分类号：O157.2　　单位代码：10335

密　级：　　学　　号：11006131

浙江大学

博士学位论文

中文论文题目：几类编码问题研究中的组合学方法

英文论文题目：Combinatorial Approaches to Several Selected Topics in Coding Theory

申请人姓名：高　斐

指导教师：葛根年　教授

合作导师：

专业名称：应用数学

研究方向：组合设计与编码

所在学院：理学院数学系

论文提交日期：二〇一三年 四月

几类编码问题研究中的组合学方法

论文作者签名：_____

指导教师签名：_____

论文评阅人 1：孙智伟 \ 教授 \ 南京大学

评阅人 2：李方 \ 教授 \ 浙江大学

评阅人 3：常彦勋 \ 教授 \ 北京交通大学

评阅人 4：符方伟 \ 教授 \ 南开大学

评阅人 5：殷剑兴 \ 教授 \ 苏州大学

答辩委员会主席：冯克勤 \ 教授 \ 清华大学

委员 1：冯克勤 \ 教授 \ 清华大学

委员 2：李松 \ 教授 \ 浙江大学

委员 3：武俊德 \ 教授 \ 浙江大学

委员 4：谈之奕 \ 教授 \ 浙江大学

委员 5：葛根年 \ 教授 \ 浙江大学

答辩日期：二〇一三年 五月

Combinatorial Approaches to Several Selected Topics in Coding Theory

Author's signature: _____

Supervisor's signature: _____

External Reviewers: Zhiwei Sun\Professor\Nanjing University

Fang Li\Professor\Zhejiang University

Yanxun Chang\Professor\Beijing Jiaotong University

Fangwei Fu\Professor\Nankai University

Jianxing Yin\Professor\Soochow University

Examining Committe Chairperson:

Keqin Feng\Professor\Tsinghua University

Examining Committe Members:

Keqin Feng\Professor\Tsinghua University

Song Li\Professor\Zhejiang University

Junde Wu\Professor\Zhejiang University

Zhiyi Tan\Professor\Zhejiang University

Gennian Ge\Professor\Zhejiang University

Date of oral defence: May 2013

致　谢

本文得以顺利完成，首先要感谢我的导师葛根年教授。在五年的学习中，他用言传身教的方式，让我学到了太多。感谢葛老师带领我走上科研的道路，每一篇论文从思想、写作到完稿无不倾注了他大量的心血。同时也感谢葛老师让我参加了多次学术会议，扩大了我的视野。导师精深的理论知识，广阔的学科视野，严谨的治学态度，高尚的敬业精神时刻感染着我，成为我奋发向上的动力，也将成为我今后学习和追求的目标。

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

衷心感谢福建师范大学的张胜元教授，同济大学的杨亦挺博士和浙江大学的冯涛博士等。在这段时间里，他们给了我许多的指导和帮助，同时扩展了我的知识面，在此表示诚挚的感谢。

最后，感谢所有一直关心我的老师和朋友，特别要感谢我的家人给予我的理解和支持。

由于能力和时间有限，论文中必有缺点和错误之处，请各位专家学者不吝赐教！

摘　要

伴随着以计算机科学为代表的第三次工业革命的爆发，古老的组合数学重新焕发青春，而编码理论更是现代计算机科学和数字通信技术的核心。组合数学、计算机理论和数字通信技术的研究对象都具有离散性质，三门学科之间存在着天然的联系。在本篇论文中，我们将从组合数学的视角出发考察编码理论中的几类问题，包括常用的最优线性纠错码，电力线通信中的非线性纠错码，以及用于多媒体防伪和信号压缩感知的信息编码等。

在论文的第一部分，我们将研究两类优良线性分组纠错码的组合构造方法。由于线性码具有高效的编码算法，是在实际生活中最为常用的编码。在第 2 章中，我们将展示利用差集的轨道矩阵来构造线性码码链的想法。这一方法是受到 Ding 等人从差集构造循环码以及 Lander 使用关联结构得到子模码等相关工作的启发而获得的。在这一章中，我们将从具有素数阶半正则自同构群的循环差集出发，研究其关联矩阵在同构作用下的轨道形成的分块阵列。利用阵列的 Smith 标准型中的不变因子序列分布情况，我们从轨道矩阵中选取适当的行空间序列构造线性码码链。很多例子都显示，这一构造方法得到的码链中包含了许多达到各种理论上界的最优线性码。

但遗憾的一点是，上述方法构造的线性码不一定保持循环性，因此其解码复杂度可能较高。为了克服这一缺点，我们将在第 3 章中研究一类可以通过信息传递等迭代算法快速译码的分组线性纠错码，即低密度奇偶校验码（LDPC 码）。这是一类性能非常接近 Shannon 极限的好码，已经在当前各种最新的通信标准中占据主导地位。通过对基于循环群上的差矩阵内的元素进行二元矩阵散布，我们可以获得正则的拟循环低密度校验矩阵。与文献中从其它组合结构得到的码进行比较后发现，我们的方案在性能上与前人结果非常接近，但具有更大的灵活性，可以选择的参数更广。

第 4 章和第 5 章一起构成了论文的第二部分。我们将在其中讨论在电力线通信技术中具有重要应用的两类非线性分组纠错码，它们分别是置换码和常重复合码，其中后者可以看作是前者的推广形式。当然，这两类编码在其它领域也都具有广泛的应用。目前关于置换码的研究进展非常缓慢，事实上，我们只能构造出最小距离不超

过 3 的最优置换码。而对于一般的距离条件，关于其码字个数的上下界估计都是极其困难的。在第 4 章里，我们通过将置换码对应到 Cayley 图上的顶点独立集，从而利用图论中的方法对码字数目的下界进行估计。在渐近意义下，即当码长 n 趋于无穷时，我们的结果将传统的 Gilbert–Varshamov 型下界提高了 $\Omega(\ln(n))$ 倍。

第 5 章中将探讨的常重复合码，可以看作置换码放松了每个字母只能在码字中出现一次这一条件后得到的推广形式；另一方面，它也可以被看作是传统的二元常重码的一类扩展。从二十世纪九十年代后期以来，人们才逐渐展开关于最优常重复合码的系统性研究。其中 Chee 等人于 2008 年确定出了重量为 3 时，所有长度和距离的最优三元常重复合码所含的码字个数。在这一章中，我们将延续前人的工作，利用可分组码以及各种组合设计中的递归方法，完全构造出重量为 4 且最小距离为 5 时，所有长度的最优三元常重复合码。

以上两个部分中研究的几类编码，都属于信道编码中的分组纠错码。而在论文的最后一部分，即第 6 章和第 7 章中，我们将把关注点转移到两类信息编码问题上。为了应对数字多媒体内容的盗版和篡改等问题，一种通行的方法是向这些内容中嵌入数字指纹。但普通的指纹只能追踪单个非法用户，而对于合谋犯罪无能为力。第 6 章所考虑的可分码就是在这一背景下由 Cheng 等人提出的，它可以用来抵抗合谋犯罪中最为常见的平均攻击模型。本章中研究了强度 $t = 2$ 时，可分码的上下界问题。我们利用坐标分组的想法，大幅改进了前人提出的上界。特别的，当可分码是一个线性码时，其上界可以被进一步降低，并且我们将利用正交表构造出了达到这一上界的线性可分码。另一方面，我们分别使用概率方法和 Stein–Lovász 定理，得到了可分码的一些下界结果。其中，在码长固定而字母表大小趋向无穷的这一渐近意义下，由前一方法得到的可分码的大小和我们改进后的上界具有相同的阶。

在第 7 章中，我们展示了使用代数曲线构造压缩感知矩阵的方法。压缩感知理论研究如何从极少次数的测量结果中恢复出原始的稀疏信号，这一过程也可以被理解成实数域上的信源编码问题。受到 DeVore 想法的启发，我们从有限域上的代数曲线出发，利用除子的 Riemann–Roch 空间内所有函数在曲线的一些有理点处的取值，构造出合适的二元感知矩阵。通过选取适当的参数，DeVore 构造的矩阵也可以由我

们的方法给出。数值模拟也显示，当矩阵规模较小时，我们的矩阵和已知最优的随机 Gauss 矩阵在信号恢复性能上相差不大。

关键词：编码理论，Cayley 图，差集，差矩阵，代数曲线，低密度奇偶校验码，独立集，概率方法，可分码，Stein–Lovász 定理，压缩感知，置换码，组合数学

Abstract

Along with the outbreak of the third industrial revolution, combinatorics enjoyed a great resurgence. It studies the discrete objects as computer science and digital communication technology do. Meanwhile, coding theory plays a fundamental role in the latter two fields. In this dissertation, we will study several topics in coding theory from a combinatorial point-of-view. These problems include the optimal linear error-correcting block codes, the nonlinear block codes used in powerline communications, the separable codes designed to prevent collusion attacks for digital fingerprintings, and the sparse signal sampling in compressed sensing theory.

In the first part, we will investigate two kinds of optimal linear codes. Due to the highly efficient encoding algorithms, linear codes are the most commonly used coding schemes in daily lives. In Chapter 2, we will present how to construct submodule code chains from the orbit matrices of difference sets. Our idea comes from Ding's and Lander's works. They studied the cyclic codes from difference sets and the submodule codes from incidence structures, respectively. In this chapter, we will begin with the cyclic difference sets possessing a semi-regular automorphism of a prime order and investigate the orbits of incidence matrices under this automorphism. Using information about invariant factors of the Smith normal forms of orbit matrices, submodule code chains are obtained. A lot of examples will demonstrate that our resultant codes are optimal since their minimum Hamming distances can reach some theoretical upper bounds of linear codes. However, a weakness of these codes is that they usually do not remain the cyclic property. Therefore, the decoding complexity of them will be potentially higher.

To overcome this drawback, we will consider a class of linear codes with highly efficient encoding and decoding algorithms in Chapter 3, namely the low-density parity-check (LDPC) codes. These codes can be effectively decoded with recursive methods such as message-passing algorithms. LDPC codes play important roles in almost every modern

communication standard since their performances are extremely close to the Shannon limit. Based on the binary dispersion of entries in difference matrices over a cyclic group, we will get regular LDPC codes with quasi-cyclic property which can be equipped with even faster encoding and decoding algorithms. Comparing with those from other combinatorial structures in literature, our codes are equally well in the performance and with much more flexibility on parameters.

The second part consists of Chapters 4 and 5. Our focuses are two classes of nonlinear error-correcting codes widely used in powerline communications, namely the permutation codes (PCs) and the constant-composition codes (CCCs). We remark that both codes have been found to have important applications in other areas as well. The researches on PCs went very slow. In fact, we only know how to construct optimal PCs with minimum Hamming distance no larger than 3. For the general distances, even the good upper or lower bounds on code sizes are difficult to get. In Chapter 4, we will provide a lower bound of PCs via graph theory. To be specific, we shall establish a connection between PCs and independent sets of a well-chosen Cayley graph. The lower bound of PCs then comes along with analysis of independence number of the graph. Our result asymptotically improves the classical Gilbert–Varshamov bound with a factor of $\Omega(\ln(n))$ with distance d fixed and code length n going to infinity.

Chapter 5 is dedicated to constant-composition codes. These codes can be regarded as a relaxation of PCs by loosening the requirement that every symbol occurs exactly once in each codeword. They can also be regarded as a generalization of classical binary constant-weight codes. The systematic study of CCCs only began in late 1990s. Today, the problem of determining the maximum size of a CCC constitutes a central problem in their investigation. In 2008, Chee et al. completely solved the case of ternary CCCs with weight 3. In this chapter, we will follow their work and construct optimal ternary CCCs with weight 4 and distance 5 for all lengths. Our main tools are group divisible codes and several combinatorial recursive methods.

All codes in the above two parts belong to the category of channel coding. In the last

part, we shall switch our attention to some coding problems in information theory. In order to fight against the pirates of multimedia contents, digital fingerprintings are embedded to all legitimate distributions. Moreover, if we want to defend the collusion attacks, these fingerprintings have to be delicately encoded. Separable codes (SCs) in Chapter 6 were introduced by Cheng and Miao to resist the averaging attack which is the most common collusion mode. We will investigate the upper and lower bound of SCs for strength two in this chapter. By grouping coordinates, we can tremendously cut down the known upper bound. On the special case that an SC coincidences with a linear vector space over a finite field, the upper bound can be further reduced. Linear SCs matching this bound are constructed via orthogonal arrays as well. On the other hand, probabilistic method and Stein–Lovász theorem will be applied to obtain the lower bounds of SCs. When we fix the code length and let the alphabet size go to infinity, codes from probabilistic method share the same order to the upper bound we have just derived.

Lastly, we present a way to acquire good compressed sensing matrices from algebraic curves over finite fields in Chapter 7. The theory of compressed sensing studies the problem of recovering sparse signals from outcomes of a small number (comparing to the signal length) of measurements. This setup can be easily restated in the language of a source coding problem. Inspired by DeVore's method based on polynomials over finite fields, we will start with the algebraic curves. By evaluating the values of functions in the Riemann–Roch space of a divisor at some rational points of the curve, binary sensing matrices are constructed. With a proper choice of parameters, DeVore's results are included in our scheme as a special case. Numerical simulations will also show that our matrices are equally as good as the best known random Gaussian matrices when the signals are not too long.

Keywords: algebraic curves, Cayley graph, coding theory, combinatorics, compressed sensing, difference matrices, difference sets, independent sets, low-density parity-check codes, permutation codes, probabilistic methods, separable codes, Stein–Lovász theorem

目 次

致谢 I
摘要 III
Abstract VII
目次
1 绪论 1
1.1 组合数学与编码理论 1
1.2 线性纠错码 3
1.3 非线性纠错码 6
1.4 信息编码 9
2 线性码码链的差集构造 13
2.1 预备知识 14
2.2 线性码码链 17
2.3 不等价循环差集 24
3 LDPC 码的差矩阵构造 27
3.1 LDPC 码简介 27
3.2 拟循环 LDPC 码与差矩阵 29
3.3 数值模拟与分析 32
4 置换码下界的改进 35
4.1 置换码简介 35
4.2 已知的上下界 37
4.3 Cayley 图与独立集 38
4.4 改进置换码下界 40
5 最优常重复合码的组合递归构造 47
5.1 常重复合码简介 47
5.2 准备知识 49

5.3 确定 $A_3(n,5,[3,1])$ 的值 56
5.4 确定 $A_3(n,5,[2,2])$ 的值 67
5.5 表格附录 76
6 可分码上下界的研究 85
6.1 可分码简介 85
6.2 预备知识 85
6.3 改进 $\overline{2}$-可分码的上界 89
6.4 可分码的构造 94
7 压缩感知矩阵的构造 101
7.1 压缩感知理论简介 101
7.2 准备知识 104
7.3 主要结果 107
7.4 一些例子 110
8 讨论与展望 117
参考文献 121
攻读博士学位期间主要研究成果 139

图 目 录

3.1 LDPC 码性能比较,码率 0.75 33
3.2 LDPC 码性能比较,码率 0.9 34

7.1 16×64 阶感知矩阵的完美恢复率比较 112
7.2 32×512 阶感知矩阵的完美恢复率比较 113

表 目 录

2.1 由 Singer 差集得到的二元线性码码链 21
2.2 由 Singer 差集得到的多元线性码码链 22
2.3 由 Segre 差集得到的线性码码链 23
2.4 由 Glynn 第 I 和第 II 型差集得到的线性码码链 23
2.5 由 Dillon–Dobbertin 差集得到的线性码码链 24

4.1 当 $d=4$ 和 5 时，(n,d)-置换码的下界（$8\le n\le 20$） 43

5.1 当 $n\le 10$ 时，$A_3(n,5,[3,1])$ 和 $A_3(n,5,[2,2])$ 的值 48
5.2 最优 $(16,5,[3,1])_3$-码的 37 个码字 65
5.3 最优 $(12,5,[2,2])_3$-码的 30 个码字 70
5.4 6^6 型 $[3,1]$-GDC(5) 中的 180 个码字 76
5.5 6^u2^1 型 $[3,1]$-GDC(5) 的基础码字，$u\in[4,7]$ 77
5.6 6^v4^1 型 $[3,1]$-GDC(5) 的基础码字，$v\in[4,9]$ 78
5.7 最优 $(n,5,[3,1])_3$-码的基础码字，$n\in\{24,30,42,54\}$ 79
5.8 最优 $(4t,5,[2,2])_3$-码的基础码字，$t\in\{6,7,9,11,13,17\}$ 80
5.9 最优 $(4t+1,5,[2,2])_3$-码的基础码字，$t\in\{6,7,9,11,13,17\}$ 81
5.10 最优 $(4t+2,5,[2,2])_3$-码的基础码字，$t\in[6,11]\cup\{13,14,17\}$ 82
5.11 最优 $(4t+11,5,[2,2])_3$-码的码字，$t\in\{0,1,2\}$ 82
5.12 最优 $(n,5,[2,2])_3$-码的基础码字，$n\in\{35,39,43,47\}$ 83

1 绪论

1.1 组合数学与编码理论

1.1.1 组合数学

组合数学(Combinatorics),是一门既古老又年轻的数学分支。当前世界上的许多组合学家都认为中国是组合数学的发源地。例如约在公元前2200年的易经上,就曾描绘了据说是刻画在黄河里神龟背上的两个数字配置图,即洛书与河图。

本世纪50年代以来,由于数字集成电路的迅猛发展,带动了以离散量为信息处理对象的数字电子计算机技术的飞跃发展,促进了以数字信号为传输对象的通信技术的日益兴盛。在这种条件下,以研究离散对象在各种约束条件下的安排与配置问题的组合数学,被赋予了新的任务和内容,已经成为深受人们重视的一门独立的数学分支。组合数学在理论上与数论、集合论、代数学、概率统计等有密切关系,在信息编码、计算机科学、数字通信、物质结构、生物遗传工程、试验设计、人工智能以及社会管理科学许多领域中,都有重要的应用。

作为组合数学来说,它所包含的内容应当是极其丰富的,而且将会随着科学技术的发展而不断扩大它的范畴,给它下一个确切的定义为时尚早。目前文献中,通常把组合数学的内容分为下列三方面:

(1) 研究事物安排的存在性,即把一组事物(通常是有限个事物)进行某种安排,使之满足一定的约束条件,研究这种安排是否存在。如果这种安排不总是可能时,那么就要分析在怎样的(必要的、充分的或充分且必要的)条件下,才能获得这种安排。

(2) 事物安排的计数与分类。如果某种安排是可能的,我们就可以来计算这类安排的数目,或者按一定的原则对它们进行分类。

(3) 研究各种安排的性质。当人们已经能够构造出某种安排时,就可以进一步研究某种安排的结构与特性。

概括的说,组合数学就是研究离散事物(简称元素)按照一定规则进行安排的存在性、构造法,以及计数、优化等方面内容的数学分支。它与离散数学、集合论、数论、

概率统计、代数以及编码理论等学科密切相关。在新的信息时代中,组合数学已经成为计算机科学发展的一个不可分割的部分。

1.1.2 编码理论

编码理论是应用数学、计算机和通信技术的交叉学科,在科学技术领域中,起着重要的作用。例如,在数学上,它促进了格的发展;在计算机领域中,基于编码的公共密钥体系解决了大量用户的安全通信问题;在通信领域,基于编码的信息表示(即信源编码)节省了信道资源,而信道编码(纠错编码)可以对抗信道噪声,降低发射功率,减小多用户间的干扰等。根据不同的编码属性,产生了不同的编码应用。因此,编码理论主要包括以下三个方面的内容:

(1)以保证数字信息传输和处理的可靠性为目的的差错控制编码(Error-Control Coding),又称为信道编码(Channel Coding)。

(2)以提高数字信息传输、存储处理的有效性为宗旨的信源编码(Source Coding)。

(3)以增加数字信息传输、存储的安全性为目标的数据加密编码(Data Encryption)。

这三方面内容与通信系统的三大关键问题,即可靠性、有效性和安全性是相对应的。差错控制编码技术类别繁多,应用面广,在上述三类编码中占有较大的比例。因此通常使用的"编码"这一术语,常常指差错控制编码译码技术。

