分类号：O157.2　　单位代码：10335

学　　号：11335032

浙江大学

# 博士学位论文

中文论文题目：高密度数据存储与光纤通信中相关码类的研究

英文论文题目：**Several codes related to high-density data storage and optical fiber communication**

申请人姓名：丁报昆

指导教师：冯涛　特聘研究员

专业名称：应用数学

研究方向：组合数学与编码理论

所在学院：数学科学学院

**论文提交日期　2018 年 3 月 20 日**

# 高密度数据存储与光纤通信中相关码类的研究

**论文作者签名：** _____

**指导教师签名：** _____

论文评阅人1：_____

评阅人2：_____

评阅人3：_____

评阅人4：_____

评阅人5：_____

答辩委员会主席：曹海涛　教授　南京师范大学

委员1：曹海涛　教授　南京师范大学

委员2：吴佃华　教授　广西师范大学

委员3：吴志祥　教授　浙江大学

委员4：葛根年　教授　浙江大学

委员5：冯 涛　特聘研究员　浙江大学

答辩日期：2018 年 4 月 29 日

**Several codes related to high-density data storage and optical fiber communication**

**Author's signature:** _____

**Supervisor's signature:** _____

External Reviewers: _____

_____

_____

_____

_____

Examining Committee Chairperson:

Prof. Haitao Cao, Nanjing Normal University

Examining Committee Members:

Prof. Haitao Cao, Nanjing Normal University

Prof. Dianhua Wu, Guangxi Normal University

Prof. Zhixiang Wu, Zhejiang University

Prof. Gennian Ge, Zhejiang University

Prof. Tao Feng, Zhejiang University

Date of oral defence: April 29th, 2018

# 浙江大学研究生学位论文独创性声明

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

学位论文作者签名：　　签字日期：　　年　　月　　日

# 学位论文版权使用授权书

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

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：　　导师签名：

签字日期：　　年　　月　　日　　签字日期：　　年　　月　　日

# 致　　谢

匆匆数载，转眼间我的博士生涯即将结束，回顾过去的五年，期间有太多的人和事值得怀念。在这几年的学习生涯中，我感受到了许多良师益友的深切鼓励和关怀，在此我想表达我最诚挚的感谢。

首先我要感谢葛根年教授和冯涛研究员，在五年的博士生涯里，他们两位在学习和生活上给予了我很大的帮助。葛老师严谨踏实的学术作风，渊博的知识以及广阔的视野对我有莫大的帮助。冯涛老师是一位良师益友，他活跃的思维和对待学术的认真态度也对我产生了很大的影响。感谢他们两位一直以来对我的关心和指导，虽然没能达到两位老师的期许，但今后我会继续努力。同时，也要感谢其他指导过我的老师，能够和你们交流讨论是我的荣幸。

感谢和我一起学习的各位同门：魏恒嘉、胡思煌、李抒行、张一炜、汪馨、上官冲、张韬、Jerod Michel、顾玉杰、马景学、钱昺辰、孔祥梁、戚立波、奚元霄、徐子翔、韩雪姣、谢城飞、兰昭君、叶左、余文俊、李伟聪、何智文、陶然等，在这段学习与生活的时光里，我们留下了很多美好的回忆，感谢诸位师兄弟对于我的悉心指导和照顾。

感谢我亲爱的父母、家人和同学，特别感谢父母一直以来对我的关怀，感谢周世超同学对于我的鞭策和鼓励，感谢大家的关心。

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

# 摘　　要

本学位论文主要研究了高密度数据存储和光纤通信中的相关码类，利用有限几何，椭圆曲线，常循环码，有理函数以及 $r$-简单矩阵这些工具构造了最优的字符结对码，$b$-字符码以及渐近最优的光正交签名码。

在第 2 章中，我们研究字符结对码。字符结对码可以抵抗字符结对信道中的结对错误，而字符结对信道每次都输出成对的字符。研究那些有着极大最小结对距离的码是非常重要的，因为这样的码有着最好的纠正结对错误的能力，这样的码被称作为最大距离可分（MDS）字符结对码。本章主要构造有限域 $\mathbb{F}_q$ 上的线性 MDS 字符结对码。首先，我们证明最小结对距离为 5 的 MDS 字符结对码存在当且仅当其长度 $5 \leq n \leq q^2+q+1$。对于最小结对距离为 6 的情形，则可以利用圆角集构造所有长度 $q+2 \leq n \leq q^2$ 的 MDS 字符结对码。最后，利用椭圆曲线我们构造了对于一般结对距离 $d+2$，长度 $7 \leq d+2 \leq n \leq q+\lfloor 2\sqrt{q} \rfloor + \delta(q) - 3$ 的 MDS 字符结对码，其中 $\delta(q)=0$ 或 1。

在第 3 章中，我们考虑 $b$-字符读取信道，这个信道每次读取连续的 $b>2$ 个字符。在本章中，我们建立了对应的 Singleton 界。达到这个界的码我们称作为最大距离可分（MDS）$b$-字符码，它们是最优的因为它们有着极大最小 $b$-距离。通过一个基于有限几何的方法，我们构造了几个 MDS $b$-字符码的无穷类。所得的码有着非常丰富的参数，并且在某些参数下，我们已经完全决定了线性 MDS $b$-字符码的存在性。

在第 4 章中，基于有限域上的有理函数和多项式，我们给出了四类光正交签名码（OOSPC）的直接构造。利用 $r$-简单矩阵，我们则可以递归地构造 OOSPC。这些构造都可以导出渐近最优 OOSPC 的无穷类。

在第 5 章中，我们简要地介绍一下另一个关于几乎设计的工作，以及尚在研究的其它课题。

**关键词：** 字符结对码，$b$-字符码，光正交签名码，有限几何，常循环码，椭圆曲线，有理函数，$r$-简单矩阵

# Abstract

This thesis involves several codes related to high-density data storage and optical fiber communication. We use powerful tools including projective geometry, elliptic curves, constacyclic codes, rational functions and r-simple matrices to construct optimal symbol-pair codes, optimal b-symbol codes and asymptotically optimal OOSPCs.

In Chapter 2, we study symbol-pair codes which can protect against pair-errors in symbol-pair channels, whose outputs are overlapping pairs of symbols. The research of symbol-pair codes with the largest minimum pair-distance is interesting since such codes have the best possible error-correcting capability. A symbol-pair code attaining the maximal minimum pair-distance is called a maximum distance separable (MDS) symbol-pair code. In this chapter, we focus on constructing linear MDS symbol-pair codes over the finite field $\mathbb{F}_q$. We show that a linear MDS symbol-pair code over $\mathbb{F}_q$ with pair-distance $5$ exists if and only if the length $n$ ranges from $5$ to $q^2+q+1$. As for codes with pair-distance $6$, length ranging from $q+2$ to $q^2$, we construct linear MDS symbol-pair codes by using a configuration called ovoid in projective geometry. With the help of elliptic curves, we present a construction of linear MDS symbol-pair codes for any pair-distance $d+2$ with length $n$ satisfying $7 \leq d+2 \leq n \leq q+\lfloor 2\sqrt{q} \rfloor + \delta(q) - 3$, where $\delta(q) = 0$ or $1$.

In Chapter 3, we consider $b$-symbol read channels, where the read operation is performed as a sequence of $b > 2$ consecutive symbols. In this chapter, we establish a Singleton-type bound for $b$-symbol codes. Codes meeting the Singleton-type bound are called maximum distance separable (MDS) codes, and they are optimal in the sense they attain the maximal minimum $b$-distance. We introduce a construction method using projective geometry, and then construct several infinite families of linear MDS $b$-symbol codes over finite fields. The lengths of these codes have a large range. And in some sense, we completely determine the existence of linear MDS $b$-symbol codes over finite fields for certain parameters.

In Chapter 4, we give four direct constructions for OOSPCs based on polynomials and rational functions over finite fields. We also use $r$-simple matrices to present a recursive construction for

OOSPCs. These constructions yield new families of asymptotically optimal OOSPCs.

In Chapter 5, we briefly introduce another work, namely adesign, and some other topics that are still under investigation.

**Keywords:** symbol-pair codes, b-symbol codes, optical orthogonal signature pattern codes, finite geometry, constacyclic codes, elliptic curves, rational functions, r-simple matrices

# 插　　图

# 表　格

# 目　　次

# 1 绪论

## 1.1 字符结对码与 $b$-字符码

现代的社会是一个高速发展的社会，科学技术蓬勃发展，人们之间的交流越来越密切，信息的流通也空前便利，我们正身处在一个“大数据”的时代。在这样一个数字化的时代，信息技术产生的对象的类型和数量日益增多，面对这些海量的、高增长率和多样化的信息，普通的存储手段已经越来越难适应。

在高密度存储的背景下，尽管我们的编码方式没有改变，但是字符的读取操作却已发生变化。对于一个向量 $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$，当我们从字符结对信道中读取时得到的读取向量为

$$\pi(\mathbf{x}) = ((x_0, x_1), (x_1, x_2), \cdots, (x_{n-1}, x_0)).$$

也就是说，我们都是从信道中成对地读取字符，而在这个过程中发生的错误则表现为单个字符或者多个字符的错误读取。Cassuto 和 Blaum [8] 首次研究了抵抗这样的错误的码，我们称作为字符结对码。Chee 等[10] 则建立了字符结对码的 Singleton 界，达到 Singleton 界的码是最优的，因为它可以抵抗最大数目的结对错误，构造这样的码是一个非常重要且有趣的问题。本文第 2 章利用线性代数方法，圆角集以及椭圆曲线码构造了三类最优的字符结对码，这部分的工作发表在《Designs, Codes and Cryptography》。

最近，Yaakobi 等[55] 将字符结对读取信道的框架推广到 $b > 2$ 个字符连续读取的框架中，在这样的信道中，每一步读取操作都读取连续的 $b$ 个字符。也就是说，当我们从信道中读取向量 $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$ 时，我们得到的是

$$\pi_b(\mathbf{x}) = ((x_0, \cdots, x_{b-1}), (x_1, \cdots, x_b), \cdots, (x_{n-1}, x_0, \cdots, x_{b-2})).$$

本文第 3 章研究了这样的信道中的码的性质，同时构造了几类最优的码，这部分的工作发表在《Finite Fields and Their Applications》。

## 1.2 光正交签名码

光码分多址（optical code-division multiple access）是将 CDMA 技术与光纤通信技术相结合的一种新技术，结合两种通信方式的特点，具有很强的技术优势和广阔的应用前景。OCDMA 技术首先会给每个用户分配一个地址码（扩频序列），标志着这个用户的身份，不同的用户有不同的地址码，且它们相互正交或准正交，如此就可以将不同的用户接入到相同的频带和时隙上，进而可以实现多个用户共享同一个光纤信道，有效提高系统总容量，而光正交码（optical orthogonal code）就是这样一个拥有良好相关性质的地址码。如果我们将 OCDMA 扩展到一个二维空间上，那么每个二维位平面都可以用一个二维 $(0,1)$ 矩阵来编码，这样的矩阵我们称作为二维光正交签名（optical orthogonal signature pattern）。OOSP 的构造是空间的 OCDMA 中至关重要的问题，我们希望每个光正交签名在二维平面移动后与自身都是可区分的，同时两个不同的光正交签名在移动后也应该同样是可区分的。满足特定要求的二维光正交签名的集合称作为光正交签名码（OOSPC），对于其码字数目 $\Theta(m,n,w,\lambda)$ 我们有如下 Johnson 界：

$$\begin{aligned}\Theta(m,n,w,\lambda) &\leq J(m,n,w,\lambda)\\ &= \left\lfloor \frac{1}{w} \left\lfloor \frac{mn-1}{w-1} \left\lfloor \frac{mn-2}{w-2} \left\lfloor \cdots \left\lfloor \frac{mn-\lambda}{w-\lambda} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor \right\rfloor .\end{aligned} \tag{1-1}$$

基于有限域上的有理函数，多项式方法以及 $r$-简单矩阵，本文第 4 章给出了渐近最优 OOSPC 的直接构造和递归构造，这部分的内容发表在《IEEE Transactions on Information Theory》。

# 2 字符结对码

## 2.1 介绍

字符结对码的研究源于高密度数据存储技术的高速发展，在这个背景下，尽管编码过程仍然同于往常，但是字符是成对地读取的。如果一个信道的输出模式表现为成对字符的读取，那么我们就称这样的信道为字符结对信道。一个结对错误则是在一次结对读取中，其中一个或多个字符的错误读取。设计相应的码来抵抗一定数量的结对错误是至关重要的。

Cassuto 和 Blaum 在文献[8] 中首次研究了抵抗结对错误的码，包括码的纠错条件，码的构造与解码，以及码的大小的上下界。在那之后，Cassuto 和 Litsyn[9] 给出了字符结对码的代数构造以及码率的渐近界。而 Yaakobi 等[54,55] 则提出了循环字符结对码的有效解码算法。

2013 年，Chee 等[10] 建立了字符结对码的 Singleton 界并构造了达到界的无穷码类，这样的码被称为最大距离可分字符结对码，或简记为 MDS 字符结对码。 MDS 字符结对码的构造是一个非常实用和有趣的问题，因为对于固定的长度和维数，这样的码有着最好的纠正结对错误的能力。文献[10] 中的作者利用交错的技巧，相关的图论工具以及组合结构等构造了 MDS 字符结对码。Kai 等[31] 则利用循环码和常循环码构造了 MDS 字符结对码。

传统意义下的 MDS 码同时也是 MDS 字符结对码[10]，其它已知的码类都列在表 2-1 中。在本章中，我们构造了有限域 $\mathbb{F}_q$ 上的线性 MDS 字符结对码，主要有以下三类：

1. 线性 MDS $(n,5)_q$ 字符结对码存在当且仅当 $5 \le n \le q^2+q+1$；
2. 对任意 $q \ge 3$，$\max\{6, q+2\} \le n \le q^2$，都存在线性 MDS $(n,6)_q$ 字符结对码。
3. 对于一般的 $n, d$ 满足 $7 \le d+2 \le n \le q + \lfloor 2\sqrt{q} \rfloor + \delta(q) - 3$，都存在线性的 MDS $(n, d+2)_q$ 字符结对码，其中

$$\delta(q) = \begin{cases} 0, & \text{如果 } q = p^a, a \ge 3, a \text{ 是奇数且 } p \mid \lfloor 2\sqrt{q} \rfloor; \\ 1, & \text{其它情况.} \end{cases}$$

**表 2-1　已知的 MDS 字符结对码**

| 最小结对距离 | $q$ | $n$ | 参考文献 |
|---|---|---|---|
| $2, 3$ | $q \geq 2$ | $n \geq 2$ | [10] |
| $4$ | $q \geq 2$ | $n \geq 2$ | [10] |
| $5$ | 偶素数幂 | $n \leq q+2$ | [10] |
| | 奇素数 | $5 \leq n \leq 2q+3$ | [10] |
| | 素数幂 | $n \mid q^2-1, n > q+1$ | [31] |
| | 素数幂 | $n = q^2+q+1$ | [31] |
| | 素数幂, $q \equiv 1 \pmod 3$ | $n = \frac{q^2+q+1}{3}$ | [31] |
| $6$ | 素数幂 | $n = q^2+1$ | [31] |
| | 奇素数幂 | $n = \frac{q^2+1}{2}$ | [31] |
| $7$ | 奇素数 | $n = 8$ | [10] |

将我们的结论与已知的结果相比较可以看出，我们构造的无穷类有着更加丰富的参数。我们构造的码类的长度遍历一个大区间中的所有整数，而对应的之前的结果中的长度只是其中一个小区间，或者只是其中的某些点。

## 2.2　准备工作

假设 $\Sigma$ 是含有 $q$ 个元素的字母表，其中每个元素我们称作为一个字符。对于 $\Sigma^n$ 中的一个向量 $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$，我们定义它的字符结对读取向量为

$$\pi(\mathbf{x}) = ((x_0, x_1), (x_1, x_2), \cdots, (x_{n-1}, x_0)).$$

在本章中，我们令 $q$ 为素数幂，$\mathbb{F}_q$ 为包含 $q$ 个元素的有限域。我们主要考虑 $\mathbb{F}_q$ 上的向量，故令 $\Sigma = \mathbb{F}_q$。

显然地，$\mathbb{F}_q^n$ 中的每个向量 $\mathbf{x}$ 都有唯一的字符结对读取向量 $\pi(\mathbf{x}) \in (\mathbb{F}_q \times \mathbb{F}_q)^n$。对 $\mathbb{F}_q^n$ 中的两个向量 $\mathbf{x}, \mathbf{y}$ 而言，我们定义它们之间的结对距离为:

$$D_p(\mathbf{x}, \mathbf{y}) := |\{0 \leq i \leq n-1 : (x_i, x_{i+1}) \neq (y_i, y_{i+1})\}|,$$

其中下标都是在模 $n$ 的意义下取值。对于 $\mathbb{F}_q^n$ 中的任意向量 $\mathbf{x}$，我们定义其结对重量为:

$$wt_p(\mathbf{x}) = |\{0 \leq i \leq n-1 : (x_i, x_{i+1}) \neq (0, 0)\}|,$$

其中下标都是在模 $n$ 的意义下取值。

文献[8] 中建立了结对距离和 Hamming 距离之间的如下联系。

**命题 2.2.1** 取 $\mathbf{x}$ 和 $\mathbf{y}$ 为 $\mathbb{F}_q^n$ 中两个满足 $0 < d_H(\mathbf{x},\mathbf{y}) < n$ 的向量，其中 $d_H$ 表示的是 *Hamming* 距离，那么我们有

$$d_H(\mathbf{x},\mathbf{y}) + 1 \leq D_p(\mathbf{x},\mathbf{y}) \leq 2d_H(\mathbf{x},\mathbf{y}).$$

同时，结对距离和结对重量也有如下关系成立。

**命题 2.2.2** 对所有 $\mathbf{x},\mathbf{y} \in \mathbb{F}_q^n$，我们有 $D_p(\mathbf{x},\mathbf{y}) = wt_p(\mathbf{x}-\mathbf{y})$.

$\mathbb{F}_q$上长度为 $n$ 的码 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 的一个非空子集，$\mathcal{C}$ 的每个元素称作为码字。$\mathcal{C}$ 的最小结对距离定义为:

$$D_p(\mathcal{C}) = \min\{D_p(\mathbf{x},\mathbf{y}) : \mathbf{x},\mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\},$$

同时，$\mathcal{C}$ 的大小定义为其所包含的码字的数目。通常情况下，$\mathbb{F}_q$ 上长度为 $n$，大小为 $M$，最小结对距离为 $d$ 的码记作为 $(n,M,d)_q$ 字符结对码。如果 $\mathcal{C}$ 还是 $\mathbb{F}_q^n$ 的一个子空间，那么我们就说 $\mathcal{C}$ 是一个线性字符结对码。当 $\mathcal{C}$ 是一个线性码时，它的最小结对距离就是 $\mathcal{C}$ 中非零码字的最小结对重量。我们主要考虑的是 $\mathbb{F}_q$ 上的线性字符结对码。

最小结对距离 $d$ 是一个重要的参数，它决定了码的纠错能力。因此，对于固定长度 $n$，构造字符结对码使得其结对距离 $d$ 尽可能大是有着重大意义的。文献[10]证明了如下 Singleton 界。

**定理 2.2.3** （*Singleton* 界）取 $q \geq 2$，$2 \leq d \leq n$，如果 $\mathcal{C}$ 是一个 $(n,M,d)_q$ 字符结对码，那么 $M \leq q^{n-d+2}$。

达到 Singleton 界的字符结对码被称作为最大距离可分 (MDS) 字符结对码。一个 MDS $(n,M,d)_q$ 字符结对码我们简记为 MDS $(n,d)_q$ 字符结对码。文献[31] 的作者们给出了如下定理，对于我们的构造很有帮助。

**定理 2.2.4** 令 $\mathcal{C}$ 为 $\mathbb{F}_q$ 上一个参数为 $[n, n-d_H, d_H]$ 的线性码。如果最小结对距离 $d \geq d_H+2$，那么 $\mathcal{C}$ 是一个 *MDS* $(n, d_H+2)_q$ 字符结对码。

现在我们已经做好了充分的准备，我们可以给出如下关于线性 MDS 字符结对码存在性的充分条件。

**定理 2.2.5** *如果存在一个 $\mathbb{F}_q$ 上 $d_H$ 行，$n \geq d_H + 2 \geq 4$ 列的矩阵 $H = [H_0, H_1, \cdots, H_{n-1}]$，其中 $H_i$ $(0 \leq i \leq n-1)$ 表示的是 $H$ 的第 $i$ 列，满足：*

1. *任意 $d_H - 1$ 列线性无关；*
2. *任意循环连续的 $d_H$ 列线性无关，即对所有 $0 \leq i \leq n-1$，$H_i, H_{i+1}, \cdots, H_{i+d_H-1}$线性无关，其中下标都是在模 $n$ 的意义下取值；*

*那么就存在一个 MDS $(n, d_H + 2)_q$ 字符结对码。*

**证明** 令 $\mathcal{C}$ 是以 $H$ 为校验矩阵的线性码。第一个条件则说明 $\mathcal{C}$ 是一个长度为 $n$，大小为 $q^{n-d_H}$，最小 Hamming 距离大于等于 $d_H$ 的线性码。对于 $\mathcal{C}$ 中 Hamming 重量为 $d_H$ 的码字 $c$（如果存在的话），第二个条件保证了 $d_H$ 个非零元不在循环连续的坐标上。因此，从命题 2.2.1 和 2.2.2 可得 $wt_p(c) \geq d_H + 2$。对于其它 Hamming 重量大于 $d_H + 1$ 的码字 $c'$，显然有 $wt_p(c') \geq d_H + 2$。综上，我们有最小结对距离 $d \geq d_H + 2$，$\mathcal{C}$ 是一个 MDS $(n, d_H + 2)_q$ 字符结对码。 □

## 2.3 最小结对距离为 5 的 MDS 字符结对码

首先我们来看 MDS $(n, 5)_q$ 字符结对码的存在条件。

**引理 2.3.1** *对任意素数幂 $q$，线性 MDS $(n, 5)_q$ 字符结对码只有当长度 $n$ 满足 $5 \leq n \leq q^2 + q + 1$ 时才有可能存在。*

**证明** 一个线性 MDS $(n, 5)_q$ 字符结对码的校验矩阵 $H$ 的行数为 3。从命题 2.2.1 我们知道结对距离为 $d = 5$ 的字符结对码的最小 Hamming 距离 $d_H \geq 3$。因此，$H$的任意两列线性无关，而 $\mathbb{F}_q$ 上长度为 3 且两两线性无关的向量集合的大小最大为 $q^2 + q + 1$。 □

在本节中我们主要说明对所有 $5 \leq n \leq q^2 + q + 1$，MDS $(n, 5)_q$ 字符结对码的存在性。根据定理 2.2.5，我们要做的就是构造一个 $\mathbb{F}_q$ 上 3 行，$n$ 列的矩阵 $H$，使其满足以下条件：

1. 任意两列线性无关；

2. 任意循环连续的三列线性无关。

首先，我们考虑怎么构造一个大小为 $3 \times (q^2+q+1)$ 的矩阵 $H(q)$，然后我们再考虑怎么把矩阵 $H(q)$ 进行适当的调节，从而得到一个合适的大小为 $3 \times n$，$5 \le n \le q^2+q+1$ 的矩阵 $H(q;n)$。我们从集合 $\{(0,0,1)^{\mathrm{T}}, (1,a,b)^{\mathrm{T}}, (0,1,c)^{\mathrm{T}} : a,b,c \in \mathbb{F}_q\}$ 中选择向量作为 $H(q)$ 的列向量，我们所要做的就是将这些向量排序使得任意循环连续的三列线性无关。

首先我们考虑 $q$ 是奇数的情况，记 $\mathbb{F}_q$ 中的元素为 $\{x_0, x_1, \ldots, x_{q-1}\}$。我们首先将 $q^2$ 个形为 $\{(1,a,b)^{\mathrm{T}} : a,b \in \mathbb{F}_q\}$ 的向量划分为 $q$ 个不相交的集合：$B_i = \{(1,a,a^2+x_i)^{\mathrm{T}} : a \in \mathbb{F}_q\}$，$0 \le i < q$。我们将 $B_i$ 中的向量排列如下，其中下标都是在模 $q$ 的意义下取值，

$$B_i = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_i & x_{i+1} & x_{i+2} & \cdots & x_{i+q-1} \\ x_i^2+x_i & x_{i+1}^2+x_i & x_{i+2}^2+x_i & \cdots & x_{i+q-1}^2+x_i \end{bmatrix}.$$

那么现在我们就可以按以下步骤构造矩阵 $H(q)$：将所有的 $B_i$ 排列为 $B_{q-1}, B_{q-2}, \ldots, B_1, B_0$，在两个循环连续的集合之间插入 $(0,1,2x_i)^{\mathrm{T}}$。值得注意的是，$B_0$ 和 $B_{q-1}$ 也是需要考虑的，我们在它们之间插入 $(0,1,2x_{q-1})^{\mathrm{T}}$ 并令这个向量作为 $H(q)$ 的第一列。最后，向量 $(0,0,1)^{\mathrm{T}}$ 可以放在任何地方，这里我们就将它放在最后一列，也就是说，我们构造了如下矩阵，

$$H(q) = \begin{bmatrix} 0 & & 0 & & 0 & & \ldots & & 0 & \cdots & & 0 & & 0 \\ 1 & B_{q-1} & 1 & B_{q-2} & 1 & B_{q-3} & \ldots & B_{i+1} & 1 & B_i & \cdots & B_1 & 1 & B_0 & 0 \\ 2x_{q-1} & & 2x_{q-2} & & 2x_{q-3} & & \ldots & & 2x_i & \cdots & & 2x_0 & & 1 \end{bmatrix}.$$

**命题 2.3.2** *当 $q$ 是奇数时，上述矩阵 $H(q)$ 中任意循环连续的三列线性无关。*

**证明** 通过计算任意循环连续三列的行列式我们可以直接证明这一点。 □

接下来，我们主要考虑 $q$ 是偶数且 $q \neq 2,4$ 的情况。令 $\omega$ 为 $\mathbb{F}_q$ 的本原元，记 $\mathbb{F}_q$ 中的元素为 $\{x_0, x_1, \ldots, x_{q-1}\}$，其中取 $x_0 = 0$，$x_1 = 1$，$x_2 = \omega$，$x_3 = \omega^2$，$x_4 = \omega+1$，$x_5 = \omega^2+\omega$。首先，我们仍然如同之前一样定义 $B_i$ 并将它们排列为 $B_{q-1}, B_{q-2}, \ldots, B_1, B_0$。现在我们要做的就是决定什么样的向量 $(0,1,y)^{\mathrm{T}}$ 可以插入到两个集合 $B_{j+1}$ 和 $B_j$ 之间。我们要求的是 $(0,1,y)^{\mathrm{T}}$，$(1,x_j,x_j^2+x_j)^{\mathrm{T}}$，$(1,x_{j+1},x_{j+1}^2+x_j)^{\mathrm{T}}$ 线性无关且 $(0,1,y)^{\mathrm{T}}$，$(1,x_j,x_j^2+x_{j+1})^{\mathrm{T}}$，$(1,x_{j-1},x_{j-1}^2+x_{j+1})^{\mathrm{T}}$ 线性无关。显然地，$y$ 可以取 $x_j+x_{j-1}$ 和 $x_j+x_{j+1}$ 之外的任何值。

