, 根据引理 4.2, 元素 $1, \gamma, \ldots, \gamma^6$ 在 $\mathbb{F}_{q^k}$ 上是线性无关的. 比较它们在 $\overline{u}\cdot\overline{v} = \overline{s}\cdot\overline{t}$ 展开式两端的系数, 我们得到

$$u_1v_1 = s_1t_1, \tag{4.21}$$

$$u_1v_1^{q^l} + u_1^{q^l}v_1 = s_1t_1^{q^l} + s_1^{q^l}t_1, \tag{4.22}$$

$$u_1v_2^{q^l} + u_2^{q^l}v_1 + u_1^{q^l}v_1^{q^l} = s_1t_2^{q^l} + s_2^{q^l}t_1 + s_1^{q^l}t_1^{q^l}, \tag{4.23}$$

$$u_1v_2 + u_2v_1 + u_1^{q^l}v_2^{q^l} + u_2^{q^l}v_1^{q^l} = s_1t_2 + s_2t_1 + s_1^{q^l}t_2^{q^l} + s_2^{q^l}t_1^{q^l}, \tag{4.24}$$

$$u_1^{q^l}v_2 + u_2v_1^{q^l} + u_2^{q^l}v_2^{q^l} = s_1^{q^l}t_2 + s_2t_1^{q^l} + s_2^{q^l}t_2^{q^l}, \tag{4.25}$$

$$u_2^{q^l}v_2 + u_2v_2^{q^l} = s_2^{q^l}t_2 + s_2t_2^{q^l}, \tag{4.26}$$

$$u_2v_2 = s_2t_2. \tag{4.27}$$

与定理 4.3中的讨论类似，我们得到

$$\{u_1v_1^{q^l}, u_1^{q^l}v_1\} = \{s_1t_1^{q^l}, s_1^{q^l}t_1\}(\text{由(4.21)和(4.22)可得}), \tag{4.28}$$

$$\{u_1v_2^{q^l}, u_2^{q^l}v_1\} = \{s_1t_2^{q^l}, s_2^{q^l}t_1\}(\text{由(4.21),(4.23)及(4.27)可得}), \tag{4.29}$$

$$\{u_1^{q^l}v_2, u_2v_1^{q^l}\} = \{s_1^{q^l}t_2, s_2t_1^{q^l}\}(\text{由(4.21),(4.25)及(4.27)可得}), \tag{4.30}$$

$$\{u_2^{q^l}v_2, u_2v_2^{q^l}\} = \{s_2^{q^l}t_2, s_2t_2^{q^l}\}(\text{由(4.26)和(4.27)可得}). \tag{4.31}$$

同样地, 由于(4.21)-(4.27)这七个公式具有高度对称性, 它们在 (a), (b), (c), (d) 的作用下是不变的:

(a) $(u_i, v_i, s_i, t_i) \mapsto (u_{3-i}, v_{3-i}, s_{3-i}, t_{3-i})$, $i=1,2$;

(b) $(u_i, v_i, s_i, t_i) \mapsto (v_i, u_i, s_i, t_i)$, $i=1,2$;

(c) $(u_i, v_i, s_i, t_i) \mapsto (u_i, v_i, t_i, s_i)$, $i=1,2$;

(d) $(u_i, v_i, s_i, t_i) \mapsto (s_i, t_i, u_i, v_i)$, $i=1,2$.

它们共同构成了阶为 16 的一个群 G, 该群 G 作用在这八个参数之间是传递的. 我们将会在下面的证明中充分利用这种对称性.

情况 **1.** 假定 u_i, v_i, s_i, t_i $(i = 1, 2)$ 中至少有一个为 0. 根据上文提到的对称性, 不失一般性, 我们假定 $u_1 = 0$. 根据(4.21), 我们可以推出 $s_1 t_1 = 0$. 可知 u_1 在 G 中的稳定子的阶为 2 (即 (c) 型作用), 其作用在 $\{s_1, t_1\}$ 上是传递的. 因此, 不失一般性, 我们假定 $s_1 = 0$. 因为 $\overline{u}$ 和 $\overline{s}$ 都是非零的, 我们有 $u_2 s_2 \neq 0$. 于是(4.23)和(4.25)可以分别简化为 $u_2^{q^l} v_1 = s_2^{q^l} t_1$ 以及 $u_2 v_1^{q^l} = s_2 t_1^{q^l}$. 特别地, 如果 $v_1 = 0$, 那么显然有 $t_1 = 0$.