通信的目的是要把对方需要的信息及时可靠地传递给对方。Shannon 在 1948 年发表的重要论文《通信的数学原理》中[146],首次系统阐述了这个问题,并且指出点对点通信问题可以分解为独立的两部分。首先发送方使用信源编码器将信息进行编码,形成比特流;理想情况下,信源编码器应该在保持足够准确度的前提下,尽量去除掉原信息中的冗余,而用最少的比特数来表示出该信息。接下来,信道编码器对比特流进行编码,添加上一些冗余信息,这些冗余比特经过特别仔细的选择,使得比特流在传输时能够最大限度地对抗信道内的噪声干扰。最后接收方利用译码器对收到的比特流进行解调制,以最大可能恢复出原始的信息。

在差错控制系统中,信道编码存在着多种实现方式,同时信道编码也有多种分类方法。

（1）按照信道编码的不同功能，可以将它分为检错码（Error Detecting Code）和纠错码（Error Correcting Code）。检错码仅能检测错误，例如在计算机串口通信中常用到的奇偶校验码等；纠错码可以纠正错误，当然同时有检错功能，当发现不可纠正的错误时可以发出出错指示。

（2）按照信息位和校验位之间的检验关系，可以将其分为线性码和非线性码。如果信息位与检验位之间的关系为线性关系，即满足一组线性方程，称为线性码；否则称为非线性码。

（3）按照信息码元和校验码元之间的约束方式不同，可以分为分组码（Block Code）和卷积码（Convolutional Code）。在分组码中，编码后的码元序列每 n 位分为一组，其中 k 位信息码元，$r = n - k$ 个校验位。校验码元仅与本码字的信息码元有关；卷积码则不同，校验码元不但与本信息码元有关，而且与前面码字的信息码元也有约束关系。

（4）按照用于编码中使用的字母表大小，可以分为二进制信道编码（二元码）和多进制信道编码（多元码）。

除了以上信道编码的分类方法之外，我们还可以按照信息元在编码后是否保持原来的形式将其分为系统码和非系统码；按照纠错类型的不同，分为纠正随机错误码和纠正突发错误码；按照信道编码所采用的数学方法，分为代数码、几何码和算术码等。

1.2 线性纠错码

设 Q 是一个包含“0”元素的 q-元有限集，并设 n 是一个正整数。我们将 Q 上的 n 长向量集合 Q^n 的子集 $\mathcal{C}$ 称为**码**，其中参数 n 被称为码的**长度**（Length），而将集合中含有向量的个数 $|\mathcal{C}|$ 称为码的**大小**（Size）。码 $\mathcal{C}$ 中的每个向量 $\mathtt{x} \in \mathcal{C}$ 被称为一个**码字**（Codeword），它的 Hamming **重量** $wt(\mathtt{x})$ 被定义为其中非零位置的数目。两个不同码字 $\mathtt{x}, \mathtt{y} \in \mathcal{C}$ 之间的 Hamming **距离** $d(\mathtt{x}, \mathtt{y})$ 是其取值不同的位置的数目。码 $\mathcal{C}$ 的**最小 Hamming 重量**是 $wt(\mathcal{C}) = \min\{wt(\mathtt{x}) \mid \mathtt{x} \in \mathcal{C} \setminus \{\mathtt{0}\}\}$，其中 $\mathtt{0}$ 是全零向量；而码 $\mathcal{C}$ 的**最小 Hamming 距离**是 $d(\mathcal{C}) = \min\{d(\mathtt{x}, \mathtt{y}) \mid \mathtt{x}, \mathtt{y} \in \mathcal{C}, \mathtt{x} \neq \mathtt{y}\}$。我们也将 Hamming 重量与 Hamming 距离简称为**重量**与**距离**。

特别的，如果将字母表 Q 取作某个 q 元有限域 $\mathbb{F}_q$，其中 q 是一个素数幂，并且码 $\mathcal{C}$ 构成了向量空间 $\mathbb{F}_q^n$ 中的一个 k-维线性子空间（$0 \leq k \leq n$），那么我们称 $\mathcal{C}$ 是限域域 $\mathbb{F}_q$ 上的一个$[n,k]_q$ **线性码**。注意到，对于一个线性码，它的最小重量和最小距离总是相等的，因此我们将不再加以区分。如果一个 $[n,k]_q$ 线性码的最小距离为 d，那么将其记作 $[n,k,d]_q$ 码。

线性码较之于非线性码最大的优势是它们的编码复杂度较低。我们将在本文中首先讨论从组合设计结构中构造出好的线性码的一些想法。当然，关于什么是“好码”的观点不尽相同。由于每个 $[n,k,d]_q$ 线性码都可以用于纠正信道传输过程中发生的任意 $\lfloor d/2 \rfloor$ 个错误，我们称一个 $[n,k,d]_q$ 码是**最优的**，如果它的最小距离达到了所有 $[n,k]_q$ 码中的最大值。在第 2 章中，我们将提出一个从差集出发得到线性码码链的方法。许多例子都显示出这样构造的线性码中有很多是最优的。另一方面，我们也可以从实用角度看，将那些具有低译码复杂度，并且码率接近 Shannon 界的线性码称为好码，低密度奇偶校验码（Low-Density Parity-Check Code，LDPC 码）就是其中的代表。在第 3 章，组合设计理论中的差矩阵将被用来构造这样的二元 LDPC 码的校验矩阵。

1.2.1 线性码码链与循环差集

在数字通信中，循环码（Cyclic Code）是一类重要的纠错码。尽管循环码的纠错能力并不是最好的，但由于它们具有高效的编码译码算法而被广泛应用于数据存储系统和数字通信系统中[38,77,179]。在已知的循环码构造方法中，（循环）差集及相关序列成为最优和近似最优循环码的一个重要的来源[6,59,134,142,151,182,192]。另一类在分组线性纠错码的研究中发挥巨大贡献的是各种组合结构的关联矩阵，例如 Tonchev 的专著中就展示了许多这样的构造方法[172]。Lander 也早在 1983 年提出了从对称设计构造一列线性码的想法[114]。人们还发现具有素数阶半正则自同构群的对称设计与自正交码之间有着紧密联系。这一关系促使大家对由对称设计导出的自正交码的分类进行研究[94,126,133,171]。

第 2 章的内容将是对于上面两个想法的延续和推广。我们将从差集出发，选择它的一个素数阶半正则自同构群，考察差集的关联矩阵在这个同构群作用下的轨道。根据点轨道和区组轨道之间关联关系（即轨道矩阵）的 Smith 标准型中不变因子的分

布情况，我们可以得到轨道矩阵行空间的一列线性码码链。大量的例子都说明，这一方法在构造最优线性码方面拥有巨大潜力。另外，我们还分析了由全部五类不等价的 $(511, 255, 127)$-循环 Hadamard 差集导出的所有线性码码链中线性码的参数情况。这一工作是在导师葛根年教授与研究员冯涛博士指导下，由博士研究生李抒行与笔者共同完成的。

1.2.2 LDPC 码与差矩阵

现代数字通信系统几乎都采用了纠错编码技术，可以提供一定的编码增益。LDPC 码就是一种性能非常接近 Shannon 极限的好码，能提供较高的编码增益，可用来大大降低无线设备的发送功率并减小天线尺寸，因此研究 LDPC 码具有巨大的实际意义和经济价值。

LDPC 码是线性分组码的一种，它的校验矩阵是一种稀疏矩阵，也就是矩阵中大部分的元素都是零。奠定了噪声信道编码理论基础的 Shannon 定理在理论上的证明是非构造的，他采用的信道编码是随机码，没有提出具体的编码译码算法。二十世纪六十年代初，Gallager 在他的博士论文中提出了两个创造性的观点[83]：用简单的校验矩阵的随机置换和级联模拟随机码；在信息的先验概率和信道特性已知情况下的迭代译码算法。他在论文中对 LDPC 码进行了系统全面的论述，奠定了 LDPC 码研究的理论基础。但由于当时计算能力和存储能力的限制，人们没有认识到 LDPC 码的优越性。

从 Gallager 提出 LDPC 码到 MacKay 等人重新发现的 30 多年间，只有少数人关注过 LDPC 码，其中 Tanner 提出的 LDPC 码的二部图表示是期间的主要进展[167]。从 Tanner 图上，我们可以直观的理解 LDPC 码的迭代译码过程。在 1999 年，MacKay 等人总结前人工作[125]，在文献中详细论述了 LDPC 码的理论和实际性能，证明了 LDPC 码是一种实用好码，推广了 Gallager 的概率迭代译码算法，说明了实用译码方法的详细实现方法。他们的工作极大推动了 LDPC 码的发展，是 LDPC 码历史上最重要的一个里程碑。现今，LDPC 码已经被采纳进许多最新的行业或国家标准，如欧洲 DVB-S2 标准，IEEE 802.16e 标准，中国数字电视地面广播 GB20600 标准等。同时，LDPC 码也是第四代移动通信系统的主要备选方案。

在第 3 章中，我们将提出一类从差矩阵出发构造二元 LDPC 码的想法，即对循环

群上的差矩阵中的元素进行二元矩阵散布，获得围长不小于 6 的正则拟循环 LDPC 码。事实上，利用各种已知的组合结构构造 LDPC 码的想法并不罕见。但我们利用散布的方法得到的 LDPC 码和之前的结果相比较，具有更大的灵活性，可以覆盖更广的参数范围。并且数值模拟也表明，我们构造出的码与各种已知方法在性能上非常接近，这其中还包括一些已经入选各类最新通信标准协议的码类。

1.3 非线性纠错码

正如我们之前提到的，非线性纠错码通常比线性码的编码译码复杂度高，但是在一些特殊应用场景中，非线性码却具有巨大的潜力。在第 4 章和第 5 章中，我们将分别讨论置换码（Permutation Code）和常重复合码（Constant-Composition Code）。它们都在电力线通信（Power Line Communication，PLC）领域具有重要应用。

电力线通信技术是指利用电力线传输数据和媒体信号的一种通信方式。该技术将经过调制的高频载波信号加载于电流，然后通过电力线传输，接受信息的调制解调器在接收端再把高频载波信号从电流中分离出来并传送到计算机、电视电话等终端以实现信息传递。电力线通信技术最大的优势是不需要重新布线，在现有电力线设备上实现包含语音视频等在内的各种多媒体数据业务的承载，实现四网合一。在中国，三网已经开始进行融合，这对电力线通讯需求也就越来越强烈。

电力线通信技术于 20 世纪初伴随着电力供应的普及而出现。大约在 1922 年左右，第一个用于遥感勘测的窄带电力线载频通信系统已经开始运作在高压输电线上。而在 1940 年，已经出现了诸如婴儿报警器一类的家用消费产品。自上世纪 70 年代开始，一项被称为 X10 的技术流行起来，它作为一种实现家庭自动化的方式，可以通过电力线通信设备调制信息并加载到家庭电力布线上传输，达到远程控制照明设备和家用电器等功能。到 80 年代中期，数字通信技术和数字信号处理等领域展现出巨大的潜在市场前景，这驱动工业与科学界进一步研发生产更加具有竞争力的廉价可靠系统。1991 年美国电子工业协会确认了三种家庭总线，电力线是其中一种。欧洲委员会于 2003 年至 2006 年资助了一个电力线和网络实时进行能源管理的项目 REMPLI。由思科、英特尔、惠普、松下和夏普等 13 家公司成立“家用电力线网络联盟”（HomePlug Powerline Alliance），致力于创造共同的家用电线网络通讯技术标

准。目前部署最广泛的电力线网络标准来自于该联盟，其中最新的 HomePlug AV 规范，已于 2010 年 12 月被 IEEE 1901 小组作为其基础标准。该联盟称已有超过 4 千 5 百万的 HomePlug 设备已经部署在世界各地，占目前全球宽带电力线通信市场中的 80% 以上。其他公司与组织也提出了各自不同的技术规范，如通用电力线协会（Universal Powerline Association），HD-PLC 联盟，ITU-T 的 G.hn 规范。

在中国，20 世纪 40 年代已有日本生产的载波机在东北运行，作为长距离调度的通信手段。从 1999 年起，中国电力科学研究院就开始对高速电力线通信进行研究，并在 2001 年 8 月，在沈阳建立了第一个实验网络。又从 2001 年 12 月起，国电通信中心开始组织国内外厂商在北京居民区开展电力线通信应用试验，这些公司包括韩国的 Xeline（14Mb/s 系统）、瑞士 ASCOM 公司（4.5Mb/s 系统）、美国 Leap 公司（14Mb/s）、西班牙的 DS2 公司. 福建电力试验研究院（10Mb/s 系统），以及中国电力科学研究院（14Mb/s 系统）等。中国福建省电力试验研究院研制成功“数字化输电线路技术”的核心产品——电力调制解调器及多个相关产品，其传输速率达到 10M。同时国电通信中心采用国内外电力线通信组网设备，在北京某生活小区成功地进行了互联网接入试验，并获得了较理想效果。随着研究的深入，电力线通信技术也向更高速率发展。例如将速率提高到 100Mb/s，甚至 200Mb/s。届时，高速电力线通信将为宽带接入通信做出更大贡献科学技术的竞争已不仅仅是技术专利的竞争，而是标准的竞争。包括家用电力线网络联盟，通用电力线协会，HD-PLC 联盟等多个竞争组织都发布了其技术规范。2008 年 12 月，ITU-T 采用了 G.hn/G.9960 推荐标准作为其高速电力线、同轴电缆和电话线通讯的标准。美国国家能源营销者协会也参与了国际电子电气工程协会（IEEE）的 IEEE P1901 工作组，开发高速电力线载波通信的全球标准。该工作组于 2009 年 7 月批准了“IEEE 1901 电力线网络宽带标准草案”，定义了媒介访问控制和物理层技术规范。这一草案已于 2011 年 2 月 1 日获得 IEEE 组织的批准和发布。

目前，电力线通信技术主要存在以下方面的问题有待进一步研究。硬件平台：主要包括通信方式的合理选择、通信网络结构的优化选择等。扩频方式：OFDM 技术和多维网格编码方式各有优点，哪一种适合低压网还有待研究。电力网结构非常复杂，网络拓扑千变万化，如何优化通信网结构也是值得研究的问题。软件平台：主要包括进一步研究 PLC 通信理论，改进信号处理技术和编码技术以适应 PLC 特殊的环境。

网络管理问题：除了上网、打电话外，低压电力线还可以完成远程自动读出水、电、气表数据；永久在线连接，构建的防火、防盗、防有毒气体泄漏等的保安监控系统；构建的医疗急救系统等等。因此利用电力线可以传输数据、语音、视频和电力，实现四网合一，也就是说家中的任何电器都可以接入到网络中，和骨干网连接。但是如何实现四种网络的无缝连接，以及由此带来的非常复杂、庞大的网络管理问题需要进一步的研究。

1.3.1 置换码与 Cayley 图上的独立集

置换码是一类特殊的非线性码，其码字长度与字母表大小相同，并且每个码字都是由字母表中全部符号构成的一个置换排列。或者，我们也可以等价的定义置换码为 n 阶置换群 S_n 的任意一个子集。

关于置换码的存在性研究始于三十多年前[57,78]，然而直到近十年以前，依然仅有少数人关注。自 2000 年以来，研究者陆续发现了置换码在电力线通信[76,132,177]，分组密码设计[54]，和多层闪存[101,102] 中的应用，置换码因而开始经历一次强力复苏。在电力线通信应用中，我们可以通过将传输电流调制成为一族 n 个相互接近的频率，从而在不影响电力输送的同时传递信息。接收端除了获得电力，还可以将频率的变化解调制为字母符号，解读信息[39,132]。为了让信息的传送不对电力传送产生干扰，这些调制后的频率越恒定越好，一种可行的方式就是采用置换码对信息进行编码。进一步的研究表明，使用置换码来编码信息可以有效克服电力线通信过程中占主导的窄带噪声和脉冲噪声，提高信息传递的可靠性[76,177]。

目前已知的关于置换码大小的研究，还只有一些初等的结果。我们将在第 4 章中深入讨论置换码大小的下界，并将传统的 Gilbert–Varshamov 型下界提高 $\Omega(\ln(n))$ 倍。这一章中用到的两个主要工具都来自于图论：独立集与 Cayley 图。图的独立集是指其中顶点的一个子集合，使得其中任意两点之间都没有边相连。图的所有独立集中最大的那个含有的顶点数被定义为图的独立数。独立数是图论中最重要的参数之一，与图的染色数、最大团等具有紧密关联，在图谱理论、Ramsey 理论等研究中都发挥作用。而 Cayley 图则是代数图论研究中的核心方法之一。通过建立置换群 S_n 上的 Cayley 图，每一个置换码都可以一一对应于 Cayley 图上的独立集。仔细计算图上任意顶点的诱导子图内的最大度后，我们可以得到关于独立数的估计，进而导出置

换码的下界。这一工作是与同济大学杨亦挺博士合作完成的，已经发表在 SCI 期刊《IEEE Transactions on Information Theory》。

1.3.2 常重复合码与组合递归方法

一个码 $\mathcal{C} \subseteq Q^n$ 被称为**常重复合码**，若字母表 Q 中任意元素在 $\mathcal{C}$ 中所有码字内出现的次数都是一样的。从定义可以看出，这是对置换码中要求的削弱。另一方面，它也可以看作是经典二元常重码向多元情形的自然推广。除了在电力线通信中的应用，常重复合码还广泛使用在多存取通信[72]（Multiple Access Communication），确定离散无记忆信道中零错误决策反馈容量[170]，球形码（Spherical Codes）调制[73]，DNA 码[106,127]，跳频（Frequency Hopping）技术[41] 等领域。

对常重复合研究始于 20 世纪 80 年代初，其核心问题是确定最优常重复合码所含有的码字数量。三元常重码的码字个数在许多文献中都有研究[20,33,86,163]。在 2008 年，Chee 等人构造出了所有重量为 3 的最优三元常重复合码[31]。

在第 5 章中，我们将解决一类参数下最优常重复合码的构造问题。具体说来，我们将确定出重量为 4 且最小距离为 5 时，所有长度下的三元常重复合码码字个数的上界，并且还将构造出达到这一上界的最优码。在这一章中，我们将大量使用各种组合递归方法，例如 Wilson 基本构造法、膨胀法、组填入法等。这些方法在传统的组合设计理论中均已展现出强大的能量。通过应用可分组码这一与组合设计理论中可分组设计相对应的编码概念作为骨架，我们将递归构造出所有需要的最优常重复合码。这一工作已经发表在 SCI 期刊《IEEE Transactions on Information Theory》上。

1.4 信息编码

在论文的最后一部分，我们将谈论多媒体取证和压缩感知等信息论研究中的两类编码问题。

1.4.1 多媒体数字指纹中的可分码

高带宽通信技术的普及和多媒体标准的发展导致了多媒体内容的急剧增长，多媒体数据已经成为我们相互沟通的主要载体。但那些用于便捷分享的技术同样也有利于非法或欺诈内容的传播。多媒体内容的替换、重包装和分发给政治和经济生活

带来了严峻的威胁。同时,我们还需要一种安全可靠的策略来控制多媒体信息的交流。多媒体取证就是要采用数字领域的证据,证明多媒体内容的是否被篡改,被怎样篡改,有哪些用户参与了篡改。

正如物理指纹是罪案调查中重要的取证对象之一,数字指纹技术给多媒体内容的每一个合法分发加入一个唯一的识别信息,使多媒体取证能够使用这些特殊的数字指纹识别信息来判断多媒体内容。除了惟一性,我们还需要分发的数字指纹具有各种良好的性质,如不能破坏原来的信息,不易被用户去除或破坏等。这样在发生泄密或篡改事件时,我们就可以通过调查数字指纹来追踪罪犯。

当在数多媒体数据中嵌入指纹时,一个必须考虑的问题是合谋(Collusion)犯罪。假设出版商发行了一个嵌入指纹的数字图像,如果一群获得它的用户可以通过比较他们的拷贝很容易的发现所有的标记。那么用户就能去掉这些标记,篡改这些差异,并重新发布这幅图像而不用担心被追踪到。合谋问题首先由 Blakley 等人提出[16]。1998 年,Boneh 和 Shaw 引入了 t-安全(t-Secure)码来获得抵抗合谋的安全指纹[21]。他们指出在数字指纹方案中合谋是最重要的问题,并且提出了针对合谋攻击的一个清晰解决办法。