构造一个二部图，左顶点集对应着 $\mathbb{F}_q$，右顶点集中的点为 $\{L_j : 0 \le j < q\}$，其中符号 $L_j$ 表示的是集合 $B_{j+1}$ 和 $B_j$ 之间的位置。$y \in \mathbb{F}_q$ 与 $L_j$ 连边当且仅当向量 $(0,1,y)^{\mathrm{T}}$ 可以被插入到位置 $L_j$，即 $y \neq x_j + x_{j-1}$ 且 $y \neq x_j + x_{j+1}$。这个二部图的一个完美匹配则对应着一个合适的插入方案。

由上述讨论可知，右顶点集的每个点的度为 $q-2$，又因为我们预先设定 $x_0 = 0$，$x_1 = 1$，$x_2 = \omega$，$x_3 = \omega^2$，$x_4 = \omega + 1$，$x_5 = \omega^2 + \omega$，所以我们有：

- $L_1$ 与任意 $y \in \mathbb{F}_q$ 连边，除了 1 和 $\omega + 1$；
- $L_2$ 与任意 $y \in \mathbb{F}_q$ 连边，除了 $\omega + 1$ 和 $\omega^2 + \omega$；
- $L_3$ 与任意 $y \in \mathbb{F}_q$ 连边，除了 $\omega^2 + \omega$ 和 $\omega^2 + \omega + 1$；
- $L_4$ 与任意 $y \in \mathbb{F}_q$ 连边，除了 $\omega^2 + \omega + 1$ 和 $\omega^2 + 1$。

即使只是在这个四个顶点中，我们有任意 $y \in \mathbb{F}_q$ 至少与它们中的两个连边，故而我们可以得出：

- 因为右顶点集的每个顶点度为 $q-2$，所以右顶点集中任意 $\Delta \le q-2$ 个顶点的邻居数目至少为 $q - 2 \ge \Delta$；
- 右顶点集中任意 $q-1$ 或 $q$ 个顶点的邻居数目为 $q$。

综上，著名的 Hall 定理[27] 保证了上述二部图完美匹配的存在性，这也就对应着一个合适的插入方案。

然而，在 $q = 4$ 时我们无法利用上述框架，所以这个情况被单独列出。但是，在经过相似的过程和适当的调整后我们依然可以得到一个合适的方案。因为解释过程过于繁琐，我们直接给出 $H(4)$ 而不详加解释。

$$H(4) = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & \omega & \omega+1 & 1 & \omega+1 & \omega & 1 & 0 & 1 & 0 & \omega+1 & \omega & 1 & 1 & 1 & \omega & \omega+1 & 0 & 0 \\ 0 & 0 & 1 & \omega+1 & \omega & \omega+1 & \omega+1 & \omega & 0 & 1 & \omega & \omega & 0 & 1 & \omega+1 & 1 & \omega & 0 & 1 & \omega+1 & 1 \end{bmatrix}.$$

目前为止，对所有的素数幂 $q \ge 3$，我们构造了相应的矩阵 $H(q)$。接下来，我们讨论如何通过适当的调整，从 $H(q)$ 得到一个大小为 $3 \times n$ 的矩阵 $H(q;n)$，$5 \le n \le q^2 + q + 1$。记 $n = \alpha(q+1) + \beta$，其中 $0 \le \beta \le q$。大家肯定有很多方法达到同样的目的，我们给出其中一个策略如下。

- 如果 $\beta \neq 2$，选择 $H(q)$ 的前 $n-1$ 列，然后再插入向量 $(0,0,1)^{\mathrm{T}}$。
- 如果 $\beta = 2$，选择 $H(q)$ 的前 $n-1$ 列，然后再插入向量 $(0,0,1)^{\mathrm{T}}$ 作为新的第三列。

$\beta = 2$ 的情况被单独列出是因为我们仍然要遵守第一个条件，而 $\{(0,1,x)^{\mathrm{T}}$，$(0,0,1)^{\mathrm{T}}$，$(0,1,y)^{\mathrm{T}}\}$ 显然不是线性无关的。

上述构造的正确性，可以由命题 2.3.2 和对一些包含 $(0,0,1)^{\mathrm{T}}$ 的三元组，以及三元组 $\{(0,1,a)^{\mathrm{T}}, (0,1,b)^{\mathrm{T}}, (1,c,d)^{\mathrm{T}}\}$（$\beta=2$ 时）的检查来确定。

我们列举 $q=5$ 作为一个例子，主要列举了矩阵 $H(5)$，调节后的矩阵 $H(5;13)$（对应着 $\beta\neq 2$）和 $H(5;14)$（对应着 $\beta=2$）。

$$H(5)=\begin{bmatrix} 0&1&1&1&1&1&0&1&1&1&1&1&0&1&1&1&1&1&0&1&1&1&1&1&0&1&1&1&1&1&0\\ 1&4&0&1&2&3&1&3&4&0&1&2&1&2&3&4&0&1&1&1&2&3&4&0&1&0&1&2&3&4&0\\ 3&0&4&0&3&3&1&2&4&3&4&2&4&1&1&3&2&3&2&2&0&0&2&1&0&0&1&4&4&1&1 \end{bmatrix},$$

$$H(5;13)=\begin{bmatrix} 0&1&1&1&1&1&0&1&1&1&1&1&0\\ 1&4&0&1&2&3&1&3&4&0&1&2&0\\ 3&0&4&0&3&3&1&2&4&3&4&2&1 \end{bmatrix},$$

$$H(5;14)=\begin{bmatrix} 0&1&0&1&1&1&1&0&1&1&1&1&1&0\\ 1&4&0&0&1&2&3&1&3&4&0&1&2&1\\ 3&0&1&4&0&3&3&1&2&4&3&4&2&4 \end{bmatrix}.$$

最后，对于 $q=2$ 的情况，我们列出矩阵 $H(2)$，$H(2;5)$ 和 $H(2;6)$。

$$H(2)=\begin{bmatrix} 1&0&0&1&0&1&1\\ 0&1&0&1&1&1&0\\ 0&0&1&0&1&1&1 \end{bmatrix}, H(2;5)=\begin{bmatrix} 1&0&0&1&1\\ 0&1&0&1&0\\ 0&0&1&1&1 \end{bmatrix}, H(2;6)=\begin{bmatrix} 1&0&0&1&0&1\\ 0&1&0&1&1&0\\ 0&0&1&1&1&1 \end{bmatrix}.$$

我们已经完成了 MDS $(n,5)_q$ 字符结对码的构造，其中 $q\geq 2$ 为任意素数幂，$5\leq n\leq q^2+q+1$。结合引理 2.3.1 和上述构造我们可以得出如下定理。

**定理 2.3.3** *对任意素数幂 $q$，线性 MDS $(n,5)_q$ 字符结对码存在当且仅当 $5\leq n\leq q^2+q+1$。*

## 2.4　利用有限几何构造 MDS 字符结对码

记 $V(r+1,q)$ 是有限域 $\mathbb{F}_q$ 上 $r+1$ 维的向量空间。$\mathbb{F}_q$ 上 $r$ 维射影空间，我们记作为 $PG(r,q)$，是一类几何对象，它的点，线，面，……，超平面分别是 $V(r+1,q)$ 中的 1，2，3，……，$r$ 维子空间，射影空间的维数总是比向量空间的维数少一。更多关于有限几何的知识请参考文献[43]。

射影空间 $PG(r,q)$ 中的点我们记作为 $\langle(a_0,a_1,\cdots,a_r)\rangle$，表示的是由非零向量 $(a_0,a_1,\cdots,a_r)$ 张成的子空间，其中 $a_i\in\mathbb{F}_q$，$0\leq i\leq r$。我们把 $a_0,a_1,\cdots,a_r$ 称作为齐次坐标，

因为这些坐标在乘以一个张量 $\lambda \in \mathbb{F}_q$ 的意义下是等价的，也就是说 $\langle(\lambda a_0, \lambda a_1, \cdots, \lambda a_r)\rangle = \langle(a_0, a_1, \cdots, a_r)\rangle$。显然地，我们可以得到，射影空间 $PG(r,q)$ 中点的数目为 $\frac{q^{r+1}-1}{q-1}$。

对一个整数 $r \geq 2$，如果我们选择 $PG(r,q)$ 中的 $n \geq r+3$ 个点，并且把它们当作矩阵 $H$ 的列向量，那么由定理 2.2.5 我们可以自然地得出下述定理。

**定理 2.4.1** 如果存在 $PG(r,q)$ 中 $n \geq r+3 \geq 5$ 个点的集合，满足：

1. 任意 $r$ 个点张成一个超平面；
2. 存在一个合适的排序 $\mathcal{P}_0, \mathcal{P}_1, \cdots, \mathcal{P}_{n-1}$，使得任意循环连续的 $r+1$ 个点不落在一个超平面上，即 $\mathcal{P}_i, \mathcal{P}_{i+1}, \cdots, \mathcal{P}_{i+r}$ 不落在一个超平面上，$0 \leq i \leq n-1$，其中下标都是在模 $n$ 的意义下取值；

那么就存在一个线性 *MDS* $(n, r+3)_q$ 字符结对码。

我们考虑 $r = 3$ 的情形，这样我们就可以利用 $PG(3,q)$ 中的一个结构，叫做圆角集（ovoid）。首先我们给出它的定义。

**定义 2.4.2** [43] $PG(3,q)$ 中的一个点集 $\mathcal{O}$ 被称作为一个圆角集，如果满足：

1. 每条线与 $\mathcal{O}$ 中的至多两个点相交；
2. $\mathcal{O}$ 中的每个点恰巧落在 $q+1$ 条切线上（与 $\mathcal{O}$ 恰巧交于一点的线），且这 $q+1$ 条切线共面。

圆角集已经被广泛研究，关于它的性质我们引用下述的两个引理[43]。

**引理 2.4.3** 每个圆角集包含 $q^2+1$ 个点。

**引理 2.4.4** 每个面交圆角集 $\mathcal{O}$ 于一个或 $q+1$ 个点。

显然地，我们可以导出如下引理。

**引理 2.4.5** 对 $PG(3,q)$ 中的一个圆角集 $\mathcal{O}$，存在 $q+1$ 个面，每个面包含 $q+1$ 个 $\mathcal{O}$ 中的点，并且这些面相交于 $\mathcal{O}$ 中的一条线，同时这些面覆盖了 $\mathcal{O}$ 中的所有点。

**证明** 固定任意两个点 $A, B \in \mathcal{O}$，从 $\mathcal{O} \setminus \{A, B\}$ 中选择一个点 $P$。由引理 2.4.4 可知，面 $ABP$ 交 $\mathcal{O}$ 于 $q+1$ 个点。接着，我们选择一个不落在面 $ABP$ 上的点 $Q \in \mathcal{O}$。那么，同样地，我们又得到了一个面 $ABQ$ 交 $\mathcal{O}$ 于 $q+1$ 个点。如果我们一直这样做，就可以得到 $q+1$ 个面，每个包含 $q+1$ 个 $\mathcal{O}$ 中的点。这些面交于同一条线，而这条线交 $\mathcal{O}$ 于 $A, B$两点。 □

取 $q \geq 5$ 为一个素数幂。假设 $A$ 和 $B$ 为圆角集 $\mathcal{O}$ 中的两个点，面 $\pi_0, \pi_1, \cdots, \pi_q$ 交于线 $AB$ 且覆盖了 $\mathcal{O}$ 中的所有点。记点集 $\pi_i \setminus \{A, B\}$ 为 $\alpha_i$，$0 \leq i \leq q$。显然，每个集合有 $q-1$ 个点。圆角集的结构如图 2-1 所示。

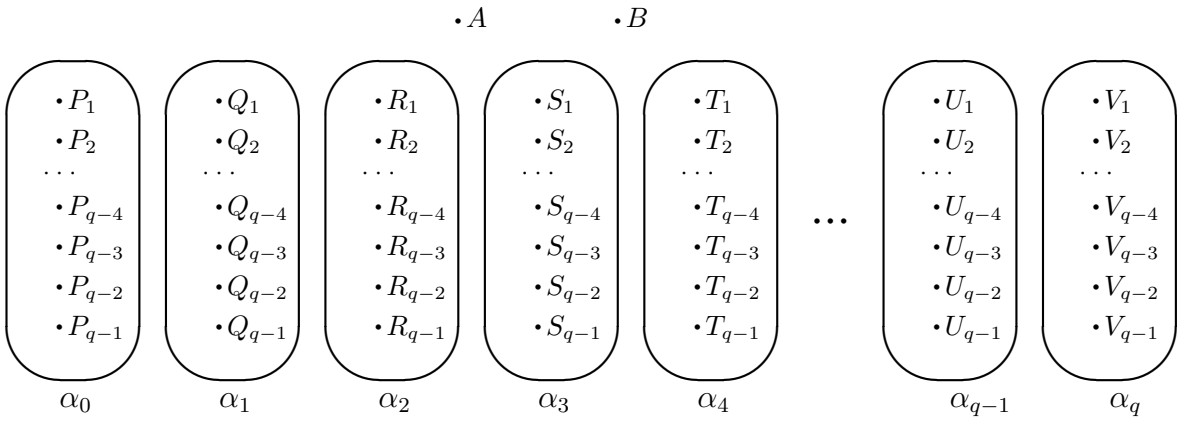


**图 2-1　射影空间 $PG(3, q)$ 中的圆角集.**

注意到 $PG(3, q)$ 中的面和超平面是同一个几何对象，圆角集 $\mathcal{O}$ 中的点自然地满足定理 2.4.1 中的第一个条件。因此，想要构造 MDS 字符结对码，我们只要将 $\mathcal{O}$ 中的点排序并使得任意循环连续的四个点不共面。在本节剩下的部分，我们主要讨论 $\mathcal{O}$ 中点的排序问题。大家肯定有很多种方法可以达到这个目的，我们展示其中一个策略如下。

我们始终选择点 $A, B$ 以及任意的 $P_1 \in \alpha_0, Q_1 \in \alpha_1$ 作为前四个点。显然，这四个点不共面。此外，我们标记最后三个点为 $X, Y, Z$。对于四个有序点 $P, Q, R, S$，我们说 $S$ 是一个合适的点，如果 $S$ 不落在面 $PQR$ 上。换言之，如果 $S$ 与排序恰好在它之前的三个点不共面，那么它就是一个合适的的点。我们给 $\mathcal{O}$ 中的点排序，首先保证任意连续四个点不共面，然后我们再确保 $X, Y, Z, A$ 不共面，$Y, Z, A, B$ 不共面以及 $Z, A, B, P_1$ 不共面。

下面的几个小结论会在我们的证明中反复使用。

1. 两个面交于一线，一条线交 $\mathcal{O}$ 于至多两个点，所以两个面至多共同包含 $\mathcal{O}$ 中的两个点。

2. 假设我们有三个有序点 $P, Q, R$，其中 $P \in \alpha_i, Q \in \alpha_j, R \in \alpha_k$，$i, j, k$ 中至多两个相

等，那么 $PQR$ 交 $\alpha_i$ 于至多两个点（其中一个是 $P$）。如果此时 $\alpha_i$ 中仍然还剩至少两个点未排序，那么我们始终可以选择一个合适的点 $P' \in \alpha_i$。同样的结论对 $\alpha_j$ 和 $\alpha_k$ 也成立。

3. 我们始终可以从两个集合 $\alpha_i$ 和 $\alpha_j$，或者从三个集合 $\alpha_i, \alpha_j$ 和 $\alpha_k$ 中轮流地选择合适的点直到每个集合中只剩下一个点。

4. 如果三个点 $X, Y, Z$ 中恰巧有两个点属于同一个集合 $\alpha_i$，那么这两个点和 $A$ 张成了面 $\pi_i$，且不包含剩下的那个点，故 $X, Y, Z, A$ 不共面。

5. 如果 $Y \in \alpha_i, Z \in \alpha_j, i \neq j$，那么 $Y, A, B$ 张成面 $\pi_i$，$Z, A, B$ 张成面 $\pi_j$，故 $Y, Z, A, B$ 不共面。

6. 如果 $Z$ 不在集合 $\alpha_0$ 中，那么 $A, B, P_1$ 张成一个面，$A, B, Z$ 张成另一个面，即 $Z, A, B, P_1$ 不共面。

现在我们已经做好了充分的准备来给 $\mathcal{O}$ 中的 $n$ 个点排序使得任意循环连续的四个点不共面，进而得到 MDS $(n, 6)_q$ 字符结对码。因为 MDS $(n, 6)_q$ 字符结对码在 $n \leq q + 1$[10] 和 $n = q^2 + 1$[31] 时已经被构造，所以我们限制 $q + 2 \leq n \leq q^2$。我们分下述两种情形讨论。

### 2.4.1 $q$ 是奇数

对于 $q + 2 \leq n \leq 2q$，$2q < n \leq q^2 - q$ 和 $q^2 - q < n \leq q^2$ 这三种情形我们分别给出三种不同的策略。

**引理 2.4.6** *对奇素数幂 $q \geq 5$，我们可以给 $n$ 个点排序使得任意循环连续的四个点不共面，$q + 2 \leq n \leq 2q$。*

**证明** 在选取 $A, B, P_1, Q_1$ 这四个点后，我们选取一个合适的 $R_1 \in \alpha_2$ 作为第五个点，然后选择一个合适的点 $S_1 \in \alpha_3$ 作为第六个。从 $\alpha_2$ 和 $\alpha_3$ 中轮流地选择合适的点直到我们已经排列了 $n$ 个点，$q + 2 \leq n \leq 2q$。

目前为止，我们已经排列了 $n$ 个点使得任意连续四个点不共面。对于最后三个点 $X, Y, Z$，我们有 $X, Z$ 在同一个集合 $\alpha_i$ 中，$Y, Z$ 在不同的集合中，$Z$ 不在 $\alpha_0$ 中。综上可得，任意循环连续的四个点不共面。 □

**引理 2.4.7** 对奇素数幂 $q \geq 5$，我们可以给 $n$ 个点排序使得任意循环连续的四个点不共面，$2q < n \leq q^2 - q$。

**证明** 在选取 $A, B, P_1, Q_1$ 这四个点后我们轮流地从 $\alpha_0$ 和 $\alpha_1$ 中选择合适的点直到每个集合只剩下一个点。假设我们已经将点排列为 $A, B, P_1, Q_1, P_2, Q_2, \cdots, P_{q-2}, Q_{q-2}$。对集合 $\alpha_2$ 和 $\alpha_3$，$\alpha_4$ 和 $\alpha_5$ 等重复上述步骤。这样的集合的数目为 $q+1$，是个偶数。所以，我们可以一直这么做直到我们已经排列了 $n$ 个点，$2q < n \leq q^2 - q$。

目前为止，我们已经排列了 $n$ 个点使得任意连续四个点不共面。对于最后三个点 $X, Y, Z$，我们有 $Y, Z$ 不在同一个集合 $\alpha_i$ 中，$Z$ 不在 $\alpha_0$ 中。所以，我们只需要确认 $X, Y, Z, A$ 不共面。唯一需要考虑的特殊情况是这三个点落在不同的集合 $\alpha_i, \alpha_{i+1}, \alpha_{i+2}$ 中。例如，我们已经把点排列为 $A, B, P_1, \cdots, S_{q-3}, R_{q-2}, S_{q-2}, T_1$，$R_{q-2}, S_{q-2}, T_1$ 是最后三个点。在这种情况下，如果 $R_{q-2}, S_{q-2}, T_1, A$ 共面，那么我们在 $\alpha_4$ 中找一个不落在面 $R_{q-2}S_{q-3}S_{q-2}$ 和 $R_{q-2}S_{q-2}A$ 上的点作为新的最后的点。因为 $R_{q-2}S_{q-3}S_{q-2}$ 交 $\alpha_4$ 于至多两个点，$R_{q-2}S_{q-2}A$ 交 $\alpha_4$ 于 $T_1$，$\alpha_4$ 中总共有 $q-1 \geq 4$ 个点，所以我们这样做总是能成功的。综上可得，任意循环连续的四个点不共面。 □

当 $q^2 - q < n \leq q^2$ 时，我们需要排列更多的点。对一对集合 $\alpha_i, \alpha_{i+1}$，$i = 0, 2, 4, \cdots, q-3$，我们首先轮流地选取合适的点直到每个集合中剩下三个点。然后我们给定相应的策略来排列剩下来的这些点，我们重复这个过程直到我们将 $\alpha_0, \alpha_1, \cdots, \alpha_{q-2}$ 中的所有点排序完成。在那之后，我们从 $\alpha_{q-1}$ 和 $\alpha_q$ 中轮流地取点直到我们已经排列了足够的点。在下面的引理中，我们首先限制 $q^2 - q < n < q^2$ 然后我们再单独讨论 $n = q^2$ 的情形。

**引理 2.4.8** 对奇素数幂 $q \geq 5$，我们可以给 $n$ 个点排序使得任意循环连续的四个点不共面，$q^2 - q < n \leq q^2$。

**证明** 在选取 $A, B, P_1, Q_1$ 这四个点后我们轮流地从 $\alpha_0$ 和 $\alpha_1$ 中选择合适的点直到每个集合只剩下三个点。假设我们已经将点排列为 $A, B, P_1, Q_1, P_2, Q_2, \cdots, P_{q-5}, Q_{q-5}, P_{q-4}, Q_{q-4}$。然后我们选取合适的 $P_{q-3} \in \alpha_0$ 作为下一个点，接着选择 $\alpha_0$ 中剩下来的两个点 $P_{q-2}, P_{q-1}$ 和任意的 $Q_{q-3} \in \alpha_1$。再选择合适的 $Q_{q-2} \in \alpha_1$，然后是最后剩下来的点 $Q_{q-1} \in \alpha_1$。也就是说我们的排序是 $A, B, \cdots, P_{q-4}, Q_{q-4}, P_{q-3}, P_{q-2}, P_{q-1}, Q_{q-3}$,$Q_{q-2}, Q_{q-1}$。因为 $P_{q-4}, P_{q-3}, P_{q-2}$ 张成面 $\pi_0$ 而 $Q_{q-4}$ 在 $\pi_1$ 上，故 $P_{q-4}, Q_{q-4}, P_{q-3}, P_{q-2}$ 不共面。同样地，$Q_{q-4}, P_{q-3}, P_{q-2}, P_{q-1}$ 不共面，$P_{q-3}, P_{q-2}, P_{q-1}, Q_{q-3}$ 不共面，$P_{q-1}, Q_{q-3}, Q_{q-2}, Q_{q-1}$ 也不共面。我们已经排列了 $\alpha_0$ 和 $\alpha_1$ 中所有的点使得任意连续四个点不共面。下一步我们轮

流地从 $\alpha_2$ 和 $\alpha_3$ 中选取合适的点，然后重复同样的步骤。我们可以一直重复这整个过程直到我们将 $\alpha_0, \alpha_1, \cdots, \alpha_{q-2}$ 中的所有点排序完成。最后，我们轮流地从 $\alpha_{q-1}$ 和 $\alpha_q$ 中选取合适的点，直到我们已经排列了 $n$ 个点，$q^2-q<n\leq q^2-1$。

目前为止，我们已经排列了 $n$ 个点使得任意连续四个不共面。$\alpha_0, \alpha_1, \cdots, \alpha_{q-2}$ 中总共有 $q^2-2q+1$ 个点，$n>q^2-q$，$q\geq 5$。因此对于最后三个点 $X, Y, Z$，我们有 $X, Z$ 在相同的集合 $\alpha_i$ 中，$i=q-1$ 或者 $q$， $Y, Z$ 在不同的集合中，以及 $Z$ 不在 $\alpha_0$ 中。所以，任意循环连续四个点不共面。

当 $n=q^2-1$ 时，假设我们已经将点排列为 $A, B, P_1, Q_1, \cdots, U_{q-4}, V_{q-4}, U_{q-3}, V_{q-3}, U_{q-2}, V_{q-2}$。这说明 $U_{q-4}, V_{q-4}, U_{q-3}, V_{q-3}$不共面，$U_{q-3}, V_{q-3}, U_{q-2}, V_{q-2}$ 也不共面。当 $n=q^2$ 时，我们新增一个点 $V_{q-1}$ 并令顺序为 $U_{q-4}, V_{q-4}, U_{q-3}, V_{q-3}, V_{q-2}, U_{q-2}, V_{q-1}$。显然，$V_{q-4}, U_{q-3}$，$V_{q-3}, V_{q-2}$ 不共面，$V_{q-3}, V_{q-2}, U_{q-2}, V_{q-1}$ 也不共面。通过相似的讨论，我们可以知道任意循环连续的四个点不共面。 □

我们已经排列了 $\mathcal{O}$ 中的 $n$ 个点使得任意循环连续四个点不共面，$q\geq 5$，$q+2\leq n\leq q^2$。因此我们得到了 MDS $(n,6)_q$ 字符结对码，$q+2\leq n\leq q^2$。我们排除了 $q=3$ 的情形因为每个面 $\pi_i$ 上的点过少，在下个例子中我们直接给出 $q=3$ 时的 MDS 字符结对码。

例 2.4.9 对 $n\in\{6,7,8,9,10\}$ 都存在线性 *MDS* $(n,6)_3$ 字符结对码，其所对应的校验矩阵由下述矩阵的前 $n$ 列组成

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 1 & 2 & 2 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 & 2 & 0 & 2 & 2 & 1 & 1 \\ 0 & 0 & 1 & 1 & 2 & 2 & 1 & 0 & 2 & 0 \end{bmatrix}.$$

### 2.4.2 $q$ 是偶数

$q$ 是偶数与 $q$ 是奇数的不同之处在于面 $\pi_0, \pi_1, \cdots, \pi_q$ 的数目是个奇数。当 $q+2\leq n<q^2-q+2$ 时，我们可以像 $q$ 是奇数的情形一样，排列 $q$ 个面 $\pi_0, \pi_1, \cdots, \pi_{q-1}$ 上的 $n$ 个点。当 $q^2-q+2\leq n\leq q^2$ 时，我们首先排列前三个集合 $\alpha_0, \alpha_1, \alpha_2$ 上的点，然后我们可以像 $q$ 是奇数时一样操作，因为此时剩下的集合的数目是偶数。

**引理 2.4.10** 对偶数幂 $q\geq 8$，我们可以给 $n$ 个点排序使得任意循环连续的四个点不共面，$q+2\leq n\leq q^2$。

**证明** 当 $q+2 \leq n < q^2-q+2$ 时，我们排列 $q$ 个面 $\pi_0, \pi_1, \cdots, \pi_{q-1}$ 上的 $n$ 个点，就如同 $q$ 是奇数时那样。当 $q^2-q+2 \leq n \leq q^2$ 时，关键步骤就是给集合 $\alpha_0, \alpha_1, \alpha_2$ 中的点排序。