(1.1) 假定 $v_1 = 0$ 以及 $t_1 = 0$. 由于 $\overline{v}$ 和 $\overline{t}$ 都是非零的, 我们有 $v_2 \neq 0$ 以及 $t_2 \neq 0$ 成立. 根据公式(4.31), 我们有 $u_2 v_2^{q^l} = s_2 t_2^{q^l}$ 或者 $u_2 v_2^{q^l} = s_2^{q^l} t_2$ 成立. 根据引理 4.3以及(4.27)中的 $u_2 v_2 = s_2 t_2$, 我们推出 $\frac{v_2}{t_2} = \frac{s_2}{u_2} \in \mathbb{F}_q^*$ 或者 $\frac{v_2}{s_2} = \frac{t_2}{u_2} \in \mathbb{F}_q^*$ 成立. 在任何一种可能性中, 我们都有 $\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$.

(1.2) 假定 $v_1 t_1 \neq 0$. 根据引理 4.3, 由 $u_2^{q^l} v_1 = s_2^{q^l} t_1$ 和 $u_2 v_1^{q^l} = s_2 t_1^{q^l}$, 我们可以推出 $\frac{u_2}{s_2} = (\frac{t_1}{v_1})^{q^l} = (\frac{u_2}{s_2})^{q^{2l}}$, 由于 n 是奇数, 而 $\gcd(l, k) = 1$, 于是 $\frac{u_2}{s_2} = \frac{t_1}{v_1} \in \mathbb{F}_{q^k}^* \cap \mathbb{F}_{q^{2l}}^* = \mathbb{F}_q^*$. 在这种情况下, 我们仍然可以证明 $\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$.

因此, 我们完成了情况 1 的证明.

情况 **2.** 假定 u_i, v_i, s_i, t_i $(i = 1, 2)$ 中任何一个都不为 0. 回顾(4.28)中的等式

$$\{u_1 v_1^{q^l}, u_1^{q^l} v_1\} = \{s_1 t_1^{q^l}, s_1^{q^l} t_1\}.$$

根据 (a) 型对称和 (c) 型对称, 不失一般性, 我们假定 $u_1 v_1^{q^l} = s_1 t_1^{q^l}$ 以及 $u_1^{q^l} v_1 = s_1^{q^l} t_1$. 由(4.21), 我们有 $s_1 t_1 = u_1 v_1$. 应用引理 4.3, 我们可以推出 $u_1 s_1^{-1} = t_1 v_1^{-1} \in \mathbb{F}_q^*$. 我们可以直接推断由(4.29)-(4.31)给出的八种可能情况都直接导致 $\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$ 成立. 我们分以下三种情况讨论.

(2.1) 如果 $(u_1 v_2^{q^l}, u_2^{q^l} v_1) = (s_1 t_2^{q^l}, s_2^{q^l} t_1)$, 这种情况与定理 4.3证明中情况 2 的 (2.2) 完全一样.

(2.2) 如果 $(u_1^{q^l} v_2, u_2 v_1^{q^l}) = (s_1^{q^l} t_2, s_2 t_1^{q^l})$. 那么 $\frac{t_2}{v_2} = (\frac{u_1}{s_1})^{q^l} = \frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q^*$. 于是我们有 $\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$ 成立.

(2.3) 如果以上两种情况都不成立, 那么我们有

$$(u_1 v_2^{q^l}, u_2^{q^l} v_1) = (s_2^{q^l} t_1, s_1 t_2^{q^l}),$$
$$(u_1^{q^l} v_2, u_2 v_1^{q^l}) = (s_2 t_1^{q^l}, s_1^{q^l} t_2)$$

同时成立. 于是, $\frac{u_1}{t_1} = (\frac{s_2}{v_2})^{q^l} = (\frac{u_1}{t_1})^{q^{2l}} \in \mathbb{F}_q^*$. 所以 $\frac{u_1}{t_1} = \frac{s_2}{v_2} = \frac{u_2}{t_2} = \frac{s_1}{v_1} \in \mathbb{F}_q^*$. 于是我们有 $\{\overline{u}\mathbb{F}_q, \overline{v}\mathbb{F}_q\} = \{\overline{s}\mathbb{F}_q, \overline{t}\mathbb{F}_q\}$ 成立.