为了抵抗合谋犯罪中最常见的平均攻击方法,Trappe 等人在 2003 年提出了 t-弹性与抗合谋码(t-Resilient AND Anti-Collusion Code,t-AND-ACC)的概念用来配合编码调制,达到检测最多 t 个恶意用户参与的平均攻击[173]。为了克服 t-AND-ACC 所支持的授权用户数目较少的劣势,Cheng 与 Miao 提出了 t-弹性逻辑抗合谋码(t-Resilient Logical Anti-Collusion Code,t-LACC),和 $\bar{t}$-可分码($\bar{t}$-Separable Code,$\bar{t}$-SC)这两个新概念[36]。事实上,一个二元 $\bar{t}$-可分码等价于一个 t-LACC。在后续的工作中 $\bar{t}$-可分码的存在性问题成为关注的重点[35],作者给出了 $\bar{t}$-可分码的一些上下界,并构造了长度为 2 和 3 时,部分字母表上的最优 $\bar{2}$-可分码。

在第 6 章中,我们会继续研究 $\bar{2}$-可分码的上下界问题。利用坐标分组的想法,我们大幅降低了 Cheng 等人提出的上界。特别的,当可分码是一个线性向量空间的时候,其上界可以被进一步的降低,并且我们可以利用正交表构造出一族达到上界的线性可分码。另一方面,我们分别使用删除法和 Stein–Lovász 定理,得到了可分码的一些下界结果。这两个方法中,前者属于随机构造,而后者是确定性的。其中,在码长固

定而字母表大小趋向无穷的这一渐近意义下，由随机方法构造出的可分码的码字个数和我们之前给出的上界具有相同的阶。

1.4.2 压缩感知理论

信号采样研究如何从自然界的模拟信号中获取可用计算机处理的数字信号。传统的信号采样方法依据的是著名的 Shannon–Nyquist 采样定理，即精确还原一个信号所需要的采样速率至少为信号带宽的 2 倍，这一速率被称为 Nyquist 速率。不断增大的数据量和高带宽信号的使用，对 Nyquist 速率下的信号采样提出了严峻的挑战[70]。事实上，为了方便传输，经过信号采样所得到的数据，需要首先被压缩，即信源编码。大部分在采样过程中获得的数据，在信源编码过程中随即被舍弃。Donoho 在其开创性的文章中对这种高速率采样伴随信源编码的模式提出了质疑，提出将采样和编码过程合并的目标[67]。

Donoho[67] 以及 Candès 和 Tao[29] 首先提出了实现这一目标的新颖的采样技术，称之为压缩感知（Compressed Sensing）。在信号处理领域中，存在大量的可压缩信号和具有稀疏表示的信号。压缩感知的模型指出，如果信号本身是可压缩的，或者在某组基下有稀疏的表示，那么可以通过远低于 Nyquist 速率的采样过程，获取包含信号本质信息的高度压缩的数据，从而将采样和压缩的过程合为一体。从压缩的数据恢复原始信号的过程，可以归结为求解一个优化问题。应用压缩感知的模型，在保证恢复出的信号质量的同时，采样速率（采样次数）可以大大降低，这一重大突破代表了信号采样领域令人兴奋的新进展。由于信号采样起着联系模拟信号和数字信号的基础作用，这个思想一经提出，就引起了多个领域的研究者的高度关注。这也使得压缩感知逐渐发展为一个多学科综合的热点领域。

目前，压缩感知的研究主要集中在以下三个方面：基础理论研究，感知矩阵的构造，恢复算法的设计。其中感知矩阵的构造是压缩感知中的核心问题。对于有限维的稀疏信号，可以通过做随机投影的方式进行采样。如果感知矩阵的每个元素相互独立，并且服从某一种概率分布，在一定的采样次数下，信号可以以极高的概率被恢复出来[29]。用这些随机矩阵作为感知矩阵，可以达到采样次数的下界[44]。随机矩阵的良好性质，使其成为广泛使用的感知矩阵。另一方面，构造确定性矩阵的研究也在逐步展开[5,22,25]。构造确定性矩阵的动机在于：针对具体的应用环境，采用确定性矩阵

和与之相适应的恢复算法，可以进一步提高数据采样的效率[130]。由于随机矩阵在硬件层面的实现难度很大，所以实际应用中，确定性矩阵必将成为感知矩阵的重要实现手段。

在第 7 章中，我们准备借鉴编码理论中代数几何码的思想，推广 DeVore 关于由有限域上多项式构造感知矩阵的想法[56]。简单的说，我们从有限域上的代数曲线出发，利用除子的 Riemann–Roch 空间内的函数在曲线有理点处的取值，构造出二元感知矩阵。通过选取适当的参数，DeVore 的矩阵也可以由我们的方法给出。数值模拟的结果也显示，当矩阵规模较小时，我们的矩阵和已知最优的随机 Gauss 矩阵在信号恢复性能上相差不大。这一工作是在福建师范大学张胜元教授访问浙江大学期间，与张教授以及博士研究生李抒行等人合作完成的，结果已经发表于 SCI 期刊《IEEE Transactions on Information Theory》。

2 线性码码链的差集构造

在数字通信中,循环码是一类重要的纠错码。尽管循环码的纠错能力并不是最好的,但由于具有高效的编码译码算法,它们被广泛应用于数据存储系统和数字通信系统中[38,77,179]。例如,BCH 码被应用在诸如卫星通信,光盘播放器,DVD,磁盘驱动器,固态驱动器,和二维条形码等之中;Reed–Solomon 码的应用全面覆盖了从深空通信到消费类电子产品的各方面。循环码还广泛应用在消费类电子产品如 CD,DVD,蓝光光盘,如 DSL 和 WiMAX 的数据传输技术,诸如 DVB 和 ATSC 的广播系统,以及如 RAID 6 系统等计算机应用之中。在已知的循环码构造方法中,循环差集及相关序列成为最优和近似最优循环码的一个重要的来源[6,59,134,142,151,182,192]。

另一类在分组线性纠错码的研究中发挥巨大贡献的组合结构是关联矩阵(Incidence Matrix)。在 Tonchev 的综合性手册中展示了许多从各种组合设计对象的关联矩阵构造线性码的方法[172]。Lander 也曾于 1983 年就提出了利用对称设计(Symmetric Design)的关联矩阵构造线性码链的想法[114]。研究者发现,具有素数阶半正则自同构群的对称设计和自正交码之间有着紧密联系。这一关系促使学者对由对称设计导出的自正交码进行分类研究[94,126,133,171]。

在这一章中,我们将遵循并推进 Ding 等人关于差集得到循环码以及 Lander 关于对称矩阵得到线性码链的想法,深入研究从差集的轨道矩阵构造线性码码链的问题。正如我们的例子将展示的那样,这一方法可以得到很多最优线性码。虽然受限于我们的计算能力,得到的这些最优码并没有新的参数,但我们依然相信我们的方法是获得新参数最优码的一个很好的候选方案。另一方面,正如 Lander 指出的,由对称设计导出的子模码链(Submodule Code Chain)可以看成是设计的不变量,因此我们的想法也应该可以在研究差集的同构问题中发挥作用。例如我们可以将五类不等价的 $(511, 255, 127)$-循环 Hadamard 差集根据它们导出的码链进行进一步的分类。我们希望这一从码到设计的信息反馈可以在今后差集的理论研究中得到应用。

本章其余部分的安排如下:第 2.1 节将用来介绍组合设计理论与编码理论中的相关概念,进行知识准备;然后,我们在第 2.2 节中将会展示从差集的关联矩阵与轨

道矩阵出发，构造线性码码链的想法；最后，我们将在第 2.3 节中仔细分析从不等价 $(511, 255, 127)$-循环 Hadamard 差集中导出的所有线性码码链的情况。

2.1 预备知识

2.1.1 组合设计

定义 2.1. 我们将二元对 $(X, \mathcal{B})$ 称为一个**集合系统**(Set System)，其中：X 是一个有限集，里面的元素被称为**点**(Points)；$\mathcal{B} \subseteq 2^X$，里面的元素被称为**区组**(Blocks)。我们将点集 X 的大小被称为这个集合系统的**阶**(Order)。假设 K 是一些非负整数构成的集合，如果 $\mathcal{B}$ 中的每个区组 $B \in \mathcal{B}$ 的大小都落在 K 中，即 $|B| \in K$，则我们称集合系统 $(X, \mathcal{B})$ 是**K-均匀的**(K-uniform)。

定义 2.2. 设 $\mathcal{D} = (X, \mathcal{B})$ 是一个 v 阶集合系统，记 $|\mathcal{B}| = b$。我们定义 $\mathcal{D}$ 的**关联矩阵**(Incidence Matrix)为 $b \times v$ 阶二元矩阵 $\mathtt{A}$，其中 $\mathtt{A}(i, j) = 1$ 当且仅当第 j 个点属于第 i 个区组之中，否则 $\mathtt{A}(i, j) = 0$。

我们称两个集合系统是**同构的**，指的是这两个集合系统的关联矩阵可以通过行重排或列重排而完全相同。一个集合系统的**自同构**是它到自身的一个同构，即点集上的一个保持区组集合不变的置换。换言之，一个集合系统的自同构指的是这样一对置换矩阵 $(\mathtt{P}, \mathtt{Q})$，使得 $\mathtt{A} = \mathtt{PAQ}$，其中 $\mathtt{A}$ 是集合系统的关联矩阵。我们将那些既没有不动点也没有不动区组的自同构称为**半正则的**(Semi-Regular)。

定义 2.3. 设 v, k, t 和 λ 为四个正整数，其中 $v \geq k \geq t$。令 $\mathcal{D} = (X, \mathcal{B})$ 是一个 $\{k\}$-均匀的 v 阶集合系统，若 X 中任意 t 个不同点都恰好只同时出现在 λ 个区组中，那么我们称集合系统 $\mathcal{D}$ 是一个**t-(v, k, λ) 设计**。若 $t = 2$，我们也将其简记为 (v, k, λ)-设计。

在一个 2-(v, k, λ) 设计 $\mathcal{D} = (X, \mathcal{B})$ 中，区组的数目 $b = |\mathcal{B}| = \lambda v(v-1)/(k(k-1))$，而每个点落在 $r = \lambda(v-1)/(k-1)$ 个区组中。如果 $v = b$，或者等价的 $k = r$，我们就称设计 $\mathcal{D}$ 是**对称的**。Tonchev 编著的手册[172] 中，已经展示了许多从设计的关联矩阵出发构造线性码的方法。而文献[171] 讨论了具有素数阶半正则自同构的 2-(v, k, λ) 设计与多元自正交码之间的关系。正是这一联系激起了关于对称设计导出自正交码的同构分类研究[94,126,133]。

定义 2.4. 令 G 为 v 阶有限群，其运算为加法，记群中的单位元为 0。设 D 是群 G 中的一个 k 元子集，又设 λ 为给定的正整数。如果对于群 G 中任意非单位元 $g \in G \setminus \{0\}$，都恰有由 D 中元素组成的 λ 个序对 (x, y) 使得 $g = x - y$，则称 D 为 G 中的一个(v, k, λ)-差集。特别的，如果群 G 是一个 Abel 群，或循环群，则我们也称差集 D 是 Abel 的，或循环的。我们定义一个 (v, k, λ)-差集的阶为 $n = k - \lambda$。

定义 2.5. 设 G 为 v 阶 Abel 群，其中的运算为加法。设 $a \in G$，对于子集合 $S \subseteq G$，令

$$S + a = \{x + a \mid x \in S\} \text{ 。}$$

我们将 $S + a$ 称为 S 的一个平移（Translation）。

下面的两个定理说明了 (v, k, λ)-差集与 (v, k, λ)-对称设计之间的关系。

定理 2.6：设 G 为 v 阶有限群，其运算为加法。则存在 G 中的 (v, k, λ)-差集的充分必要条件是存在一个正则的 (v, k, λ)-对称设计，它有一个与 G 同构的自同构群 $\tilde{G}$，并且 $\tilde{G}$ 在此设计的点集上正则的。

定理 2.7：设 G 为 v 阶 Abel 群，D 为 G 的 k-子集。令

$$\mathtt{dev}(D) = \{D + g \mid g \in G\},$$

则 D 为 G 中一个 (v, k, λ)-差集的充分必要条件是，$(G, \mathtt{dev}(D))$ 构成一个 (v, k, λ)-对称设计。

当差集是基于循环群时，与之相对应的设计也具有一个循环自同构。而循环差集是优良线性码的重要构造来源[6,59,134,142,151,182,192]。在下一节中，我们将研究如何从具有素数阶半正则自同构的差集构造一系列好的线性码。

2.1.2 线性码与对称设计

我们首先回忆一下线性码的定义。设 $\mathbb{F}_q$ 是 q 阶有限域，其中 q 是一个素数幂。设 n, k, d 是三个正整数，满足 $n \geq k$ 和 $n \geq d$。一个 $[n, k, d]_q$ 线性码指的是向量空间 $\mathbb{F}_q^n$ 中的一个 k 维子空间 $\mathcal{C}$，使得其中任意两个不同码字之间的距离不小于 d。我们称一个 $[n, k, d]_q$ 码是最优的，如果它的最小距离 d 达到了所有 $[n, k]_q$ 码中的最大值。

对于有限域 $\mathbb{F}_q$ 上的两个线性码，如果其中一个码可以通过重排坐标，或将所有码字中某一位置的元素乘以一个非零元素等操作变换得到另一个码，则我们称它们为**等价的**。

事实上，(v,k,λ)-对称设计的关联矩阵的行空间可以看作是任意有限域 $\mathbb{F}_q$ 上的一个 v 长线性码。这个码的维数和有限域 $\mathbb{F}_q$ 的大小密切相关。

性质 2.8：假设 $\mathcal{C}$ 是一个 (v,k,λ)-对称设计的关联矩阵中所有行向量在有限域 $\mathbb{F}_q$ 上张成的行空间中所有向量组成的 v 长线性码。则，

1．如果 $q \mid k-\lambda$，那么 $2 \le \dim \mathcal{C} \le (v+1)/2$；

2．如果 $q \nmid k-\lambda$，并且 $q \mid k$，那么 $\dim \mathcal{C} = v-1$；

3．如果 $q \nmid k-\lambda$，并且 $q \nmid k$，那么 $\dim \mathcal{C} = v$。

下面我们展示一个从 Singer 差集得到对称设计，进而生成线性码的例子。设 $m \ge 2$ 为一整数，p 为一素数幂。众所周知，射影几何 PG$(m-1,p)$ 的点和超平面构成了一个参数为

$$\left(\frac{p^m-1}{p-1}, \frac{p^{m-1}-1}{p-1}, \frac{p^{m-2}-1}{p-1}\right)$$

的对称设计。这样的参数被称为**经典参数**（Classical Parameter）$[p,m]$。这个对称设计也可以利用如下方法从一个差集中得到。令 α 是有限域 $\mathbb{F}_{p^m}$ 的乘法群生成元，即 $\langle\alpha\rangle = \mathbb{F}_{p^m}^{\times}$。那么整数集合 $D = \{0 \le i \le v-1 \mid \mathtt{Trace}(\alpha^i) = 0\}$ 就构成了循环群 $\mathbb{Z}/(v\mathbb{Z})$ 中的一个具有经典参数 $[p,m]$ 的循环差集，其中 $v = (p^m-1)/(p-1)$。这里 Trace 表示从有限域 $\mathbb{F}_{p^m}$ 到其子域 $\mathbb{F}_p$ 的**迹函数**

$$\mathtt{Trace}(\beta) = \sum_{i=0}^{m-1} \beta^{p^i}, \quad \beta \in \mathbb{F}_{p^m}。$$

我们将这样构造的差集称为 Singer 差集。

考虑一个具有经典参数 $[2,4]$ 的 Singer 差集：循环群 $\mathbb{Z}_{15} := \mathbb{Z}/(15\mathbb{Z})$ 的子集 $D = \{0,1,2,4,5,8,10\}$ 构成了这样一个 $(15,7,3)$-循环差集。此时，$(G, \mathtt{dev}(D))$ 就是一个 $(15,7,3)$-对称设计，它的关联矩阵 A 是一个 15×15 的循环矩阵，其中的第一行是 [111011001010000]。由于这个差集的阶是 $k-\lambda = 7-3 = 4$，所以对于任意奇素

数幂 q，矩阵 A 的行空间在有限域 $\mathbb{F}_q$ 上都构成一个 $[15,15,1]_q$ 线性码，即全空间 $\mathbb{F}_q^{15}$。而如果我们选取 $q=2$，那么 A 的行空间就是一个 $[15,5,7]_2$ 循环线性码，并且这个码是最优的[92]。

2.2 线性码码链

2.2.1 线性码码链与格

在上一节中，我们展示了一个从对称设计构造线性码的方法，但是这一方法每次都只能得到一个码，而我们希望能够做得更好。Lander 曾提出了一种从对称设计中获得一列线性码码链的有趣方法[114]。其中的基本想法是，我们每次只选择关联矩阵中的一部分行来生成线性码。在详细叙述这一想法之前，我们还需要一些关于格的基本知识。

对于正整数 m，我们定义**秩**(Rank)为 m 的**格**(Lattice)是有理向量空间 $\mathbb{Q}^m$ 中一个秩为 m 的自由 $\mathbb{Z}$-模中所有向量组成的集合。而我们最感兴趣的是那些由 $m\times m$ 阶有理矩阵的行向量生成的格，例如设计的关联矩阵等。此时，我们将这个矩阵称为格的**生成矩阵**(Generating Matrix)。如果一个方阵的行列式是单位元，即 ±1，那么我们称其为**幺模**(Unimodular)矩阵。注意到，如果 V 和 U 是同一个格 L 的两个生成矩阵，那么必定存在一个整系数的幺模矩阵 P，使得 $\mathrm{V}=\mathrm{PU}$，反之亦成立。

对于任意素数 p，都有许多种方法可以从一个格 L 中构造出有限域 $\mathbb{F}_p$ 上的线性码。如果 $L\subseteq\mathbb{Z}^m$，那么最简单的一个方法就是对 L 进行模 p 约分(Reduction Module p)。不仅如此，我们还可以将这一方法推广到从格 L 中构造出一个线性码的无穷码链出来。令

$$\pi^m:\mathbb{Z}^m\to\mathbb{F}_p^m$$

是一个“模 p 约分”的同态映射。对于整数 $\alpha=\ldots,-2,-1,0,1,2,\ldots$，定义有限域 $\mathbb{F}_p$ 上如下的码 $\mathcal{C}_\alpha$：

$$\mathcal{C}_\alpha=\pi^m(p^{-\alpha}L\cap\mathbb{Z}^m)。$$

显然的，我们有

$$\cdots\subseteq\mathcal{C}_{-1}\subseteq\mathcal{C}_0\subseteq\mathcal{C}_1\subseteq\mathcal{C}_2\subseteq\cdots。$$

这些码 $\mathcal{C}_\alpha$ 的维数与格 L 的生成矩阵 V 的不变因子(Invariant Factors)密切相关。

性质 2.9: 设 $L \subseteq \mathbb{Z}^m$ 为一个格,整数矩阵 V 是它的生成矩阵。令 π_i 是矩阵 V 中恰被 p^i 整除的那些不变因子 d 的数目。那么对于所有 $\alpha < 0$,均有

$$\dim \mathcal{C}_\alpha = 0 ,$$

而对于任意 $\alpha \geq 0$,均有

$$\dim \mathcal{C}_\alpha = \pi_0 + \cdots + \pi_\alpha 。$$

证明. 由于 $L \subseteq \mathbb{Z}^m$,我们从 $\mathcal{C}_\alpha$ 的构造方法就可以知道,对于所有 $\alpha < 0$ 均有 $\dim \mathcal{C}_\alpha = 0$。

设 P 和 Q 是两个整数幺模矩阵,使得 PVQ 是一个对角矩阵 S:

$$\mathtt{PVQ} = \mathtt{S} = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_m \end{pmatrix} 。$$

那么 $\mathtt{PV} = \mathtt{SQ}^{-1}$,并且 $\mathtt{SQ}^{-1}$ 也是格 L 的生成矩阵。此时存在整数向量 $\mathtt{v}_1, \ldots, \mathtt{v}_m \in \mathbb{Z}^m$ 使得矩阵 $\mathtt{SQ}^{-1}$ 的行向量是 $d_1\mathtt{v}_1, \ldots, d_m\mathtt{v}_m$。考察上述的构造方法我们发现,集合 $\{\pi^m(\mathtt{v}_i) \mid d_i \not\equiv 0 \pmod{p^{\alpha+1}}\}$ 是线性码 $\mathcal{C}_\alpha$ 的一组基。所以等式 $\dim \mathcal{C}_\alpha = \pi_0 + \cdots + \pi_\alpha$ 成立。 □