取合适的 $R_1 \in \alpha_2$ 作为第五个点，然后从集合 $\alpha_0, \alpha_1, \alpha_2$ 中轮流地选择合适的点直到每个集合还剩三个点。假设我们已经将点排列为 $A, B, P_1, Q_1, R_1, \cdots, P_{q-4}, Q_{q-4}, R_{q-4}$。接着，选择合适的点 $P_{q-3} \in \alpha_0$，$P_{q-2} \in \alpha_0$。在那之后选取 $\alpha_0$ 中的最后一个点 $P_{q-1}$，任意的 $Q_{q-3} \in \alpha_1$，合适的 $Q_{q-2} \in \alpha_1$，以及 $\alpha_1$ 中最后一个点 $Q_{q-1}$。最后选取任意的 $R_{q-3} \in \alpha_2$，合适的 $R_{q-2} \in \alpha_2$，以及 $\alpha_2$ 中的最后一个点 $R_{q-1}$。目前为止我们已经将点排列为 $P_{q-4}, Q_{q-4}, R_{q-4}, P_{q-3}, P_{q-2}, P_{q-1}, Q_{q-3}, Q_{q-2}, Q_{q-1}, R_{q-3}, R_{q-2}, R_{q-1}$。显然，我们有 $R_{q-4}, P_{q-3}, P_{q-2}, P_{q-1}$；$P_{q-3}, P_{q-2}, P_{q-1}, Q_{q-3}$；$P_{q-1}, Q_{q-3}, Q_{q-2}, Q_{q-1}$；$Q_{q-3}, Q_{q-2}, Q_{q-1}, R_{q-3}$ 以及 $Q_{q-1}, R_{q-3}, R_{q-2}, R_{q-1}$ 都不共面。

我们已经将 $\alpha_0, \alpha_1$ 和 $\alpha_2$ 中的所有点排序完成，使得任意连续四个点不共面，剩下来的面的数目是偶数。我们先从 $\alpha_3$ 和 $\alpha_4$ 中轮流地选取合适的点，然后像引理 2.4.8 一样排序。 □

下面的例子中我们给出 $q=4$ 时的 MDS 字符结对码。

例 2.4.11 记 $\mathbb{F}_4$ 的本原元为 $w$，对 $n \in \{6,8,9,10,11,12,13,14,15,16,17\}$ 都存在线性 *MDS* $(n,6)_4$ 字符结对码，其所对应的校验矩阵由下述矩阵的前 $n$ 列组成

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & w & 1+w & 1 & w & 1+w & w & w & 1+w & 1 & w & 1 & 1+w & 1+w & 1 \\ 0 & 0 & 1 & 0 & w & 0 & 1+w & 0 & 1 & 1 & w & w & w+1 & w & 1+w & 1+w & 1 \\ 0 & 0 & 0 & 1 & 0 & w & 0 & 1+w & 1 & w & 1 & w & w & 1+w & 1+w & 1 & 1+w \end{bmatrix}.$$

线性 *MDS* $(7,6)_4$ 字符结对码的校验矩阵为：

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & w & 1+w & 1 & w \\ 0 & 0 & 1 & 0 & w & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & w & w \end{bmatrix}.$$

综上所述，我们可以总结得出如下定理。

**定理 2.4.12** 对任意素数幂 $q$，$q \geq 3$，$\max\{6, q+2\} \leq n \leq q^2$，都存在线性 *MDS* $(n,6)_q$ 字符结对码。

## 2.5 利用椭圆曲线构造 MDS 字符结对码

前两节构造了结对距离为 5 和 6 的 MDS 字符结对码。在本节中，我们利用椭圆曲线码构造结对距离 ($\geq 7$) 的 MDS 字符结对码。首先我们简要叙述一些关于椭圆曲线码的基本事实。

令 $E/\mathbb{F}_q$ 是 $\mathbb{F}_q$ 上对应函数域为 $\mathbb{F}_q(E)$ 的椭圆曲线。令 $E(\mathbb{F}_q)$ 是 $E$ 上所有 $\mathbb{F}_q$-有理点的集合。假设 $D = \{P_1, P_2, \cdots, P_n\}$ 是 $E(\mathbb{F}_q)$ 的真子集，$G$ 是度为 $k$ 的除子$(0 < k < n)$，$\mathrm{Supp}(G) \cap D = \emptyset$，在不会造成误解的情况下，我们也写作 $D = P_1 + P_2 + \cdots + P_n$。主除子 $\mathrm{div}(f) \geqslant -G$ 的所有有理函数 $f \in \mathbb{F}_q(E)$ 以及零函数构成的 $\mathbb{F}_q$-向量空间我们记作为 $\mathscr{L}(G)$（参见[50]）。

代数几何码 $C_{\mathscr{L}}(D, G)$ 定义为下述赋值映射的像：

$$ev : \mathscr{L}(G) \to \mathbb{F}_q^n;\ f \mapsto (f(P_1), f(P_2), \cdots, f(P_n)).$$

我们知道 $C_{\mathscr{L}}(D, G)$ 是一个参数为 $[n, k, d_H]$ 的线性码，最小 Hamming 距离 $d_H$ 有如下两个选择:

$$d_H = n - k, \text{ 或者 } d_H = n - k + 1.$$

一个 $[n, k, d_H]$ 线性码被称作为 MDS 码，如果 $d_H = n - k + 1$；被称作为几乎 MDS 码，如果 $d_H = n - k$。

假设 $O$ 是 $E$ 上的一个 $\mathbb{F}_q$-有理点。有理点的集合 $E(\mathbb{F}_q)$ 形成了一个交换群，零元素为 $O$ （元素之间的加法我们参考[49]），且同构于 Picard 群 $\mathrm{div}^o(E)/\mathrm{Prin}(\mathbb{F}_q(E))$，其中 $\mathrm{Prin}(\mathbb{F}_q(E))$ 是包含所有主除子的子群，分别记 $\oplus$ 和 $\ominus$ 为 $E(\mathbb{F}_q)$ 中的加法和减法。

对不熟悉上述抽象语言的读者而言， $\mathbb{F}_q$ 上的椭圆曲线 $E$ 其实就是通过一个非奇异 Weierstrass 方程

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q,$$

和无穷远处的一个点 $O$ 来定义的。$E$ 上 $\mathbb{F}_q$-有理点的集合 $E(\mathbb{F}_q)$ 是无穷远点 $O$ 和 Weierstrass 方程在 $\mathbb{F}_q$ 上的解（有限点）的集合，即

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}.$$

显然，面 $\mathbb{F}_q^2$ 上的线和 $\mathbb{F}_q$ 上的三次曲线 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ 至多交于三点。那么，$E(\mathbb{F}_q)$ 上的群结构就可以被如下定义。

- 无穷远点 $O$ 是零元素。也就是说，对所有 $P \in E(\mathbb{F}_q)$，令 $P \oplus O = P$。
- 任意有限点 $P \in E(\mathbb{F}_q)$ 的相反点 $\ominus P$ 定义为有限点 $Q$，使得线 $PQ$ 只交椭圆曲线 $E$ 于 $P$ 和 $Q$ 两点。如果 $P, Q$ 两点重合，那么 $PQ$ 就被看作为 $P$ 点处的切线。此外，$O$ 的相反点是它本身。
- 对任意有限点 $P, Q \in E(\mathbb{F}_q)$，它们的和 $P \oplus Q$ 定义为点 $\ominus R \in E(\mathbb{F}_q)$，其中 $R$ 是 $PQ$ 与 $E$ 的第三个交点。

为了简便起见，我们取除子 $G = mO$，这里 $mO$ 只是 $m$ 个 $O$ 的形式和，不是我们定义的加法 $\oplus$。

**命题 2.5.1** [13,59] 令 $E$ 是 $\mathbb{F}_q$ 上包含 $\mathbb{F}_q$-有理点 $O$ 的椭圆曲线，$D = \{P_1, P_2, \cdots, P_n\}$ 是 $E(\mathbb{F}_q)$ 的子集且 $O \notin D$，$G = kO$ $(0 < k < n)$。赋予 $E(\mathbb{F}_q)$ 一个零元素为 $O$ 的群结构，记

$$N(k, O, D) = |\{S \subset D : |S| = k, \oplus_{P \in S} P = O\}|.$$

那么代数几何码 $C_{\mathscr{L}}(D, G)$ 的最小 *Hamming* 距离 $d_H = n - k + 1$ 时当且仅当

$$N(k, O, D) = 0.$$

$d_H = n - k$ 时当且仅当

$$N(k, O, D) > 0.$$

**证明** 我们已经知道 $C_{\mathscr{L}}(D, G)$ 的最小 Hamming 距离有两个选择：$n - k$, $n - k + 1$。$d_H = n - k$ 当且仅当存在一个函数 $f \in \mathscr{L}(G)$ 使得赋值 $ev(f)$ 的重量为 $n - k$。这等价于说， $f$ 在 $D$ 中有 $k$ 个零点，记作 $P_{i_1}, \cdots, P_{i_k}$。也就是说，

$$\mathrm{div}(f) \geq -kO + (P_{i_1} + \cdots + P_{i_k}),$$

等价于

$$\mathrm{div}(f) = -kO + (P_{i_1} + \cdots + P_{i_k}).$$

这样的 $f$ 的存在性等价于说

$$P_{i_1} \oplus \cdots \oplus P_{i_k} = O,$$

即 $N(k, O, D) > 0$。因此，代数几何码 $C_{\mathscr{L}}(D, G)$ 有最小 Hamming 距离 $n - k + 1$ 当且仅当 $N(k, O, D) = 0$。 □

我们主要考虑 $n > q+1$ 的情形，因为 $n \leq q+1$ 时，长度为 $n$ 的 MDS 字符结对码可以由 Reed-Solomon 码构造。在这种情形下，椭圆曲线码的最小 Hamming 距离 $d_H$ 与 MDS 码的猜想有关，而这个猜想对椭圆曲线码而言已经被证实了[36,39]。

**命题 2.5.2** [36,39] 令 $C_{\mathscr{L}}(D,G)$ 是命题 2.5.1 中构造的长度 $n > q+1$ 的椭圆曲线码，那么子集和问题总是有解，即

$$N(k,O,D) > 0.$$

因此，长度 $n > q+1$ 的椭圆曲线码有确定的最小 *Hamming* 距离 $d_H = n-k$。

也就是说，长度 $n > q+1$ 的椭圆曲线码都是几乎 MDS 码。为了使几乎 MDS 码有极大的最小结对距离，我们要使极小码字中的零尽可能分散。因此，为了从椭圆曲线构造 MDS 字符结对码，我们只要说明极小码字中没有 $k$ 个循环连续的零。

**引理 2.5.3** 令 $C_{\mathscr{L}}(D,G)$ 是命题 2.5.1中构造的长度 $n > q+1$ 的椭圆曲线，如果在任意码字中都没有 $k$ 个循环连续的零，那么 $C_{\mathscr{L}}(D,G)$ 达到极大最小结对距离 $n-k+2$。

为了从椭圆曲线得到长的码字，我们需要以下两个关于椭圆曲线的结果。

**引理 2.5.4** （*Hasse-Weil* 界[49]） 令 $E$ 是 $\mathbb{F}_q$ 上的椭圆曲线，那么 $E$ 上 $\mathbb{F}_q$-有理点的数目满足

$$|E(\mathbb{F}_q)| \leq q + \lfloor 2\sqrt{q} \rfloor + 1.$$

**引理 2.5.5** （*Hasse-Deuring*[22]） $E$ 上 $\mathbb{F}_q$-有理点的最大数目 $N(\mathbb{F}_q)$ 满足

$$N(\mathbb{F}_q) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor, & \text{如果 } q = p^a,\ a \geq 3,\ a \text{ 是奇数且 } p \mid \lfloor 2\sqrt{q} \rfloor; \\ q + \lfloor 2\sqrt{q} \rfloor + 1, & \text{其它情况,} \end{cases}$$

其中，$E$ 取遍 $\mathbb{F}_q$ 上的所有椭圆曲线。

记

$$\delta(q) = \begin{cases} 0, & \text{如果 } q = p^a,\ a \geq 3,\ a \text{ 是奇数且 } p \mid \lfloor 2\sqrt{q} \rfloor; \\ 1, & \text{其它情况.} \end{cases}$$

由有较大的最小 Hamming 距离的经典纠错码构造 MDS 字符结对码，关键点在于坐标的排序。对一般的码而言，这似乎是一个非常困难的过程。在接下来的部分，我们主要处理椭圆曲线码的情形。

**定理 2.5.6** 令 $N(\mathbb{F}_q) = q + \lfloor 2\sqrt{q} \rfloor + \delta(q)$，对任意 $7 \leq d+2 \leq n \leq N(\mathbb{F}_q) - 3$，都存在线性 *MDS* $(n, d+2)_q$ 字符结对码。

**证明** 满足 $d+2 = n$ 的 MDS 字符结对码的存在性见[10]。下面我们只考虑 $7 \leq d+2 < n \leq N(\mathbb{F}_q) - 3$ 的情形。由引理 2.5.5，我们取 $E$ 为 $\mathbb{F}_q$ 上包含 $\mathbb{F}_q$-有理点 $O$ 的最大椭圆曲线，即

$$|E(\mathbb{F}_q)| = N(\mathbb{F}_q).$$

在椭圆曲线码的构造中取除子 $G = kO$。

情形 (I): $N = N(\mathbb{F}_q)$ 是奇数，那么 $E(\mathbb{F}_q)$ 中没有二阶元素。假设

$$E(\mathbb{F}_q) = \{P_1, P_2, \cdots, P_{N-2}, P_{N-1}, O\},$$

其中

$$P_1 \oplus P_2 = P_3 \oplus P_4 = \cdots = P_{N-2} \oplus P_{N-1} = O. \tag{2-1}$$

1. 对奇数 $d$ 和偶数 $n$ : $7 \leq d+2 < n \leq N-1$，这种情况下 $k = N-1-d$ 是奇数。取

   $$D = \{P_1, P_2, \cdots, P_{N-2}, P_{N-1}\}.$$

   那么从等式 (2-1) 我们可知不存在循环连续的 $k$ 个点的和为 $O$。那么，由引理 2.5.3 可知，$C_{\mathscr{L}}(D, G)$ 是一个参数为 $(N-1, d+2)_q$ 的 MDS 字符结对码。通过删除成对的点 $(P_1, P_2)$，$(P_3, P_4)$ 等，我们可以得到参数为 $(n, d+2)_q$ 的 MDS 字符结对码，其中 $n$ 满足 $7 \leq d+2 < n \leq N-1$ 且是偶数。

2. 对偶数 $d$ 和奇数 $n$ : $7 \leq d+2 < n \leq N-2$，这种情况下 $k = N-2-d$ 是奇数。取

   $$D = \{P_1, P_2, \cdots, P_{N-2}\}.$$

   那么从等式 (2-1) 我们可知不存在循环连续的 $k$ 个点的和为 $O$。那么，由引理 2.5.3 可知，$C_{\mathscr{L}}(D, G)$ 是一个参数为 $(N-2, d+2)_q$ 的 MDS 字符结对码。通过删除成对的点 $(P_1, P_2)$，$(P_3, P_4)$ 等，我们可以得到参数为 $(n, d+2)_q$ 的 MDS 字符结对码，其中 $n$ 满足 $d+2 < n \leq N-2$ 且是奇数。

3. 对偶数 $d$ 和偶数 $n$ : $7 \leq d+2 < n \leq N-3$，这种情况下 $k = N-3-d$ 是偶数。记 $N-3 = (k+1)s + r$，$s \geq 1$，$0 \leq r \leq k$。取预赋值集

   $$D_0 = \{P_1, P_2, \cdots, P_{N-5}, P_{N-4}, P_{N-2}\}$$

并利用下述算法排序：

**步骤 1.** 对集合 $\{P_1, P_2, \cdots, P_{sk+r-2}, P_{sk+r-1}\}$ 而言，我们把 $P_{N-i-4}$ 插入到 $P_{ik-1}$ 和 $P_{ik}$ 之间，$1 \leq i \leq s-1$，把 $P_{N-4}$ 插入到 $P_{sk-1}$ 和 $P_{sk}$ 之间，把 $P_{N-2}$ 插入到$P_{sk+r-1}$ 之后。换言之，我们排序如下

$$\begin{aligned} D_1 = \ & \{P_1, \cdots, P_{k-1}, P_{N-5}, P_k, \cdots, P_{(s-1)k-1}, P_{N-3-s}, P_{(s-1)k}, \\ & \cdots, P_{sk-1}, P_{N-4}, P_{sk}, P_{sk+1}, \cdots, P_{sk+r-1}, P_{N-2}\}. \end{aligned}$$

在这步之后，序列

$$P_1, \cdots, P_{k-1}, P_{N-5}, P_k, \cdots, P_{(s-1)k-1}, P_{N-3-s}, P_{(s-1)k}, \cdots, P_{sk-1}, P_{N-4}, P_{sk}, \cdots, P_{sk+r-1}$$

中不存在 $k$ 个连续的点的和为 $O$。我们可以通过多种方法说明这点，比如 $P_1 + \cdots + P_{k-1} + P_{N-5} = P_{k-1} + P_{N-5} \neq O$ 因为 $P_{k-1} + P_k = O$ 且 $P_k \neq P_{N-5}$。$P_k + P_{k+1} + \cdots + P_{2k-1} = P_k + P_{2k-1} \neq O$ 因为 $P_{2k-1} + P_{2k} = O$ 且 $P_k \neq P_{2k}$。但是，在序列的尾部

$$P_{(s-1)k+r+1}, \cdots, P_{sk-1}, P_{N-4}, P_{sk}, P_{sk+1}, \cdots, P_{sk+r-1}, P_{N-2}, P_1, \cdots, P_{k-r-1}$$

中可能存在 $k$ 个循环连续的点使得它们的和为 $O$。比如，$k = 6$，$N = 19$ 时，由步骤 1，我们可知

$$D_1 = P_1, \cdots, P_5, P_{14}, P_6, \cdots, P_{11}, P_{15}, P_{12}, P_{13}, P_{17}.$$

在序列

$$P_1, \cdots, P_5, P_{14}, P_6, \cdots, P_{11}, P_{15}, P_{12}, P_{13}$$

中不存在 6 个连续的点使得它们的和为 $O$。但是，在序列的尾部

$$P_{10}, P_{11}, P_{15}, P_{12}, P_{13}, P_{17}, P_1, P_2$$

中可能存在 6 个循环连续的点使得它们的和为 $O$。

**步骤 2.** 在 $r$ 是偶数的情况下，我们知道下述两个等式至多一个成立：

$$P_{(s-1)k+r+2} \oplus \cdots \oplus P_{N-4} \oplus \cdots \oplus P_{N-2} = P_{(s-1)k+r+2} \oplus P_{N-4} \oplus P_{sk+r-1} \oplus P_{N-2} = O,$$

和

$$P_{(s-1)k+r+3} \oplus \cdots \oplus P_{N-4} \oplus \cdots \oplus P_{N-2} \oplus P_1 = P_{N-4} \oplus P_{sk+r-1} \oplus P_{N-2} \oplus P_1 = O.$$

如果第一个等式成立，那么交换 $P_{(s-1)k+r+1}$ 和 $P_{(s-1)k+r+2}$；如果第二个成立，那么交换 $P_1$ 和 $P_2$；如果两个都不成立，那我们什么都不需要做。

对任意$i=1,\cdots,\frac{k-r-2}{2}$，同样地，下述两个等式至多一个成立：

$$P_{(s-1)k+r+2i+2}\oplus\cdots\oplus P_{N-4}\oplus\cdots\oplus P_{N-2}\oplus P_1\oplus\cdots\oplus P_{2i}=P_{(s-1)k+r+2i+2}\oplus P_{N-4}\oplus P_{sk+r-1}\oplus P_{N-2}=O,$$

和

$$P_{(s-1)k+r+2i+1}\oplus\cdots\oplus P_{N-4}\oplus\cdots\oplus P_{N-2}\oplus P_1\oplus\cdots\oplus P_{2i-1}=P_{N-4}\oplus P_{sk+r-1}\oplus P_{N-2}\oplus P_{2i+1}=O.$$

如果第一个等式成立，那么交换 $P_{(s-1)k+r+2i+1}$ 和 $P_{(s-1)k+r+2i+2}$；如果第二个成立，那么交换 $P_{2i+1}$ 和 $P_{2i+2}$；如果两个都不成立，那我们什么都不需要做。当 $r$ 是奇数时，对应的算法和偶数的情况类似，检验 $k$ 个循环连续的点的和，然后做相应的交换操作。

我们继续之前的例子，如果

$$P_{10}\oplus P_{11}\oplus P_{15}\oplus P_{12}\oplus P_{13}\oplus P_{17}=P_{10}\oplus P_{15}\oplus P_{13}\oplus P_{17}=O,$$

那么交换 $P_9$ 和 $P_{10}$。这种情况下，我们立刻可以得到

$$P_{11}\oplus P_{15}\oplus P_{12}\oplus P_{13}\oplus P_{17}\oplus P_1=P_{15}\oplus P_{13}\oplus P_{17}\oplus P_1\neq O,$$

所以我们不需要重新排列 $P_1$ 和 $P_2$ 等。

通过上述的算法，我们可以得到一个重新排序过的赋值集 $D$，其中不存在 $k$ 个循环连续的点的和为 $O$。因此，由引理 2.5.3 可知，椭圆曲线码 $C_{\mathscr{L}}(D,G)$ 是一个 MDS 字符结对码，参数为 $(N-3,d+2)_q$。同样地，通过从预赋值集中成对地删点，我们可以得到 MDS 字符结对码，参数为 $(n,d+2)_q$，$n$ 满足 $d+2<n\leq N-3$ 且是偶数。

4. 对奇数 $d$ 和奇数 $n$：$7\leq d+2<n\leq N-2$，这种情况下 $k=N-2-d$ 是偶数，记 $N-2=(k+1)s+r$，$s\geq 1$，$0\leq r\leq k$。取预赋值集为

$$D_0=\{P_1,P_2,\cdots,P_{N-3},P_{N-2}\}$$

并重新排序为

$$\begin{aligned}D=\ &\{P_1,\cdots,P_{k-1},P_{N-3},P_k,\cdots,P_{(s-1)k-1},P_{N-1-s},\\&P_{(s-1)k},\cdots,P_{sk-1},P_{N-2},P_{sk},P_{sk+1},\cdots,P_{sk+r}\}.\end{aligned}$$

如果 $r$ 是偶数，且 $r=k$，那么用 $P_{N-1}$ 替代 $P_{sk+r}$；否则，保持不变。显然，不存在 $k$ 个循环连续的点的和为 $O$。如果 $r$ 是奇数，那么同样地，当 $d$ 和 $n$ 是偶数时，在序

列的尾部可能存在 $k$ 个循环连续的点的和为 $O$。在这种情况下，我们只要和情况 3 中同样地操作，得到一个重新排序的赋值集 $D$ 使得不存在 $k$ 个循环连续的点的和为 $O$。

因此，由引理 2.5.3 可知，$C_{\mathscr{L}}(D,G)$ 是一个 MDS 字符结对码，参数为 $(N-2,d+2)_q$。同样地通过从预赋值集中成对地删点，我们可以得到 MDS 字符结对码，参数为 $(n,d+2)_q$，$n$ 满足 $7 \leq d+2 < n \leq N-2$ 且是奇数。

综上，当 $N = N(\mathbb{F}_q)$ 是奇数时，对任意 $7 \leq d+2 \leq n \leq N(\mathbb{F}_q)-3$，都存在 MDS $(n,d+2)_q$ 字符结对码。

情形 (II): $N = N(\mathbb{F}_q)$ 是偶数。证明过程是相似的，需要注意的是群 $E(\mathbb{F}_q)$ 中存在一个或者三个二阶非零元，在生成预赋值集时可以利用这些元素，剩下的部分都是相似的，这里我们省略细节。 □

**注解 1** 从上述证明中我们可知，在某些情况中构造的 *MDS* 字符结对码的长度可以达到 $N(\mathbb{F}_q)-2$ 或者 $N(\mathbb{F}_q)-1$。为了提供一个简洁的证明，我们省略了这些细节。同样地，也有利用其它曲线构造几乎 *MDS* 码的工作[2]。利用椭圆曲线的优势在于我们可以将椭圆曲线码上的组合问题转化为几何对象上的问题，使得这个问题能够更加容易地处理。怎么利用其它几乎 *MDS* 码构造 *MDS* 字符结对码则是一个比较困难的问题。

我们最后通过一个小例子来补充解释上述的算法与注解。

例 2.5.7 令 $E$ 是有限域 $\mathbb{F}_{13}$ 上由等式

$$y^2 = x^3 + 9$$

定义的椭圆曲线。通过软件 *MAGMA* 或者通过直接计算可知，$E$ 有 $N = 21$ 个 $\mathbb{F}_{13}$-有理点。它们为 $P_1 = (0,3), P_2 = (0,10), P_3 = (1,6), P_4 = (1,7), P_5 = (2,2), P_6 = (2,11), P_7 = (3,6), P_8 = (3,7), P_9 = (5,2), P_{10} = (5,11), P_{11} = (6,2), P_{12} = (6,11), P_{13} = (7,1), P_{14} = (7,12), P_{15} = (8,1), P_{16} = (8,12), P_{17} = (9,6), P_{18} = (9,7), P_{19} = (11,1), P_{20} = (11,12)$ 以及无穷远点 $P_{21} = O$。所以，它达到了 *Hasse-Weil* 界。

*1. MDS* $(20,18)_{13}$ 字符结对码的构造

在这个情况下，$n = 20, d = 16, k = 4$ 都是偶数，所以它属于 $d,n$ 都是偶数的情形。

排序后的赋值集

$$D_1 = \{P_1, P_2, P_3, P_{19}, P_4, P_5, P_6, P_7, P_{18}, P_8, P_9, P_{10}, P_{11}, P_{17}, P_{12}, P_{13}, P_{14}, P_{15}, P_{20}, P_{16}\}$$

满足任意循环连续 4 个点和不为零。由引理 2.5.3 可知，$C_{\mathscr{L}}(D_1, 4O)$ 是一个 *MDS* 字符结对码，参数为 $(20, 18)_{13}$。

2. *MDS* $(19, 17)_{13}$ 字符结对码的构造

在这个情况下，$n = 19, d = 15$ 是奇数，$k = 4$ 是偶数，所以它属于 $d, n$ 都是奇数的情形。赋值集 $D$ 如下

$$\{P_1, P_2, P_3, P_{18}, P_4, P_5, P_6, P_7, P_{17}, P_8, P_9, P_{10}, P_{11}, P_{19}, P_{12}, P_{13}, P_{14}, P_{15}, P_{16}\}.$$

因为 $r = k$，所以我们把 $P_{16}$ 替换成 $P_{20}$，即得到新的赋值集

$$D' = \{P_1, P_2, P_3, P_{18}, P_4, P_5, P_6, P_7, P_{17}, P_8, P_9, P_{10}, P_{11}, P_{19}, P_{12}, P_{13}, P_{14}, P_{15}, P_{20}\}$$

满足任意循环连续 4 个点和不为零。由引理 2.5.3 可知，$C_{\mathscr{L}}(D', 4O)$ 是一个 *MDS* 字符结对码，参数为 $(19, 17)_{13}$。

## 2.6　总结

在本章中，我们给出了 MDS 字符结对码存在性的一个充分条件，由此我们利用线性代数方法，有限几何中的圆角集以及椭圆曲线码构造了三类最优码。与之前已有的结果相比较，我们的码的参数更加丰富。在下一章中，我们会考虑字符结对码的推广形式：*b*-字符码。