情况 2 同样得到证明.

综上所述, 我们证明了 $U \in \mathcal{G}_q(n, 2k)$ 是一个 Sidon 空间.

□

5 总结与展望

本章主要简略叙述作者接下来工作的展望.

构造的推广以及 m-ovoids 及其对应强正则图的自同构群

在第 2 章中, 我们利用已知的强正则凯莱图构造了辛极空间 $\mathrm{W}(2r-1,p^e)$ 中大量具有新参数的 m-ovoids. 在这章里我们仅应用了一种类型的强正则凯莱图, 在这种强正则凯莱图之外, 可能还有更多的其他类型的强正则凯莱图可以通过定理 2.3得到更多可能的结果. 与此同时, 这样的构造方法也可以推广到其他有限经典极空间中去, 我们可能由此可以得到更多有意思的结论.

我们在注 2.1中提到, 这样构造得到的 m-ovoids 具有一个亚循环群作为其自同构群, 该亚循环群同时也是相关的强正则凯莱图的自同构群. 但这个亚循环群不是这两者的全自同构群, 寻找由定理 2.3得到的 m-ovoids 的全自同构群是一个相当有意思并且有挑战性的问题. 进一步地, 探寻 m-ovoids 的全自同构群与其相关的强正则凯莱图的全自同构群之间的关系也是相当有意义的.

除此之外, 其他几类有限经典极空间上的 intriguing sets 问题仍然有很多探索的空间. 同时, intriguing sets 和组合数学中其他组合结构的联系可以被应用来构造更多的组合对象.

子空间码的构造与边界问题

第 4 章中, 我们仅利用 Sidon 空间构造了一类码字很多的循环子空间码, 并且证明了一定条件的循环子空间码的存在性. 目前关于循环子空间码构造的研究所使用的工具十分有限, 我们可以寻找更多的方法以使这个问题得到突破. 另一类关于子空间码的问题是子空间码码字个数的上界与下界问题, 这类问题也将成为我接下来可能关注的方向.

参 考 文 献

[1] Ahlswede R, Cai N, Li S -Y R, Yeung R W. Network information flow[J]. IEEE Trans. Inform. Theory. 2000, 46(4):1204–1216. DOI: 10.1109/18.850663.

[2] Bamberg J. Finite Geometries Fifth Irsee Conference[R], 2017. http://cage.ugent.be/~ml/irsee5/slides/Bamberg.pdf.

[3] Bamberg J, Kelly S, Law M, Penttila T. Tight sets and m-ovoids of finite polar spaces[J]. J. Combin. Theory Ser. A. 2007, 114(7):1293-1314. DOI: 10.1016/j.jcta.2007.01.009.

[4] Bamberg J, Lee M, Melissa K, Xiang Q. A new infinite family of hemisystems of the Hermitian surface[J]. Combinatorica. 2018, 38(1):43-66. DOI: 10.1007/s00493-016-3525-4.

[5] Bamberg J, Law M, Penttila T. Tight sets and m-ovoids of generalised quadranles[J]. Combinatorica. 2009, 29(1):1-17. DOI: 10.1007/s00493-009-2179-x.

[6] Brouwer A E, Haemers W H. Spectra of graphs[M]. [S.l.]: Universitext, Springer, New York, 2012: xiv+250. DOI: 10.1007/978-1-4614-1939-6.

[7] Brouwer A E, Wilson R M, Xiang Q. Cyclotomy and strongly regular graphs[J]. J. Algebraic Combin. 1999, 10(1):25-28. DOI: 10.1023/A:1018620002339.

[8] Bannai E, Ito T. Algebraic combinatorics I: Association schemes[M]. [S.l.]: The Benjamin/Cummings, London, 1984.

[9] Baumert L D, Mills W H, Ward R L. Uniform cyclotomy[J]. J. Number Theory. 1982, 14(1):67–82. DOI: 10.1016/0022-314X(82)90058-0.

[10] Brouwer A E, Cohen A M, Neumaier A. Distance-regular graphs[M]. [S.l.]: Springer-Verlag, Berlin, 1989: xviii+495.

[11] Ben-Sasson E, Etzion T, Gabizon A, Raviv N. Subspace polynomials and cyclic subspace codes[J]. IEEE Trans. Inform. Theory. 2016, 62(3):1157-1165. DOI: 10.1109/TIT.2016.2520479.