简言之,我们的想法就是从一个对称设计的关联矩阵 A 出发,计算它的 Smith 标准型 $\mathtt{S} = \mathtt{PAQ}$,其中 $\mathtt{P}, \mathtt{Q}, \mathtt{S}$ 都是 $v \times v$ 阶整数矩阵,并且 S 是对角矩阵 $\mathtt{S} = \mathrm{diag}(d_1, \ldots, d_v)$。那么域 $\mathbb{F}_p$ 上的码 $\mathcal{C}_\alpha$ 由基向量 $\{\pi^m(\mathtt{v}_i) \mid d_i \not\equiv 0 \pmod{p^{\alpha+1}}\}$ 生成,其中 $\mathtt{v}_1, \ldots, \mathtt{v}_v$ 是矩阵 $\mathtt{Q}^{-1}$ 的全部行向量。

让我们继续考虑具有经典参数 $[2, 4]$ 的 Singer 差集的例子。这个差集所对应的对称设计的关联矩阵 A 是一个循环矩阵,其中第一行是 [111011001010000]。计算 A 的 Smith 标准型,我们得到

$$\mathtt{S} = \mathtt{PAQ} = \mathrm{diag}(1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 4, 4, 4, 28) 。$$

选取 $p = 2$,即我们考虑从 A 生成的二元码。令矩阵 $\mathtt{Q}^{-1}$ 的行向量分别为 $\mathtt{v}_1, \ldots, \mathtt{v}_{15}$。那么 $\mathcal{C}_0$ 的一组基是 $\{\pi^{15}(\mathtt{v}_i) \mid 1 \leq i \leq 5\}$,而 $\mathcal{C}_1$ 的基向量是

$\{\pi^{15}(\mathrm{v}_i) \mid 1 \le i \le 11\}$，这是因为 S 的对角线上分别有 5 和 11 个元素在模 2 和模 4 时不等于零。通过计算这两个码的参数知道，$\mathcal{C}_0$ 是一个 $[15,5,7]_2$ 线性码，而 $\mathcal{C}_1$ 是一个 $[15,11,3]_2$ 线性码，这两个码都是最优的。不仅如此，$\mathcal{C}_0$ 和 $\mathcal{C}_1$ 的对偶（Dual）码分别是具有参数 $[15,10,4]_2$ 和 $[15,4,8]_2$ 的线性码，它们也是最优的！

2.2.2 线性码码链与轨道矩阵

令 $\mathcal{D}$ 是一个 2-(v,k,λ) 设计。假设 $\mathcal{D}$ 具有一个 t 阶的无不动点或不动区组的半正则自同构 φ，其中 t 是一个素数。注意到，如果这个设计是对称的，那么任意无不动点的自同构也没有不动区组。我们可以将设计 $\mathcal{D}$ 的点集和区组集重新排序，使得关联矩阵 A 具有如下的分块形式：

$$\mathrm{A} = \begin{pmatrix} \mathrm{A}_{1,1} & \cdots & \mathrm{A}_{1,v/t} \\ \vdots & \ddots & \vdots \\ \mathrm{A}_{b/t,1} & \cdots & \mathrm{A}_{b/t,v/t} \end{pmatrix},$$

其中每个子矩阵 $\mathrm{A}_{i,j}$ 都是 t 阶的循环矩阵，它的行由循环群 $\langle\varphi\rangle$ 作用下的第 i 个区组轨道中的区组进行标号，而列则是用 $\langle\varphi\rangle$ 作用下的第 j 个点轨道中的点标号。定义 $(b/t)\times(v/t)$ 阶矩阵

$$\mathrm{M} = \begin{pmatrix} m_{1,1} & \cdots & m_{1,b/t} \\ \vdots & \ddots & \vdots \\ m_{b/t,1} & \cdots & m_{b/t,v/t} \end{pmatrix},$$

其中 $m_{i,j}$ 是矩阵 $\mathrm{A}_{i,j}$ 中每行含有的“1”的数目。换言之，任意给定的第 i 个区组轨道中的区组，都包含有第 j 个点轨道中的 $m_{i,j}$ 个点；而任意给定的第 j 个点轨道中的点，都包含在第 i 个区组轨道中的 $m_{i,j}$ 个区组中。我们称矩阵 M 是设计 $\mathcal{D}$ 关于自同构 φ 的**轨道矩阵**（Orbit Matrix）。

使用轨道矩阵 M 作为格的生成矩阵，我们可以得到许多的最优码。例如经典参数 $[2,6]$ 的 Singer 差集对应于一个 $(63,31,15)$-对称设计。这个设计具有一个 $t=3$ 阶的半正则自同构。通过上面的构造方法，我们可以得到一列二元线性码码链。其中 $\mathcal{C}_2$ 是一个二元 $[21,12]_2$ 线性码，它的最小重量是 $d=5$，这是一个最优码。同时，它的对偶码 $\mathcal{C}_2^{\perp}$ 也是一个最优 $[21,9,8]_2$ 线性码。

2.2.3 更多例子

在这一小节中，我们将展示更多从各类差集中构造线性码码链的例子。列标“阶”表示我们用来构造轨道矩阵的半正则自同构群的阶数；列标“链”表示线性码处于线性码码链中的位置；列标“码”和“对偶码”分别表示得到的线性码及其对偶码。记号 ★ 表示所得到的线性码是最优码，即它的最小重量达到了理论上界。而表中其它参数的码也都是近似最优的，即它们的最小重量虽然没有达到理论界，但在所有已知的码中是最好的。

在表 2.1 和表 2.2 中，我们分别展示了从 Singer 差集得到二元和多元线性码码链的例子。

定义 2.10. 设 q 是一个素数幂。如果射影平面 $\mathrm{PG}(2,q)$ 中一个由 m 点组成的集合 A 中任意三个点都不共线，那么我们把 A 称为一个 m-弧（m-Arc）。当 q 是奇数时，我们将 $(q+1)$-弧称为椭圆（Oval）；而当 q 是偶数时，我们将 $(q+2)$-弧称为超椭圆（Hyperoval）。

一类特殊的超椭圆被称为单项式超椭圆（Monomial Hyperoval），它们在射影平面 $\mathrm{PG}(2,2^d)$ 中具有以下的射影等价表示：

$$D(x^k)=\{(1,t,t^k)\mid t\in\mathbb{F}_{2^d}\}\cup\{(0,1,0),(0,0,1)\}\ 。$$

射影平面 $PG(2,2^d)$ 中已知的单项式超椭圆有：

1. Segre 超椭圆 $D(x^6)$，其中 $d\geq 5$ 是一个奇数；
2. Glynn 第 I 型超椭圆 $D(x^{\sigma+\gamma})$，其中：$d\geq 7$ 是一个奇数；$\sigma=2^{(d+1)/2}$；若 $d\equiv 1 \pmod 4$，我们取 $\gamma=2^{(3d+1)/4}$，否则取 $\gamma=2^{(d+1)/4}$；
3. Glynn 第 II 型超椭圆 $D(x^{3\sigma+4})$，其中 $d\geq 11$ 是一个奇数，并且 $\sigma=2^{(d+1)/2}$。

由下面的定理我们知道，单项式超椭圆与循环差集之间具有紧密的联系。我们将超椭圆对应的差集也用相同的名字称呼，例如 Segre 差集，Glynn 差集等。

定理 2.11 (Evans 等[75])：令 $q=2^d$。如果 $D(x^k)$ 是射影平面 $\mathrm{PG}(2,q)$ 中的一个超椭圆，那么集合 $D_{k,d}=\mathrm{Im}(\tau)\setminus\{0\}$ 是循环群 $\mathbb{F}_q^\times$ 上的一个 $(q-1,q/2-1,q/4-1)$-差

表 2.1　由 Singer 差集得到的二元线性码码链

差集	阶	链	码	对偶码
$(2^4-1, 2^3-1, 2^2-1)$	1	C_0	$[15,5,7]_2$★	$[15,10,4]_2$★
		C_1	$[15,11,3]_2$★	$[15,4,8]_2$★
$(2^5-1, 2^4-1, 2^3-1)$	1	C_0	$[31,6,15]_2$★	$[31,25,4]_2$★
		C_1	—	$[31,15,8]_2$★
		C_2	$[31,26,3]_2$★	$[31,5,16]_2$★
$(2^6-1, 2^5-1, 2^4-1)$	1	C_0	$[63,7,31]_2$★	$[63,56,4]_2$★
		C_3	$[63,57,3]_2$★	$[63,6,32]_2$★
	3	C_1	—	$[21,11,6]_2$★
		C_2	$[21,12,5]_2$★	$[21,9,8]_2$★
	7	C_1	$[9,4,4]_2$★	—
		C_2	—	$[9,3,4]_2$★
$(2^8-1, 2^7-1, 2^6-1)$	3	C_1	—	$[85,68,6]_2$
		C_2	—	$[85,60,8]_2$
		C_3	—	$[85,24,24]_2$
		C_4	—	$[85,16,32]_2$
	5	C_1	—	$[51,42,4]_2$★
		C_2	$[51,17,16]_2$	—
		C_3	—	$[51,16,16]_2$
		C_4	—	$[51,8,24]_2$★
	17	C_1, C_2	$[15,5,7]_2$★	$[15,10,4]_2$★
		C_3, C_4	$[15,11,3]_2$★	$[15,4,8]_2$★
$(2^9-1, 2^8-1, 2^7-1)$	7	C_2	—	$[73,45,10]_2$
		C_3	—	$[73,36,16]_2$
$(2^{10}-1, 2^9-1, 2^8-1)$	11	C_1	—	$[93,87,2]_2$★
		C_2	—	$[93,77,6]_2$★
		C_3	$[93,36,20]_2$	—
		C_2	—	$[93,35,20]_2$
		C_4	$[93,88,2]_2$★	$[93,5,48]_2$★
	31	C_1, C_2	$[33,6,16]_2$★	—
		C_3	$[33,16,8]_2$★	—
		C_4	—	$[33,15,8]_2$
		C_5	—	$[33,5,16]_2$★

表 2.2　由 Singer 差集得到的多元线性码码链

差集	阶	链	码	对偶码
$(\frac{3^4-1}{3-1}, \frac{3^3-1}{3-1}, \frac{3^2-1}{3-1})$	2	C_0	—	$[20,15,4]_3$★
		C_1	$[20,4,12]_3$★	—
	5	C_0	$[8,3,5]_3$★	$[8,5,3]_3$★
		C_1	$[8,6,2]_3$★	$[8,2,6]_3$★
$(\frac{3^5-1}{3-1}, \frac{3^4-1}{3-1}, \frac{3^3-1}{3-1})$	11	C_1	$[11,6,5]_3$★	$[11,5,6]_3$★
$(\frac{3^6-1}{3-1}, \frac{3^5-1}{3-1}, \frac{3^4-1}{3-1})$	2	C_0	—	$[182,172,4]_3$★
	7	C_0	$[52,4,34]_3$★	$[52,48,2]_3$★
		C_3	$[52,49,2]_3$★	$[52,3,36]_3$★
	13	C_0	$[28,4,18]_3$★	—
		C_3	—	$[28,3,18]_3$★
$(\frac{3^8-1}{3-1}, \frac{3^7-1}{3-1}, \frac{3^6-1}{3-1})$	41	C_0	$[80,5,53]_3$★	$[80,75,3]_3$★
		C_5	$[80,76,2]_3$★	$[80,4,54]_3$★
$(\frac{3^9-1}{3-1}, \frac{3^8-1}{3-1}, \frac{3^7-1}{3-1})$	757	C_1	$[13,7,4]_3$★	$[13,6,6]_3$★
$(\frac{4^3-1}{4-1}, \frac{4^2-1}{4-1}, 1)$	3	C_0	$[7,4,3]_4$★	$[7,3,4]_4$★
$(\frac{4^5-1}{4-1}, \frac{4^4-1}{4-1}, \frac{4^3-1}{4-1})$	11	C_0	—	$[31,25,4]_4$★
$(\frac{4^7-1}{4-1}, \frac{4^6-1}{4-1}, \frac{4^5-1}{4-1})$	43	C_0	—	$[127,119,4]_4$★
$(\frac{5^4-1}{5-1}, \frac{5^3-1}{5-1}, \frac{5^2-1}{5-1})$	13	C_0	—	$[12,8,4]_5$★
		C_1	—	$[12,3,8]_5$★
$(\frac{5^5-1}{5-1}, \frac{5^4-1}{5-1}, \frac{5^3-1}{5-1})$	11	C_0	—	$[71,65,4]_5$★
		C_2	$[71,66,3]_5$	—
	71	C_1	$[11,6,5]_5$★	$[11,5,6]_5$★
$(\frac{5^6-1}{5-1}, \frac{5^5-1}{5-1}, \frac{5^4-1}{5-1})$	31	C_0	$[126,7,95]_5$★	—
		C_3	—	$[126,6,95]_5$
$(\frac{3^5-1}{3-1}, \frac{3^4-1}{3-1}, \frac{3^3-1}{3-1})$	11	C_0	$[11,6,5]_9$★	$[11,5,6]_9$★

表 2.3　由 Segre 差集得到的线性码码链

差集	阶	链	码	对偶码
$(2^9-1, 2^8-1, 2^7-1)$	7	C_0, C_1	$[73, 18, 24]_2$	$[73, 55, 6]_2$
		C_3	$[73, 36, 16]_2$	—
		C_4	$[73, 45, 10]_2$	—
$(2^{11}-1, 2^{10}-1, 2^9-1)$	23	C_1, C_2	$[89, 22, 28]_2$	—
		C_3	$[89, 33, 20]_2$	$[89, 56, 11]_2$
		C_5	$[89, 55, 12]_2$	$[89, 34, 20]_2$
		C_6, C_7	$[89, 66, 8]_2$	$[89, 23, 28]_2$
	89	C_3, C_4, C_5	$[23, 11, 8]_2$★	$[23, 12, 7]_2$★

表 2.4　由 Glynn 第 I 和第 II 型差集得到的线性码码链

差集	阶	链	码	对偶码
$(2^9-1, 2^8-1, 2^7-1)$	7	C_1	$[73, 18, 24]_2$	$[73, 55, 6]_2$
		C_3	$[73, 36, 16]_2$	—
		C_4	$[73, 45, 10]_2$	—
$(2^{11}-1, 2^{10}-1, 2^9-1)$	23	C_0	$[89, 11, 40]_2$★	$[89, 78, 4]_2$★
		C_1	$[89, 22, 28]_2$	—
		C_7	$[89, 66, 8]_2$	$[89, 23, 28]_2$
		C_8	$[89, 77, 4]_2$★	—
	89	C_3	$[23, 11, 8]_2$★	$[23, 12, 7]_2$★

集，其中映射

$$\begin{aligned} \tau : \mathbb{F}_q &\to \mathbb{F}_q \\ x &\mapsto \tau(x) = x + x^k , \end{aligned}$$

而 $\mathtt{Im}(\tau)$ 表示映射 τ 的象集。

表 2.3 和表 2.4 中分别展示了从 Serge 差集以及从 Glynn 第 I 和第 II 型差集中得到最优线性码的例子。

设 m 是一个正整数，对于每个满足 $\gcd(a, m) = 1$ 的整数 a，定义 $\Delta_h(x) = (x+1)^d + x^d + 1$，其中 $d = 4^h - 2^h + 1$。那么对于有限域的乘法群 $\mathbb{F}_{2^m}^{\times}$ 的一个生成元 α，集合

$$B_a = \log_\alpha \left(\mathbb{F}_{2^m} \setminus \Delta_a(\mathbb{F}_{2^m}) \right)$$

被称为 Dillon–Dobbertin 差集。当 $a = 1$ 和 $a = 2$ 时，Dillon–Dobbertin 差集分别等价

表 2.5　由 Dillon–Dobbertin 差集得到的线性码码链

差集	a	阶	链	码	对偶码
$(2^8-1, 2^7-1, 2^6-1)$	3	3	C_2	$[85, 24, 24]_2$	—
			C_3	$[85, 60, 8]_2$	$[85, 25, 24]_2$
		5	C_1	$[51, 8, 24]_2$★	—
			C_2	$[51, 16, 16]_2$	—
			C_3	—	$[51, 17, 16]_2$
			C_4	$[51, 42, 4]_2$★	—
		17	C_1, C_2	$[15, 4, 8]_2$★	$[15, 11, 3]_2$★
			C_3, C_4	$[15, 10, 4]_2$★	$[15, 5, 7]_2$★
$(2^9-1, 2^8-1, 2^7-1)$	4	7	与 Glynn 第 I 和第 II 型差集中相同		
$(2^{10}-1, 2^9-1, 2^8-1)$	3	11	C_7	$[93, 82, 4]_2$★	—
$(2^{11}-1, 2^{10}-1, 2^9-1)$	3	23	C_2	$[89, 11, 40]_2$★	$[89, 78, 4]_2$★
			C_6	$[89, 11, 40]_2$★	—
		89	与 Glynn 第 I 和第 II 型差集中相同		
	4	23	C_1, C_2	$[89, 22, 28]_2$	—
			C_3	$[89, 33, 20]_2$	—
			C_5	$[89, 55, 12]_2$	$[89, 34, 20]_2$
			C_6, C_7	$[89, 66, 8]_2$	$[89, 23, 28]_2$
		89	与 Glynn 第 I 和第 II 型差集中相同		

于 Singer 差集和 Segre 差集。在表 2.5 中，我们展示从这类差集得到的线性码码链情况，其中列标“a”表示差集中参数 a 的取值。

2.3　不等价循环差集

一个 (v, k, λ)-循环差集被称为是 Hadamard 的，如果存在正整数 n 使得 $v = 4n-1$，$k = 2n-1$，并且 $\lambda = n-1$。循环 Hadamard 差集与循环 Hadamard 矩阵以及二级自相关序列（Two-Level Autocorrelation Sequence）具有紧密联系。它们在各种数字通信系统中都具有重要作用[90,143,148]。Baumert 在 1971 年猜想，循环 Hadamard 差集中群 G 的阶数 v 只有以下三种可能的情况：

1. $v = p$，其中 p 是一个素数并且 $p \equiv 3 \pmod 4$；

2. $v = p(p+2)$，其中 p 和 $p+2$ 都是素数；

3. $v = 2^n - 1$，其中 n 是任意一个大于等于 2 的正整数。

在实际工程应用中，第三类长度最为常用。著名的极大长度序列（Maximal Length Sequence，记为 m-序列），就属于上述第三类[89]。研究者已经完全探讨了以下

参数的情况：Baumert 与 Fredericksen 在 1967 年研究了参数 $(127, 63, 31)$[10]；Cheng 在 1982 年研究了参数 $(255, 127, 63)$[37]；Dreier 与 Smith，以及 Kim 独立的研究了参数 $(511, 255, 127)$[69,105]；Gaal 与 Golomb 在 2001 年研究了参数 $(1023, 511, 255)$[82]。在这一节中，我们将分析所有从 $(511, 255, 127)$-循环 Hadamard 差集中生成的线性码码链。

由文献[69,105] 知道，一共存在 5 类不等价的 $(511, 255, 127)$-循环差集。利用循环差集与自相关序列之间的对应关系（对于所有 $i = 0, 1, \ldots, 2^n - 2$，序列 s 中第 i 位的值 $s(i) = 0$ 当且仅当 $i \in D$），我们将这 5 类不等价的 $(511, 255, 127)$-循环 Hadamard 差集表示为 5 个二元序列，其中 α 是有限域 $\mathbb{F}_{2^9}$ 的某个本原元，$\mathtt{Trace}$ 表示 $\mathbb{F}_{2^9}$ 到 $\mathbb{F}_2$ 的迹函数，而 $i = 0, 1, \ldots, 510$：