# 3 $b$-字符码

## 3.1 介绍

Yaakobi 等[55] 将字符结对读取信道的框架推广到了 $b > 2$ 个字符连续读取的框架中，在这样的信道中，每一步读取操作都读取连续的 $b$ 个字符。同时，他们也将字符结对码中已知的部分结果推广到了 $b$-字符读取信道上。在本章中，我们继续 $b$-字符码的研究。我们建立了 $b$-字符码的 Singleton 界，达到界的码被称为最大距离可分 $b$-字符码，简记为 MDS $b$-字符码。同样地，MDS $b$-字符码是最优的，因为它们有着极大的最小 $b$-距离，因而有最好的抵抗错误的能力。我们将 MDS $b$-字符码的构造问题转化为一个合适的矩阵的构造问题，进而利用有限几何的知识，我们又将问题转化为射影空间中点的排序问题。由此，我们构造了如下的几类有限域上的线性 MDS $b$-字符码。

(1) 对任意素数幂 $q$，$7 \leq n \leq q^3+q^2+q+1$，都存在 MDS $(n,7)_q$ 3-字符码（定理 3.3.8）。

(2) 对任意素数幂 $q \geq 3$，$9 \leq n \leq q^4+q^3+q^2+q+1$，都存在 MDS $(n,9)_q$ 4-字符码（定理 3.3.10）。

(3) 对任意素数幂 $q$，$q \geq b \geq 5$，$2b+1 \leq n \leq q^b - bq^{b-1} + \frac{b^2+3b}{2}$，都存在 MDS $(n,2b+1)_q$ $b$-字符码（定理 3.3.11）。

(4) 对任意素数幂 $q \geq b-1$，$b \geq 3$ 或者对 $q=2, b=4$，都存在长度 $n \geq 2b$ 的 MDS $(n,2b)_q$ $b$-字符码（定理 3.3.13）。

(5) 对任意素数幂 $q \geq 3$，$n \geq 10$，都存在 MDS $(n,10)_q$ 5-字符码（定理 3.3.14）。

(6) 对任意素数幂 $q$，$b \geq 4$，都存在 MDS $(\frac{q^{b+1}-1}{q-1}, 2b+1)_q$ $b$-字符码（定理 3.4.2）。

同时，在第 3.5 节中，我们也提出如下两个猜想。

- 对任意素数幂 $q$，$b > 2$，$2b+1 \leq n \leq \frac{q^{b+1}-1}{q-1}$，都存在线性 MDS $(n,2b+1)_q$ $b$-字符码。

- 对任意素数幂 $q$，$b>2$，$n\geq 2b$，都存在线性 MDS $(n,2b)_q$ $b$-字符码。

前四类码是我们主要的结果。$\mathbb{F}_q$ 上线性 MDS $(n,2b+1)_q$ $b$-字符码只有当 $2b+1\leq n\leq \frac{q^{b+1}-1}{q-1}$ 时才有可能存在（引理 3.3.3），而第 (4) 类码则说明对于 $b=3,d_3=6$ 或者 $b=4,d_4=8$，有限域 $\mathbb{F}_q$ 上线性 MDS $b$-字符码对任意长度 $n\geq 2b$ 都存在。因此，对某些参数而言，上述的几类码其实完全决定了相应的 MDS $b$-字符码的存在性。

第 (5) 和第 (6) 类码主要是为了支撑我们的猜想。(5) 说明在第 (4) 类码中的限制条件 $q\geq b-1$ 不是必要的，(6) 则证明了长度为 $\frac{q^{b+1}-1}{q-1}$ 的码的存在性。此外，我们还证明了任意 MDS $(n,d_b)_q$ $b$-字符码，$d_b<n$，同时也是 MDS $(n,d_b+1)_q$ $(b+1)$-字符码（定理3.2.5）。因此，由上面的每一类码我们都可以导出新的 MDS $b$-字符码。

## 3.2 准备工作

假设 $\Sigma$ 是含有 $q$ 个元素的字母表，其中每个元素我们称作为一个字符。令 $b$ 是一个大于等于 1 的整数，对于 $\Sigma^n$ 中的一个向量 $\mathbf{x}=(x_0,x_1,\cdots,x_{n-1})$，我们定义它的 $b$-字符读取向量为

$$\pi_b(\mathbf{x})=((x_0,\cdots,x_{b-1}),(x_1,\cdots,x_b),\cdots,(x_{n-1},x_0,\cdots,x_{b-2}))\in(\Sigma^b)^n.$$

在本章中，我们始终令 $q$ 为素数幂， $\mathbb{F}_q$ 为包含 $q$ 个元素的有限域。我们主要讨论有限域 $\mathbb{F}_q$ 上的向量，故令 $\Sigma=\mathbb{F}_q$。对于 $\mathbb{F}_q^n$ 中的两个向量 $\mathbf{x},\mathbf{y}$，我们有

$$\pi_b(\mathbf{x}+\mathbf{y})=\pi_b(\mathbf{x})+\pi_b(\mathbf{y}),$$

$\mathbf{x}$ 和 $\mathbf{y}$ 之间的 $b$-距离定义为

$$D_b(\mathbf{x},\mathbf{y}):=|\{0\leq i\leq n-1:(x_i,\cdots,x_{i+b-1})\neq(y_i,\cdots,y_{i+b-1})\}|,$$

其中，下标都是在模 $n$ 的意义下取值。同样地， $\mathbf{x}\in\mathbb{F}_q^n$ 的 $b$-重量定义为

$$wt_b(\mathbf{x}):=|\{0\leq i\leq n-1:(x_i,\cdots,x_{i+b-1})\neq\mathbf{0}\}|,$$

其中，下标都是在模 $n$ 的意义下取值， $\mathbf{0}$ 表示全零向量。两个向量 $\mathbf{x}$ 和 $\mathbf{y}$ 之间的 Hamming 距离写作为 $d_H(\mathbf{x},\mathbf{y})$，向量 $\mathbf{x}$ 的 Hamming 重量写作为 $wt_H(\mathbf{x})$。显然地，我们可以得到以下 $b$-距离和 $b$-重量之间的联系。

**命题 3.2.1** *对于 $\mathbb{F}_q^n$ 中的所有向量 $\mathbf{x},\mathbf{y}$，$D_b(\mathbf{x},\mathbf{y})=wt_b(\mathbf{x}-\mathbf{y})$。*

**证明** 对于 $\mathbb{F}_q^n$ 中的任意两个向量 $\mathbf{x}, \mathbf{y}$，我们有$D_b(\mathbf{x}, \mathbf{y}) = d_H(\pi_b(\mathbf{x}), \pi_b(\mathbf{y})) = wt_H(\pi_b(\mathbf{x}) - \pi_b(\mathbf{y})) = wt_H(\pi_b(\mathbf{x} - \mathbf{y})) = wt_b(\mathbf{x} - \mathbf{y})$。 □

对于字母表 $\{0, 1\}$ 上的向量而言，文献[55]中已经给出了 Hamming 重量和 $b$-重量之间的联系。鉴于文献[55]的证明对于有限域 $\mathbb{F}_q$上的向量同样适用，我们直接给出以下命题。

**命题 3.2.2** 假设 $\mathbf{x} \in \mathbb{F}_q^n$ 是一个满足条件 $0 < wt_H(\mathbf{x}) \leq n - (b-1)$的向量。那么，

$$wt_H(\mathbf{x}) + b - 1 \leq wt_b(\mathbf{x}) \leq b \cdot wt_H(\mathbf{x}).$$

如果我们考虑 $\mathbb{F}_q^n$ 中的一个非零向量的 $b$-重量和 $(b+1)$-重量，那么有下一个命题成立。

**命题 3.2.3** 对于 $\mathbb{F}_q^n$ 中的任意非零向量 $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$，如果 $wt_b(\mathbf{x}) < n$，那么 $wt_{b+1}(\mathbf{x}) \geq wt_b(\mathbf{x}) + 1$。

**证明** 如果 $(x_i, \cdots, x_{i+b-1}) \neq \mathbf{0}$，那么 $(x_i, \cdots, x_{i+b-1}, x_{i+b}) \neq \mathbf{0}$，其中下标都是在模 $n$ 的意义下取值，$0 \leq i \leq n-1$。所以，我们始终有 $wt_{b+1}(\mathbf{x}) \geq wt_b(\mathbf{x})$。又因为 $wt_b(\mathbf{x}) < n$，我们可以找到某些 $j$，$0 \leq j \leq n-1$，使得 $(x_j, \cdots, x_{j+b-1}) = \mathbf{0}$，$x_{j+b} \neq 0$ 成立。由此可得，$(x_j, \cdots, x_{j+b-1}, x_{j+b}) \neq \mathbf{0}$，$wt_{b+1}(\mathbf{x}) \geq wt_b(\mathbf{x}) + 1$。 □

以四个向量 $v_1 = 1110000, v_2 = 1100001, v_3 = 1101000, v_4 = 1010100$ 作为例子说明。它们的 Hamming 重量都是 3，而它们的 3-重量分别为 5,5,6,7，4-重量分别为 6,6,7,7。通过这样一个简单的观察，我们发现，一个向量的 $b$-重量与其非零元的分布有关。总体趋势为，非零元越紧密，向量的 $b$-重量越小。对于给定 Hamming 重量的向量，当它的非零元处于循环连续的位置时，它的 $b$-重量最小。

有限域 $\mathbb{F}_q$ 上长度为 $n$ 的码 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 中的一个非空子集，$\mathcal{C}$ 中的元素被称作为码字。码 $\mathcal{C}$ 的最小 $b$-距离定义为

$$d_b = \min\{D_b(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\},$$

码 $\mathcal{C}$ 中码字的数目称为码 $\mathcal{C}$ 的大小。通常而言，有限域 $\mathbb{F}_q$ 上长度为 $n$，大小为 $M$，最小 $b$-距离为 $d_b$ 的码记作为 $(n, M, d_b)_q$ $b$-字符码。

$b = 1$ 时，$b$-字符码对应的是被广泛研究的传统意义上的码；而 $b = 2$ 时，则对应着字符结对码。如果码 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 的一个子空间，那么码 $\mathcal{C}$ 就称作为线性 $b$-字符码。在本章中，我们主要研究有限域 $\mathbb{F}_q$ 上的线性 $b$-字符码，$b > 2$。

**定理 3.2.4** （*Singleton*界）令 $q \geq 2$，$b \leq d_b \leq n$，如果码 $\mathcal{C}$ 是一个 $(n, M, d_b)_q$ $b$-字符码，那么我们有 $M \leq q^{n-d_b+b}$。

**证明** 假设 $\mathcal{C}$ 是一个 $(n, M, d_b)_q$ $b$-字符码，其中 $q \geq 2$，$b \leq d_b \leq n$。对于 $\mathcal{C}$ 中码字，任意连续 $d_b - b$ 位对于 $b$-距离的贡献至多为 $d_b - 1$。又因为 $\mathcal{C}$ 的最小 $b$-距离为 $d_b$，将 $\mathcal{C}$ 中所有码字的最后 $d_b - b$ 位删除后，我们得到的长度为 $n - d_b + b$ 的向量仍然互不相同。而有限域 $\mathbb{F}_q$ 上，长度为 $n - d_b + b$ 的向量的最大数目为 $q^{n-d_b+b}$。 □

一个大小为 $M = q^{n-d_b+b}$ 的 $(n, M, d_b)_q$ $b$-字符码 $\mathcal{C}$ 被称作为最大距离可分（MDS）$(n, d_b)_q$ $b$-字符码。

**定理 3.2.5** 如果一个线性 *MDS* $(n, d_b)_q$ $b$-字符码 $\mathcal{C}$ 满足 $d_b < n$，那么它也是一个 *MDS* $(n, d_b + 1)_q$ $(b + 1)$-字符码。

**证明** 从命题 3.2.1 和 3.2.3 我们可以得到 $d_{b+1} \geq d_b + 1$，那么 $|\mathcal{C}| = q^{n-d_b+b} \geq q^{n-d_{b+1}+b+1}$，由此得证。 □

这个定理虽然很简单，但是却非常实用。我们可以从本章的每类 MDS $b$-字符码，或者文献[8–11,23,31,37,54,55] 中的每类 MDS 字符结对码导出新的 MDS 码。

现在，我们已经可以给出 MDS $b$-字符码的存在性的一个充分条件。

**定理 3.2.6** 如果有限域 $\mathbb{F}_q$上存在一个 $d + b - 2$ 行，$n \geq d + 2b - 2 \geq 2b$ 列的矩阵，记作 $H = [H_0, H_1, \cdots, H_{n-1}]$，其中 $H_i$ $(0 \leq i \leq n - 1)$ 表示的是 $H$ 的第 $i$ 列，满足下面两个条件：

1. $H$ 的任意 $d - 1$ 列线性无关；
2. 任意循环连续的 $d+b-2$ 列线性无关，即对所有 $0 \leq i \leq n-1$，$H_i, H_{i+1}, \cdots, H_{i+d+b-3}$ 线性无关，其中下标都是在模 $n$ 的意义下取值。

那么，就存在一个线性 *MDS* $(n, d + 2b - 2)_q$ $b$-字符码。

**证明** 假设 $\mathcal{C}$ 是以 $H$ 为校验矩阵的线性码。那么第一个条件说明了 $\mathcal{C}$ 是一个参数为 $[n, n - d - b + 2, \geq d]_q$ 的线性码，它的大小为 $q^{n-d-b+2}$。对于 $\mathcal{C}$ 中的一个非零码字 $c = (c_0, c_1, \cdots, c_{n-1})$，如果存在 $j$ 使得 $c_j = c_{j+1} = \cdots = c_{j+b-2} = 0$ 且 $c_{j+b-1} \neq$

0，其中下标都是在模 $n$ 的意义下取值，那么我们考虑将 $c$ 循环移位后的向量 $v = (c_{j+b-1}, \cdots, c_{n-1}, c_0, \cdots, c_{j+b-2})$，移位过程主要是将连续的零移到了向量的末尾，也就是说，我们可以将向量 $v$ 改写成 $v = (v_0, v_1, \cdots, v_t, 0, \cdots, 0)$，其中 $t \leq n-b$，$v_0, v_t \neq 0$。因为任意循环连续的 $d+b-2$ 列线性无关，所以我们有 $t \geq d+b-2$。又因为集合 $\{v_0, v_1, \cdots, v_t\}$ 中至少有 $d$ 个非零元，所以我们很容易就可以得出 $wt_b(c) = wt_b(v) \geq d + 2b - 2$。如果不存在这样的 $j$ 使得 $c_j = c_{j+1} = \cdots = c_{j+b-2} = 0, c_{j+b-1} \neq 0$，那么显然 $wt_b(c) = n$。综上可得， $d_b \geq d + 2b - 2$。 □

## 3.3 利用有限几何构造 MDS $b$-字符码

**引理 3.3.1** *射影空间 $PG(r, q)$ 中存在 $q+1$个超平面，它们包含了射影空间中的所有点且相交于一个 $(r-2)$ 维射影空间。*

**证明** 在射影空间 $PG(r, q)$ 中固定一个 $(r-2)$ 维子空间 $U$。选择 $PG(r, q) \setminus U$ 中任意一个点 $P_0$，那么 $P_0$ 和 $U$ 张成了一个超平面 $V_0$。接着，我们再从 $PG(r, q) \setminus V_0$ 中选取一个点 $P_1$，同样地， $P_1$ 和 $U$ 张成了另一个超平面 $V_1$。重复这个步骤直到所有的点都被覆盖，由此我们得到了 $q+1$ 个超平面 $V_0, \cdots, V_q$，它们相交于 $U$。 □

在定理 3.2.6 中，如果我们固定 $d = 3$，从射影空间 $PG(b, q)$（$b \geq 2$）中选取 $n$ 个点并且把它们当作矩阵 $H$ 的列向量，那么我们就可以得到下面这个引理。

**引理 3.3.2** *如果射影空间 $PG(b, q)$ 中存在 $n \geq 2b+1$ 个点的有序排列，使得任意循环连续的 $b+1$ 个点都不落在一个 $(b-1)$ 维射影空间中，那么就存在一个线性 MDS $(n, 2b+1)_q$ $b$-字符码。*

由上述引理可知，想要构造 MDS $b$-字符码，我们的主要任务就是给射影空间 $PG(b, q)$ 中的点排序，使得任意循环连续的 $b+1$ 个点都不落在一个 $(b-1)$ 维射影空间中。因此，码的构造问题就转化成了空间中点的排序问题。

另一方面，因为码字中的任意一个非零元对 $b$-重量的贡献至多为 $b$，所以一个最小 $b$-距离为 $2b+1$ 的 $b$-字符码的 Hamming 距离至少为 3。换言之，任意线性的 MDS $(n, 2b+1)_q$ $b$-字符码的校验矩阵中肯定不包含线性相关的两列，所以只有当 $n \leq \frac{q^{b+1}-1}{q-1}$ 时，线性的 MDS $(n, 2b+1)_q$ $b$-字符码才有可能存在。

**引理 3.3.3** 有限域 $\mathbb{F}_q$ 上线性 *MDS* $(n, 2b+1)_q$ $b$-字符码只有当 $2b+1 \leq n \leq \frac{q^{b+1}-1}{q-1}$ 时才有可能存在。

### 3.3.1 $b = 2$

射影平面 $PG(2,q)$ 是一个点和线的关联结构，满足：

- 过任意两个不同的点有且仅有一条线；
- 任意两条不同的线交且仅交于一点；
- 存在四个点使得任意三点不共线。

从引理 3.3.1 我们得知， $PG(2,q)$ 中的所有点分布在 $q+1$ 条线上，这些线交于一点，如图 3-1 所示。

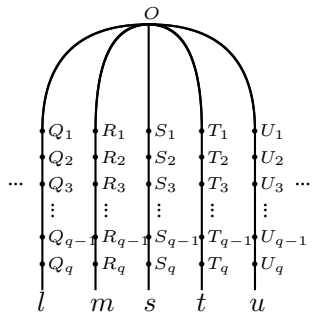


**图 3-1 射影平面 $PG(2,q)$ 的结构.**

**引理 3.3.4** 对任意素数幂 $q \geq 3$，$3 \leq n \leq q^2+q+1$，存在 $PG(2,q)$ 中的 $n$ 个点的有序排列使得任意循环连续的三个点不共线。

**证明** 我们采用图 3-1 中的符号，有很多种方法可以达到这个目的，这里我们给出其中一个策略。

- $q$ 是奇数

在这种情况下，过 $O$ 点有偶数条线。我们选取 $O$ 点作为第一个点，然后我们从线 $l$ 和 $m$ 上轮流地选择点。假设我们已经将点排成 $O, Q_1, R_1, Q_2, R_2, \cdots, Q_q, R_q$。下一步我们选择一个不落在线 $Q_qR_q$ 上点 $S_1$ 作为下一个点，然后再选择一个不落在线 $R_qS_1$ 上的点 $T_1$ 作为再下一个。接着，我们就从线 $s$ 和线 $t$ 上轮流选点。我们可以一直这么做直到我们已经排了 $n$ $(3 \leq n \leq q^2+q+1)$ 个点。

注意到我们这样的排法可以做到使得任意三个连续的点不共线，需要注意的只是那些“循环连续”的部分。如果记我们排列的最后三个点为 $P_{n-3}, P_{n-2}$ 和 $P_{n-1}$，那么我们要做的就是要确保 $P_{n-2}, P_{n-1}, O$ 这三个点不共线，并且$P_{n-1}, O, Q_1$ 这三个点也不共线。因为 $P_{n-1}$ 永远不会落在线 $OP_{n-2}$ 上，所以 $P_{n-2}, P_{n-1}, O$ 不共线是显然的。当点 $P_{n-1}$ 落在线 $l$ 上，也就是说当 $4 \leq n \leq 2q$ 且 $n$ 是偶数时，$P_{n-1}, O, Q_1$这三个点是有可能共线的。如果这种情况发生了，我们可以另外选择一个不落在线 $l, m$ 和 $P_{n-3}P_{n-2}$ 上的点来替换 $P_{n-1}$，而且这个是肯定可以做到的。

- $q$ 是偶数

这种情况与上一种情况的区别在于，过点 $O$ 有奇数条线。当 $n \leq q^2+1$ 时，我们可以选择偶数条线，然后像上一种情况那样排点。当 $n > q^2+1$ 时，我们首先选择三条线 $l, m, s$ 出来，我们先将这三条线上的点排列好，然后剩下的偶数条线上的点就可以像之前一样排列。同样地，我们选择 $O$ 点作为我们的第一个点，然后我们轮流地从三条线 $l, m, s$ 上选择点，保证任意连续三个点不共线。因为两条线交且仅交于一点，我们可以一直这样做直到每条线上只剩下了一个点。假设我们已经将点排列成 $O, Q_1, R_1, S_1, Q_2, \cdots, Q_{q-1}, R_{q-1}, S_{q-1}$，选择 $R_q, S_q$ 作为下两个点，然后选择不落在线 $R_qS_q$ 和 $Q_qS_q$ 上的一个点 $T_1$，让 $Q_q$ 成为下一个点，紧接着选择不落在线 $Q_qT_1$ 上的一个点 $U_1$，不落在线 $Q_qU_1$ 上的一个点 $T_2$。目前为止，我们已经将点排列成 $O, Q_1, R_1, S_1, \cdots, Q_{q-1}, R_{q-1}, S_{q-1}R_q, S_q, T_1, Q_q, U_1, T_2$ 并且任意连续三个不共线，剩下来的偶数条线上的点可以和上一种情况同样排列。 □

在上面的引理中，我们排除了 $q = 2$ 的情况，这种情况下点的数目不多，我们把它作为如下一个例子。

例 3.3.5 我们可以将 $PG(2, 2)$ 中的 $3 \leq n \leq 7$ 个点有序排列使得任意循环连续的三个点不共线，如表3-1 所示，其中 $H$ 的列向量代表的是点。

**注解 2** 根据上述讨论，我们其实也可以得到 *MDS* $(n, 5)_q$ 字符结对码，$5 \leq n \leq q^2+q+1$，同样的码在上一章中我们已经通过线性代数方法构造而得。此处的讨论，除了提供另一种证明思路，给读者一个更加直观的感受之外，也能从某种程度上说明我们方法的优越性，因为相较之前已有的结果而言，这里得到的码的参数非常丰富。此外，这里的讨论在之后引理 3.3.9 的证明中也是不可或缺的。

**表 3-1　射影平面 $PG(2,2)$ 中点的有序排列**

| $n$ | $H$ |
|---|---|
| 3 | $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ |
| 4 | $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ |
| 5 | $\begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$ |
| 6 | $\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ |
| 7 | $\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ |

### 3.3.2　$b = 3, d_3 = 7$

首先，我们叙述 3 维射影空间中的几个公理，主要给出了对象（点、线、面）之间的关系。

- 任意两个不同的点只与一条线相关联；
- 任意两个不同的面交且仅交于一条线；
- 给定任意一个面 $\pi$ 以及 $\pi$ 外的任意一条线 $l$，有且仅有一个点与它们都相关联；
- 给定一条线 $l$，与它相关联（至少包含线上的两点）的每个面均包含 $l$ 上的所有点；
- 两条不同的线交于一点当且仅当它们共面；
- 存在五个点的集合使得任意四个都不共面。

从引理 3.3.1 我们知道，$PG(3,q)$ 中的所有点落在 $q+1$ 个面上，这些面交于一条线，如图 3-2 所示。例如，线 $l, l_1, \cdots, l_q$ 构成一个面，线 $l, m_1, \cdots, m_q$ 构成另一个面，这两个面相交于线 $l$。

**引理 3.3.6** *对任意素数幂 $q \geq 3$，$4 \leq n \leq q^3+q^2+q+1$，存在 $PG(3,q)$ 中 $n$ 个点的有序排列，使得任意循环连续的四个点不共面。*

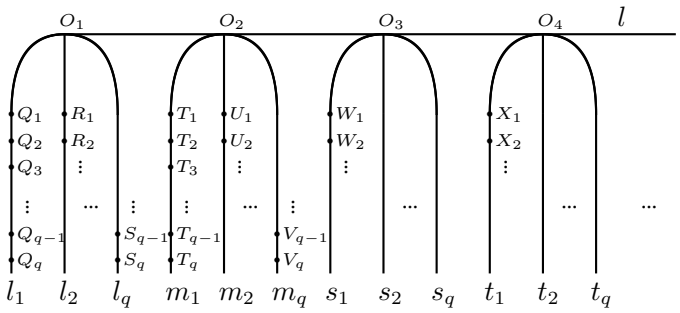


**图 3-2 射影空间 $PG(3,q)$ 的结构**

**证明** 固定一条线 $l$，记过 $l$ 的 $q+1$ 个面分别为 $\pi_0,\cdots,\pi_q$。在图 3-2 中我们展示了其中四个，记线 $l,l_1,l_2,\cdots,l_q$ 构成的面为 $\pi_0$，紧接着的三个面为 $\pi_1,\pi_2,\pi_3$。我们给出其中一种排序的策略。

- $q$ 是奇数

这种情况下过 $l$ 有偶数个面，分别记作为 $\pi_0,\cdots,\pi_q$。选择 $O_1,O_2$ 作为前两个点，然后从线 $l_1$ 和 $m_1$ 上轮流选点。假设我们已经将点排列为 $O_1,O_2,Q_1,T_1,Q_2,\cdots,T_{q-1},Q_q,T_q$，显然地，$O_1,O_2,Q_1,T_1$ 不共面，$O_2,Q_1,T_1,Q_2$ 也不共面。对于其它的任意连续四个点，我们有其中两个点落在 $l_1$ 上，另外两个落在 $m_1$ 上。如果这四个点共面，则 $l_1$ 和 $m_1$ 交于一点。假设它们交于点 $O'$，那么点 $O'$ 落在面 $\pi_0$ 和 $\pi_1$ 上，因此 $O'$ 也落在 $l$ 上，矛盾。综上，我们有任意连续四个点不共面。

接着我们选择三个点 $R_1,U_1,R_2$ 使得它们分别不落在面 $Q_qT_{q-1}T_q$, $Q_qT_qR_1$, $T_qR_1U_1$ 上。然后我们轮流地从线 $l_2$ 和 $m_2$ 上选点，我们可以一直这么做直到我们排列完了线 $l_1,\cdots,l_q,m_1,\cdots,m_q$ 上的所有点。

假设我们已经将点排列为 $O_1,O_2,Q_1,T_1,\cdots,S_{q-1},V_{q-1},S_q,V_q$。我们选择接下来的六个点为 $O_3,O_4,W_1,X_1,W_2,X_2$，其中 $W_1,W_2$ 是 $s_1$ 上的任意两个点，$X_1,X_2$ 是 $t_1$ 上的任意两个点。然后，我们可以同样地给 $\pi_2$ 和 $\pi_3$ 中的点排序。我们可以重复这样的过程直到我们排列完了所要求的 $n$ 个点，$4\le n\le q^3+q^2+q+1$。

在之前的步骤里，我们排列了 $n$ 个点使得任意连续四个不共面。那么为了达到循环连续的要求，我们需要考虑这个有序排列的末尾部分。记最后的四个点为 $P_{n-4},P_{n-3},P_{n-2}$ 和 $P_{n-1}$，也就是说我们要确保以下几点：