[12] Braun M, Etzion T, Östergård P R J, Vardy A, Wassermann A. Existence of q-analogs of Steiner systems[J]. Forum Math. Pi. 2016, 4:e7, 14. DOI: 10.1017/fmp.2016.5.

[13] Bachoc C, Serra O, Zémor G. An analogue of Vosper's theorem for extension fields[J]. Math. Proc. Cambridge Philos. Soc. 2017, 163(3):423–452. DOI: 10.1017/S0305004117000044.

[14] Cossidente A, Culbert C, Ebert G L, Marino G. On m-ovoids of $W_3(q)$[J]. Finite Fields Appl. 2008, 14(1):76-84. DOI: 10.1016/j.ffa.2006.04.001.

[15] Calderbank R, Kantor W M. The geometry of two-weight codes[J]. Bull. London Math. Soc.,1986, 18(2):97-122. DOI: 10.1112/blms/18.2.97.

[16] Cossidente A, Pavese F. Intriguing sets of $W(5,q)$, q even[J]. J. Combin. Theory Ser. A. 2014, 127:303-313. DOI: 10.1016/j.jcta.2014.07.006.

[17] Cossidente A, Pavese F. On intriguing sets of finite symplectic spaces[J]. Des. Codes Cryptogr. 2018, 86(5):1161-1174. DOI: 10.1007/s10623-017-0387-8.

[18] Carlet C, Guilley S. Complementary dual codes for counter-measures to side-channel attacks[J]. Adv. Math. Commun. 2016, 10(1):131–150. DOI: 10.3934/amc.2016.10.131.

[19] Carlet C, Li C J, Mesnager S. Linear codes with small hulls in semi-primitive case[J]. Des. Codes Cryptogr. 2019, 87(12):3063–3075. DOI: 10.1007/s10623-019-00663-4.

[20] Carlet C, Mesnager S, Tang C M, Qi Y F. Euclidean and Hermitian LCD MDS codes[J]. Des. Codes Cryptogr. 2018, 86(11):2605–2618. DOI: 10.1007/s10623-018-0463-8.

[21] Carlet C, Mesnager S, Tang C M, Qi Y F. New characterization and parametrization of LCD codes[J]. IEEE Trans. Inform. Theory. 2019, 65(1):39–49. DOI: 10.1109/TIT.2018.2829873.

[22] Carlet C, Mesnager S, Tang C M, Qi Y F, Pellikaan R. Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$[J]. IEEE Trans. Inform. Theory. 2018, 64(4):3010–3017. DOI: 10.1109/TIT.2018.2789347.

[23] Chen B C, Liu H W. Constructions of cyclic constant dimension codes[J]. Des. Codes Cryptogr. 2018, 86(6):1267–1279. DOI: 10.1007/s10623-017-0394-9.

[24] Drudge K. Extremal sets in projective and polar spaces[D], PhD thesis. The University of Western Onatario, 1998.

[25] Ding C S, Yang J. Hamming weights in irreducible cyclic codes[J]. Discrete Math. 2013, 313(4):434–446. DOI: 10.1016/j.disc.2012.11.009.

[26] Etzion T, Vardy A. Error-correcting codes in projective space[J]. IEEE Trans. Inform. Theory. 2011, 57(2):1165–1173. DOI: 10.1109/TIT.2010.2095232.

[27] Feng T, Momihara K, Xiang Q. Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes[J]. Combinatorica. 2015, 35(4):413-434. DOI: 10.1007/s00493-014-2895-8.

[28] Feng T, Xiang Q. Strongly regular graphs from unions of cyclotomic classes[J]. J. Combin. Theory Ser. B. 2012, 102(4):982-995. DOI: 10.1016/j.jctb.2011.10.006.

[29] Feng K Q, *An introduction to algebraic number theory*, Science Press, Beijing, 2000.

[30] Feng T, Momihara K. Three-class association schemes from cyclotomy[J]. J. Combin. Theory Ser. A. 2013, 120(6):1202–1215. DOI: 10.1016/j.jcta.2013.03.002.

[31] Godsil C, Royle G. Algebraic Graph Theory[M]. [S.l.] Graduate Texts in Mathematics, Springer-Verlag, New York, 2001: xx+439.