1. m511（m-序列）：$s(i) = \mathtt{Trace}(\alpha^i)$；
2. G511（GMW-序列）：$s(i) = \mathtt{Trace}(\alpha^i + \alpha^{11i} + \alpha^{43i})$；
3. M511-1：$s(i) = \mathtt{Trace}(\alpha^i + \alpha^{23i} + \alpha^{31i})$；
4. M511-2：$s(i) = \mathtt{Trace}(\alpha^i + \alpha^{51i} + \alpha^{57i} + \alpha^{83i} + \alpha^{111i} + \alpha^{125i} + \alpha^{183i})$；
5. M511-3：$s(i) = \mathtt{Trace}(\alpha^i + \alpha^{7i} + \alpha^{57i} + \alpha^{77i} + \alpha^{83i} + \alpha^{103i} + \alpha^{111i} + \alpha^{127i} + \alpha^{183i})$。

由于 $511 = 7 \cdot 73$，我们需要考虑阶 t 为 7 和 73 的半正则自同构群。事实上，后一种 $t = 73$ 情形非常简单：所有五类差集生成的线性码码链中只含有 $\tilde{\mathcal{C}}_0$ 和 $\tilde{\mathcal{C}}_1$ 两种线性码，它们的重量分布分别为 $1 + x^7$ 和 $1 + 7x^3 + 7x^4 + x^7$。其中细微的区别在于，GMW-序列给出的是 $\mathcal{C}_0 = \tilde{\mathcal{C}}_0$ 和 $\mathcal{C}_1 = \tilde{\mathcal{C}}_1$，而其它四类都给出 $\mathcal{C}_0 = \mathcal{C}_1 = \tilde{\mathcal{C}}_0$ 和 $\mathcal{C}_2 = \tilde{\mathcal{C}}_1$。

当半正则自同构群阶数是 $t = 7$ 的时候，情况会复杂一些，我们将结果罗列如下。注意到，所有的码都是二元的。

- m511：
  - #1：$[73, 1, 73] = [73, 1, 73] \subseteq [73, 28, 9] \subseteq [73, 37, 9] \subseteq [73, 46, 9]$；
  - #2：$[73, 1, 73] \subseteq [73, 7, 32] \subseteq [73, 19, 9] \subseteq [73, 37, 9] \subseteq [73, 55, 4] \subseteq [73, 67, 1]$；
- G511:

- #1 和 #2 与 m511 的 #1 和 #2 相同；
- #3:$[73,1,73] \subseteq [73,13,24] \subseteq [73,19,9] \subseteq [73,37,9] \subseteq [73,55,4] \subseteq [73,61,1]$；
- #4:$[73,1,73] \subseteq [73,13,24] \subseteq [73,28,9] \subseteq [73,37,9] \subseteq [73,46,4] \subseteq [73,61,1]$；
- #5:$[73,4,32] \subseteq [73,7,32] \subseteq [73,25,9] \subseteq [73,37,4] \subseteq [73,49,4] \subseteq [73,67,1] \subseteq [73,70,1]$；
- #6:$[73,4,32] \subseteq [73,10,28] \subseteq [73,19,9] \subseteq [73,37,4] \subseteq [73,55,4] \subseteq [73,64,1] \subseteq [73,70,1]$；
- #7:$[73,7,32] \subseteq [73,10,32] \subseteq [73,16,9] \subseteq [73,37,4] \subseteq [73,58,4] \subseteq [73,64,1] \subseteq [73,67,1]$；
- #8:$[73,7,32] \subseteq [73,10,28] \subseteq [73,25,9] \subseteq [73,37,4] \subseteq [73,49,4] \subseteq [73,64,1] \subseteq [73,67,1]$；

• M511-1 和 M511-2：

- #1:$[73,1,73] \subseteq [73,19,21] \subseteq [73,28,16] \subseteq [73,37,9] \subseteq [73,46,9] \subseteq [73,55,6]$；

• M511-3：

- #1:$[73,19,21] = [73,19,21] \subseteq [73,28,16] \subseteq [73,37,9] \subseteq [73,46,9] \subseteq [73,55,6]$。

其中 # 表示不等价的码链的计数，例如 GMW-序列在 7 阶半正则自同构作用下得到的不同码链共有 8 条。

3 LDPC 码的差矩阵构造

3.1 LDPC 码简介

定义 3.1. 令 H 是一个定义在二元域 $\mathbb{F}_2$ 上的矩阵，如果其中 “1” 的数目相对很少，我们称这个矩阵是*稀疏*的。以稀疏矩阵 H 作为校验矩阵的（二元）码就被称为*低密度奇偶校验码*（Low-Density Parity-Check Code，LDPC 码）。

LDPC 码可以利用软输入软输出的迭代译码算法进行解码，例如和积算法（Sum-Product Algorithm）等置信传播（Belief-Propagating）算法，就能够达到惊人的高效率[83,125,137]。在二进制输入的加性 Gauss 白噪声（Additive White Gaussian Noise，AWGN）信道下，码率为 1/2、码长为 10^7 的非规则 LDPC 码通过置信传播迭代方法译码，当错误概率为 10^{-6} 时，距离 Shannon 界仅差 0.0045dB，这是目前距离 Shannon 界最近的好码[42]。

早在 1962 年，Gallager 就在他的博士论文中对 LDPC 码的系统全面的论述，奠定了 LDPC 码研究的理论基础[83]。但由于当时计算能力和存储能力的限制，人们没有认识到 LDPC 码的优越性。从 Gallager 提出 LDPC 码到 MacKay 等人重新发现的 30 多年间，只有少数人关注过 LDPC 码，其中 Tanner 提出的 LDPC 码的二部图表示是期间的主要进展[167]。从 Tanner 图上，我们可以直观的理解 LDPC 码的迭代译码过程。在二十世纪末，MacKay 等人总结前人工作[125]，在论文中详细论述了 LDPC 码的理论和实际性能，证明了 LDPC 码是一种实用好码，推广了 Gallager 的概率迭代译码算法，描述了实用译码方法的详细实现方法，极大的推动了 LDPC 码的发展，是 LDPC 码历史上的一个里程碑。此后，LDPC 码的研究在译码算法的简化、密度进化的改进、非规则码的度数设计、校验矩阵的构造、距离特性和性能界的分析、在通信和数据存储中的应用以及 LDPC 码的实现等各方面展开，取得了很多有价值的研究成果，并在实际系统中得到了应用。

已有的 LDPC 码构造方法可以大致划分为以下两类：第一类是随机码（Random Code），例如文献[83,125,136,137,140,149]；第二类是结构化码（Structured Code），例如文

献[111,168,169,176]。随机码是由计算机基于特定设计规则或图结构搜索得到的，例如图的围长（Girth）和点度分布（Degree Distribution）等性质要求。而结构化码则是使用一定的代数和组合方法构造码字。通常长度较大的随机 LDPC 码比相似参数下的结构化 LDPC 码更加接近 Shannon 极限，但随机码的问题在于它们没有足够的代数信息来支持简单高效的编码方案。与之相对的，结构化码通常在编码过程中拥有巨大优势，特别是循环码（Cyclic Code）和拟循环码（Quasi-Cyclic Code）的编码仅需要最简单的移位寄存器就能够完成[111,121,166,168]。当采用串行编码（Serial Encoding）时，复杂度和校验位（Parity-Check Bits）的数目呈线性关系，而当采用并行编码（Parallel Encoding）时，复杂度是码长的线性函数。在实际应用场景中，码字的长度不会太大。此时结构化 LDPC 码在比特错误率（Bit-Error Rate）、块错误率（Block-Error Rate）和差错平底/最低误码率（Error-Floor）等综合指标上，与随机码并不存在明显的差距。

定义 3.2. 令二元稀疏矩阵 H 是一个 LDPC 码 $\mathcal{C}$ 的校验矩阵。如果 H 的每一列都具有相同的列重量 γ，并且每一行都有相同的行重量 ρ，那么我们就将这个 LDPC 码 $\mathcal{C}$ 称为是**正则的**（Regular），或(γ, ρ)-**正则的**。其中的参数 γ 和 ρ 都应相对于码的长度而言非常小。如果校验矩阵 H 的行重量或列重量不是固定的，那么就将码 $\mathcal{C}$ 称为**不规则的**（Irregular）。

在几乎所有已知的 LDPC 码构造方法中，都对于校验矩阵 H 的行与列提出了以下的要求：任意两行（或两列）都最多只有一个位置同时是“1”。我们将这个条件称为**行列限制**（Row-Column Constraint）。对于矩阵 H 的行列限制保证了以 H 为校验矩阵的 LDPC 码所对应的 Tanner 图[167]（Tanner Graph）中不含有长度为 4 的圈，即此时 Tanner 图的围长至少为 6[111,122,139]。具有高围长的 LDPC 码在迭代译码过程中具有更快的收敛性。令 $\gamma_{\min}$ 表示 H 的最小列重量，那么行列限制还保证了得到的 LDPC 码的最小 Hamming 距离不会小于 $\gamma_{\min}+1$，见文献[111,122,139]。尽管这个关于最小距离的下界对于小长度和不规则的 LDPC 码而言并不好，但其对于具有大的列重量的规则 LDPC 码而言，这一下界通常是紧的，例如那些从几何对象[111] 和从有限域[113,190]导出的 LDPC 码。

3.2 拟循环 LDPC 码与差矩阵

3.2.1 拟循环 LDPC 码

如果 LDPC 码的校验矩阵 H 是个由一些相同大小的二元稀疏循环方阵组成的阵列(或块),那么这样的 LDPC 码就被称为是拟循的(Quasi-Cyclic),记作 QC-LDPC 码。大量的模拟实验表明,使用采用使用信息传递算法(Message-Passing Algorithm)进行译码,通过精巧代数构造的拟循环 LDPC 码在在噪声信道中具有非常好的性能[122,139],其表现可以非常接近 Shannon 极限。这些码在 AWGN 信道和二进制删除信道中的性能表现甚至好于那些基于计算机搜索得到的随机或伪随机 LDPC 码[113]。此外,拟循环 LDPC 码还在编码译码算法的硬件实现过程中具有巨大优势。其编码过程可以由线性复杂度的移位寄存器实现[120]。而在译码的时候,它们的拟循环结构可以简化线敷设[34](Wire Routing),还能部分应用并行算法[34,180],使我们能在译码的复杂性和速度之间平衡取舍。拟循环 LDPC 码的这些优良性质激发了更多学者的兴趣,纷纷投入对这类 LDPC 码的设计、构造方法和性质的研究浪潮中。

在此,我们将展示一种利用置换矩阵对一般群上的矩阵进行二元散布从而获得拟循环 LDPC 码的方法。

定义 3.3. 如果有限域 $\mathbb{F}_2$ 上的一个方阵中的每行和每列都恰好只有一个“1”,那么我们将这样的矩阵称为**置换矩阵**(Permutation Matrix,PM)。所有的 v 阶置换矩阵在普通矩阵乘法的意义下构成了一个群 $\mathcal{P}_v$,这个群的大小是 $v!$。

定义 3.4. 设 $(G,+)$ 为 v 阶交换群。我们用群 G 中的元素标记一个 $v\times v$ 阶矩阵的行和列。定义映射:

$$\begin{aligned} \delta : G &\rightarrow \mathbb{F}_2^{v\times v} \\ g &\mapsto \delta(g) \end{aligned}$$

其中矩阵 $\delta(g)$ 在 (i,j) 位置的值为 1 当且仅当 $j-i=g\in G$。我们将这一矩阵表示称为群元素 g 的**G-重二元矩阵散布**(G-Fold Binary Matrix Dispersion),或简称为**二元矩阵散布**。

容易发现，对于任意群元素 $g \in G$，其二元矩阵散布 $\delta(g)$ 都是一个 v 阶置换矩阵，从而 δ 是从 $(G,+)$ 到 $(\mathcal{P}_v, \cdot)$ 的一个群同态。

现在考虑一个 $m \times n$ 阶矩阵 $\mathtt{W} = [w_{i,j}]$，其中的元素取自群 G。通过将矩阵中的每一个元素 $w_{i,j} \in G$ 用它的二元矩阵散布函数的象 $\delta(w_{i,j})$ 替代，我们可以得到一个 $m \times n$ 的 v 阶置换矩阵阵列

$$\begin{bmatrix} \delta(w_{0,0}) & \delta(w_{0,1}) & \cdots & \delta(w_{0,n-1}) \\ \delta(w_{1,0}) & \delta(w_{1,1}) & \cdots & \delta(w_{1,n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \delta(w_{m-1,0}) & \delta(w_{m-1,1}) & \cdots & \delta(w_{m-1,n-1}) \end{bmatrix}。$$

这是一个大小为 $mv \times nv$ 的二元矩阵。我们将其记作 $\delta(\mathtt{W})$，并称之为 $\mathtt{W}$ 的**二元矩阵散布**。

特别的，如果选取的群 G 是一个 v 阶循环群 $\mathbb{Z}_v := \mathbb{Z}/v\mathbb{Z} = \{0,1,\ldots,v-1\}$，并且将 $v \times v$ 阶矩阵的行标列标按照自然顺序标记，那么群元素 $k \in \mathbb{Z}_v$ 的二元矩阵散布 $\delta(k)$ 中，第 (i,j) 位置上的取值为“1”当且仅当 $j - i \equiv k \pmod{v}$，而其它时候都取值为“0”。由于这个矩阵的第一行中只在第 k 列有唯一一个“1”，并且其它的行都是第一行循环右移得到的，因此我们将这样的矩阵称为**循环置换矩阵**（Circulant Permutation Matrix，CPM）。特别的，$\delta(0)$ 就是 v 阶单位矩阵 $\mathtt{I}_v$；而矩阵 $\delta(k)$ 可以看作是将 $\mathtt{I}_v$ 的每一行都右循环移动 k 个位置所得到的，其中 $k = 0,1,\ldots,v-1$。

令 $\mathtt{W}$ 是群 $\mathbb{Z}_v$ 上的一个 $m \times n$ 阶矩阵，那么 $\delta(\mathtt{W})$ 是一个拟循环矩阵。如果我们将 $\delta(\mathtt{W})$ 用作一个线性码 $\mathcal{C}$ 的校验矩阵，那么这个线性码拟循 LDPC 码。此时，$\mathcal{C}$ 可以在线性时间复杂度内完成编码译码过程。我们需要注意到，一般 Abel 群 G 上的矩阵 $\mathtt{W}$ 的二元散布并不一定具有这一优良性质。

3.2.2 差矩阵

为了使用群 G 上的 $m \times n$ 阶矩阵 $\mathtt{W}$ 的二元散布 $\delta(\mathtt{W})$ 作为拟循环 LDPC 码的校验矩阵，我们通常要求 $\delta(\mathtt{W})$ 对应的 Tanner 图中不含有长度为 4 的圈。利用之前提到的行列限制要求，我们有如下引理。

引理 3.5：令 $\mathtt{W} = [w_{i,j}]$ 是一个 $m \times n$ 阶矩阵，其中每个元素来自于一个 v 阶 Abel 群 G。那么矩阵 $\mathtt{W}$ 的二元散布 $\delta(\mathtt{W})$ 满足行列限制，当且仅当对于任意不同的两行 $0 \le i \ne j \le m-1$，n 个差 $w_{i,k} - w_{j,k}$ 都是两两不同的，$k = 0,1,\ldots,n-1$。

特别的，对于 $n = v$ 的极限情况，上面引理中的要求恰好和一类被称为差矩阵（Difference Matrix，DM）的组合学设计结构非常相似。

定义 3.6. 令 $(G, \circ)$ 是一个 v 阶群。一个$(v, k; \lambda)$-差矩阵，或 $(v, k; \lambda)$-DM，指的是一个 $k \times v\lambda$ 阶矩阵 $\mathtt{D} = [d_{i,j}]$，其中的元素属于群 G，并且对于任意不同的两行 $0 \le i \ne j \le k-1$，多重集合 $\{d_{i,l} \circ d_{j,l}^{-1} \mid 0 \le l \le v\lambda - 1\}$ 中都含有 G 中每个元素恰好 λ 次。如果 $\lambda = 1$，我们使用简化记号 (v, k)-DM。

当 G 是一个 Abel 群时，我们通常使用加号作为群运算符号，即考虑多重集合 $\{d_{i,l} - d_{j,l} \mid 0 \le l \le v\lambda - 1\}$。而当 $G = \mathbb{Z}_v$ 是一个循环群时，这样的差矩阵也被称为循环的（Cyclic），并记作 $(v, k; \lambda)$-CDM。需要注意到，由 $(v, k; \lambda)$-差矩阵中的任意几行组成的子矩阵依然是一个差矩阵。

关于差矩阵的研究主要起源于正交阵列的构造问题，见文献[12,48] 等。但差矩阵在其它许多方面都具有重要应用，例如构造没有保密性需求的认证码[157]（Authentication Code without Secrecy），软件测试[45,46]，数据压缩[110]，以及与常重码相关的广义 Steiner 三元系[183]（General Steiner Triple System）等。

关于差矩阵的存在性或不存在性的研究，有下面这些充分性的或必要性的结果。

定理 3.7 (Jungnickel[104])：如果 $k > v\lambda$，那么不存在 $(v, k; \lambda)$-差矩阵。

定理 3.8 (Drake[68])：令 G 是一个偶数阶的群，其大小 $|G| = v$。如果 λ 是一个奇数，并且 G 的 Sylow 2-子群是一个循环群，那么不存在 G 上的 $(v, 3; \lambda)$-差矩阵。特别的，当 λ 为奇数时，不存在 $(v, 3; \lambda)$-差矩阵，使得 $v \equiv 2 \pmod 4$；也不存在偶数阶循环群 $\mathbb{Z}_v$ 上的 $(v, 3; \lambda)$-差矩阵。

定理 3.9 (Ge[85])：存在一个 $(g, 4; 1)$-差矩阵当且仅当 $g \ge 4$ 并且 $g \not\equiv 2 \pmod 4$。

定理 3.10 (Evans[74])：存在一个 $\mathbb{Z}_v$ 上的 $(v, 5; 1)$-循环差矩阵，当且仅当 v 是奇数并且 $v \notin \{3, 9\}$，可能的例外是 $v = 9p$，其中 p 是一个奇素数，并且 $p \notin \{5, 7, 11, 13, 17, 23, 29, 31, 109\}$。

定理 3.11 (Buratti[24])：存在一个 v 阶群 G 上的 $(v, p; 1)$-差矩阵，其中 p 是 v 的最小素因子。

我们再列举一些差矩阵的已知构造方法。第一个方法是在两个群的直积上构造差矩阵。

定理 3.12 (Buratti[24]): 令 H 是群 G 的一个正规子群。如果同时存在群 H 上的 $(u,k;\lambda)$-差矩阵和群 G/H 上的 $(v/u,k;\lambda')$-差矩阵，那么群 G 上存在一个 $(v,k;\lambda\lambda')$-差矩阵。特别的，如果存在一个群 G 上的 $(v,k;\lambda)$-差矩阵和一个群 H 上的 $(u,k;\lambda')$-差矩阵，那么存在群 $G\times H$ 上的一个 $(vu,k;\lambda\lambda')$-差矩阵。

下面这个构造方法被称为张量积（Tensor Product）或 Kronecker 乘积法。

定理 3.13 (Shrikhande[147]): 如果存在群 G 上的一个 $(v,k;\lambda)$-差矩阵和一个 $(v,k';\lambda')$-差矩阵，那么存在群 G 上的一个 $(v,kk';\lambda\lambda')$-差矩阵。

下面两个定理中的构造方法都利用到了群的具体结构。

定理 3.14 (Drake[68]): 令 $\mathrm{EA}(g)$ 是（唯一的）由素数阶循环群直积（Direct Product）得到的 g 阶群。有限域 $\mathbb{F}_q$ 的乘法表是群 $\mathrm{EA}(q)$ 上的一个 $(q,q;1)$-差矩阵。

定理 3.15 (Colbourn 与 Colbourn[50]): 令 v 和 k 是两个正整数，满足条件 $\gcd(v,(k-1)!)=1$。对于每个 $i=0,1,\ldots,k-1$ 和 $j=0,1,\ldots,v-1$，令 $d_{i,j}\equiv ij \pmod v$。则 $\mathtt{D}=[d_{i,j}]$ 就是一个 (v,k)-循环差矩阵。特别的，如果 v 是一个奇素数，那么对于所有整数 $k\le v$，都存在一个 (v,k)-循环差矩阵。