(1) $P_{n-1},O_1,O_2,Q_1$ 不共面

这一点只有当 $P_{n-1}$ 落在 $\pi_0$ 上时才会不满足，即当 $5\le n\le 2q^2+1$ 且 $n$ 是奇数时。在这种情况下，我们选择一个不落在 $\pi_0,\pi_1,P_{n-4}P_{n-3}P_{n-2}$ 和 $P_{n-3}P_{n-2}O_1$ 上的点作为新的最后一个点，而这是肯定可以做到的。

(2) $P_{n-2}, P_{n-1}, O_1, O_2$ 不共面

在我们的策略里，这一点是可以保证的，因为 $P_{n-2}$, $P_{n-1}$ 是从不同的面 $\pi_i$ 上选取的。

(3) $P_{n-3}, P_{n-2}, P_{n-1}, O_1$ 不共面

如果 $P_{n-3}$, $P_{n-1}$ 落在线 $l_i$ 上，$1 \leq i \leq q$，那么我们可以和情况 (1) 一样处理。否则，只有当 $P_{n-3}$, $P_{n-2}$, $P_{n-1}$ 来自三条不同的线时，它们才可能与点 $O_1$共面。比如， $T_q$, $R_1, U_1$ 分别取自 $m_1, l_2, m_2$。在这种情况下，因为剩下来的点足够多，我们始终可以找到一个新的合适的点来代替。

• $q$ 是偶数

这种情况与 $q$ 是奇数的情况的不同之处在于我们考虑的面的数目为奇数。当 $n \leq q^3+q$ 时，我们选取偶数个面，然后像 $q$ 是奇数的情况一样操作。当 $n > q^3 + q$ 时，我们首先将线 $l_1, \cdots, l_q, m_1, \cdots, m_q, s_1, \cdots, s_q$ 上的点排序，然后剩下来的偶数个面就和之前一样操作。注意到我们有 $3q$ 条线，是一个偶数，所以我们仍然可以成对地考虑不同平面 $\pi_i$ 中的线，$i = 0, 1, 2$，排序方法和上一种情况类似。同样地，我们可以给 $n$ 个点排序，$4 \leq n \leq q^3 + q^2 + q + 1$，使得任意循环连续的四个点不共面。 □

例 3.3.7 我们可以给 $PG(3, 2)$ 中的 $4 \leq n \leq 15$ 个点排序，使得任意循环连续的四个点不共面，如表 3-2 所示，其中 $H$ 的前 $n$ 列表示的是排列好的 $n$ 个点。

结合引理 3.3.2，3.3.6 和例子 3.3.7，我们可以得出以下定理。

**定理 3.3.8** 对任意素数幂 $q$，$7 \leq n \leq q^3 + q^2 + q + 1$，总是存在线性的 *MDS* $(n, 7)_q$ 3-字符码。

### 3.3.3 $b = 4, d_4 = 9$

从引理 3.3.1 我们知道，4 维射影空间 $PG(4, q)$ 中的所有点被 $(q+1)$ 个 3 维射影子空间所覆盖，这些子空间相交于一个平面，就如图 3-3 所示。线 $l_0, l_1, \cdots, l_q$ 交于一点 $O$ 且构成一个面 $\pi$。同样地，$\{l_0, m_{11}, m_{12}, \cdots, m_{1q}\}, \{l_0, m_{21}, m_{22}, \cdots, m_{2q}\}, \cdots, \{l_0, m_{q1}, m_{q2}, \cdots, m_{qq}\}$ 分别构成面 $\pi_{01}, \pi_{02}, \cdots, \pi_{0q}$。面 $\pi, \pi_{01}, \cdots, \pi_{0q}$ 相交于 $l_0$ 且共同构成了 3 维空间 $V_0$。总体上，我们有 $q+1$ 个这样的子空间，记作为 $V_0, V_1, \cdots, V_q$，它们相交于面 $\pi$ 且共同构成了 $PG(4, q)$。

**表 3-2 射影空间 $PG(3,2)$ 中点的有序排列**

| $n$ | $H$ |
|---|---|
| 5 | $\begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$ |
| 7 | $\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$ |
| 8 | $\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$ |
| 10 | $\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ |
| 13 | $\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$ |
| $4,6,9,11,12,14,15$ | $\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$ |

在射影平面 $PG(2,q)$ 中，我们给点排序使得任意循环连续的三个点不共线。为了达到这个目的，我们交替地从不同的线取点。在之后，在 $PG(3,q)$中，我们给点排序使得任意循环连续的四个点不共面，为此我们从不相交的线上轮流地取点。给 $PG(4,q)$ 中的点排序使得任意循环连续的五个点不包含在一个 3 维射影空间中是一个更加复杂和繁琐的问题，然而大体的思路是很类似的，因此我们只描述一个大致的想法，具体的细节并不逐一讨论。

**引理 3.3.9** *对任意素数幂 $q \geq 3$，$5 \leq n \leq q^4+q^3+q^2+q+1$，都存在 $PG(4,q)$ 中 $n$ 个点的有序排列，使得任意循环连续的五个点不包含在一个 3 维射影空间中。*

**证明** 我们沿用图 3-3 中的记号。注意到在每个 3 维空间 $V_i$ 中，$0 \leq i \leq q$，总共有 $q+1$ 个面（包括 $\pi$）相交于一条线。除了面 $\pi$ 我们记 $V_i$ 中剩下的 $q$ 个面分别为 $\pi_{i1}, \cdots, \pi_{iq}$。选取 $O$ 作为第一个点。注意到对同一个面 $\pi_{ij}$ 中的两条线而言，就比如 $m_{11}$ 和 $m_{12}$，如果我们将 $m_{11}$ 中的每个点与 $O$ 相连，那么我们就得到了 $q+1$ 条线，每条线与 $m_{12}$ 交且仅交于一点。换言之，我们可以建立同一个面 $\pi_{ij}$ 上任意两条线上的点的一一对应。考虑 $\pi_{ij} \setminus l_i$ 中

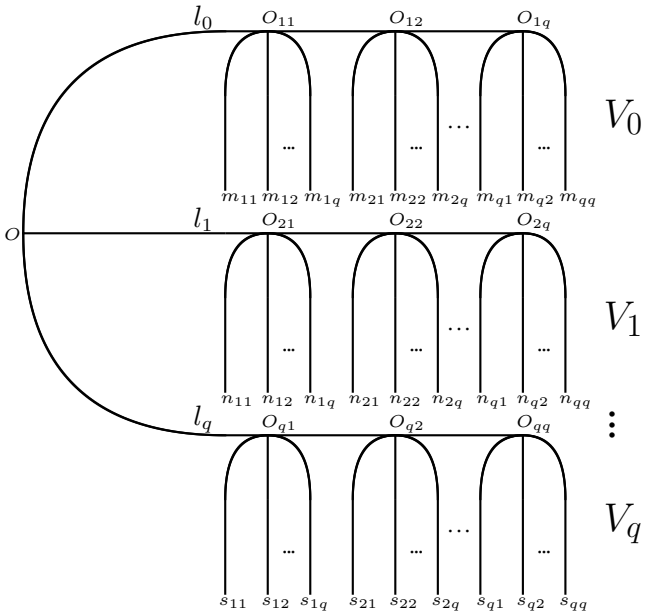


**图 3-3　射影空间 $PG(4,q)$ 的结构.**

的点，比如 $m_{11},\cdots,m_{1q}$ 上的点。模仿引理 3.3.4 中的做法，我们可以很轻易地给这些点排序使得任意连续三个点不共线。此外，我们还添加另外一个要求，希望任意连续的两个点与 $O$ 不共线，而经过上述的讨论，这一点也是可以做到的。

选取两个面 $\pi_{ij}$ 和 $\pi_{st}$ $(i\neq s)$，假设我们已经将两个面上的点排列为 $P_0,\cdots,P_{q^2}$ 和 $Q_0,\cdots,Q_{q^2}$。在此基础上，我们从两个序列中轮流地选点，排列为 $P_0,Q_0,P_1,Q_1,\cdots,P_{q^2}$，$Q_{q^2}$。如果我们任意选择连续的五个点，那么可知其中三个形成一个面 $\pi_{ij}$ 或者 $\pi_{st}$，另外两个形成一条不过 $O$ 的线。因为在 3 维射影空间中，如果面和线相关联，那么面必定包含整条线；面外的一条线是必定与面相交于一点的。所以，我们可知任意连续的五个点都不包含在一个 3 维空间中。$\pi_{ij}$ 这样的面的数目是 $q(q+1)$，是一个偶数。因此，我们可以一直成对地考虑来自不同空间 $V_i$ 的面。与引理 3.3.4 和 3.3.6 类似，我们可以重复这个过程，直到我们已经将 $n$ 个点排序，$5\leq n\leq q^4+q^3+q^2+q+1$，使得任意循环连续的五个点不落在一个 3 维空间中。 □

结合引理 3.3.2 和引理 3.3.9，我们就可以得到如下结论。

**定理 3.3.10** *对任意素数幂 $q\geq 3$，$9\leq n\leq q^4+q^3+q^2+q+1$，总是存在线性的 MDS $(n,9)_q$ 4-字符码。*

### 3.3.4 更多的构造

首先对于一般的 $b \geq 5$ 我们说明 MDS $b$-字符码的存在性，这个结果当 $q$ 远大于 $b$ 时表现很好。

**定理 3.3.11** *对任意素数幂 $q$，$q \geq b \geq 5$，$2b+1 \leq n \leq q^b - bq^{b-1} + \frac{b^2+3b}{2}$，总是存在线性的 MDS $(n, 2b+1)_q$ $b$-字符码。*

**证明** 根据引理 3.3.2，我们的主要任务是给 $PG(b,q)$ 中的 $n$ 个点排序，使得任意循环连续的 $b+1$ 个点不包含在一个 $(b-1)$ 维空间中。首先在 $PG(b,q)$ 中，我们显然可以找到 $b+1$ 个点张成整个空间。假设我们已经排序了 $k$ 个点，$b+1 \leq k < q^b - bq^{b-1} + 2b$，记为 $P_1, P_2, \cdots, P_k$，使得任意循环连续的 $b+1$ 个点不落在一个 $(b-1)$ 维空间中。

考虑 $\{P_{k-b+1}, P_{k-b+2}, \cdots, P_k\}$, $\{P_{k-b+2}, P_{k-b+3}, \cdots, P_k, P_1\}$, $\cdots$, $\{P_1, P_2, \cdots, P_b\}$ 张成的 $b+1$ 个 $(b-1)$ 维空间，分别记作为 $V_0, V_1, \cdots, V_b$。如果剩下来的点，即 $PG(b,q) \setminus \{P_1, P_2, \cdots, P_k\}$ 中的点没有被 $V_0, V_1, \cdots, V_b$ 完全覆盖，那么我们始终可以找到一个新的点 $P_{k+1}$。

接下来，我们就来考虑上述的 $b+1$ 个空间所能覆盖的剩下的点的最大数目。因为 $PG(b,q)$ 中的两个 $(b-1)$ 维子空间必然交于一个 $(b-2)$ 维空间，所以 $V_0$ 覆盖了 $\frac{q^b-1}{q-1}$ 个点，而其它 $V_i$ 至多覆盖 $\frac{q^b-1}{q-1} - \frac{q^{b-1}-1}{q-1}$ 个新的点。同时，当我们计算点的数目时还需要排除 $P_{k-b+1}, P_{k-b+2}, \cdots, P_k, P_1, \cdots, P_b$ 这些点。比如，在计算 $V_0$ 中点的数目时，我们需要排除 $P_{k-b+1}, P_{k-b+2}, \cdots, P_k$ 这些点。而当我们计算 $V_1$ 中点的数目时，我们只需要排除点 $P_1$，因为 $P_{k-b+2}, \cdots, P_k$ 这些点落在 $V_0$ 和 $V_1$ 的交中。当 $k < 2b$ 时，$P_{k-b+1}, P_{k-b+2}, \cdots, P_k, P_1, \cdots, P_b$ 这 $2b$ 个点可能有重合的情况，因此当 $k = b+1$ 时，我们所应该排除的点的数目取最小值 $2b$。所以 $b+1$ 个射影空间 $V_0, V_1, \cdots, V_b$ 至多覆盖 $PG(b,q) \setminus \{P_1, P_2, \cdots, P_k\}$ 中的 $(b+1)\frac{q^b-1}{q-1} - b\frac{q^{b-1}-1}{q-1} - 2b$ 个点。所以当 $k < q^b - bq^{b-1} + 2b$ 时，我们始终可以发现一个新的合适的点 $P_{k+1}$。

因为 $q \geq b$，所以由上述讨论，我们始终可以有序排列 $2b$ 个点，使得任意循环连续的 $b+1$ 个点不包含于一个 $(b-1)$ 维空间中。假设我们已经排列了至少 $2b$ 个点，即 $k \geq 2b$。此时，$P_{k-b+1}, P_{k-b+2}, \cdots, P_k, P_1, \cdots, P_b$ 中的点是不会重合的，$b+1$ 个 $(b-1)$ 维空间至多覆盖 $(b+1)\frac{q^b-1}{q-1} - b\frac{q^{b-1}-1}{q-1} - \frac{b^2+3b}{2}$ 个 $PG(b,q) \setminus \{P_1, P_2, \cdots, P_k\}$ 中的点。由此得证。 □

根据定理 3.2.6，如果我们令 $d = 2$ 且考虑向量空间 $V(b,q)$ 中的向量作为 $H$ 的列向量，那么我们可以得到如下引理。

**引理 3.3.12** 如果存在向量空间 $V(b,q)$ 中 $n \geq 2b$ 个向量的有序排列使得任意循环连续的 $b$个向量线性无关，那么就存在一个线性的 *MDS* $(n,2b)_q$ $b$-字符码。

类似于定理 3.3.11，我们可以导出如下的定理。

**定理 3.3.13** 对任意素数幂 $q \geq b-1, b \geq 3$ 或者 $q=2, b=4$，总是存在长度 $n \geq 2b$ 的 *MDS* $(n,2b)_q$ $b$-字符码。

**证明** 在一个 $b$ 维向量空间 $V(b,q)$ 中，显然我们可以找到 $b$ 个向量张成整个空间。假设我们已经有 $k \geq b$ 个向量的有序排列，记作 $v_1, v_2, \cdots, v_k$，使得任意循环连续的 $b$ 个向量线性无关。

首先，我们考虑 $\{v_{k-b+2}, v_{k-b+3}, \cdots, v_k\}, \{v_{k-b+3}, v_{k-b+4}, \cdots, v_k, v_1\}, \cdots, \{v_1, v_2, \cdots, v_{b-1}\}$ 张成的 $(b-1)$ 维子空间，分别记作为 $V_1, V_2, \cdots, V_b$。两个 $(b-1)$ 维空间必定交于一个 $(b-2)$ 维向量空间。接着我们考虑上述空间所能覆盖的向量的最大数目。$V_1$ 覆盖了 $q^{b-1}-1$ 个非零向量，其它的 $V_i$ 覆盖至多 $q^{b-1}-q^{b-2}$ 个新的非零向量，$2 \leq i \leq b$。同时，当我们计数时应该排除 $v_{k-b+2}, \cdots, v_k, \cdots, v_1, v_{b-1}$ 这些点。因此，它们总共可以覆盖 $bq^{b-1}-(b-1)q^{b-2}-2(b-1)-1$ 个非零向量。除非所有的非零向量都被上述的 $b$ 个向量空间覆盖，否则我们始终可以找到一个新的合适的点 $v_{k+1}$。换言之，如果 $q^b - bq^{b-1} + (b-1)q^{b-2} + 2(b-1) \geq 1$，我们始终可以找到一个新的合适的点，也就是说 $q \geq b-1$ 或者 $q=2, b=4$。 □

**注解 3** 文献[55] 中的作者通过交替的技巧也构造了 $d_b = 2b$ 的 $b$-字符码。但是他们构造的码字的长度必须是 $b$ 的倍数，而我们的并没有这个限制。

在上述的过程中，对于 $b=2,3,4$，$2b+1 \leq n \leq \frac{q^{b+1}-1}{q-1}$，我们给出了 $PG(b,q)$ 中 $n$ 个点的有序排列，使得任意循环连续的 $b+1$ 个点线性无关。而下面这个结果则表明如果我们排列点时足够仔细，定理 3.3.13 中 $q \geq b-1$ 这个条件并不是必要的。

**定理 3.3.14** 对于任意素数幂 $q \geq 3$，$n \geq 10$，总是存在线性的 *MDS* $(n,10)_q$ 5-字符码。

**证明** 对于 $n \geq 10$，我们总是可以找到整数 $n_1, n_2, \cdots, n_t$ 使得 $n = n_1 + n_2 + \cdots + n_t$，其中 $t \geq 2$，$5 \leq n_i \leq \frac{q^5-1}{q-1}$。由之前的讨论可知，我们可以找到 $PG(4,q)$ 中的 $t$ 个有序排列，

记作 $S_1, S_2, \cdots, S_t$，每个序列分别有 $n_i$ 个点且任意循环连续的 5 个点线性无关。令这些序列的前 4 个点都相同，这是很容易做到的，然后将这些序列首尾串联起来就得到我们需要的 $n$ 长的序列。 □

## 3.4 利用常循环码构造 MDS $b$-字符码

一个 $q$ 元长度为 $n$ 的线性码 $\mathcal{C}$ 被称作为 $\eta$-常循环的，$\eta \in \mathbb{F}_q^*$，如果它在如下的 $\mathbb{F}_q^n$ 上的 $\eta$-常循环移动后是不变的：

$$(c_0, c_1, \cdots, c_{n-1}) \to (\eta c_{n-1}, c_0, \cdots, c_{n-2}).$$

如果我们把每个码字 $c = (c_0, c_1, \cdots, c_{n-1})$ 写作多项式表示形式 $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$，那么一个 $\eta$-常循环码就可以看作商环 $\mathbb{F}_q[x]/\langle x^n - \eta\rangle$ 的理想，$xc(x)$ 则对应着 $c(x)$ 的 $\eta$-常循环移动。此外，$\mathbb{F}_q[x]/\langle x^n - \eta\rangle$ 是一个主理想环，$\mathcal{C}$ 是由 $x^n - \eta$ 的首一因子 $g(x)$ 生成。我们称 $g(x)$ 为 $\mathcal{C}$ 的生成多项式，记作 $\mathcal{C} = \langle g(x)\rangle$。

令 $\eta \in \mathbb{F}_q$ 为 $r$ 次本原单位根。因为 $\gcd(n, q) = 1$，故在 $\mathbb{F}_q$ 的扩域中存在一个 $rn$ 次本原单位根 $\omega$，使得 $\omega^n = \eta$。由此可得，

$$x^n - \eta = \prod_{i=0}^{n-1}(x - \omega^{1+ir}).$$

令 $\Omega = \{1 + ir | 0 \le i \le n-1\}$。对任意 $j \in \Omega$，取 $\mathcal{C}_j$ 为包含 $j$ 的模 $rn$ 的 $q$-分圆陪集。令 $\mathcal{C}$ 为有限域 $\mathbb{F}_q$ 上 $g(x)$ 生成的长度为 $n$ 的 $\eta$-常循环码。那么集合 $Z = \{j \in \Omega | g(\omega^j) = 0\}$ 称作为 $\mathcal{C}$ 的定义集。我们可知 $\mathcal{C}$ 的定义集是一些模 $rn$ 的 $q$-分圆陪集的并，且满足 $\dim(\mathcal{C}) = n - |Z|$。

与循环码类似，对于常循环码也有如下 BCH 界。

**定理 3.4.1** （常循环码的 BCH 界[31]） *$\mathcal{C}$ 为有限域 $\mathbb{F}_q$ 上长度为 $n$ 的 $\eta$-常循环码，其中 $\eta \in \mathbb{F}_q$ 为 $r$ 次本原单位根。令 $\omega$ 为 $\mathbb{F}_q$ 的扩域中的一个 $rn$ 次本原单位根使得 $\omega^n = \eta$。假设 $\mathcal{C}$ 的生成多项式的根包含以下集合 $\{\omega^{1+ri} | i_1 \le i \le i_1 + d - 2\}$，那么 $\mathcal{C}$ 的最小 Hamming 距离为 $d$。*

本章的其它构造提供了相当丰富的参数，与它们不同的是，我们接下来的这个构造只关注 $n = \frac{q^{b+1}-1}{q-1}$ 的情形。我们这么做主要是想给我们之后提出的两个猜想提供足够的支撑。

**定理 3.4.2** 对任意素数幂 $q$，$b \geq 4$，总是存在线性的 *MDS* $(\frac{q^{b+1}-1}{q-1}, 2b+1)_q$ $b$-字符码。

**证明** 取 $n = \frac{q^{b+1}-1}{q-1}$，$\omega$ 为 $\mathbb{F}_q$ 的本原元，$\delta$ 是 $\mathbb{F}_{q^{b+1}}$ 的本原元使得 $\delta^n = \omega$。注意到 $g(x) = (x-\delta)(x-\delta^q)\cdots(x-\delta^{q^b}) \in \mathbb{F}_q[x]$ 整除 $x^n - \omega$。令 $\mathcal{C}$ 为 $\langle g(x)\rangle \subseteq \mathbb{F}_q[x]/(x^n-\omega)$，那么 $\mathcal{C}$ 是一个参数为 $[n, n-b-1, d]_q$ 的线性码，其中 $3 \leq d \leq b+2$。

如果 $d = b+2$，那么显然 $d_b \geq 2b+1$。

如果 $3 \leq d \leq b+1$，令 $c(x) = \sum_{i=0}^{n-1} c_i x^i$ 为 $\mathcal{C}$ 中一个非零码字。如果存在 $j$ 使得 $c_j = c_{j+1} = \cdots = c_{j+b-2} = 0$，$c_{j+b-1} \neq 0$，其中下标都是在模 $n$ 的意义下取值，那么对于某些 $a_i \in \mathbb{F}_q$, $t \leq n-b$, $a_0, a_t \neq 0$, $x^{n-j-b+1}c(x) = \sum_{i=0}^{t} a_i x^i \in \mathcal{C}$。因为 $g(x)|c(x)$，故 $3 \leq d \leq b+1, t \geq b+1$，因此我们有 $wt_b(x^{n-j-b+1}c(x)) = wt_b(c(x)) \geq 2b+1$。如果不存在 $j$ 使得$c_j = c_{j+1} = \cdots = c_{j+b-2} = 0, c_{j+b-1} \neq 0$，那么显然 $wt_b(c(x)) = n$。综上所述，$d_b \geq 2b+1$。 □

## 3.5 总结

在本章中，我们建立了 $b$-字符码的 Singleton 界，并且我们说明了一个线性的 MDS $b$-字符码如果同时满足 $d_b < n$，那么它也是一个 MDS $(b+1)$-字符码。我们给出了 MDS $b$-字符码存在性的一个充分条件，只要我们找到一个合适的矩阵，那么相应地我们就可以构造一个 MDS $b$-字符码。在特定条件下，这个充分条件转化成给 $PG(b,q)$ 中的点的排序问题，我们要求将点有序排列使得任意循环连续的 $b+1$ 个点不落在一个 $(b-1)$ 维射影空间中。在此基础上，我们构造了几类 MDS $b$-字符码，对于特定的参数，我们完全决定了 MDS $b$-字符码的存在性。

我们在构造码的过程中所用的方法是很有趣的，也很值得进一步的研究。考虑我们根据引理 3.3.1 所建立的结构，我们的主要目标是给 $PG(b,q)$ 中的点有序排列，使得任意循环连续的 $b+1$ 个点不落在一个 $(b-1)$ 维的射影空间中。我们的主要思路大体如下，当 $b$ 是偶数时，在 $PG(b,q)$ 中任意两个来自不同 $(b-1)$ 维射影子空间中的 $\frac{b}{2}$ 维射影子空间相交于一点。例如，当 $b=2$ 时，任意两条线交于一点；当 $b=4$ 时，$\pi_{ij}$ 和 $\pi_{st}$ 交于点 $O$ $(i \neq s)$。对于一对 $\frac{b}{2}$ 维射影空间，我们首先单独将每个空间中的点排序使得任意连续 $\frac{b}{2}+1$ 个点张成对应的空间，然后我们再从这两个有序序列中交替地选点，就像我们在引理 3.3.4 和引理 3.3.9 中做的那样。当 $b$ 是奇数时，$PG(b,q)$ 中任意两个来自不同 $(b-1)$ 维射影子空间的 $\frac{b-1}{2}$ 维射影子空间没有交集。例如，当 $b=3$ 时，在引理 3.3.1 建立的结构中，不同面上的线之间没有交集。同样地，对于一对 $\frac{b-1}{2}$ 维射影子空间，我们首先单独将每个空间

中的点排序使得任意连续 $\frac{b-1}{2}+1$ 个点张成对应的空间，然后我们再从这两个有序序列中交替地取点，就好比我们在引理 3.3.6 中做的那样。

通过上述的讨论，我们看似可以给定一个策略或者说一个算法，对任意 $b$ 都可以给 $PG(b,q)$ 中的点排序使其达到我们的要求，进而对任意 $b$，$2b+1 \leq n \leq \frac{q^{b+1}-1}{q-1}$ 构造线性的 MDS $(n, 2b+1)_q$ $b$-字符码。然而，就我们目前的尝试来看，我们相信这样的一个严格证明会是很复杂和繁琐的，我们更愿意将这写作猜想的形式，以期可以找到一个更加简洁明了的证明。

**猜想 1** *对任意素数幂 $q$，$b>2$，$2b+1 \leq n \leq \frac{q^{b+1}-1}{q-1}$，总是存在线性的 MDS $(n, 2b+1)_q$ $b$-字符码。*

仿照之前小节 3.3.4 中的讨论我们也有以下的猜想。

**猜想 2** *对任意素数幂 $q$，$b>2$，$n \geq 2b$，总是存在线性的 MDS $(n, 2b)_q$ $b$-字符码。*

# 4 光正交签名码

## 4.1 介绍

光码分多址（OCDMA）技术使用具有良好相关性质的扩频序列来识别每个用户，将不同的用户接入到相同的频带和时隙上，进而可以允许多个用户共享同一个光纤信道，有效提高系统总容量[21][45][46][53]。光正交码（OOC）就是这样一类可以应用到 OCDMA 系统中的具有良好相关性质的扩频序列。空间的 OCDMA 是将 OCDMA 扩展到一个二维空间用以传输图像与多路访问，相关的基础知识和应用可以参考[33][44][58]。Kitayama 和他的同事[32][34] 演示证明了给二维像素阵列编码的途径与方法。这个二维图像多路传输技术可以应用于医学图像的传输等许多实际问题中[44][58]。在空间的 OCDMA 中，每个放大的二维位平面都可以用一个 $(0,1)$ 矩阵来编码，这样的矩阵我们称作为二维光正交签名（OOSP），更多的细节请参考[28][32]。

文献[32] 中指出，空间的 OCDMA 的一个关键点在于二维光正交签名的构造。OOSP 的构造与 OCDMA 中码的构造相类似，都有着相关性和码字数目的要求。每个 OOSP 在一个二维平面上移动后与它本身都应该是可区分的（自相关性），任意两个不同的 OOSP 在移动后也应该同样是可区分的（互相关性）[28][32]。这些限制条件要求相关性应该比 OOSP 的重量（1 的数目）小很多。现在我们首先来介绍光正交签名码的定义。