[32] Gluesing-Luerssen H, Lehmann H. Distance distributions of cyclic orbit codes[J]. Des. Codes Cryptogr. 2021, 89(3):447–470. DOI: 10.1007/s10623-020-00823-x.

[33] Gluesing-Luerssen H, Morrison K, Troha C. Cyclic orbit codes and stabilizer subfields[J]. Adv. Math. Commun. 2015, 9(2):177–197. DOI: 10.3934/amc.2015.9.177.

[34] Gabidulin E M, Pilipchuk N I, Bossert M. Decoding of random network codes[J]. Probl. Inf. Transm. (Engl. Transl.) 2010, 46(4):22-55. DOI: 10.1134/S0032946010040034.

[35] Hirschfeld J W P, Thas J A. General Galois Geometries[M]. [S.l.]: Springer, London, 2016: xvi+409.

[36] Ireland K, Rosen M. A classical introduction to modern number theory[M]. [S.l.]: 2nd edition, vol. 84 of Graduate Texts in Mathematic, Springer-Verlag, New York, 1990: xiv+389.

[37] Jin L F, Xing C P. Algebraic geometry codes with complementary duals exceed the asymptotic Gilbert-Varshamov bound[J]. IEEE Trans. Inform. Theory. 2018, 64(9):6277–6282. DOI: 10.1109/TIT.2017.2773057.

[38] Kelly S. Constructions of intriguing sets of polar spaces from field reduction and derivation[J]. Des. Codes Cryptogr. 2007, 43(1):1-8. DOI: 10.1007/s10623-007-9046-9.

[39] Kharaghani H, Suda S. Symmetric Bush-type generalized Hadamard matrices and association schemes[J]. Finite Fields Appl. 2016, 37:72–84. DOI: 10.1016/j.ffa.2015.09.003.

[40] Kohnert A, Kurz S. Construction of large constant dimension codes with a prescribed minimum distance[J]. Lecture Notes in Comput. Sci. 2008, 5392:31–42. DOI: 10.1007/978-3-540-89994-5_4.

[41] Köetter R, Kschischang F R, Coding for errors and erasures in random network coding[J]. IEEE Trans. Inform. Theory. 2008, 54(8):3579–3591. DOI: 10.1109/TIT.2008.926449.

[42] Li C J, Ding C S, Li S X. LCD cyclic codes over finite fields[J]. IEEE Trans. Inform. Theory. 2017, 63(7):4344–4356. DOI: 10.1109/TIT.2017.2672961.

[43] Li C J, Zeng P. Constructions of linear codes with one-dimensional hull[J]. IEEE Trans. Inform. Theory. 2019, 65(3):1668–1676. DOI: 10.1109/TIT.2018.2863693.

[44] Li S X, Li C J, Ding C S, Liu H. Two families of LCD BCH codes[J]. IEEE Trans. Inform. Theory. 2017, 63(9):5699–5717.

[45] Liu X S, Liu H L. Matrix-product complementary dual codes. preprint, arXiv:1604.03774.

[46] Lidl R, Niederreiter H. Finite Fields[M]. [S.l.]: Cambridge Univ. Press, Cambridge, 1997: xiv+755.

[47] Ling S, Xing C P. Coding theory: A first course[M]. [S.l.]: Cambridge Univ. Press, Cambridge, 2004: xii+222.

[48] Momihara K. Certain strongly regular Cayley graphs on $\mathbb{F}_{2^{2(2s+1)}}$ from cyclotomy[J]. Finite Fields Appl. 2014, 25:280-292. DOI: 10.1016/j.ffa.2013.10.006.

[49] Momihara K, Xiang Q. Strongly regular Cayley graphs from partitions of subdifference sets of the Singer difference sets[J]. Finite Fields Appl. 2018, 50:222-250. DOI: 10.1016/j.ffa.2017.11.010.

[50] Massey J L. Linear codes with complementary duals[J]. Discret. Math. 1992, 106/107: 337–342. DOI: 10.1016/0012-365X(92)90563-U.

[51] Mesnager S, Tang C M, Qi Y F. Complementary dual algebraic geometry codes[J]. IEEE Trans. Inform. Theory. 2018, 64(4):2390–2397. DOI: 10.1109/TIT.2017.2766075.