注意到，Colbourn 等人的结论可以看作是 Drake 定理的推广。由于他们得到的差矩阵具有循环性质，这类矩阵将是我们用来构造拟循环 LDPC 码的主要原料。

3.3 数值模拟与分析

令 $\mathtt{D}$ 是在有限 Abel 群 $(G,+)$ 上的 (v,k)-差矩阵，设 $\mathtt{W}$ 是 $\mathtt{D}$ 的一个 $m\times n$ 阶子矩阵。容易验证，$\delta(W)$ 满足行列限制。因此用 $\delta(W)$ 作为校验矩阵的 LDPC 码具有围长不低于 6 的性质。由于拟循环 LDPC 码在编码译码过程中的具有巨大优势，我们将主要考虑从循环群 $\mathbb{Z}_v$ 得到的校验矩阵 $\delta(\mathtt{W})$。

第一个例子中，我们选择 421 阶循环群 $\mathbb{Z}_{421}$。令 $\mathtt{D}=[d_{i,j}]$ 是一个 5×421 阶矩

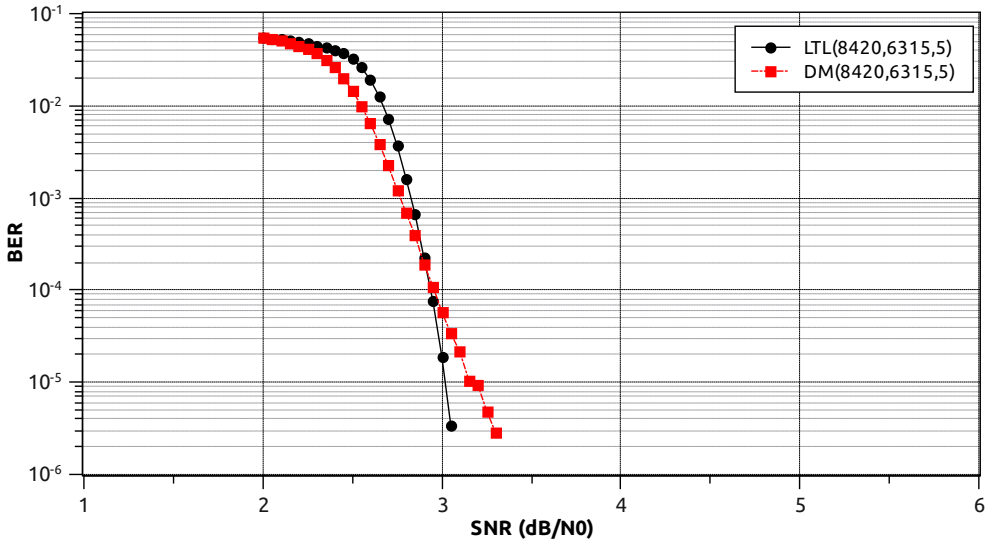

图 3.1　LDPC 码性能比较，码率 0.75

阵，其中的元素 $d_{i,j} = i \cdot j \in \mathbb{Z}_{421}, 0 \le i \le 4, 0 \le j \le 420$。由定理 3.15 知道，D 是一个 $(421, 5)$-循环差矩阵。令 W 是由 D 中前 20 列组成的一个大小为 5×20 的子矩阵，这个矩阵的二元散布 $\mathrm{H} = \delta(\mathrm{W})$ 是一个 2105×8420 阶的二元矩阵，其中每一列的重量都是 5，而每一行的重量都是 20。我们用 H 作为校验矩阵生成一个拟循环 LDPC 码 $\mathcal{C}$，其长度是 8420，维数是 6319，码率为 0.75。这个码和 Lan 等人文章中的例子具有相同的参数[112]。我们在图 3.1 中展示了这两个码的性能比较，其中“LTL$(8420, 6315, 5)$”表示 Lan 等人文中的例子，而“DM$(8420, 6315, 5)$”表示我们的码。图中的横轴表示信噪比（Signal-Noise Ratio，SNR），而纵轴表示比特错误率（Bit-Error Rate，BER）。从图中可以发现，在低信噪比环境中（小于 2.8dB），我们的码具有更低的比特错误率。而在信噪比高于 3.0dB 的时候，虽然我们的比特错误率高于 Lan 等人的例子，但是其绝对值在 10^{-4} 以下，在实际应用中完全足够。另一方面，如果从码的构造角度看，他们的码是基于有限域上区组长度为 5 的平衡不完全区组设计（Balanced Incomplete Block Design，BIBD）的。这一方法只能从每个设计中得到唯一一个列重量等于 5 的 LDPC 码。而我们的构造中只需要用到最基本的整数乘法，并且从同一个差矩阵出发，就可以得出任意列重量不超过 421 的 LDPC 码，具有更大的灵活性。

在第二个例子中，我们将展示利用 $\mathbb{Z}_{91}$ 上的 $(91, 7)$-循环差矩阵来产生一个拟循

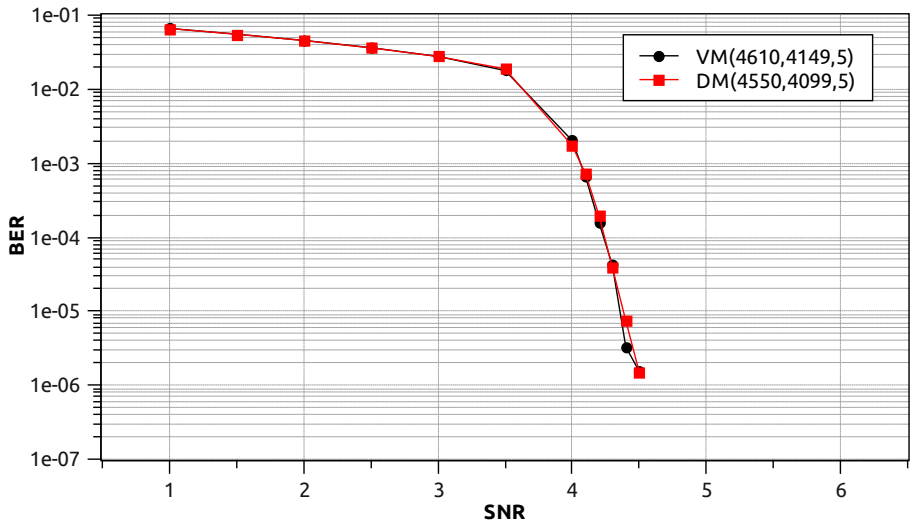

图 3.2　LDPC 码性能比较，码率 0.9

环 LDPC 码，并比较它的性能。我们从这个循环差矩阵中挑出其中的前 5 行和前 50 列，将其进行二元矩阵散布，得到一个 455×4550 阶的矩阵 H。利用 H 的核空间，我们得到一个长度是 4550，码率高达 0.9 的线性码。将这个码与 Vasic 与 Milenkovic 文中的例子做比较[176]。从图 3.2 中可以看到，这两个码字具有几乎相同的“比特错误率—信噪比”曲线。但在他们的构造中，使用了循环差族（Cyclic Difference Family）和许多有限域的乘法计算，比我们的构造方法的计算复杂度高很多，而且不易推广到一般的列重量。

4 置换码下界的改进

4.1 置换码简介

置换码(Permutation Code)有时又被称为置换阵列(Permutation Array)。关于它的研究开始于三十多年前[57,78],然而直到近十年以前,对其关注度并不高。但由于学者陆续发现了它在电力线数据传输[76,132,177],分组密码设计[54],和在多层闪存[101,102]等领域中的应用,置换码开始经历一次强力的复苏。

在电力线通讯应用中,我们可以通过将电流调制成为一族 n 个接近的频率,从而实现在不影响电力输送的同时传递信息。接收端除了获得电力,还可以将频率的变化解调制为字母符号,翻译出所传递的信息[39,132]。为了让信息的传送不对电力传输产生干扰,这些调制后的频率越恒定越好。一种可行的方式就是利用置换码对信息进行编码,使得这 n 个频率在长度为 n 的码字中都恰好只出现一次。

在电力线通信模型中,主要有以下三类噪声:

- 由于线路上的其它电子设备造成的窄带(Narrowband)噪声,这类噪声的特点是时间长、影响大,但只干扰频谱中窄小的一段;
- 脉冲噪声(Impulse Noise),它出现的时间最短,但会同时影响较宽的频段;
- 由传输信道(如电线等)的特性所决定的信号衰减和高斯白噪声(White Gaussian Noise)。

在传统的数据传输媒介中(如电话线和卫星通讯等),高斯白噪声是影响系统性能的主要因素。但在我们的模型中,另外两类噪声错误造成的影响更为显著。研究发现,使用置换码来编码信息可以有效克服这两类的错误[76,177]。因此我们需要寻找满足一定(距离)要求的 n 长置换码,使其包含有最多可能的码字数目,从而能够编码更多的信息。

定义 4.1. 令 S_n 表示作用在 n 个元素(通常选取 $\{1,2,\ldots,n\}$)上的全部置换构成的

对称群，那么一个**置换码**（Permutation Code）指的就是 $\mathcal{C} \subseteq S_n$ 的一个子集。我们称码 $\mathcal{C}$ 的**长度**为 n，而其中的每个置换被称为**码字**。

置换码 $\mathcal{C}$ 的纠错能力与它的最小距离相关。对于两个不同的置换 $\sigma, \pi \in S_n$，我们定义它们之间的 Hamming **距离** $d_H(\sigma, \pi)$ 为其不同的位置个数，即

$$d_H(\sigma, \pi) = |\{i \in [n] \mid \sigma(i) \neq \pi(i)\}|,$$

其中 $[n] = \{1, 2, \ldots, n\}$。等价的，我们称 σ 和 π 之间的距离为 δ，若 $\sigma\pi^{-1}$ 恰好固定 $n - \delta$ 个点，亦即

$$\left|\{i \in [n] \mid \sigma\pi^{-1}(i) = i\}\right| = n - \delta。$$

注意到，等式 $d_H(\sigma, \pi) = d_H(id, \sigma\pi^{-1})$ 总是成立的，其中 id 表示 S_n 中的单位元（Identity）。因此，我们总是可以不失一般性的假设 $id \in \mathcal{C}$。

定义 4.2. 若置换码 $\mathcal{C} \subseteq S_n$ 中任意两个不同置换间的 Hamming 距离都不小于 d，则我们称 $\mathcal{C}$ 具有**最小 Hamming 距离** d。我们将长度为 n、最小 Hamming 距离为 d 的置换码记作 (n, d)-**置换码**，或简记为 PA(n, d)，并将所有 PA(n, d) 中包含有的最多的码字个数记为 $M(n, d)$。

为了处理不同的噪声错误模型，也有学者提出了基于其它距离度量的置换码，例如 Chebyshev 距离[107,108] 等。在本章中，我们将只考虑 Hamming 距离，故有时将其简称为距离。

在本章中，我们将在置换码和一类特殊图中的独立集之间建立一一对应关系，进而利用图论工具和方法研究对应图的独立数，以此获得关于置换码大小 $M(n, d)$ 的下界信息。尽管利用码与独立集之间联系的这一想法具有很强的通用性，但问题的难点在于如何针对各种特定的码类选择可行的图论性质和相关参数进行计算研究。

例如 Jiang 与 Vardy[103] 以及其后的 Vu 与 Wu[178] 等也使用了码和独立集的联系，分别提高了关于二元和 q 元（非线性）码的 Gilbert–Varshamov 界。Jiang 与 Vardy 在文章中估计了图中任意顶点的邻域中含有的边数 t，发现这个数目相对较小，从而由这一局部稀疏性出发得到了他们的结论。

而我们将采用一个不同的图论性质。具体说来，我们将考虑图中任意顶点邻域中的最大度数 m，通过估计 m 来改进关于置换码大小的 Gilbert–Varshamov 型下界。

我们选择这一性质是由于它具有最佳的可行性:我们可以很好的估算参数 m,而参数 t 的计算是几乎不可行的。

应该指出,图的一些其它性质同样可以用来推导关于独立数的估计,我们建议大家参阅 Alon 与 Spencer 的专著《The Probabilistic Method》[3],书中从图论观点出发,对于独立数问题进行了一般性的讨论。

本章内容安排如下:我们将首先在第 4.2 节中回顾置换码一些已知的上下界;然后在第 4.3 节中介绍一些相关的图论概念和定理;最后,我们关于 $M(n,d)$ 下界的改进将在第 4.4 节中详细讨论。

4.2 已知的上下界

关于置换码的一个核心研究问题就是确定 $M(n,d)$ 的值,但现在看来这一问题非常的困难。事实上,除了长度 n 很小的时候以外,我们对于最小距离 d 满足 $4 \leq d \leq n-1$ 时的情形,所知极其有限[49,60,71,79]。因此,现在大家的主要精力都还集中在研究 $M(n,d)$ 的上下界。以下的结论可以由基本的组合技巧得到。

引理 4.3: 1. $M(n,2) = n!$, $M(n,3) = n!/2$, $M(n,n) = n$;

2. $M(n,d) \leq n\,M(n-1,d)$;

3. $M(n,d) \leq n!/(d-1)!$。

在继续讨论之前,我们想先引入一个记号 $D(n,k)$,它将极大简化下文中的论证过程。

定义 4.4. 设 n 为正整数,k 为非负整数,且 $0 \leq k \leq n$。令 $D(n,k)$ 表示 S_n 中与单位元 id 距离恰好为 k 的那些置换组成的集合:

$$D(n,k) := \{\sigma \in S_n \mid d_H(\sigma, id) = k\}\ 。$$

那么集合 $D(n,k)$ 的大小是

$$|D(n,k)| = \binom{n}{k} D_k\ ,$$

其中 D_k 表示 k 阶错排(Derangement)数。

例 4.5. 由于每个非单位置换都至少移动了两个元素，故 $D(n,1)=\emptyset$。集合 $D(n,2)$ 和 $D(n,3)$ 分别由长度为 2 的圈（又称对换，Transposition）和长度为 3 的圈组成。集合 $D(n,4)$ 中的元素有两类，分别是长度为 4 的圈，以及两个不交 2-圈的合成。

关于置换码的 Gilbert–Varshamov 界和球填充（Sphere Packing）界广为所知。在 d 较小的时候，这两个界通常比其它已知的界更紧。

定理 4.6：

$$\frac{n!}{\sum_{k=0}^{d-1}|D(n,k)|}\leq M(n,d)\leq\frac{n!}{\sum_{k=0}^{\lfloor\frac{d-1}{2}\rfloor}|D(n,k)|}。$$

利用群 S_n 的表示理论和线性规划方法，Dukes 与 Sawchuck 改进了 $d=4$ 时的上界。

定理 4.7 (Dukes 与 Sawchuck[71])：*如果存在整数 $k\geq 2$ 使得 $k^2\leq n\leq k^2+k-2$，那么*

$$\frac{n!}{M(n,4)}\geq 1+\frac{(n+1)n(n-1)}{n(n-1)-(n-k^2)((k+1)^2-n)((k+2)(k-1)-n)}。$$

对于小参数的 n 和 d，研究者设计了许多计算机搜索策略来寻找具有给定自同构群的置换码，这些结果通常给出了目前最佳的 $M(n,d)$ 下界。而当一个仅指定了平凡自同构群的穷举搜索程序运行结束时，我们也就完全确定了 $M(n,d)$ 的值。有兴趣的读者可以参考 Smith 与 Montemanni 文中的表格和相关文献[152]。

4.3 Cayley 图与独立集

4.3.1 Cayley 图

定义 4.8. 假设 H 是一个（有限）群，S 是 H 的一个子集。若染色有向图 $\Gamma=\Gamma(H,S)$ 满足以下条件：

- 群 H 中的元素与图的顶点 $V(\Gamma)$ 一一对应；
- S 中的每个元素 s 都被赋予一种颜色 c_s；
- 对于任意 $g\in H$ 和 $s\in S$，对应于 g 和 gs 的两个顶点间的有向边使用 c_s 进行染色。

则我们将图 Γ 称为 Cayley 图，而将集合 S 称为**生成集**（Generating Set）。

在几何群论中，生成集 S 通常是对称的，即 $S = S^{-1}$，并且不包含群的单位元。此时，若我们再选取所有的颜色都相同，则得到的 Cayley 图就是一个简单图，即图中不含自圈（Loop），并且边都是无向的。

4.3.2 图的独立数

定义 4.9. 设图 $G = (V, E)$ 为简单图，$V(G)$ 和 $E(G)$ 分别为图 G 的顶点集和边集。设 S 是 $V(G)$ 的非空子集，若 S 中任意两点均不构成 $E(G)$ 中的一条边，则称 S 为 G 的一个（顶点）**独立集**（Independent Set）。又若不存在 G 的独立集 P，使得 $|P| > |S|$，则称 S 为 G 的**最大独立集**，此时记 $\alpha(G) = |S|$，称 $\alpha(G)$ 为图 G 的**独立数**（Independence Number），即

$$\alpha(G) = \max\left\{|S| \mid S \subseteq V(G), S \text{ 是 } G \text{ 的一个独立集}\right\} 。$$

图的独立数是图论研究中的重要课题之一，曾被许多学者深入探讨过。它还与图的其它重要参数有着紧密的关联，例如染色数（Chromatic Number），团数（Clique Number）等。在此，我们将利用到 Li 等人关于独立数的一个结论[118,119]。为此我们需要对于整数 $m \geq 1$ 和 $x \geq 0$，定义函数

$$f_m(x) = \int_0^1 \frac{(1-t)^{1/m}}{m + (x-m)t} dt。$$

这个函数具有以下的性质。

性质 4.10：设 x 和 m 为两整数。若 $0 \leq x \leq m$，则 $f_m(x) \leq 1/(1+x)$。若 $m \geq 1$，则

$$f_m(x) \geq \frac{\ln(x/m) - 1}{x} 。$$

定义 4.11. 设 $G = (V, E)$ 为简单图，a 是图中的一个顶点。令 $V' = \{b \in V(G) \mid (a, b) \in E(G)\}$，$E' = \{(b, c) \in E(G) \mid b, c \in V'\}$，则我们将以 V' 和 E' 为顶点集与边集的图 $G' = (V', E')$ 称为图 G 关于顶点 a 的**诱导子图**。

Li 等人利用诱导子图中的最大度估计了原图中独立数的大小，下面就是他们的定理。

定理 4.12 (Li 等[118,119]): 令 m 是一个正整数。设 G 为含有 N 个顶点的简单图，其平均度数为 Δ。如果 G 中每个顶点的诱导子图中的最大度都小于 m，那么

$$\alpha(G) \geq N \cdot f_m(\Delta) \geq N \cdot \frac{\ln(\Delta/m) - 1}{\Delta} 。$$

4.4 改进置换码下界

在这一节中，我们将在群 $H = S_n$ 中选择合适的生成集 S 构造出一个 Cayley 图，从而改进关于置换码大小 $M(n,d)$ 的 Gilbert–Varshamov 型下界。

令 $S(n,k) = \cup_{i=1}^{k} D(n,i)$，其中 $k \leq n$ 为一正整数。则我们感兴趣的 Cayley 图为

$$\Gamma(n,d) := \Gamma(S_n, S(n,d-1)) 。$$

由 $S(n,k)$ 的定义知，两个不同的置换 σ 和 π 之间的距离 $d_H(\sigma,\pi) \leq k$，当且仅当 $\sigma\pi^{-1} \in S(n,k)$。即在图 $\Gamma(n,d)$ 中，顶点 σ 和 π 之间有一条边相连的充分且必要条件是它们的距离小于 d。因此，我们可以将每个置换码 PA(n,d) 和图 $\Gamma(n,d)$ 中的一个独立集建立如下的一一对应关系。

引理 4.13: 一个 (n,d)-置换码中全部码字对应的顶点集合是 Cayley 图 $\Gamma(n,d)$ 中的一个独立集。反之，图 $\Gamma(n,d)$ 中任意一个独立集的顶点也构成了一个 (n,d)-置换码的码字集合。