取正整数 $m,n,w,\lambda$ 满足 $mn > w \geq \lambda$。$(m,n,w,\lambda)$-光正交签名码（OOSPC）$\mathcal{C}$ 是一族 $m \times n$ 的二元矩阵（码字）的集合，所有码字的 Hamming 重量（1 的数目）均为 $w$ 且满足下述两个相关性性质：

(1)（自相关性）

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{i,j}a_{i\oplus_m\delta,j\oplus_n\tau} \leq \lambda$$

对所有 $A=(a_{i,j}) \in \mathcal{C}$ $(0 \leq i \leq m-1, 0 \leq j \leq n-1)$，所有整数 $\delta$ 和 $\tau$，$0 \leq \delta < m$，$0 \leq \tau < n$，$(\delta,\tau) \neq (0,0)$ 成立；

(2)（互相关性）

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{i,j}b_{i\oplus_m\delta,j\oplus_n\tau} \le \lambda$$

对任意两个不同的矩阵 $A=(a_{i,j})$，$B=(b_{i,j})\in\mathcal{C}$ $(0\le i\le m-1, 0\le j\le n-1)$，所有整数 $\delta$ 和 $\tau$，$0\le\delta<m$，$0\le\tau<n$ 成立，其中 $\oplus_m$（或者 $\oplus_n$）表示的是模 $m$（或者模 $n$）的加法，且上述任意一个不等式至少存在一种情况使得等号成立。

用 $\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{i,j}a_{i,j\oplus_n\tau}\le\lambda\,(0<\tau<n)$ 替代自相关性质，用 $\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} a_{i,j}b_{i,j\oplus_n\tau}\le\lambda\,(0\le\tau<n)$ 替代互相关性质时，对应的是二维光正交码（2-D $(m\times n,w,\lambda)$-OOC）。显然，循环移动一个大小为 $b$ 的 $(m,n,w,\lambda)$-OOSPC 的行之后我们就可以得到一个大小为 $mb$ 的 2-D $(m\times n,w,\lambda)$-OOC。而一般情况下，我们是不能从二维光正交码得到光正交签名码的。关于最优 2-D $(m\times n,w,\lambda)$-OOC 的构造参见[1][3][6][7][25][29][40][52][57]。当 $m=1$，$n=v$ 时，一个 2-D $(m,n,w,\lambda)$-OOSPC 实际上就是一个一维 $(v,w,\lambda)$ 光正交码（简记为 1-D $(v,w,\lambda)$-OOC）。更多关于 1-D OOC 的结论，请参考文献[5][4][15][20][26][38][47][51]。

对任意二元矩阵 $A=(a_{ij})\in\mathcal{C}$，其中行用 $\mathbb{Z}_m$，列用 $\mathbb{Z}_n$ 作为索引，我们定义集合 $X_A=\{(i,j)\in\mathbb{Z}_m\times\mathbb{Z}_n : a_{ij}=1\}$。那么，$\mathcal{F}=\{X_A : A\in\mathcal{C}\}$ 其实就是 $(m,n,w,\lambda)$-OOSPC 的一个集合论表示。所以一个 $(m,n,w,\lambda)$-OOSPC 就可以看作 $\mathbb{Z}_m\times\mathbb{Z}_n$ 中 $w$-子集的集合，且相关性性质如下：

$(1')$（自相关性）

$$|X\cap(X+(\delta,\tau))|\le\lambda$$

对所有 $X\in\mathcal{F}$ 和 $(\delta,\tau)\in\mathbb{Z}_m\times\mathbb{Z}_n\setminus\{(0,0)\}$ 成立；

$(2')$（互相关性）

$$|X\cap(Y+(\delta,\tau))|\le\lambda$$

对不同的 $X,Y\in\mathcal{F}$ 和任意$(\delta,\tau)\in\mathbb{Z}_m\times\mathbb{Z}_n$ 成立。

OOSPC 中码字的数目称为它的大小。对于给定的 $m,n,w,\lambda$，令 $\Theta(m,n,w,\lambda)$ 表示所有 $(m,n,w,\lambda)$-OOSPC 可能的最大的大小。一个大小为 $\Theta(m,n,w,\lambda)$ 的 $(m,n,w,\lambda)$-OOSPC 被称为是最优的。基于常重码的 Johnson 界[30] 我们可以得出如下关于 $\Theta(m,n,w,\lambda)$ 的界：

$$\begin{aligned}\Theta(m,n,w,\lambda) &\le J(m,n,w,\lambda)\\ &= \left\lfloor\tfrac{1}{w}\left\lfloor\tfrac{mn-1}{w-1}\left\lfloor\tfrac{mn-2}{w-2}\left\lfloor\cdots\left\lfloor\tfrac{mn-\lambda}{w-\lambda}\right\rfloor\cdots\right\rfloor\right\rfloor\right\rfloor\right\rfloor.\end{aligned}\tag{4-1}$$

文献[48] 中指出，一个大小为 $u$ 的 $(m,n,w,\lambda)$-OOSPC 等价于一个基区组数目为 $u$ 的严格 $\mathbb{Z}_m\times\mathbb{Z}_n$-不变的 $(\lambda+1)$-$(mn,w,1)$ 填充设计。当 $m$ 和 $n$ 互素时，$(m,n,w,\lambda)$-OOSPC 实际上是一个 1-D $(mn,w,\lambda)$-OOC[56]。然而当 $m$ 和 $n$ 不互素时，构造最优 $(m,n,w,\lambda)$-OOSPC

**表 4-1　渐近最优的光正交签名码**

| 参数 | 条件 | 大小 | 出处 |
|---|---|---|---|
| $(m,n,4,2)$ | 无限制 | | 文献[48] |
| $(p,p,p+1,2)$ | $p\geq 3$ 且为素数 | $p-1$ （最优） | 文献[12] |
| $(p,p,p,\lambda)$ | $p\geq 3$ 且为素数，$2\leq\lambda<p$ | $p^{\lambda-1}-1$ | 定理 4.2.2 |
| $(q-1,n,n-\lambda,\lambda)$ | $q$ 是素数幂，<br>$q-1\equiv 0\pmod n, n>2\lambda$ | $\frac{1}{n}\sum_{e_1=0}^{\lambda}\sum_{d\mid n}q^{\lfloor\frac{\lambda-e_1}{d}\rfloor}\mu(d)$ | 定理 4.2.6 |
| $(q-1,q_1^2-1,q_1-1,2)$ | $q,q_1$ 是素数幂，$q\geq q_1^2$ | $q^2q_1$ | 例 4.2.10 |
| $(q+1,n,n,2\lambda)$ | $q$ 是素数幂，<br>$q-1\equiv 0\pmod n, n>2\lambda$ | $\frac{\lvert\widetilde{\mathcal{F}_\lambda}\rvert}{n(q+1)}$ | 定理 4.3.3 |
| $(p^m,p^n,p,\lambda)$ | $p\geq 3$ 是素数，$2\leq\lambda<p$<br>$m,n$ 是正整数 | $(p^{\lambda-1}-1)p^{m\lambda+n\lambda-2\lambda}$ | 推论 4.4.9 |
| $(p^m,p^n,p+1,2)$ | $p$ 是素数，$m,n$ 是正整数 | $(p-1)p^{2m+2n-4}$ | 推论 4.4.10 |
| $(m'p^m,n'p^n,p,\lambda)$ | $p$ 是素数，$2\leq\lambda<p$，$m,m',n,n'$ 是正整数，$m'n'$ 的最小素因子不小于 $p$ | $(p^{\lambda-1}-1)p^{m\lambda+n\lambda-2\lambda}\cdot(m'n')^{\lambda}$ | 推论 4.4.11 |

便变得很难，这也是我们的兴趣所在。就目前而言，许多组合方法都被用来构造最优 OOSPC，如差填充[41][42][56]，Steiner 四元系[48] 以及 $G$-设计[12] 等。

同理于渐近最优的 1-D OOC[17][18]，构造渐近最优的 OOSPC 也是一个有趣的话题。一个 $(m,n,w,\lambda)$-OOSPC $\mathcal{C}$ 被称作为渐近最优的如果它满足：

$$\lim_{m,n\to\infty}\frac{|\mathcal{C}|}{J(m,n,w,\lambda)}=1.$$

就我们所知，唯一一类渐近最优的 OOSPC 是由 Sawa[48] 通过渐近最优的 1-D $(m,4,2)$-OOC 得出的。

Omrani[40] 等利用有限域上的多项式和有理函数构造了几类渐近最优的 2-D OOC。Chu 和 Golomb[14] 利用 $r$-简单矩阵构造了几类渐近最优的 OOC。在本章中，我们利用多项式方法，有理函数以及 $r$-简单矩阵来直接构造和递归构造 OOSPC，所得的码与已有的组合构造不同且有着一般化的重量参数。从而，我们得到了几类新的渐近最优的 OOSPC，如表 4-1 中所示。

## 4.2 基于多项式函数的渐近最优构造

在本节中，我们利用多项式函数得到三类渐近最优的 OOSPC。

### 4.2.1 $(p,p,p,\lambda)$-OOSPC

取素数 $p \geq 3$，对 $\mathbb{Z}_p$ 上的任意多项式 $f(x)$，定义其关联矩阵为

$$C(i,j) = 1 \text{ 当且仅当 } f(j) = i, \tag{4-2}$$

其中 $(i,j) \in \mathbb{Z}_p \times \mathbb{Z}_p$。

**构造 4.2.1** 取素数 $p \geq 3$，整数 $\lambda$ 满足 $2 \leq \lambda < p$。令 $\mathcal{G}_\lambda$ 为 $\mathbb{Z}_p$ 上所有满足 $2 \leq deg(f(x)) \leq \lambda$ 的非零多项式 $f(x)$ 的集合。$\mathcal{G}_\lambda$ 中两个多项式 $f(x)$ 和 $g(x)$ 是等价的当且仅当 $f(x+k)+l = g(x)$ 对某些 $k,l \in \mathbb{Z}_p$ 成立。令 $\mathcal{G}_\mathcal{C}$ 是从每个等价类中取一个多项式后组成的集合，$\mathcal{C}$ 是 $\mathcal{G}_\mathcal{C}$ 中所有多项式的关联矩阵的集合。

如果 $f(x) \in \mathcal{G}_\lambda$，那么 $f(x+k)+l \in \mathcal{G}_\lambda$ 对任意 $k,l \in \mathbb{Z}_p$ 成立。显然，构造 4.2.1 中定义的是一个等价关系。对于任意 $f(x) \in \mathcal{G}_\lambda$，对比系数后我们发现 $f(x+k)+l = f(x)$ 当且仅当 $k = l = 0$，即 $f(x+k)+l \neq f(x)$ 对任意$(l,k) \in \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{(0,0)\}$ 成立。所以 $\mathcal{G}_\lambda$ 中每个多项式的等价类恰好包含 $p^2$ 个元素，$|\mathcal{G}_\mathcal{C}| = \frac{|\mathcal{G}_\lambda|}{p^2}$。

**定理 4.2.2** 构造 4.2.1 中定义的码 $\mathcal{C}$ 是一个大小为 $p^{\lambda-1}-1$ 的 $(p,p,p,\lambda)$-*OOSPC*，相对于 *Johnson* 界而言它是渐近最优的（$p$ 趋向于无穷时）。

**证明** 首先我们证明 $\mathcal{C}$ 是一个 $(p,p,p,\lambda)$-OOSPC。假设自相关性条件不满足，那么我们可以找到一个对应着 $f(x) \in \mathcal{G}_\mathcal{C}$ 的矩阵 $C_f$ 以及 $(\delta,\tau) \in \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{(0,0)\}$ 满足 $\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} C_f(i,j)C_f(i+\delta, j+\tau) > \lambda$。因为 $C_f(i,j)C_f(i+\delta,j+\tau) = 1$ 当且仅当 $f(j) = i$，$f(j+\tau) = i+\delta$，所以多项式 $f(x+\tau)-f(x)-\delta$ 会有超过 $\lambda$ 个零点，因此 $f(x+\tau)-\delta = f(x)$（如果 $f(x+\tau)-f(x)-\delta$ 是个非零多项式，它的次数不大于 $\lambda$，也就不会有超过 $\lambda$ 个零点，矛盾）。之前我们指出，$f(x+k)+l \neq f(x)$ 对所有 $(l,k) \in \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{(0,0)\}$ 成立，所以这里我们就推出了矛盾。

假设互相关性条件不满足，那么我们可以找到两个不同的矩阵 $C_f$ 和 $C_g$，分别对应着多项式 $f(x), g(x) \in \mathcal{G}_\mathcal{C}$，和 $(\delta,\tau) \in \mathbb{Z}_p \times \mathbb{Z}_p$ 使得 $\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} C_f(i,j)C_g(i+\delta,j+\tau) > \lambda$。一方面，因为 $f(x)$ 和 $g(x)$ 来自不同的等价类，所以 $g(x+\tau)-f(x)-\delta$ 是一个次数不超过 $\lambda$ 的非零多

项式，因此 $g(x+\tau)-f(x)-\delta$ 有至多 $\lambda$ 个零点。另一方面，因为 $C_f(i,j)C_g(i+\delta,j+\tau)=1$ 当且仅当 $f(j)=i, g(j+\tau)=i+\delta$ 时成立，所以多项式 $g(x+\tau)-f(x)-\delta$ 会有超过 $\lambda$ 个零点，矛盾。

综上，$\mathcal{C}$ 是一个 $(p,p,p,\lambda)$-OOSPC.

最后，我们来确定 $\mathcal{C}$ 的大小，并证明它是渐近最优的。显然，$\mathcal{G}_\lambda$ 的大小为 $p^{\lambda+1}-p^2$。因为每个等价类包含 $p^2$ 个元素，所以 $\mathcal{G}_\mathcal{C}$ 的大小为 $p^{\lambda-1}-1$。因此，$\mathcal{C}$ 的大小为 $p^{\lambda-1}-1$。

由 Johnson 界我们有

$$\begin{aligned} J(p,p,p,\lambda) &= \left\lfloor \frac{1}{p}\left\lfloor \frac{p^2-1}{p-1}\left\lfloor \frac{p^2-2}{p-2}\left\lfloor \cdots \left\lfloor \frac{p^2-\lambda}{p-\lambda}\right\rfloor \cdots \right\rfloor\right\rfloor\right\rfloor\right\rfloor \\ &\leq \left(\frac{1}{p}\times\frac{p^2-1}{p-1}\times\frac{p^2-2}{p-2}\times\cdots\times\frac{p^2-\lambda}{p-\lambda}\right). \end{aligned}$$

当 $p$ 趋向于无穷时，我们有

$$\lim_{p\to\infty}\frac{p^{\lambda-1}-1}{J(p,p,p,\lambda)}=1.$$

因此，构造的 OOSPC 是渐近最优的。 □

我们通过下面的例子来阐释构造 4.2.1。

例 4.2.3 *对任意素数 $p\geq 3$，存在大小为 $p-1$ 的 $(p,p,p,2)$-OOSPC。*

**证明** 在构造 4.2.1 中取 $\lambda=2$。对一个次数为 2 的多项式 $ax^2+bx+c$，显然有 $\{a(x+k)^2+b(x+k)+c+l\colon k,l\in\mathbb{Z}_p\}=\{ax^2+b'x+c'\colon a',b'\in\mathbb{Z}_p\}$。因此，$\mathcal{G}_2$ 中的等价类为 $\{ax^2+b'x+c'\colon a',b'\in\mathbb{Z}_p\}, a\in\mathbb{Z}_p^*$。那么，$\{\{(ai^2,i)\colon i\in\mathbb{Z}_p\}\colon a\in\mathbb{Z}_p^*\}$ 就是我们想要的 $(p,p,p,2)$-OOSPC 的集合论表示。 □

### 4.2.2　$(q-1,n,n-\lambda,\lambda)$-OOSPC

在这一小节，我们通过有限域 $\mathbb{F}_q$ 上的多项式构造一类渐近最优的 OOSPC，这个方法与文献[40] 中的类似。

令 $q$ 是一个素数幂，$n,\lambda$ 是满足 $n|q-1$，$n>2\lambda$ 的整数。取 $\alpha$ 为有限域 $\mathbb{F}_q$ 的本原元，$\beta=\alpha^{\frac{q-1}{n}}$。在乘法群 $\mathbb{F}_q^*=\mathbb{F}_q\setminus\{0\}$ 中由 $\beta$ 生成的子群我们记作为 $\langle\beta\rangle$。对 $\mathbb{F}_q$ 上次数不超过 $\lambda$ 的非零多项式 $f(x)$，我们定义它的关联矩阵 $C_f$ 为

$$C(i,j)=1 \text{ 当且仅当 } f(\beta^j)=\alpha^i, \tag{4-3}$$

其中，$(i,j)\in\mathbb{Z}_{q-1}\times\mathbb{Z}_n$。因为 $f(x)$ 的次数不超过 $\lambda$，$f(x)$ 有至多 $\lambda$ 个零点，所以关联矩阵 $C_f$ 的重量至少为 $n-\lambda$。为了保证常重的性质，对于那些重量大于 $n-\lambda$ 的关联矩阵我

们随机地删除适量的 1 以保证常重量 $n-\lambda$。对于 $\mathbb{F}_q$ 上次数不超过 $\lambda$ 的两个不同的非零多项式 $f(x)$ 和 $g(x)$，多项式 $f(x)-g(x)$ 有至多 $\lambda$ 个零点。因为 $n-\lambda>\lambda$，所以 $f(x)$ 和 $g(x)$ 不会在所有的 $n-\lambda$ 个位置重合，故而 $C_f$ 和 $C_g$ 是互异的。

**构造 4.2.4** 取素数幂 $q$，正整数 $n,\lambda$ 满足 $n|q-1, n>2\lambda$。令 $\mathcal{P}_\lambda$ 是包含 $\mathbb{F}_q$ 上所有次数不超过 $\lambda$ 且满足 $\alpha^l f(\beta^k x)\neq f(x)$ 对所有 $(l,k)\in\mathbb{Z}_{q-1}\times\mathbb{Z}_n\setminus\{(0,0)\}$ 成立的非零多项式 $f(x)$ 的集合。$\mathcal{P}_\lambda$ 中的两个多项式 $f(x)$，$g(x)$ 是等价的当且仅当 $f(\beta^k x)=\alpha^l g(x)$ 对某些 $k\in\mathbb{Z}_n$，$l\in\mathbb{Z}_{q-1}$ 成立。令 $\mathcal{P}_\mathcal{C}$ 是从每个等价类中挑选一个多项式后组成的集合。令 $\mathcal{C}$ 是 $\mathcal{P}_\mathcal{C}$ 中多项式关联矩阵的集合。

显然，构造 4.2.4 中定义的是一个等价关系。如果 $f(x)\in\mathcal{P}_\lambda$，那么 $\alpha^l f(\beta^k x)\in\mathcal{P}_\lambda$。$\alpha^l f(\beta^k x)=f(x)$ 成立当且仅当 $l=0,k=0$。因此，$\mathcal{P}_\lambda$ 中每个多项式的等价类恰好包含 $n(q-1)$ 个元素，$|\mathcal{P}_\mathcal{C}|=\frac{|\mathcal{P}_\lambda|}{n(q-1)}$。$|\mathcal{P}_\lambda|$ 的计算相对而言比较冗长和乏味，我们这里只列出结论而不加以证明。

**引理 4.2.5** 如构造 4.2.4 中定义 $\mathcal{P}_\lambda$，那么

$$|\mathcal{P}_\lambda|=\sum_{e_1=0}^{\lambda}\sum_{d|n}(q-1)q^{\lfloor\frac{\lambda-e_1}{d}\rfloor}\mu(d),$$

其中 $\mu\colon\mathbb{Z}\to\{0,-1,1\}$ 表示的是 *Möbius* 函数

$$\mu(y)=\begin{cases}1, & y=1,\\ (-1)^t, & y\text{ 是个 }t\text{ 个不同素数的乘积},\\ 0, & \text{其它情况}.\end{cases}$$

**定理 4.2.6** 构造 4.2.4 中定义的码 $\mathcal{C}$ 是一个大小为

$$\frac{1}{n}\sum_{e_1=0}^{\lambda}\sum_{d|n}q^{\lfloor\frac{\lambda-e_1}{d}\rfloor}\mu(d),$$

的 $(q-1,n,n-\lambda,\lambda)$-*OOSPC*，当 $q$ 和 $n$ 趋向于无穷时，它是渐近最优的。

**证明** 首先我们证明 $\mathcal{C}$ 是一个 $(q-1,n,n-\lambda,\lambda)$-OOSPC。假设它不满足相关性性质，那么我们可以找到两个关联矩阵 $C_f$ 和 $C_g$ 以及 $(\delta,\tau)\in\mathbb{Z}_{q-1}\times\mathbb{Z}_n$ 使得 $\sum_{i=0}^{q-2}\sum_{j=0}^{n-1}C_f(i,j)C_g(i+\delta,j+\tau)>\lambda$。这里如果 $f=g$，那么 $(\delta,\tau)\neq(0,0)$。由 $\mathcal{P}_\lambda$ 和 $\mathcal{P}_\mathcal{C}$ 的定义可知，$g(\beta^\tau x)-\alpha^\delta f(x)$ 是

一个次数不超过 $\lambda$ 的非零多项式，因而 $g(\beta^\tau x)-\alpha^\delta f(x)$ 有至多 $\lambda$ 个零点。另一方面，因为 $C_f(i,j)C_g(i+\delta,j+\tau)=1$ 当且仅当 $f(\beta^j)=\alpha^i$，$g(\beta^{j+\tau})=\alpha^{i+\delta}$，多项式 $g(\beta^\tau x)-\alpha^\delta f(x)$ 在 $\langle\beta\rangle$ 中会有超过 $\lambda$ 个零点，矛盾。

由引理 4.2.5，我们有

$$|\mathcal{P}_\mathcal{C}|=\frac{|\mathcal{P}_\lambda|}{n(q-1)}=\frac{1}{n}\sum_{e_1=0}^{\lambda}\sum_{d|n}q^{\lfloor\frac{\lambda-e_1}{d}\rfloor}\mu(d).$$

最后我们证明构造的 OOSPC 是渐近最优的。考虑 $|\mathcal{P}_\mathcal{C}|$ 中最大的一项，即 $d=1$, $e_1=0$ 时的值，又因为 $w=n-\lambda$，由 Johnson 界我们有

$$\begin{aligned}&J(q-1,n,w,\lambda)\\&=\left\lfloor\tfrac{1}{n-\lambda}\left\lfloor\tfrac{n(q-1)-1}{n-\lambda-1}\left\lfloor\tfrac{n(q-1)-2}{n-\lambda-2}\left\lfloor\cdots\left\lfloor\tfrac{n(q-1)-\lambda}{n-\lambda-\lambda}\right\rfloor\cdots\right\rfloor\right\rfloor\right\rfloor\right\rfloor\\&\le\left(\tfrac{1}{n-\lambda}\times\tfrac{n(q-1)-1}{n-\lambda-1}\times\tfrac{n(q-1)-2}{n-\lambda-2}\times\cdots\times\tfrac{n(q-1)-\lambda}{n-\lambda-\lambda}\right).\end{aligned}$$

所以当 $q$ 和 $n$ 趋向于无穷时，我们有

$$\lim_{q,n\to\infty}\frac{|\mathcal{C}|}{J(q-1,n,n-\lambda,\lambda)}=1.$$

因此，构造所得的 OOSPC 是渐近最优的。 □

我们通过下面的例子阐释说明构造 4.2.4.