[52] Niu Y F, Yue Q, Wu Y S. Several kinds of large cyclic subspace codes via Sidon spaces[J]. Discrete Math. 2020, 343(5):111788, 11. DOI: 10.1016/j.disc.2019.111788.

[53] Otal K, Özbudak F. Cyclic subspace codes via subspace polynomials[J]. Des. Codes Cryptogr. 2017, 85(2):191–204. DOI: 10.1007/s10623-016-0297-1.

[54] Payne S E. Tight pointsets in finite generalized quadrangles[J]. Congr. Numer. 1987, 60:243-260.

[55] Payne S E, Thas J A. Finite Generalized Quadrangles[M]. [S.l.] Research Notes in Mathematics, Pitman (Advanced Publishing Program), Boston, 1984: vi+312.

[56] Pang B B, Zhu S X, Sun Z H. On LCD negacyclic codes over finite fields[J]. J. Syst. Sci. Complex. 2018, 31(4):1065–1077. DOI: 10.1007/s11424-017-6301-7.

[57] Rose J S. A Course on Group Theory[M]. [S.l.] Cambridge University Press, Cambridge-New York-Melbourne, 1978: ix+310.

[58] Roth R M, Raviv N, Tamo I. Construction of Sidon spaces with applications to coding[J]. IEEE Trans. Inform. Theory. 2018, 64(6):4412–4422. DOI: 10.1109/TIT.2017.2766178.

[59] Shult E E, Thas J A. m-systems of polar space[J]. J. Combin. Theory Ser. A. 1994, 68(1):184–204. DOI: 10.1016/0097-3165(94)90097-3.

[60] Sendrier N. Finding the permutation between equivalent linear codes: the support splitting algorithm[J]. IEEE Trans. Inform. Theory. 2000, 46(4):1193–1203. DOI: 10.1109/18.850662.

[61] Sendrier N, Skersys G. On the computation of the automorphism group of a linear code, in:Proceedings of IEEE ISIT2001, Washington, DC, 2001.

[62] Shi X Y, Yue Q, Yang S D. New LCD MDS codes constructed from generalized Reed-Solomon codes[J]. J. Algebra Appl. 2019, 18(8): 1950150, 23. DOI: 10.1142/S0219498819501500.

[63] Thas J A. Ovoids and spreads of finite classical polar spaces[J]. Geom. Dedicata. 1981, 10:135-143. DOI: 10.1007/BF01447417.

[64] Thas J A. Interesting pointsets in generalized quadrangles and partial geometries[J]. Linear Algebra Appl. 1989, 114/115:103–131. DOI: 10.1016/0024-3795(89)90454-0.

[65] Trautmann A -L, Manganiello F, Braun M, Rosenthal J. Cyclic orbit codes[J]. IEEE Trans. Inform. Theory. 2013, 59(11):7386-7404. DOI: 10.1109/TIT.2013.2274266.

[66] Ueberberg J. Foundations of incidence geometry:Projective and polar spaces[M]. [S.l.]:Springer, Heidelberg, 2011: xii+248.

[67] van Dam E R, Muzychuk M. Some implications on amorphic association schemes[J]. J. Combin. Theory Ser. A. 2010, 117(2):111–127. DOI: 10.1016/j.jcta.2009.03.018.

[68] Zhao W, Tang X L. A characterization of cyclic subspace codes via subspace polynomials[J]. Finite Fields Appl. 2019, 57:1–12. DOI: 10.1016/j.ffa.2019.01.002.

作者简历

王野，女，1994 年，汉族，浙江温州人。2012 年考入浙江大学理学院，2016 年本科毕业，获得理学学士学位。2016 年进入浙江大学数学科学学院应用数学专业研究生学习至今。

1. 通讯地址：中国浙江省杭州市浙江大学玉泉校区数学科学学院，310027

2. 联系方式：ye_wang@zju.edu.cn

3. 研究兴趣：编码理论、代数组合学、有限几何

4. 攻读学位期间发表的论文

- Tao Feng, Ye Wang, Qing Xiang. On m-ovoids of symplectic polar spaces, Journal of Combinatorial Theory, A, (175)105279, 14, 2020.
- Ye Wang, Ran Tao. Constructions of linear codes with small dimension hull from association schemes, submitted to Advances in Mathematics of Communications.
- Tao Feng, Ye Wang. New constructions of large cyclic subspace codes and Sidon spaces, Discrete Mathematics, (344)112273, 7, 2021.