为了能够应用定理 4.12 获得 $M(n,d)$ 的下界估计，我们需要仔细计算图 $\Gamma(n,d)$ 的相关参数。由定义知，这个 Cayley 图是一个含有 $|S_n| = n!$ 个顶点的正则图，每个顶点的度数 $\Delta(n,d)$ 都等于生成集的大小，即：

$$\Delta(n,d) = |S(n,d-1)| = \sum_{k=1}^{d-1} \binom{n}{k} D_k 。$$

我们用 $G(n,d)$ 表示 Cayley 图 $\Gamma(n,d)$ 关于顶点 id 的诱导子图。那么图 $G(n,d)$ 的顶点集为：

$$V(G(n,d)) = S(n,d-1) = \bigcup_{k=1}^{d-1} D(n,k) 。$$

图中两个不同的顶点 σ 和 π 之间有一条边相连，当且仅当它们间的距离小于 d，即 $\sigma\pi^{-1} \in S(n,d-1)$。我们将图 $G(n,d)$ 中的最大度记作 $m(n,d)$。

引理 4.14:设 $n \geq 7$ 为一正整数。当 $d \in \{2,3,4,5\}$ 时,图 $G(n,d)$ 中顶点的最大度 $m(n,d)$ 分别为:

1. $m(n,2) = m(n,3) = 0$,

2. $m(n,4) = 4n - 8$,

3. $m(n,5) = 7n^2 - 31n + 34$。

证明. 因为 $D(n,1) = \emptyset$,所以 $m(n,2) = 0$。而在图 $G(n,3)$ 中,每个顶点都是一个对换。取两个对换 (ij) 和 (kl),其中 $1 \leq i < j \leq n, 1 \leq k < l \leq n$,那么这两个对换之间的距离是:

$$d_H((ij),(kl)) = \begin{cases} 0 & 若\ |\{i,j\} \cap \{k,l\}| = 2 \\ 3 & 若\ |\{i,j\} \cap \{k,l\}| = 1 \\ 4 & 若\ |\{i,j\} \cap \{k,l\}| = 0\ 。 \end{cases}$$

因此 $m(n,3) = 0$。

由 $G(n,4)$ 的定义知道,它的顶点集是 $V(G(n,4)) = S(n,3) = D(n,2) \cup D(n,3)$,即由所有 2-圈和 3-圈组成。不失一般性的,我们分别考虑其中的两个特殊的顶点 $(12) \in D(n,2)$ 和 $(123) \in D(n,3)$。

对于 (12),我们将 $G(n,4)$ 中其它所有顶点划分成以下四个部分:

$$\begin{aligned} N_{2,1} &= \{(1x),(2x) \mid 3 \leq x \leq n\}\ , \\ N_{2,2} &= \{(12x),(21x) \mid 3 \leq x \leq n\}\ , \\ N_{2,3} &= \{(xy),(1xy),(2xy) \mid 3 \leq x,y \leq n, x \neq y\}, 和 \\ N_{2,4} &= \{(xyz),(xzy) \mid 3 \leq x < y < z \leq n\}\ 。 \end{aligned}$$

那么对于每个顶点 $\sigma \in G(n,4)$,它和 (12) 的距离 $d_H(\sigma,(12))$ 为:

$$d_H(\sigma,(12)) = \begin{cases} 3 & 若\ \sigma \in N_{2,1} \\ 2 & 若\ \sigma \in N_{2,2} \\ 4 & 若\ \sigma \in N_{2,3} \\ 5 & 若\ \sigma \in N_{2,4}。 \end{cases}$$

因此 (12) 在 $G(n,4)$ 中的邻点集合为 $N_2 := N_{2,1} \cup N_{2,2}$。

对于 (123)，我们同样将诱导子图中的其它所有顶点进行划分：

$$\begin{aligned}
N_{3,1} &= \{(12),(13),(23)\}\,, \\
N_{3,2} &= \{(132),(12x),(23x),(31x) \mid 4 \le x \le n\}\,, \\
N_{3,3} &= \{(ix),(13x),(21x),(32x) \mid 1 \le i \le 3 < x \le n\}\,, \\
N_{3,4} &= \{(xy),(ixy),(iyx) \mid 1 \le i \le 3 < x < y \le n\}\,, \text{和} \\
N_{3,5} &= \{(xyz),(xzy) \mid 4 \le x < y < z \le n\}\,。
\end{aligned}$$

那么对于 $G(n,4)$ 中其它某个顶点 σ，它和 (123) 的距离 $d_H(\sigma,(123))$ 分别是

$$d_H(\sigma,(123)) = \begin{cases} 2 & \text{若 } \sigma \in N_{3,1} \\ 3 & \text{若 } \sigma \in N_{3,2} \\ 4 & \text{若 } \sigma \in N_{3,3} \\ 5 & \text{若 } \sigma \in N_{3,4} \\ 5 & \text{若 } \sigma \in N_{3,5}。 \end{cases}$$

所以 (123) 在子图 $G(n,4)$ 中的邻域是 $N_3 := N_{3,1} \cup N_{3,2}$。

从而我们有等式：

$$\begin{aligned}
m(n,4) &= \max\{|N_2|\,,|N_3|\} \\
&= \max\{4(n-2), 3(n-3)+4\} \\
&= 4n-8\,。
\end{aligned}$$

通过类似的方法分析 $m(n,5)$，我们发现 (12) 在图 $G(n,5)$ 中有最多的邻点，其数目为 $m(n,5) = 7n^2 - 31n + 34$。这里我们需要考虑 $G(n,5)$ 中如下具有代表性的顶点：$D(n,2)$ 中的 (12)，$D(n,3)$ 中的 (123)，以及 $D(n,4)$ 中的 (12)(34) 和 (1234)。 □

将以上引理中的结论应用到定理 4.12 中，就可以得到如下关于 $M(n,d)$ 的下界估计。

表 4.1　当 $d=4$ 和 5 时，(n,d)-置换码的下界（$8 \le n \le 20$）

n	$d=4$	$d=5$
8	605	90
9	4046	509
10	31047	3386
11	268673	25885
12	2588633	223378
13	27484422	2147724
14	318853331	22767826
15	4013217263	263832788
16	54470270765	3317928906
17	793090335806	45006297715
18	12331219009156	655021291542
19	203926244407855	10181693092799
20	3574258846215948	168351610362186

定理 4.15：记 $m'(n,d)=m(n,d)+1$，并令

$$M_{IS}(n,d) := n! \cdot \int_0^1 \frac{(1-t)^{1/m'(n,d)}}{m'(n,d)+[\Delta(n,d)-m'(n,d)]\,t} \cdot dt。$$

那么 $M(n,d) \ge M_{IS}(n,d)$。

对于最小距离 d 取值为 4 和 5 的时候，我们将 $8 \le n \le 20$ 时积分 $M_{IS}(n,d)$ 的值列在了表 4.1 中。这些值是通过开源数学软件 Sage 计算得到的[155]。特别的，当 $(n,d)=(13,5)$ 时，我们的值 2147724 较之于之前文献中的结果 $M(13,5) \ge 878778$ 是极大的改进[39,152]。

在本节的最后一部分中，我们将考虑当最小距离 d 固定，而码长 n 逐渐增大时，由独立数诱导的下界 $M_{IS}(n,d)$ 会具有怎样的渐近性质。

引理 4.16：对于固定的 d，当 n 趋于无穷大时，$m(n,d)=O(n^{d-3})$。

证明. 设 σ 为 Cayley 图 $\Gamma(n,d)$ 中任意一个选定的顶点，使得 $\sigma \in D(n,k)$，$1 \le k \le d-1$。我们将估计 σ 在图 $G(n,d)$ 中的度数，即在单位元的诱导子图中有多少个顶点 π，使得 π 和 σ 之间有一条边相连。

首先，我们将根据置换 id、σ 和 π 作用于 $[n]$ 中元素所得到的象，把集合 $[n]$ 划分

成(至多)5 个两两不交的部分。

$$\begin{aligned} X &= \{i \in [n] \mid \sigma(i) \neq i, \pi(i) = i\}, \\ Y &= \{i \in [n] \mid \sigma(i) \neq i, \pi(i) = \sigma(i)\}, \\ Z &= \{i \in [n] \mid \sigma(i) \neq i, \pi(i) \neq i, \sigma(i) \neq \pi(i)\}, \\ U &= \{i \in [n] \mid \sigma(i) = i, \pi(i) \neq i\}, \quad \text{以及} \\ V &= \{i \in [n] \mid \sigma(i) = \pi(i) = i\}。 \end{aligned}$$

令 x、y、z、u 和 v 分别表示集合 X、Y、Z、U 和 V 之中元素的个数。那么三个置换之间的距离条件可以导出下面这些关系式:

$$x + y + z = k \leq d - 1, \tag{4.1}$$

$$y + z + u \leq d - 1, \tag{4.2}$$

$$x + z + u \leq d - 1, \text{ 以及} \tag{4.3}$$

$$x + y + z + u + v = n。$$

特别的,我们可以通过计算 (4.2) + (4.3) − (4.1) 得到

$$u \leq \frac{2d - 2 - (k + z)}{2} \leq d - 1 - \lfloor \frac{k + z}{2} \rfloor。$$

选定的顶点 σ 的邻点 π 的数目,由 π 作用在集合 Y、Z 和 U 的可能的象所决定。由式(4.1)知 $y + z$ 不大于 k,所以在我们的估算中,π 在 U 上的象的选择数将是最主要的因素。在我们逐项分析 k 的取值之前,我们给出以下的断言。

断言: 如果 $z = 0$,那么 $x \neq 1$,并且 $y \neq 1$。

断言的证明: 设 $Z = \emptyset$,并且 $X = \{i\}$。那么此时 $i \in \sigma(Y) = \pi(Y)$,但由 X 的定义知 $\pi(i) = i$,于是产生矛盾。利用同样的分析可知,$z = 0$ 和 $y = 1$ 不能同时成立。证毕。

当 $k = 2$ 时,由上面的断言得到 $x = 0$ 或者 $y = 0$。这时可分别由式(4.2)或式(4.3)得出 $u \leq d - 3$。因为 $|Y \cup Z| \leq k = 2$,并且 $|U| \leq d - 1 - k = d - 3$,所以 π 的数目被它在 $Y \cup Z$ 和 U 上可能的象所决定,即

$$\begin{aligned} \deg(\sigma) &\leq 2! \cdot \binom{n-2}{d-3} \cdot (d-3)! \\ &= O(n^{d-3})。 \end{aligned}$$

当 $k=3$ 时。如果 $z=0$，那么由断言得知或者 $x=0$ 且 $y=3$，或者 $x=3$ 且 $y=0$。在这两种情况下，不等式 $u \leq d-4$ 均成立。而如果 $z \geq 1$，那么我们得到 $u \leq d-1-\lfloor \frac{k+z}{2} \rfloor \leq d-3$。因此总有 $\deg(\sigma)=O(n^{d-3})$。

而当 $k \geq 4$ 时，我们有 $u \leq d-1-\lfloor \frac{k+z}{2} \rfloor \leq d-3-\lfloor \frac{k-3}{2} \rfloor \leq d-3$。此时 $\deg(\sigma)=O(n^{d-3})$。

综合上面的分析知道：

$$\begin{aligned} m(n,d) &= \max_{2\leq k\leq d-1}\{\deg(\sigma) \mid \sigma \in D(n,k)\} \\ &= O(n^{d-3})。 \end{aligned}$$

□

定理 4.17：当 d 固定，而 n 趋向于无穷大时，我们有

$$\frac{M_{IS}(n,d)}{M_{GV}(n,d)} = \Omega(\ln(n))\ ,$$

其中 $M_{GV}(n,d)$ 表示置换码的 Gilbert—Varshamov 型下界：

$$M_{GV}(n,d) := \frac{n!}{\sum_{k=0}^{d-1}|D(n,k)|}。$$

证明.

$$\begin{aligned} \frac{M_{IS}(n,d)}{M_{GV}(n,d)} &= \frac{n!\int_0^1 \frac{(1-t)^{1/m'(n,d)}}{m'(n,d)+[\Delta(n,d)-m'(n,d)]t}\,dt}{\frac{n!}{1+\Delta(n,d)}} \\ &\geq \frac{\frac{\ln(\Delta(n,d)/m'(n,d))-1}{\Delta(n,d)}}{\frac{1}{\Delta(n,d)+1}} \\ &\geq \ln\left(\frac{\Delta(n,d)}{m'(n,d)}\right)-1。 \end{aligned}$$

由于 $D_k=\lfloor \frac{k!}{e}+\frac{1}{2} \rfloor$，所以我们有

$$\Delta(n,d)=\sum_{k=0}^{d-1}\binom{n}{k}D_k=\Theta(n^{d-1})。$$

因此，

$$\begin{aligned} \frac{M_{IS}(n,d)}{M_{GV}(n,d)} &\geq \ln\left(\frac{\Delta(n,d)}{m'(n,d)}\right)-1 \\ &\geq \ln(cn^2)-1 \\ &= \Omega(\ln(n))\ , \end{aligned}$$

其中 c 是一个正的常数。 □

即在渐近意义下，我们利用对 Cayley 图 $\Gamma(n,d)$ 中独立集的估计，将置换码大小 $M(n,d)$ 的 Gilbert–Varshamov 型下界提高了 $\Omega(\ln(n))$ 倍。

5 最优常重复合码的组合递归构造

5.1 常重复合码简介

设 X 和 R 是两个有限集，我们用 R^X 表示所有长度为 $|X|$ 的向量，向量中的位置用 X 中的元素标记，而每个位置上的取值在集合 R 中，即 $\mathtt{u}=(\mathtt{u}_x)_{x\in X}$ 并且对于每个 $x\in X$ 都有 $\mathtt{u}_x\in R$。一个长度为 n 的 q 元码是指的一个集合 $\mathcal{C}\subseteq\mathbb{Z}_q^X$，其中 $|X|=n$。注意到这一定义虽然在形式上与第 1 章中略有不同，但实质是一样的。事实上，我们只需取 $X=\{1,2,\ldots,n\}$ 即可。类似的，我们可以定义重量和距离等概念。

定义 5.1. 对于两个向量 $\mathtt{u},\mathtt{v}\in\mathbb{Z}_q^X$，我们定义它们的**支撑集**为 $\mathtt{supp}(\mathtt{u},\mathtt{v})=\{x\in X\mid \mathtt{u}_x\neq\mathtt{v}_x\}$。我们用 $\mathtt{supp}(\mathtt{u})$ 表示 $\mathtt{u}$ 和零向量的支撑集，并称之为向量 $\mathtt{u}$ 的**支撑集**。

定义 5.2. 设向量 $\mathtt{u}\in\mathbb{Z}_q^X$。对于每个整数 $j=1,2,\ldots,q-1$，令

$$w_j=|\{x\in X\mid \mathtt{u}_x=j\}|\ ,$$

则我们将多元组 $\overline{w}=[w_1,\ldots,w_{q-1}]$ 称为向量 $\mathtt{u}$ 的**构型**(Composition)。

定义 5.3. 设 X 为一个 n 元集合，$q\geq 2$ 为一正整数。令 $\mathcal{C}\subseteq\mathbb{Z}_q^X$ 是一个最小距离为 $d(\mathcal{C})=d$ 的码。若码 $\mathcal{C}$ 中每个码字都具有相同的重量 w，则我们称 $\mathcal{C}$ 为**常重码**，记作 $(n,d,w)_q$-**码**。进一步的，若码 $\mathcal{C}$ 中每个码字还具有相同的构型 $\overline{w}$，则我们称 $\mathcal{C}$ 为**常重复合码**，记作 $(n,d,\overline{w})_q$-**码**。

我们将所有 $(n,d,\overline{w})_q$-码中包含的码字个数最大值被记为 $A_q(n,d,\overline{w})$，并将达到这一最大值的码称为是**最优的**。注意到，通过重排 $\overline{w}$ 中的分量或删除 $\overline{w}$ 中的零值分量，都不会对常重复合码的距离或重量性质产生影响。因此，我们可以不失一般性的假设构型 $\overline{w}$ 中的分量值满足条件 $w_1\geq\cdots\geq w_{q-1}\geq 1$。

以上定义的常重复合码可以看作是二元常重码的一类推广，将字母表从原来的 $\mathbb{Z}_2$ 扩展到了一般的 $\mathbb{Z}_q$，其中 $q\geq 2$。而我们上一章中研究的置换码也可以

表 5.1　当 $n \leq 10$ 时，$A_3(n,5,[3,1])$ 和 $A_3(n,5,[2,2])$ 的值

n	$A_3(n,5,[3,1])$	$A_3(n,5,[2,2])$
4	1	1
5	1	2
6	3	3
7	7	7
8	8	12
9	10	18
10	13	20

看做是它的一个特殊子类[150]。这一推广后的编码广泛应用于现代通信领域的各个方面，例如确定离散无记忆信道（Discrete Memoryless Channel）中零错误决策反馈容量（Zero Error Decision Feedback Capacity）[170]，多存取通信（Multiple Access Communication）[72]，球形码（Spherical Codes）调制[73]，DNA 码[106,127]，电力线通信（Powerline Communication），跳频（Frequency Hopping）技术[41] 等。

对常重复合码的研究始于 20 世纪 80 年代初，它最初被应用在决策反馈信道中，以降低传输过程时符号/字母发生错误或删除的概率[51]。然而直到 90 年代后期，人们才逐渐对其展开系统性的探究[18,19,162]。在这些研究之中，确定最优常重复合码所含有的码字数量是最为核心的问题之一，有兴趣的读者可以参见相关的文献[17,30–32,39–41,49,58,61–65,99,116,124,164,165,185–187]。

三元常重码的码字个数在许多文献中都有研究[20,33,86,163]。2002 年，Svanström 等人通过计算机搜索等方法，得到了码长不超过 10 的三元常重复合码的一些上下界结果[165]。其中重量为 4 且距离为 5 的情况被完全确定下来，我们将这些结果列在表 5.1 中。在 2008 年，Chee 等人首次提出了可分组码的概念，并且利用它构造出了所有重量为 3 的最优三元常重复合码[31]。他们的工作以及其他研究者的后续相关工作都表明，可分组码这一概念在最优常重码和常重复合码的递归构造中发挥着巨大的作用[31,188,189,191,193,194]。

在这一章中，我们将继续使用可分组码这一强有力的工具，构造出重量为 4 且最小距离为 5 时，所有长度的最优三元常重复合码。在此参数下，全部可能的码字构型共有两种，分别是 $[3,1]$-型和 $[2,2]$-型。在进入仔细讨论之前，我们先将本章的主要结论归纳为下面的这个定理，展示给读者。

定理 5.4：对于任意正整数 $n \geq 4$。最优 $(n, 5, [3,1])_3$-码的含有的码字个数是：

$$A_3(n,5,[3,1]) = \begin{cases} 1 & \text{若 } n = 4 \\ 3 & \text{若 } n = 6 \\ 10 & \text{若 } n = 9 \\ \lfloor \frac{n}{3} \lfloor \frac{n-1}{2} \rfloor \rfloor - 1 & \text{若 } n \equiv 5 \pmod 6 \\ \lfloor \frac{n}{3} \lfloor \frac{n-1}{2} \rfloor \rfloor & \text{其它情况。} \end{cases}$$

而最优 $(n, 5, [2,2])_3$-码的含有的码字个数是

$$A_3(n,5,[2,2]) = \begin{cases} 1 & \text{若 } n = 4 \\ 2 & \text{若 } n = 5 \\ 3 & \text{若 } n = 6 \\ 7 & \text{若 } n = 7 \\ \lfloor \frac{n}{2} \lfloor \frac{n-1}{2} \rfloor \rfloor - 1 & \text{若 } n \geq 8 \text{ 并且 } n \equiv 3 \pmod 4 \\ \lfloor \frac{n}{2} \lfloor \frac{n-1}{2} \rfloor \rfloor & \text{其它情况。} \end{cases}$$

本章余下的部分结构如下：在第 5.2 节中，我们将介绍后面需要用到的一些组合设计和编码理论中的基本定义和结论；在第 5.3 节和第 5.4 节中，我们分别确定最优 $(n, 5, [3,1])_3$-码和 $(n, 5, [2,2])_3$-码的大小与构造问题。由于我们的递归方法需要使用大量短长的码，为了阅读的流畅，这些辅助码都放到了第 5.5 节中。

5.2 准备知识

我们首先约定本章中的一些记号。我们将用 $\mathbb{Z}_{\geq 0}$ 和 $\mathbb{Z}_{>0}$ 分别表示非负整数和正整数集合，用 $[a,b]$ 表示整数集合 $\{a, a+1, \ldots, b\}$（其中 $a < b$ 都是整数），用花括号 $\wr \cdot \int$ 表示多重集合（Multiset）。