例 4.2.7 *存在大小为 28 的 $(12,6,4,2)$-OOSPC。*

**证明** 取 $\mathbb{Z}_{13}$ 中的本原元 2 并令 $\beta=4$。令 $\mathbb{Z}_{13}^{\square}$ 和 $\mathbb{Z}_{13}^{\not\square}$ 分别表示模 13 的二次剩余和非二次剩余。由 $\mathcal{P}_2$ 的定义我们有，

$$\mathcal{P}_2=\{bx+c\colon b,x\in\mathbb{Z}_{13}^*\}\cup\{ax^2+bx+c\colon a,b\in\mathbb{Z}_{13}^*,c\in\mathbb{Z}_{13}\}.$$

由等价关系的定义我们可以将 $\mathcal{P}_2$ 划分成 28 个等价类：

$$\begin{aligned}&\{bcx+c\colon b\in\mathbb{Z}_{13}^{\square},c\in\mathbb{Z}_{13}^*\},\\&\{2bcx+c\colon b\in\mathbb{Z}_{13}^{\square},c\in\mathbb{Z}_{13}^*\},\\&\{bcx^2+cx\colon b\in\mathbb{Z}_{13}^{\square},c\in\mathbb{Z}_{13}^*\},\\&\{2bcx^2+cx\colon b\in\mathbb{Z}_{13}^{\square},c\in\mathbb{Z}_{13}^*\},\\&\{ab^2cx^2+bcx+c\colon b\in\mathbb{Z}_{13}^{\square},c\in\mathbb{Z}_{13}^*\},\quad a\in\mathbb{Z}_{13}^*,\\&\{ab^2cx^2+2bcx+c\colon b\in\mathbb{Z}_{13}^{\square},c\in\mathbb{Z}_{13}^*\},\quad a\in\mathbb{Z}_{13}^*.\end{aligned}$$

取等价类的代表元的集合为：

$$\mathcal{P}_{\mathcal{C}} = \{x+1, 2x+1, x^2+1, 2x^2+1\}$$
$$\cup\{ax^2+bx+1 \colon a \in \mathbb{Z}_{13}^*, b \in \{1,2\}\}.$$

对任意的 $f(x) \in \mathcal{P}_{\mathcal{C}}$，我们可以得到相应的关联矩阵 $C_f$，我们列举了它们的集合论表示：

$$C_{x+1} = \{(1,0),(9,1),(2,2),(10,4),(7,5)\}$$
$$C_{2x+1} = \{(4,0),(8,1),(11,2),(6,3),(5,4),(3,5)\}$$
$$C_{x^2+x} = \{(1,0),(11,1),(6,2),(6,4),(5,5)\}$$
$$C_{2x^2+x} = \{(4,0),(10,1),(3,2),(0,3),(1,4),(1,5)\}$$
$$C_{x^2+x+1} = \{(4,0),(3,1),(0,3),(11,5)\}$$
$$C_{2x^2+x+1} = \{(2,0),(7,1),(8,2),(1,3),(4,4),(4,5)\}$$
$$C_{3x^2+x+1} = \{(9,0),(0,1),(9,2),(4,3),(5,4),(6,5)\}$$
$$C_{4x^2+x+1} = \{(5,0),(2,1),(0,2),(2,3),(8,4),(3,5)\}$$
$$C_{5x^2+x+1} = \{(11,0),(11,1),(10,2),(9,3),(6,4),(2,5)\}$$
$$C_{6x^2+x+1} = \{(3,0),(10,1),(5,2),(5,3),(1,4)\}$$
$$C_{7x^2+x+1} = \{(8,0),(1,2),(11,3),(9,4),(8,5)\}$$
$$C_{8x^2+x+1} = \{(10,0),(4,1),(7,2),(3,3),(3,4),(9,5)\}$$
$$C_{9x^2+x+1} = \{(7,0),(5,1),(11,2),(8,3),(7,4),(0,5)\}$$
$$C_{10x^2+x+1} = \{(6,0),(8,1),(4,2),(10,3),(0,4),(10,5)\}$$
$$C_{11x^2+x+1} = \{(6,1),(6,2),(7,3),(2,4),(5,5)\}$$
$$C_{12x^2+x+1} = \{(0,0),(1,1),(3,2),(6,3),(11,4),(1,5)\}$$
$$C_{x^2+2x+1} = \{(2,0),(6,1),(4,2),(8,4),(2,5)\}$$
$$C_{2x^2+2x+1} = \{(9,0),(1,1),(6,2),(0,3),(6,4)\}$$
$$C_{3x^2+2x+1} = \{(5,0),(9,1),(3,2),(1,3),(1,4),(8,5)\}$$
$$C_{4x^2+2x+1} = \{(11,0),(3,1),(2,2),(4,3),(9,4),(9,5)\}$$
$$C_{5x^2+2x+1} = \{(3,0),(7,1),(2,3),(3,4),(0,5)\}$$
$$C_{6x^2+2x+1} = \{(8,0),(0,1),(8,2),(9,3),(7,4),(10,5)\}$$
$$C_{7x^2+2x+1} = \{(10,0),(2,1),(9,2),(5,3),(0,4),(5,5)\}$$
$$C_{8x^2+2x+1} = \{(7,0),(11,1),(0,2),(11,3),(2,4),(1,5)\}$$
$$C_{9x^2+2x+1} = \{(6,0),(10,1),(10,2),(3,3),(11,4),(7,5)\}$$
$$C_{10x^2+2x+1} = \{(5,2),(8,3),(10,4),(11,5)\}$$
$$C_{11x^2+2x+1} = \{(0,0),(4,1),(1,2),(10,3),(4,5)\}$$
$$C_{12x^2+2x+1} = \{(1,0),(5,1),(7,2),(7,3),(4,4),(6,5)\}$$

为了保证常重的性质，我们在重量大于 4 的矩阵中删除适量的 1，由此我们得到了大小为 28 的 $(12,6,4,2)$-OOSPC。 □

### 4.2.3 $(q-1,n,w-\lambda,\lambda)$-OOSPC

令 $q$ 是一个素数幂，$n$ 是一个正整数满足 $n \le q-1$。令 $\alpha$ 是有限域 $\mathbb{F}_q$ 的本原元。记 $P_\lambda = \{f_0(x), f_1(x), \ldots, f_{s-1}(x)\}$ 为 $\mathbb{F}_q$ 上所有次数不大于 $\lambda$，满足 $f_i(x) \neq \alpha^k f_j(x)$ 对所有 $i,j,k, 0 \le i < j < s, 0 \le k < q-1$ 成立的非零多项式的集合。显然，$s = |P_\lambda| = \frac{q^{\lambda+1}-1}{q-1}$。

假设 $\mathcal{O} = \{O_0, O_1, \ldots, O_{t-1}\}$ 是一个最优的大小为 $t = J(1,n,w,\lambda)$ 的 1-D $(n,w,\lambda)$-OOC $(w > 2\lambda)$。对任意 $0 \le k < t, 0 \le l < s$, $O_k$ 和 $f_l(x)$ 的关联矩阵 $C_l^k$ 定义为

$$C(i,j) = 1 \text{ 当且仅当 } j \in O_k, f_l(\alpha^j) = \alpha^i, \tag{4-4}$$

其中，$(i,j) \in \mathbb{Z}_{q-1} \times \mathbb{Z}_n$。因为 $f_l(x)$ 的次数不超过 $\lambda$，$f_l(x)$ 有至多 $\lambda$ 个零点，因此 $O_k$ 和 $f_l$ 的关联矩阵的重量至少为 $w-\lambda$。为了保证常重的性质，在那些重量大于 $w-\lambda$ 的矩阵中，我们随机地删除适量的 1。对两个不同的次数不超过 $\lambda$ 的非零多项式 $f_l(x), f_{l'}(x)$，非零多项式 $f_l(x) - f_{l'}(x)$ 至多有 $\lambda$ 个零点。因为 $w-\lambda > \lambda$，所以这两个多项式 $f_l(x), f_{l'}(x)$ 不会在所有 $w-\lambda$ 个位置一致，因此 $f_l(x), f_{l'}(x)$ 对应的关联矩阵总是不同的（不管它们是否对应着同一个 $O_k$）。

**构造 4.2.8** 令 $q$ 是一个素数幂，$n$ 是一个正整数，满足 $n \le q-1$。令 $P_\lambda = \{f_0(x), f_1(x), \ldots, f_{s-1}(x)\}$ 是有限域 $\mathbb{F}_q$ 上所有次数不超过 $\lambda$，且满足 $f_i(x) \neq \alpha^k f_j(x)$ 对所有 $i,j,k, 0 \le i < j < s, 0 \le k < q-1$ 成立的非零多项式的集合。取 $\mathcal{O} = \{O_0, O_1, \ldots, O_{t-1}\}$ 为一个最优 1-D $(n,w,\lambda)$-*OOC* $(w > 2\lambda)$，大小为 $t = J(1,n,w,\lambda)$。令 $\mathcal{C}$ 是 $\mathcal{O}$ 和 $P_\lambda$ 关联矩阵的集合。

**定理 4.2.9** 构造 4.2.8 中所得的码 $\mathcal{C}$ 是一个 $(q-1,n,w-\lambda,\lambda)$-*OOSPC*，它的大小为 $\frac{q^{\lambda+1}-1}{q-1} J(1,n,w,\lambda)$。

**证明** 令 $C_l^k$ 和 $C_{l'}^{k'}$ 是分别对应着 $f_l(x), O_k$ 和 $f_{l'}(x), O_{k'}$ 的关联矩阵，假设存在 $(\delta,\tau) \in \mathbb{Z}_{q-1} \times \mathbb{Z}_n$ 使得

$$\sum_{i=0}^{q-2} \sum_{j=0}^{n-1} C_l^k(i,j) C_{l'}^{k'}(i+\delta, j+\tau) > \lambda. \tag{4-5}$$

显然，$C_l^k(i,j)C_{l'}^{k'}(i+\delta,j+\tau) = 1$ 当且仅当 $j \in O_k, j+\tau \in O_{k'}, f_l(\alpha^j) = \alpha^i, f_{l'}(\alpha^{j+\tau}) = \alpha^{i+\delta}$。从 1-D OOC 的自相关和互相关性，我们知道 $\tau = 0, k = k'$，因此 $f_{l'}(\alpha^j) = \alpha^\delta f_l(\alpha^j)$。当

$l \neq l'$（或者 $l = l', \delta \neq 0$）时，$f_{l'}(x) - \alpha^{\delta} f_l(x)$ 是一个次数不超过 $\lambda$ 的非零多项式，至多有 $\lambda$ 个零点。因而，不等式 (4-5) 当且仅当 $k = k', l = l', \delta = 0$ 和 $\tau = 0$ 时成立。

$\mathcal{C}$ 的大小为

$$\frac{q^{\lambda+1}-1}{q-1}\left\lfloor \frac{1}{w}\left\lfloor \frac{n-1}{w-1}\left\lfloor \frac{n-2}{w-2}\left\lfloor \cdots \left\lfloor \frac{n-\lambda}{w-\lambda}\right\rfloor \cdots \right\rfloor\right\rfloor\right\rfloor\right\rfloor. \tag{4-6}$$

□

由 Johnson 界我们可得

$$\begin{aligned} &J(q-1, n, w-\lambda, \lambda) \\ &= \left\lfloor \tfrac{1}{w-\lambda}\left\lfloor \tfrac{(q-1)n-1}{w-\lambda-1}\left\lfloor \tfrac{(q-1)n-2}{w-\lambda-2}\left\lfloor \cdots \left\lfloor \tfrac{(q-1)n-\lambda}{w-2\lambda}\right\rfloor \cdots \right\rfloor\right\rfloor\right\rfloor\right\rfloor. \end{aligned} \tag{4-7}$$

在下例中，我们说明上述构造的 OOSPC 在特定情形下是渐近最优的。

例 4.2.10 文献[16] 构造了一类最优 1-D $(q_1^2-1, q_1+1, 2)$-*OOC*，大小为 $J(1, q_1^2-1, q_1+1, 2)$，其中 $q_1$ 是一个素数幂。由我们的构造可得 $(q-1, q_1^2-1, q_1-1, 2)$ *OOSPC*，其中 $q \geq q_1^2$ 是一个素数幂。在这样的情况下，(4-6) 中的最大项为 $q^2 q_1$。当 $q, q_1$ 趋向于无穷时，我们有

$$\lim_{q, q_1 \to \infty} \frac{|\mathcal{C}|}{J(q-1, q_1^2-1, q_1-1, 2)} = 1. \tag{4-8}$$

因此，所得的 *OOSPC* 是渐近最优的。

**注解 4** 在某些情况下，利用构造 4.2.8，我们也可以利用渐近最优的 1-D *OOC* 构造渐近最优的 *OOSPC*。

## 4.3 基于有理函数的渐近最优的构造

在本节中，我们利用 $\mathbb{F}_q$ 上的有理函数来构造一类渐近最优的 OOSPC。

令 $q$ 是一个素数幂，我们介绍射影直线上 $q+1$ 个点的一个循环排序[40]。我们考虑 $\mathbb{F}_q^2$ 中除了 $[0,0]^T$ 的其它所有元素。两个元素 $[a,b]^T$ 和 $[c,d]^T$ 是等价的当且仅当存在 $\theta \in \mathbb{F}_q^*$ 使得 $[a,b]^T = \theta[c,d]^T$。显然，我们这里定义的是一个等价关系。这个等价关系将 $\mathbb{F}_q^2$ 划分为 $(q+1)$ 个等价类，每个等价类包含了 $(q-1)$ 个元素。从每个等价类中选取一个元素就构成了射影直线，我们记为 $\mathbb{P}^1(\mathbb{F}_q)$。此外，我们用 $[a,b]_{eq}^T$ 表示包含 $[a,b]^T$ 的等价类。

令 $h(x)=x^2+h_1x+h_0$ 是 $\mathbb{F}_q$ 上的本原多项式。取

$$H=\begin{bmatrix}0 & -h_0\\ 1 & -h_1\end{bmatrix}$$

为其关联伴随矩阵。那么由[40] 中的定理 5 可知

$$\left\{\left[H^i\begin{bmatrix}1\\0\end{bmatrix}\right]_{eq}\,\middle|\,0\le i\le q\right\}=\mathbb{P}^1(\mathbb{F}_q).$$

令 $f(x)$ 和 $g(x)$ 是 $\mathbb{F}_q$ 上两个互素的非零多项式。定义映射 $\phi$ 为

$$\phi(t)=\begin{bmatrix}f(t)\\g(t)\end{bmatrix}_{eq},\ t\in\mathbb{F}_q.$$

当 $g(t)\neq 0$ 时，我们有

$$\phi(t)=\begin{bmatrix}\frac{f(t)}{g(t)}\\1\end{bmatrix}_{eq}.$$

因而，我们把 $\phi$ 看作是一个有理函数映射。

令 $\lambda$ 是一个正整数，$\beta\in\mathbb{F}_q$ 是一个乘法阶为 $n$ 的元素，其中 $n|q-1, n>2\lambda$。令 $\widetilde{\mathcal{F}_\lambda}$ 是有限域 $\mathbb{F}_q$ 上一类有理函数的集合，其中 $f(x)$ 和 $g(x)$ 满足：

(P1) $f(x)$ 和 $g(x)$ 都是非零多项式且次数$\le\lambda$;

(P2) 对任意 $k\in\mathbb{Z}_n\setminus\{0\}, \theta\in\mathbb{F}_q^*$,

$$\begin{bmatrix}f(\beta^kx)\\g(\beta^kx)\end{bmatrix}\neq\theta\begin{bmatrix}f(x)\\g(x)\end{bmatrix};\tag{4-9}$$

(P3) $f(x)$ 是首一的;

(P4) $f(x)$ 和 $g(x)$ 是互素的。

对 $\begin{bmatrix}f(x)\\g(x)\end{bmatrix}\in\widetilde{\mathcal{F}_\lambda}$，$\begin{bmatrix}f(x)\\g(x)\end{bmatrix}$ 的关联矩阵 $C$ 为

$$C(i,j)=1\text{ 当且仅当 }\begin{bmatrix}f(\beta^j)\\g(\beta^j)\end{bmatrix}_{eq}=\left[H^i\begin{bmatrix}1\\0\end{bmatrix}\right]_{eq},\tag{4-10}$$

其中 $(i,j)\in\mathbb{Z}_{q+1}\times\mathbb{Z}_n$。记这个从 $\widetilde{\mathcal{F}_\lambda}$ 到关联矩阵的映射为 $\varphi$。由[40] 可知，这是个单射。因为 $(f,g)=1$，$f(x)$ 和 $g(x)$ 没有共同零点，所以关联矩阵的重量为 $n$。

定义两个有理函数 $\begin{bmatrix} f_a(x) \\ g_a(x) \end{bmatrix}, \begin{bmatrix} f_b(x) \\ g_b(x) \end{bmatrix} \in \widetilde{\mathcal{F}_\lambda}$ 等价当且仅当

$$H^l \begin{bmatrix} f_a(\beta^k x) \\ g_a(\beta^k x) \end{bmatrix} = \theta \begin{bmatrix} f_b(x) \\ g_b(x) \end{bmatrix} \tag{4-11}$$

对一些 $(l,k) \in \mathbb{Z}_{q+1} \times \mathbb{Z}_n, \theta \in \mathbb{F}_q^*$ 成立。显然，这是一个等价关系。如果 $\begin{bmatrix} f(x) \\ g(x) \end{bmatrix} \in \widetilde{\mathcal{F}_\lambda}$，那么 $u_{l,k}^{-1} H^l \begin{bmatrix} f(\beta^k x) \\ g(\beta^k x) \end{bmatrix} \in \widetilde{\mathcal{F}_\lambda}$，其中 $u_{l,k}$ 是 $H^l \begin{bmatrix} f(\beta^k x) \\ g(\beta^k x) \end{bmatrix}$ 第一个坐标的最大次数项的系数。在 $H^l \begin{bmatrix} f(\beta^k x) \\ g(\beta^k x) \end{bmatrix} = \theta \begin{bmatrix} f(x) \\ g(x) \end{bmatrix}$ 中令 $x = 0$。因为 $H$ 遍历了 $\mathbb{P}^1(\mathbb{F}_q)$ 中的所有点且阶为 $q+1$，我们有 $l = 0$，进而 $H^l \begin{bmatrix} f(\beta^k x) \\ g(\beta^k x) \end{bmatrix} = \theta \begin{bmatrix} f(x) \\ g(x) \end{bmatrix}$ 成立当且仅当 $l = 0, k = 0$。因此 $\widetilde{\mathcal{F}_\lambda}$ 中的每个有理函数的等价类恰好包含 $n(q+1)$ 个元素。从每个等价类中选择一个有理函数后构成的集合我们记为 $\mathcal{F}_\mathcal{C}$，显然，$|\mathcal{F}_\mathcal{C}| = \frac{|\widetilde{\mathcal{F}_\lambda}|}{n(q+1)}$。

**引理 4.3.1** 令 $\widetilde{\mathcal{F}_\lambda}$ 定义如上。那么，

$$\begin{aligned} |\widetilde{\mathcal{F}_\lambda}| = & \tfrac{1}{q-1} \sum_{m(x)} (q^{\lambda - deg(m(x))+1} - 1)^2 \hat{\mu}(m(x)) \\ & + \sum_{u(x) \in \mathcal{B}} \sum_{e_1=0}^{\lambda - deg(u(x))} \sum_{d|n, d \neq 1} q^{\lfloor \frac{\lambda - deg(u(x)) - e_1}{d} \rfloor} \\ & \times (q^{\lfloor \frac{\lambda - deg(u(x)) + d - \varepsilon_{e_1,d}}{d} \rfloor} - 1) \mu(d) \hat{\mu}_\mathcal{B}(u(x)), \end{aligned} \tag{4-12}$$

其中，第一个求和是在 $\mathbb{F}_q$ 上所有首一的次数不超过 $\lambda$ 的多项式 $m(x)$ 上进行。$\hat{\mu}$ 表示的是如下从 $\mathbb{F}_q[x]$ 到 $\{0, -1, 1\}$ 的函数

$$\hat{\mu}(m(x)) = \begin{cases} 1, & m(x) = 1, \\ (-1)^t, & \textit{m(x)} \text{ 是 } \mathbb{F}_q \text{ 上 } t \text{ 个不同的首一不可约多项式的乘积}, \\ 0, & \text{其它情况}. \end{cases}$$

令 $\mathcal{B}$ 是次数不大于 $\lambda$ 的首一多项式 $f(x) = \sum_{i=1}^{r} f_i x^{e_i} \in \mathbb{F}_q[x]$ 的集合，其中 $r = 1$，或者 $r > 1$ 且 $gcd(e_2 - e_1, \ldots, e_r - e_1, n) = d$，对某些 $d > 1$ 成立。那么，$\hat{\mu}_\mathcal{B}$ 表示的是如下从 $\mathcal{B}$

到 $\{0,-1,1\}$ 的映射

$$\hat{\mu}_{\mathcal{B}}(u(x))=\begin{cases}1, & u(x)=1,\\ (-1)^t, & u(x)\text{ 是 }t\text{ 个不同的首一的相对于 }\mathcal{B}\text{ 不可分的多项式的乘积},\\ 0, & \text{其它情况}.\end{cases} \tag{4-13}$$

**构造 4.3.2** 令 $q$ 是一个素数幂，$n,\lambda$ 是满足$n|q-1, n>2\lambda$ 的正整数。令 $\mathcal{F}_{\mathcal{C}}$ 定义如上，$\mathcal{C}$ 为 $\mathcal{F}_{\mathcal{C}}$ 中有理函数关联矩阵的集合。

**定理 4.3.3** 构造 4.3.2 中定义的码 $\mathcal{C}$ 是一个大小为 $\frac{|\widetilde{\mathcal{F}_\lambda}|}{n(q+1)}$ 的 $(q+1,n,n,2\lambda)$-*OOSPC*，当 $q$ 和 $n$ 趋向于无穷时，$\mathcal{C}$ 是渐近最优的。

**证明** 我们首先证明 $\mathcal{C}$ 是一个 $(q+1,n,n,2\lambda)$-OOSPC。

假设 $\mathcal{C}$ 不满足相关性性质。令 $C_a$ 和 $C_b$ 分别是 $\begin{bmatrix} f_a(x)\\ g_a(x)\end{bmatrix}, \begin{bmatrix} f_b(x)\\ g_b(x)\end{bmatrix}\in\mathcal{F}_{\mathcal{C}}$ 的关联矩阵，假设我们可以找到 $(\delta,\tau)\in\mathbb{Z}_{q+1}\times\mathbb{Z}_n$ 使得 $\sum\limits_{i=0}^{q}\sum\limits_{j=0}^{n-1}C_a(i,j)C_b(i+\delta,j+\tau)>2\lambda$。如果 $C_a=C_b$，那么 $(\delta,\tau)\neq(0,0)$。因为 $C_a(i,j)C_b(i+\delta,j+\tau)=1$ 当且仅当

$$\begin{bmatrix} f_a(\beta^j)\\ g_a(\beta^j)\end{bmatrix}_{eq}=\left[H^i\begin{bmatrix}1\\0\end{bmatrix}\right]_{eq},$$
$$\begin{bmatrix} f_b(\beta^{j+\tau})\\ g_b(\beta^{j+\tau})\end{bmatrix}_{eq}=\left[H^{i+\delta}\begin{bmatrix}1\\0\end{bmatrix}\right]_{eq},$$

所以会存在超过 $2\lambda$ 个元素 $j\in\mathbb{Z}_n$ 使得

$$\begin{bmatrix} f_b(\beta^{j+\tau})\\ g_b(\beta^{j+\tau})\end{bmatrix}_{eq}=\left[H^{\delta}\begin{bmatrix} f_a(\beta^j)\\ g_a(\beta^j)\end{bmatrix}\right]_{eq}.$$

令 $H^\delta=\begin{pmatrix}a_{11}&a_{12}\\ a_{21}&a_{22}\end{pmatrix}$，上述等式等价于

$$\begin{cases} f_b(\beta^{j+\tau})=\theta_j(a_{11}f_a(\beta^j)+a_{12}g_a(\beta^j))\\ g_b(\beta^{j+\tau})=\theta_j(a_{21}f_a(\beta^j)+a_{22}g_a(\beta^j))\end{cases}$$

对某些 $\theta_j\in\mathbb{F}_q^*$ 成立。因此，

$$f_b(\beta^{j+\tau})(a_{21}f_a(\beta^j)+a_{22}g_a(\beta^j))-g_b(\beta^{j+\tau})(a_{11}f_a(\beta^j)+a_{12}g_a(\beta^j))=0.$$

那么多项式 $f_b(\beta^\tau x)(a_{21}f_a(x)+a_{22}g_a(x))-g_b(\beta^\tau x)(a_{11}f_a(x)+a_{12}g_a(x))$ 必须等于零因为它在 $\langle\beta\rangle$ 中有超过 $2\lambda$ 个零点，而 $f_a(x),g_a(x),f_b(x)$,$g_b(x)$ 的次数都不超过 $\lambda$。又因为 $\gcd(f_a(x),g_a(x))=1,\gcd(f_b(x),g_b(x))=1$，$H$ 是不可逆的，我们有 $\gcd(f_b(\beta^\tau x),g_b(\beta^\tau x))=1$, $\gcd(a_{11}f_a(x)+a_{12}g_a(x),a_{21}f_a(x)+a_{22}g_a(x))=1$。由 $f_b(\beta^\tau x)(a_{21}f_a(x)+a_{22}g_a(x))=g_b(\beta^\tau x)(a_{11}f_a(x)+a_{12}g_a(x))$ 可得

$$\begin{cases} f_b(\beta^\tau x)=\theta_\tau(a_{11}f_a(x)+a_{12}g_a(x)) \\ g_b(\beta^\tau x)=\theta_\tau(a_{21}f_a(x)+a_{22}g_a(x)) \end{cases}$$

对某些 $\theta_\tau\in\mathbb{F}_q^*$ 成立，即

$$\begin{bmatrix} f_b(\beta^\tau x) \\ g_b(\beta^\tau x) \end{bmatrix}=\theta_\tau\left[H^\delta\begin{bmatrix} f_a(x) \\ g_a(x) \end{bmatrix}\right].$$

如果 $C_a=C_b$，令 $x=0$ 得 $\delta=0$，这是因为 $H$ 遍历了 $\mathbb{P}^1(\mathbb{F}_q)$ 中的点且阶为 $q+1$。因此，$\begin{bmatrix} f_a(\beta^\tau x) \\ g_a(\beta^\tau x) \end{bmatrix}=\theta_\tau\begin{bmatrix} f_a(x) \\ g_a(x) \end{bmatrix}$，矛盾。如果 $C_a\neq C_b$，因为 $\begin{bmatrix} f_a(x) \\ g_a(x) \end{bmatrix}$ 和 $\begin{bmatrix} f_b(x) \\ g_b(x) \end{bmatrix}$ 来自 $\widetilde{\mathcal{F}_\lambda}$ 中不同的等价类，我们依然可以推出矛盾。

因为 $\widetilde{\mathcal{F}_\lambda}$ 中的每个等价类中有 $n(q+1)$ 个元素，那么 $\mathcal{C}$ 的大小为 $\frac{|\widetilde{\mathcal{F}_\lambda}|}{n(q+1)}$。通过简单的计算可得，当 $q$ 和 $n$ 趋向于无穷时我们有

$$\lim_{q,n\to\infty}\frac{|\mathcal{C}|}{J(q+1,n,n,2\lambda)}=1.$$

综上，构造所得的 OOSPC 是渐近最优的。 □

我们利用下面的例子来阐释说明构造 4.3.2。

例 4.3.4 *存在大小为 5 的 $(6,4,4,2)$-OOSPC。*

**证明** 令 $q=5,n=q-1,\lambda=1$，取 $\mathbb{Z}_5$ 上的本原多项式 $h(x)=x^2+x+2$，以及 $\mathbb{Z}_5$ 的本原元 $\beta=2$。由 $\widetilde{\mathcal{F}_1}$ 的定义我们有

$$\widetilde{\mathcal{F}_1}=\left\{\begin{bmatrix} 1 \\ ax+b \end{bmatrix}:a\in\mathbb{Z}_5^*,b\in\mathbb{Z}_5\right\}\bigcup\left\{\begin{bmatrix} x+c \\ ax+b \end{bmatrix}:a,b,c\in\mathbb{Z}_5,b\neq ac\right\}.$$

由等价关系 (4-11) 可知，我们可以划分 $\widetilde{\mathcal{F}_1}$ 为五个等价类，代表元为 $\begin{bmatrix} 1 \\ x+b \end{bmatrix}$，$b \in \mathbb{Z}_5$。显然，$H = \begin{bmatrix} 0 & 3 \\ 1 & 4 \end{bmatrix}$，

$$\begin{aligned}
\left[H^0 \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right]_{eq} &= \begin{bmatrix} 1 \\ 0 \end{bmatrix}_{eq}, \quad \left[H \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right]_{eq} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}_{eq}, \\
\left[H^2 \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right]_{eq} &= \begin{bmatrix} 1 \\ 3 \end{bmatrix}_{eq} \quad \left[H^3 \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right]_{eq} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}_{eq}, \\
\left[H^4 \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right]_{eq} &= \begin{bmatrix} 1 \\ 4 \end{bmatrix}_{eq}, \quad \left[H^5 \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right]_{eq} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}_{eq}.
\end{aligned}$$

$\begin{bmatrix} 1 \\ x+b \end{bmatrix}$ $(b \in \mathbb{Z}_5)$ 的关联矩阵的集合论表示为：

$$\begin{aligned}
C_{\begin{bmatrix} 1 \\ x \end{bmatrix}} &= \{(5,0),(3,1),(4,2),(2,3)\}, \\
C_{\begin{bmatrix} 1 \\ x+1 \end{bmatrix}} &= \{(3,0),(2,1),(0,2),(4,3)\}, \\
C_{\begin{bmatrix} 1 \\ x+2 \end{bmatrix}} &= \{(2,0),(4,1),(5,2),(0,3)\}, \\
C_{\begin{bmatrix} 1 \\ x+3 \end{bmatrix}} &= \{(4,0),(0,1),(3,2),(5,3)\}, \\
C_{\begin{bmatrix} 1 \\ x+4 \end{bmatrix}} &= \{(0,0),(5,1),(2,2),(3,3)\}.
\end{aligned}$$

这五个矩阵构成了一个 $(6,4,4,2)$-OOSPC。 □

## 4.4　基于 $r$-简单矩阵的递归构造

文献[14] 介绍了 $r$-简单矩阵的概念并用循环群上的 $r$-简单矩阵给出了 1-D OOC 的递归构造。在本节中我们改进了 $r$-简单矩阵的存在性结果，并利用 $\mathbb{Z}_m \times \mathbb{Z}_n$ 上的 $r$-简单矩阵递归构造了 OOSPC。

### 4.4.1 $r$-简单矩阵

令 $G$ 是一个 $n$ 阶交换群，$r$ 是一个正整数。$G$ 上一个 $s \times t$ 的矩阵 $A = (a_{i,j})$ 被称为 $r$-简单的，如果 $A$ 的任意两个列向量的差包含 $G$ 中的元素至多 $r-1$ 次。文献[14] 证明了对任意素数 $p$，任意整数 $r$，$2 \le r \le p$，都存在一个 $\mathbb{Z}_p$ 上的 $p \times p^{r-1}$ $r$-简单矩阵。我们推广了这个结果。

**引理 4.4.1** 令 $q$ 是一个素数幂，$\alpha$ 是 $\mathbb{F}_q$ 的本原元，$r$ 是一个整数满足 $3 \le r \le q$，取 $\mathbb{F}_q$ 上一个 $r-1$ 次首一不可约多项式 $h(x)$。令 $D$ 包含以下所有列向量：

$$D_f = \left[\frac{f(0)}{h(0)}, \frac{f(1)}{h(1)}, \frac{f(\alpha)}{h(\alpha)}, \frac{f(\alpha^2)}{h(\alpha^2)}, \ldots, \frac{f(\alpha^{q-2})}{h(\alpha^{q-2})}, [x^{r-1}]f(x)\right]^T,$$

其中，$f(x) \in \mathbb{F}_q[x]$ 满足 $f(x) = 0$，或者 $deg(f(x)) < r$ 且 $f(0) = 0$，$[x^{r-1}]f(x)$ 表示的是 $x^{r-1}$ 在 $f(x)$ 中的系数。那么，$D$ 是 $\mathbb{F}_q$ 上的一个 $(q+1) \times q^{r-1}$ 的 $r$-简单矩阵。

**证明** 由构造可知，$f(x)$ 是形如 $\sum_{i=1}^{r-1} a_i x^i$, $a_i \in \mathbb{F}_q$, $1 \le i < r$ 的多项式。因此，$D$ 有 $q^{r-1}$ 列。记 $D_f$ 和 $D_g$ 是 $D$ 中分别关联互异多项式 $f(x)$ 和 $g(x)$ 的两个不同的列向量。当 $[x^{r-1}]f(x) = [x^{r-1}]g(x)$ 时，$f(x) - g(x)$ 是一个次数小于 $r-1$ 的非零多项式，$\frac{f(x)-g(x)}{h(x)}$ 有至多 $r-2$ 个零点，因此 $D_f - D_g$ 包含 0 至多 $r-1$ 次。对任意 $\tau \in \mathbb{F}_q^*$，因为 $f(x) - g(x) - \tau h(x)$ 是一个次数为 $r-1$ 的非零多项式，它至多有 $r-1$ 个零点。所以，$\frac{f(x)-g(x)}{h(x)} - \tau$ 至多有 $r-1$ 个零点，$D_f - D_g$ 包含 $\tau$ 至多 $r-1$ 次。当 $[x^{r-1}]f(x) \neq [x^{r-1}]g(x)$ 时，$f(x) - g(x) - ([x^{r-1}]f(x) - [x^{r-1}]g(x))h(x)$ 是一个次数小于 $r-1$ 的非零多项式，$f(x) - g(x) - ([x^{r-1}]f(x) - [x^{r-1}]g(x))h(x)$ 至多有 $r-2$ 个零点，故 $D_f - D_g$ 包含 $([x^{r-1}]f(x) - [x^{r-1}]g(x))$ 至多 $r-1$ 次。对任意 $\tau \in \mathbb{F}_q \setminus \{[x^{r-1}]f(x) - [x^{r-1}]g(x)\}$，因为 $f(x) - g(x) - \tau h(x)$ 是一个次数为 $r-1$ 的非零多项式，所以它至多有 $r-1$ 个零点，故 $\frac{f(x)-g(x)}{h(x)} - \tau$ 至多有 $r-1$ 个零点。

综上，$D_f - D_g$ 包含每个元素 $\tau \in \mathbb{F}_q$ 至多 $r-1$ 次。 □

由引理 4.4.1 可知，存在 $\mathbb{Z}_p$ 上的 $(p+1) \times p^{r-1}$ $r$-简单矩阵，$r \ge 3$，比[14] 中的 $p \times p^{r-1}$ $r$-简单矩阵多一行。因为 $\mathbb{F}_{p^2}$ 与 $\mathbb{Z}_p \times \mathbb{Z}_p$ 同构，我们可得如下推论。

**推论 4.4.2** 对任意素数 $p \ge 3$，任意整数 $r$，$3 \le r \le p^2$，存在一个 $\mathbb{Z}_p \times \mathbb{Z}_p$ 上的 $(p^2+1) \times p^{2r-2}$ 的 $r$-简单矩阵。

**引理 4.4.3** 令 $A=\left[(a_{i,j},a'_{i,j})\right]$ 是 $\mathbb{Z}_m\times\mathbb{Z}_n$ 上一个 $s\times t$ 的 $r$-简单矩阵，$a_{i,j}\in\mathbb{Z}_m$, $a'_{i,j}\in\mathbb{Z}_n$，$B=\left[(b_{i,k},b'_{i,k})\right]$ 是 $\mathbb{Z}_{m'}\times\mathbb{Z}_{n'}$ 上一个 $s\times t'$ 的 $r$-简单矩阵，$b'_{i,j}\in\mathbb{Z}_{n'}$。对 $1\le j\le t$，令

$$H_j=\begin{bmatrix}(a_{1,j}+mb_{1,1},a'_{1,j}+nb'_{1,1}) & (a_{1,j}+mb_{1,2},a'_{1,j}+nb'_{1,2}) & \cdots & (a_{1,j}+mb_{1,t'},a'_{1,j}+nb'_{1,t'})\\ (a_{2,j}+mb_{2,1},a'_{2,j}+nb'_{2,1}) & (a_{2,j}+mb_{2,2},a'_{2,j}+nb'_{2,2}) & \cdots & (a_{2,j}+mb_{2,t'},a'_{2,j}+nb'_{2,t'})\\ \vdots & \vdots & \ddots & \vdots\\ (a_{s,j}+mb_{s,1},a'_{s,j}+nb'_{s,1}) & (a_{s,j}+mb_{s,2},a'_{s,j}+nb'_{s,2}) & \cdots & (a_{s,j}+mb_{s,t'},a'_{s,j}+nb'_{s,t'})\end{bmatrix}.$$

那么矩阵

$$H=[H_1,H_2,\ldots,H_t]$$

是 $\mathbb{Z}_{mm'}\times\mathbb{Z}_{nn'}$ 上一个 $s\times tt'$ 的 $r$-简单矩阵。

**证明** 对 $1\le j\le t$，因为 $B$ 是 $\mathbb{Z}_{m'}\times\mathbb{Z}_{n'}$ 上的一个 $s\times t'$ 的 $r$-简单矩阵，矩阵 $\left[(mb_{i,k},nb'_{i,k})\right]$ 也是 $m\mathbb{Z}_{m'}\times n\mathbb{Z}_{n'}$ 上的 $s\times t'$ 的 $r$-简单矩阵，这保证了 $H_j$ 的 $r$-简单性。

我们分别从 $H_j$ 和 $H_{j'}$ 中取两列，$j\ne j'$。它们的差向量（$\bmod m,\bmod n$）等于 $A$ 的第 $j$ 和 $j'$ 列的差向量。$A$ 的 $r$-简单性保证了在差向量中至多有 $r-1$ 个重复的值，得证。 □

利用引理 4.4.3 以及引理 4.4.1 中已知的 $r$-简单矩阵，我们可得如下推论。

**推论 4.4.4** 令 $m,n,r$ 是正整数，使得 $mn$ 的最小素因子 $p$ 不小于 $r$，$r\ge 3$。存在一个 $\mathbb{Z}_m\times\mathbb{Z}_n$ 上的 $(p+1)\times m^{r-1}n^{r-1}$ 的 $r$-简单矩阵。

现在我们做好了足够的准备来给出我们的递归构造。

**定理 4.4.5** （基本构造）假设我们已知一个大小为 $u$ 的 $(m,n,w,\lambda)$-*OOSPC*，如果存在一个 $\mathbb{Z}_{m'}\times\mathbb{Z}_{n'}$ 上的 $w\times N$ 的 $(\lambda+1)$-简单矩阵，那么则存在一个大小为 $Nu$ 的 $(mm',nn',w,\lambda)$-*OOSPC*。

**推论 4.4.6** 令 $\mathcal{C}$ 是一个 $(m,n,w,\lambda)$-*OOSPC*，其中 $w>\lambda$。取正整数 $m'$ 和 $n'$ 使得 $m'n'$ 的最小素数因子不小于 $w-1$，那么存在一个 $(mm',nn',w,\lambda)$-*OOSPC*，大小为 $(m'n')^\lambda|\mathcal{C}|$。

**证明** 由引理 4.4.4 可知，存在一个 $w\times(m'n')^\lambda$ $(\lambda+1)$-简单矩阵，然后再应用定理 4.4.5 即可。 □

与[14]中的推论1类似，在某些情况下我们可以在新的码中加入更多的码字，进而获得比上述构造更好的码。

**推论 4.4.7** 除了基本构造中的条件，如果还存在一个大小为 $t$ 的 $(m', n', w, \lambda)$-*OOSPC*，那么就存在一个 $(mm', nn', w, \lambda)$-*OOSPC*，码字数目比基本构造中的多 $t$。

**证明** 令 $\mathcal{H} = \{H_i \colon 1 \leq i \leq |\mathcal{H}|\}$ 为 $(m', n', w, \lambda)$-OOSPC 的集合论表示。对任意 $H_i = \{(h_{i1}, h'_{i1}), (h_{i2}, h'_{i2}), \ldots, (h_{iw}, h'_{iw})\}$，构造一个新的子集

$$H'_i = \{(mh_{i1}, nh'_{i1}), (mh_{i2}, nh'_{i2}), \ldots, (mh_{iw}, nh'_{iw})\} (\mathrm{mod}\, m, \mathrm{mod}\, n).$$

将这 $t$ 个新的子集加入到新的码中即可，相关性性质依然满足。 □

### 4.4.2 应用

**定理 4.4.8** 令 $\mathcal{C}$ 是一个渐近最优的 $(m, n, w, \lambda)$-*OOSPC*（当 $m$ 和 $n$ 趋向于无穷时）。取正整数 $m'$ 和 $n'$ 使得 $m'n'$ 的最小素数因子不小于 $w-1$，那么存在一个大小为 $(m'n')^\lambda|\mathcal{C}|$ 的渐近最优的 $(mm', nn', w, \lambda)$-*OOSPC*（当 $m$ 和 $n$ 趋向于无穷时）。

**证明** 令 $|\mathcal{C}| = M$，由假设我们有 $\lim\limits_{m,n\to\infty} \frac{M}{J(m,n,w,\lambda)} = 1$。根据推论 4.4.6 可知，存在一个 $(mm', nn', w, \lambda)$-OOSPC，大小为 $M(m'n')^\lambda$。此外，我们有

$$\begin{aligned}
&\lim_{m,n\to\infty} \frac{M(m'n')^\lambda}{J(mm',nn',w,\lambda)} \\
&= \lim_{m,n\to\infty} \frac{M(m'n')^\lambda J(m,n,w,\lambda)}{J(mm',nn',w,\lambda)J(m,n,w,\lambda)} \\
&= \lim_{m,n\to\infty} \frac{(m'n')^\lambda J(m,n,w,\lambda)}{J(mm',nn',w,\lambda)} \lim_{m,n\to\infty} \frac{M}{J(m,n,w,\lambda)} \\
&= 1,
\end{aligned}$$

综上，得证。 □

**推论 4.4.9** 令 $p$ 为素数，$\lambda$ 为整数，满足 $2 \leq \lambda \leq p$。那么对任意正整数 $m, n$，存在一个大小为 $(p^{\lambda-1}-1)p^{m\lambda+n\lambda-2\lambda}$ 的 $(p^m, p^n, p, \lambda)$-*OOSPC*，在 $p$ 趋向于无穷时它是渐近最优的。

**证明** 由定理 4.2.2 可知，存在一个 $(p, p, p, \lambda)$-OOSPC，大小为 $p^{\lambda-1}-1$，再应用定理 4.4.8 即可得证。 □

**推论 4.4.10** 令 $p$ 为素数，对任意整数 $m,n$，存在一个 $(p^m,p^n,p+1,2)$-*OOSPC*，大小为 $(p-1)p^{2m+2n-4}$，并且当 $p$ 趋向于无穷时它是渐近最优的。

**证明** 由[12]可知，存在一个 $(p,p,p+1,2)$-OOSPC，大小为 $p-1$，然后再应用定理 4.4.8 即可。 □

基于定理 4.4.8 和推论 4.4.9 中已知的渐近最优的 OOSPC，我们可以得到如下的渐近最优的 OOSPC。

**推论 4.4.11** 令 $p$ 是素数，$m,n,\lambda$ 是正整数满足 $2\leq\lambda<p$，$m',n'$ 是任意整数使得 $m'n'$ 的最小素因子不小于 $p$。那么，存在一个 $(m'p^m,n'p^n,p,\lambda)$-*OOSPC*，大小为 $(p^{\lambda-1}-1)p^{m\lambda+n\lambda-2\lambda}(m'n')^{\lambda}$，且当 $p$ 趋向于无穷时它是渐近最优的。

通过应用定理 4.4.8，我们也可以从定理 4.2.6 和定理 4.3.3 得到两族更大同时也是渐近最优的码，我们这里省略这些细节。

## 4.5 总结

在本章中，基于多项式和有理函数我们给出了 OOSPC 的四个直接构造以及基于 $r$-简单矩阵的递归构造，由此，我们得到了新的渐近最优的无穷类。由最优或者渐近最优的 OOSPC 递归构造所得的码也是渐近最优的，得到的无穷类的码字的数目比之前的多很多，而这也是我们的构造的优势所在。

# 5 其它成果与在研问题

本章简要介绍在攻读博士学位期间的其它研究工作，主要包括已有的关于几乎设计（adesign）的成果以及其它两个在研的课题。

## 5.1 几乎设计

几乎设计（adesign）是 Ding 2015 年在书[24] 中提出的一类组合对象。2-几乎设计是部分平衡不完全区组设计，可以应用于组合和统计问题中。我们主要讨论了几乎设计的基本性质，构造了几类 2-几乎设计和 3-几乎设计，它们中的一些可以导出新的几乎差集，一些可以导出新的几乎差族。部分几乎设计的关联矩阵对应的码是最优的或者有较大的最小距离。这部分工作发表在《Designs, Codes and Cryptography》。

## 5.2 DNA 存储中的编码问题

基于 DNA 的存储近年来收到了广泛的关注，高数据密度以及稳定性是它的优势所在。与经典编码问题不同的是，在 DNA 存储中通常发生的错误类型为插入，删除和替换。Lenz[35] 等提出了在集合上编码的模型，以此来抵抗存储系统中发生的错误。我们对于此问题的贡献在于，利用常重码构造了可以纠正单纯插入（或单纯删除）错误的码，且码字数目达到最大。该问题尚处在研究阶段。

## 5.3 部分重复码中的均匀分布问题

部分重复码（fractional repetition codes）是在分布式存储研究中所提出的一种码，关于 FRC 已有许多成熟的研究。在 FRC 的框架下，我们将每个文件的流行度纳入考虑。对于单个节点来说，它的传输能力有限，我们显然要将那些比较流行的文件均匀地分布到每个节点中去，这样才不会造成部分节点负荷过大的局面。我们将此问题与 Steiner 系，高维幻方以及线性超图相联系得到部分结果，目前尚处于研究阶段。

# 參考文獻


[1] T. L. Alderson and K. E. Mellinger, 2-Dimensional optical orthogonal codes from singer groups, *Discrete Appl. Math.*, vol. 157, pp. 3008-3019, 2009.

[2] E. Ballico and A. Cossidente, Curves in projective spaces and almost MDS codes, *Des. Codes Cryptogr.*, vol. 24, pp. 233-237, 2001.

[3] J. Bao and L. Ji, Constructions of strictly $m$-cyclic and semi-cyclic $H(m, n, 4, 3)$, *J. Combin. Designs*, vol. 24, pp. 249-264, 2016.

[4] E. F. Brickell and V. K. Wei, Optical orthogonal codes and cyclic block designs, *Congr. Numer.*, vol. 58, pp. 175-192, 1987.

[5] M. Buratti, Cyclic designs with block size 4 and related optimal optical orthogonal codes, *Des. Codes Cryptogr.*, vol. 26, pp. 111-125, 2002.

[6] H. Cai, H. Liang and X. Tang, Constructions of optimal 2-D optical orthogonal codes via generalized cyclotomic classes, *IEEE Trans. Inform. Theory*, vol. 61, pp. 688-695, 2015.

[7] H. Cao, R. Wei and Y. Su, Combinatorial constructions for optimal optical two-dimensional orthogonal codes, *IEEE Trans. Inform. Theory*, vol. 55, pp. 1387-1394, 2009.

[8] Y. Cassuto and M. Blaum, Codes for symbol-pair read channels, *IEEE Trans. Inform. Theory*, vol. 57, pp. 8011-8020, 2011.

[9] Y. Cassuto and S. Litsyn, Symbol-pair codes: algebraic constructions and asymptotic bounds, *IEEE Int. Symp. Inf. Theory*, pp. 2348-2352, 2011.

[10] Y. M. Chee, L. Ji, H. M. Kiah, C. Wang and J. Yin, Maximum distance separable codes for symbol-pair read channels, *IEEE Trans. Inform. Theory*, vol. 59, pp. 7259-7267, 2013.

[11] B. Chen, L. Lin and H. Liu, Constacyclic symbol-pair codes: lower bounds and optimal constructions, *IEEE Trans. Inform. Theory*, vol. 63, pp. 7661-7666, 2017.

[12] J. Chen, L. Ji and Y. Li, Combinatorial constructions of optimal $(m, n, 4, 2)$ optical orthogonal signature pattern codes, *Des. Codes Cryptogr.*, vol. 86, pp. 1499-1525, 2017.

[13] Q. Cheng, Hard problems of algebraic geometry codes, *IEEE Trans. Inform. Theory*, vol. 54, pp. 402-406, 2008.

[14] W. Chu and S. W. Golomb, A new recursive construction for optical orthogonal codes, *IEEE Trans. Inform. Theory*, vol. 49, pp. 3072-3076, 2003.

[15] F. R. K. Chung, J. A. Salehi and V. K. Wei, Optical orthogonal codes: design, analysis, and applications, *IEEE Trans. Inform. Theory*, vol. 35, pp. 595-604, 1989.

[16] H. Chung and P. V. Kumar, Optical orthogonal codes-new bounds and an optimal construction, *IEEE Trans. Inform. Theory*, vol. 36, pp. 866-873, 1990.

[17] J. -H. Chung and K. Yang, Asymptotically optimal optical orthogonal codes with new parameters, *IEEE Trans. Inform. Theory*, vol. 59, pp. 3999-4005, 2013.

[18] J. -H. Chung and K. Yang, New construction of asymptotically optimal optical orthogonal codes, *Information Theory Workshop-Fall (ITW), IEEE,* pp. 129-132, 2015.

[19] C. J. Colbourn and J. H. Dinitz, The CRC handbook of combinatorial designs, CRC Press, Boca Raton, FL, 2007.

[20] C. J. Colbourn, J. H. Dinitz and D. R. Stinson, Applications of combinatorial designs to communications, cryptography, and networking, *London Math. Soc.*, Lecture Note Ser. 267, pp. 37-100, 1999.

[21] P. A. Davies and A. A. Shaar, Asynchronous multiplexing for an optical-fibre local area network, *Electron. Leu.*, vol. 19, pp. 390-392, 1983.

[22] M. Deuring, Die typen der multiplikatorenringe elliptischer funktionenkörper, *Abh. Math. Sem. Univ. Hamburg*, vol. 14, pp. 197-272, 1941.

[23] B. Ding, G. Ge, J. Zhang, T. Zhang and Y. Zhang, New constructions of MDS symbol-pair codes, *Des. Codes Cryptogr.*, vol. 86, pp. 841-859, 2018.

[24] C. Ding, Codes from difference sets, World Scientific, Singapore, 2015.

[25] T. Feng and Y. Chang, Combinatorial constructions for two-dimensional optical orthogonal codes with $\lambda = 2$, *IEEE Trans. Inform. Theory*, vol. 57, pp. 6796-6819, 2011.

[26] T. Feng, Y. Chang and L. Ji, Constructions for strictly cyclic 3-designs and applications to optimal OOCs with $\lambda = 2$, *J. Combin. Theory (A)*, vol. 115, pp. 1527-1551, 2008.

[27] P. Hall, On representatives of subsets, *London Math. Soc.*, vol. s1-10, pp. 26-30, 1935.

[28] A. A. Hassan, J. E. Hershey and N. A. Riza, Spatial optical CDMA, *IEEE J. Sel. Areas Commun.*, vol. 13, pp. 609-613, 1995.

[29] Y. Huang and Y. Chang, Two classes of optimal two-dimensional OOCs, *Des. Codes Cryptogr.*, vol. 63, pp. 357-363, 2012.

[30] S. M. Johnson, A new upper bound for error-correcting codes, *IEEE Trans. Inform. Theory*, vol. 8, pp. 203-207, 1962.

[31] X. Kai, S. Zhu and P. Li, A construction of new MDS symbol-pair codes, *IEEE Trans. Inform. Theory*, vol. 61, pp. 5828-5834, 2015.

[32] K. Kitayama, Novel spatial spread spectrum based fiber optic CDMA networks for image transmission, *IEEE J. Sel. Areas Commun.*, vol. 12, pp. 762-772, 1994.

[33] K. Kitayama, Optical code division multiple access: a practical perspective, Cambridge University Press, New York, 2014.

[34] K. Kitayama, M. Nakamura, Y. Igasaki and K. Kaneda, Image fiber-optic two dimensional parallel links based upon optical space-CDMA: experiment, *J. Lightwave Technol.*, vol. 15, pp. 202-212, 1997.

[35] A. Lenz P.H. Siegel, A. Wachter-Zeh and E. Yaakobi, Coding over sets for DNA storage, arXiv:1801.04882.

[36] J. Li, D. Wan and J. Zhang, On the minimum distance of elliptic curve codes, *IEEE Int. Symp. Inf. Theory*, pp. 2391-2395, 2015.

[37] S. Li and G. Ge, Constructions of maximum distance separable symbol-pair codes using cyclic and constacyclic codes, *Des. Codes Cryptogr.*, vol. 84, pp. 359-372, 2017.

[38] S. V. Maric and V. K. N. Lau, Multirate fiber-optic CDMA: System design and performance analysis, *J. Lightwave Technol.*, vol. 16, pp. 9-17, 1998.

[39] C. Munuera, On the main conjecture on geometric MDS codes, *IEEE Trans. Inform. Theory*, vol. 38, pp. 1573-1577, 1992.

[40] R. Omrani, G. Garg, P. V. Kumar, P. Elia and P. Bhambhani, Large families of asyptotically optimal two-dimensional optical orthogonal codes, *IEEE Trans. Inform. Theory*, vol. 58, pp. 1163-1185, 2012.

[41] R. Pan and Y. Chang, Further results on optimal $(m, n, 4, 1)$ optical orthogonal signature pattern codes, *Sci. Sin. Math.*, vol. 44, pp. 1141-1152, 2014.

[42] R. Pan and Y. Chang, $(m, n, 3, 1)$ optical orthogonal signature pattern codes with maximum possible size, *IEEE Trans. Inform. Theory*, vol. 61, pp. 1139-1148, 2015.

[43] S. Payne, Topics in finite geometry: ovals, ovoids and generalized quadrangles, *UC Denver Course Notes*, 2009.

[44] P. R. Prucnal (Editor), Optical code division multiple access: fundamentals and applications, CRC Press, Boca Raton, FL, 2006.

[45] P. R. Prucnal, M. A. Santoro and T. R. Fan, Spread spectrum fiberoptic local network using optical processing, *IEEE J. Lightwave Technol.*, LT-4, pp. 547-554, 1986.

[46] J. A. Salehi, Emerging optical code-division multiple access communications systems, *IEEE Network*, vol. 3, pp. 31-39, 1989.

[47] J. A. Salehi and C. A. Brackett, Code-division multiple access techniques in optical fiber networks: part I and part II, *IEEE Trans. Commun.*, vol. 37, pp. 824-842, 1989.

[48] M. Sawa, Optical orthogonal signature pattern codes with maximum collision parameter 2 and weight 4, *IEEE Trans. Inform. Theory*, vol. 56, pp. 3613-3620, 2010.

[49] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106 of *Graduate Texts in Mathematics*, Springer, Dordrecht, second edition, 2009.

[50] H. Stichtenoth, *Algebraic function fields and codes*, vol. 254 of *Graduate Texts in Mathematics*, Springer-Verlag, Berlin, second edition, 2009.

[51] D. R. Stinson, R. Wei and J. Yin, Packings, in: *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz (Editors), CRC Press, Boca Raton, FL, pp. 550-556, 2007.

[52] S. Sun, H. Yin, Z. Wang and A. Xu, A new family of 2-D optical orthogonal codes and analysis of its performance in optical CDMA access networks, *J. Lightwave Technol.*, vol. 24, pp. 1646-1653, 2006.

[53] S. Tamura, S. Nakano and K. Okazaki, Optical code-multiplex transmission by gold sequences, *IEEE J. Lightwave Technol.* LT-3, pp. 121-127, 1985.

[54] E. Yaakobi, J. Bruck and P. H. Siegel, Decoding of cyclic codes over symbol-pair read channels, *IEEE Int. Symp. Inf. Theory*, pp. 2891-2895, 2012.

[55] E. Yaakobi, J. Bruck and P. H. Siegel, Constructions and decoding of cyclic codes over $b$-symbol read channels, *IEEE Trans. Inform. Theory*, vol. 62, pp. 1541-1551, 2016.

[56] G. C. Yang and W. C. Kwong, Two-dimensional spatial signature patterns, *IEEE Trans. Commun.*, vol. 44, pp. 184-191, 1996.

[57] G. C. Yang and W. C. Kwong, Performance comparison of multiwavelength CDMA and WDMA+CDMA for fiber-optic networks, *IEEE Trans. Commun.*, vol. 45, pp. 1426-1434, 1997.

[58] H. Yin and D. J. Richardson, Optical code division multiple access communication networks: theory and applications, Tsinghua University Press, Beijing and Springer-Verlag GmbH Berlin Heidelberg, 2007.

[59] J. Zhang, F. Fu and D. Wan, Stopping sets of algebraic geometry codes, *IEEE Trans. Inform. Theory*, vol. 60, pp. 1488-1495, 2014.

# 攻读博士学位期间主要研究成果

1. Baokun Ding, Gennian Ge, Jun Zhang, Tao Zhang, Yiwei Zhang, New constructions of MDS symbol-pair codes, Designs, Codes and Cryptography, vol. 86, no. 4, pp. 841-859, Apr. 2018.

2. Baokun Ding, Tao Zhang, Gennian Ge, Maximum distance separable codes for $b$-symbol read channels, Finite Fields and Their Applications, vol. 49, pp. 180-197, Jan. 2018.

3. Lijun Ji, Baokun Ding, Xin Wang, Gennian Ge, Asymptotically optimal optical orthogonal signature pattern codes, IEEE Transactions on Information Theory, doi: 10.1109/TIT.2017.2787593. (**ZJU TOP 100**)

4. Jerod Michel, Baokun Ding, A generalization of combinatorial designs and related codes, Designs, Codes and Cryptography, vol. 82, no. 3, pp. 511-529, Mar. 2017.