5.2.1 几类组合设计结构

5.2.1.1 可分组设计

定义 5.5. 设 $(X,\mathcal{B})$ 为一个集合系统（参见定义 2.1），并设 $\mathcal{G}=\{G_1,\ldots,G_t\}$ 是点集 X 的一些子集构成的集族。如果三元组 $(X,\mathcal{G},\mathcal{B})$ 满足以下三个条件：

1. $\mathcal{G}$ 是 X 的一个划分，其中的每个集合 G_i 被称为组（Group）；
2. X 中任意两个不同组的点对恰好仅出现在一个区组中；
3. 任意区组和组的交都不多于一个点，即对于任意 $B\in\mathcal{B}$ 和任意 $G\in\mathcal{G}$，均有 $|B\cap G|\leq 1$。

那么，我们就将三元组 $(X,\mathcal{G},\mathcal{B})$ 称为一个**可分组设计**（Group Divisible Design，GDD）。并将多重集合 $\{\!|G|\mid G\in\mathcal{G}\}\!\}$ 称为此可分组设计的**型**（Type）。

通常我们使用指数记号（Exponential Notation）来描述可分组设计的型：我们称 $(X,\mathcal{G},\mathcal{B})$ 的型为 $g_1^{t_1}\ldots g_s^{t_s}$，指的是 $\mathcal{G}$ 中恰好有 t_i 个组的大小是 g_i，$1\leq i\leq s$。另外，如果集合系统 $(X,\mathcal{B})$ 是 K-均匀的，那么可分组设计 $(X,\mathcal{G},\mathcal{B})$ 也被称为是**K-均匀的**，此时将其简记为 K-GDD。

定义 5.6. 我们将型为 m^k 的 $\{k\}$-均匀可分组设计称为**横截设计**（Transversal Design），用记号 TD(k,m) 表示。

下面这些定理中关于可分组设计和横截设计的存在性结果将在后面两节的证明中多次用到，我们将不再一一注明引用出处。

定理 5.7 (Brouwer 等[23])：型为 g^t 的 $\{4\}$-GDD 存在的充分必要条件是 $t\geq 4$，并且

1．$g\equiv 1,5\pmod 6$，并且 $t\equiv 1,4\pmod{12}$；或者

2．$g\equiv 2,4\pmod 6$，并且 $t\equiv 1\pmod 3$；或者

3．$g\equiv 3\pmod 6$，并且 $t\equiv 0,1\pmod 4$；或者

4．$g \equiv 0 \pmod 6$。

其中有两个例外:型为 2^4 或 6^4 的 $\{4\}$-GDD 不存在。

定理 5.8 (Ge 与 Rees[88]):不存在型为 6^4 的 $\{4\}$-GDD;当 $(u,m) \in \{(7,15),\ (11,21),\ (11,24),\ (11,27),\ (13,27),\ (13,33),\ (17,39),\ (17,42),\ (19,45),\ (19,48),\ (19,51),\ (23,60),\ (23,63)\}$ 时,型为 $6^u m^1$ 的 $\{4\}$-GDD 存在性待定;对于其它满足条件 $u \geq 4$ 和 $m \equiv 0 \pmod 3$ 且 $0 \leq m \leq 3u-3$ 的参数 (u,m),都存在型为 $6^u m^1$ 的 $\{4\}$-GDD。

定理 5.9 (Abel 等[2]):用 $\mathrm{TD}(k)$ 表示那些存在 $\mathrm{TD}(k,m)$ 的正整数 m 组成的集合,则:$\mathrm{TD}(3) = \mathbb{Z}_{>0}$;$\mathrm{TD}(4) = \mathbb{Z}_{>0}\backslash\{2,6\}$;$\mathrm{TD}(5) = \mathbb{Z}_{>0}\backslash\{2,3,6,10\}$;$\mathrm{TD}(6) = \mathbb{Z}_{>0}\backslash\{2,3,4,6,10,14,18,22\}$;$\mathrm{TD}(9) \supseteq \{8,16\}$。

通过截短横截设计中的组或者区组,我们可以得到很多新的可分组设计。

定理 5.10 (**截短组,见** Hanani[93]):设 $k \geq 2$ 是一个整数,s 是一个非负整数。若存在横截设计 $\mathrm{TD}(k+s,m)$,并且整数 $g_1, g_2, \ldots, g_s$ 满足条件 $0 \leq g_i \leq m$,其中 $1 \leq i \leq s$。那么存在一个型为 $m^k g_1^1 g_2^1 \cdots g_s^1$ 的 K-GDD,其中 $K = [k, k+s]$。

定理 5.11 (**截短区组**):设整数 k 和 s 满足条件 $k \geq 2$ 和 $0 \leq s \leq k$。若存在一个横截设计 $\mathrm{TD}(k,m)$,那么型为 $(m-1)^s m^{k-s}$ 的 $\{k-s, k-1, k\}$-GDD 也存在。

定义 5.12. 设 $(X, \mathcal{G}, \mathcal{B})$ 为一个可分组设计,并设集合 $\mathcal{B}' \subseteq \mathcal{B}$。若 X 中每个点都恰好只包含在 $\mathcal{B}'$ 的一个区组中,则我们称 $\mathcal{B}'$ 为一个平行类(Parallel Class)。进一步的,若区组集 $\mathcal{B}$ 可以完全划分为若干个平行类之不交并,则称 $(X, \mathcal{G}, \mathcal{B})$ 是一个可分解分组设计(Resolvable GDD,RGDD)。

综合文献[87,145,161] 中的结论,我们有如下关于均匀可分解分组设计 {4}-RGDD 的存在性结果。

定理 5.13: 1．当 $(h,n) \in \{(2,4),(2,10),(3,4),(6,4)\}$ 时,不存在型为 h^n 的 $\{4\}$-RGDD。

2．当 (h,n) 为以下取值时,型为 h^n 的 $\{4\}$-RGDD 存在性待定:

(a) $h=2$,并且 $n\in\{34,46,52,70,82,94,100,118,130,178,184,202,214,\ 238,\ 250,\ 334\}$;

(b) $h=6$,并且 $n\in\{6,68\}$;

(c) $h=9$,并且 $n=44$;

(d) $h=10$,并且 $n\in\{4,34,52,94\}$;

(e) $h=18$,并且 $n\in\{18,38,62\}$;

(f) $h=36$,并且 $n\in\{11,14,15,18,23\}$;

(g) $h\in[14,454]\cup\{478,502,514,526,614,626,686\}$ 且 $h\equiv 2,10\pmod{12}$,并且 $n\in\{10,70,82\}$。

3. 其它满足必要条件 $n\geq 4, hn\equiv 0\pmod 4$ 并且 $h(n-1)\equiv 0\pmod 3$ 的参数 (h,n),都存在型为 h^n 的 $\{4\}$-RGDD。

5.2.1.2 成对平衡设计

定义 5.14. 假设 $(X,\mathcal{B})$ 是一个 v 阶的 K-均匀集合系统,如果 X 中任意两个不同的点都恰好仅出现在 $\mathcal{B}$ 的一个区组中,则我们将这个集合系统称为**成对平衡设计**(Pairwise Balanced Design),记作 PBD(v,K)。

设 k 为一个正整数。若成对平衡设计 PBD$(v,K\cup\{k\})$ 中至少包含一个大小为 k 的区组,则将之记为 PBD$(v,K\cup\{k^\star\})$。更进一步地,如果 $k\notin K$,则这个记号表示此成对平衡设计中恰有一个大小为 k 的区组;而如果 $k\in K$,则我们要求至少有一个区组的大小为 k。

定理 5.15 (Rees 与 Stinson[135]):假设 $v>w$ 为两个正整数。存在一个成对平衡设计 PBD$(v,\{4,w^\star\})$,当且仅当 $v\geq 3w+1$,并且:

1. $v\equiv 1,4\pmod{12}$ 且 $w\equiv 1,4\pmod{12}$;或者

2. $v\equiv 7,10\pmod{12}$ 且 $w\equiv 7,10\pmod{12}$。

定理 5.16 (Abel 等[1]):对于所有参数 $v\geq 4$ 且 $v\notin\{7,8,9,10,11,12,14,15,18,19,23\}$,都存在一个成对平衡设计 PBD$(v,\{4,5,6\})$。

5.2.1.3 填充设计

定义 5.17. 给定正整数 $v \geq k \geq t$，和正整数 λ。如果一个 v 阶的 $\{k\}$-均匀集合系统 $(X, \mathcal{B})$ 中，X 的任意 t-子集都至多包含在 λ 个区组中，则称这个集合系统是一个 t-(v,k,λ) **填充设计**(Packing Design)。

需要说明的是，当 $\lambda > 1$ 时，我们允许 $\mathcal{B}$ 中有重复的区组。

定义 5.18. 对于给定的参数 v,k,t,λ，定义函数

$$D_\lambda(v,k,t) = \max\{b \mid \text{存在区组数为 } b \text{ 的 } t\text{-}(v,k,\lambda) \text{ 填充设计}\}。$$

则 $D_\lambda(v,k,t)$ 被称为**填充数**(Packing Number)。若 $(X,\mathcal{B})$ 是区组数为 $D_\lambda(v,k,t)$ 的 t-(v,k,λ) 填充设计，则将其称为是**最优(或最大)的**。通常将 $D_1(v,k,t)$ 记作 $D(v,k,t)$。

定理 5.19 (Stinson 等[160])：如果 $v \equiv 2 \pmod 6$ 且 $\lambda \equiv 4 \pmod 6$，或者 $v \equiv 5 \pmod 6$ 且 $\lambda \equiv 1 \pmod 3$，则

$$D_\lambda(v,3,2) = U_\lambda(v,3,2) - 1; \tag{5.1}$$

对于其它的 v 和 λ，

$$D_\lambda(v,3,2) = U_\lambda(v,3,2), \tag{5.2}$$

其中

$$U_\lambda(v,k,t) = \lfloor \frac{v}{k} \lfloor \frac{v-1}{k-1} \cdots \lfloor \frac{\lambda(v-t+1)}{k-t+1} \rfloor \rfloor \rfloor。 \tag{5.3}$$

5.2.2 可分组码

给定向量 $\mathtt{u} \in \mathbb{Z}_q^X$ 和子集 $Y \subseteq X$。如果向量 $\mathtt{v} \in \mathbb{Z}_q^X$ 满足条件：

$$\mathtt{v}_x = \begin{cases} \mathtt{u}_x & \text{若 } x \in Y \\ 0 & \text{若 } x \in X \backslash Y, \end{cases}$$

则称 $\mathtt{v}$ 是$\mathtt{u}$ **关于** Y **的限制**(Restriction)，记作 $\mathtt{u}|_Y$。如果向量 $\mathtt{v} \in \mathbb{Z}_q^Y$ 满足条件 $\mathtt{v}_x = \mathtt{u}_x, x \in Y$，则将其称为$\mathtt{u}$ **关于** Y **的压缩**(Constriction)，记作 $\mathtt{u}|^Y$。

定义 5.20. 令 X 为一个大小为 n 的集合，$\mathcal{G}=\{G_1,\ldots,G_t\}$ 是 X 的一个划分，而 $\mathcal{C}\subseteq\mathbb{Z}_q^X$ 是最小距离为 d 的一个码。如果对于任意码字 $\mathtt{u}\in\mathcal{C}$，均有 $wt(\mathtt{u}|_{G_i})\leq 1$，$1\leq i\leq t$，则我们将三元组 $(X,\mathcal{G},\mathcal{C})$ 称为一个最小距离为 d 的**可分组码**（Group Divisible Code，GDC）。

进一步的，如果 $\mathcal{C}$ 中每个码字的重量都是常数 w，则记为 w-GDC(d)；如果每个码字都具有恒定构型 $\overline{w}$，则我们将其写作 $\overline{w}$-GDC(d)。

与可分组设计时类似，我们定义一个可分组码 $(X,\mathcal{G},\mathcal{C})$ 的型（Type）为 $\mathcal{G}$ 中集合大小构成的多重集 $\wr|G|\mid G\in\mathcal{G}\int$，并且也将使用指数记号来表示。我们将 $|\mathcal{C}|$ 称作分组码 $(X,\mathcal{G},\mathcal{C})$ 的大小（Size）。注意到，含 s 个码字的 $(n,d,\overline{w})_q$-码等同于一个大小为 s、型为 1^n 的 $\overline{w}$-GDC(d)。

可分组码的概念最早由 Chee 等提出[31]，文中同时给出了一些非常有用的构造方法。

性质 5.21 (组填充(Filling in Groups))：令 $d\leq 2(w-1)$。假设 $(X,\mathcal{G},\mathcal{C})$ 为一个含有 a 个码字、型为 $g_1^{t_1}\cdots g_s^{t_s}$ 的可分组码。假设对于每个 $1\leq i\leq s$，都存在一个大小为 b_i 的 $(g_i,d,w)_q$-码 $\mathcal{C}_i$。那么存在一个大小为 $a+\sum_{i=1}^s t_ib_i$ 的 $(\sum_{i=1}^s t_ig_i,d,w)_q$-码 $\mathcal{C}'$。特别地，如果 $\mathcal{C}$ 和 $\mathcal{C}_i(1\leq i\leq s)$中的码字都具有相同构型 $\overline{w}$，那么 $\mathcal{C}'$ 中的每个码字的构型也是 $\overline{w}$。

性质 5.22 (点添加(Adjoining Points))：假设 y 为正整数，并且存在一个含 a 个码字、型为 $g_1^{t_1}\cdots g_s^{t_s}$ 的（主）可分组码 w-GDC(d)。如果下面的（辅助）码也存在：

1．大小为 b 的 $(g_1+y,d,w)_q$-码；

2．大小为 c_i，型为 $1^{g_i}y^1$ 的可分组码 w-GDC(d)，$2\leq i\leq s$；

3．大小为 c_1，型为 $1^{g_1}y^1$ 的可分组码 w-GDC(d)，并且 $t_1\geq 2$。

那么存在一个大小为 $a+b+(t_1-1)c_1+\sum_{i=2}^s t_ic_i$ 的 $(y+\sum_{i=1}^s t_ig_i,d,w)_q$-码。进一步的，如果主码和辅助码都具有恒定的构型，那么得到的码也具有同样的构型。

下面的膨胀构造法（Inflation Construction）也非常有用。

性质 5.23 (**膨胀构造**): 令 $(X,\mathcal{G},\mathcal{C})$ 是一个大小为 a、型为 $g_1^{t_1}\cdots g_s^{t_s}$ 的 w-GDC(d)。如果存在横截设计 TD(w,m),那么存在一个型为 $(mg_1)^{t_1}\cdots(mg_s)^{t_s}$ 的 w-GDC(d),其含有 am^2 个码字。进一步的,如果出发的可分组码具有恒定构型 $\overline{w}$,那么得到的码也具有相同的构型。

下面的构造被称为基本构造法(Fundamental Construction),这是对于组合设计理论中 Wilson 基本构造法在编码理论中的拓广。

定理 5.24 (**基本构造**, Chee **等**[31]): 假设 $d\le 2(w-1)$。令 $(X,\mathcal{G},\mathcal{B})$ 是一个(主)可分组设计,而 $\omega: X\to\mathbb{Z}_{\ge 0}$ 是一个权重函数(Weight Function)。如果对于每个区组 $B\in\mathcal{B}$,都存在一个型为 $\{\!\{\omega(a)\mid a\in B\}\!\}$ 的(辅助)可分组码 w-GDC(d)。那么则存在一个型为 $\{\!\{\sum_{x\in G}\omega(x)\mid G\in\mathcal{G}\}\!\}$ 的可分组码 w-GDC(d)。进一步的,如果所有辅助可分组码都具有恒定构型 $\overline{w}$,那么得到的可分组码也具有相同的构型。

5.2.3 已知的上下界

在重量为 w 的常重复合码中,任意两个不同码字间的距离至少为 2,至多为 $2w$;并且当其距离为 $2w$ 时,这两个码字的支撑集是不交的。

引理 5.25 (Chee **等**[31]): 记 $w=\sum_{i=1}^{q-1}w_i$,则

$$A_q(n,d,[w_1,\ldots,w_{q-1}])=\begin{cases}\binom{n}{w}\binom{w}{w_1,\ldots,w_{q-1}} & \text{若 } d\le 2\\ \lfloor\frac{n}{w}\rfloor & \text{若 } d=2w\\ 1 & \text{若 } d\ge 2w+1\text{。}\end{cases}$$

下面的定理描述了常重复合码的 Johnson 型上界。

定理 5.26 (Svanström **等**[165]): 对于任意 $i=1,\ldots,q-1$,我们都有

$$A_q(n,d,[w_1,\ldots,w_{q-1}])\le\frac{n}{w_i}A_q(n-1,d,[w_{1,i},\ldots,w_{q-1,i}]),$$

其中

$$w_{j,i}=\begin{cases}w_j-1 & \text{若 } j=i\\ w_j & \text{若 } j\ne i\text{。}\end{cases}$$

作为引理 5.25 和定理 5.26 的推论，我们有如下结果。

推论 5.27 (Chee 等[32])：记 $w=\sum_{i=1}^{q-1}w_i$，则

$$A_q(n,d,[w_1,\ldots,w_{q-1}])\le\begin{cases}\lfloor\frac{n}{w_1}\lfloor\frac{n-1}{w-1}\rfloor\rfloor & \text{若 } d=2w-2\\ \lfloor\frac{n}{w_1}\lfloor\frac{n-1}{w_1-1}\rfloor\rfloor & \text{若 } d=2w-3\text{。}\end{cases}$$

特别的，对于距离为 5、重量为 4 的常重复合码，我们有如下形式的 Johnson 界。

推论 5.28 (Johnson 界)：

$$A_3(n,5,[3,1]) \le \left\lfloor\frac{n}{3}\left\lfloor\frac{n-1}{2}\right\rfloor\right\rfloor := U(n,5,[3,1]),\quad \text{并且} \tag{5.4}$$

$$A_3(n,5,[2,2]) \le \left\lfloor\frac{n}{2}\left\lfloor\frac{n-1}{2}\right\rfloor\right\rfloor := U(n,5,[2,2])\text{。} \tag{5.5}$$

5.3 确定 $A_3(n,5,[3,1])$ 的值

在这一节中，我们将对所有的正整数 n 都确定出 $A_3(n,5,[3,1])$ 的准确值。但在此之前，我们先引入两个记号，以简化这一节和下一节中的表述。

设 r 和 c 为正整数，我们用 $\mathcal{G}_{r,c}$ 表示集族：

$$\mathcal{G}_{r,c}:=\big\{\{i+j\cdot r\mid j=0,1,\ldots,c-1\}\mid i=0,1,\ldots,r-1\big\}\text{。}$$

注意到，$\mathcal{G}_{r,c}$ 中的集合构成了 $\mathbb{Z}_{rc}$ 的一个划分。

我们再定义向量的一种等价表示方法。假设向量 $\mathtt{u}\in\mathbb{Z}_q^X$ 的构型是 $\overline{w}$，其中 $\overline{w}=[w_1,\ldots,w_{q-1}]$。令 $w=\sum_{i=1}^{q-1}w_i$，则我们可以将 $\mathtt{u}$ 等价地表示为一个 w 元组 $\langle a_1,a_2,\ldots,a_w\rangle\in X^w$，其中

$$\begin{aligned}\mathtt{u}_{a_1}=\cdots=\mathtt{u}_{a_{w_1}} &= 1,\\ \mathtt{u}_{a_{w_1+1}}=\cdots=\mathtt{u}_{a_{w_1+w_2}} &= 2,\\ &\vdots\\ \mathtt{u}_{a_{\sum_{i=1}^{q-2}w_i+1}}=\cdots=\mathtt{u}_w &= q-1\text{。}\end{aligned}$$

当向量的重量较小时，这种表示方法更加简洁和灵活。因此，我们在下面两节中都将采用这种形式来书写常重复合码的码字。

5.3.1 一些可分组码 $[3,1]$-GDC(5)

性质 5.29: *存在大小为 8、型为 2^4 的 $[3,1]$-GDC(5);也存在大小为 28、型为 2^7 的 $[3,1]$-GDC(5)。*

证明. $(\mathbb{Z}_8, \mathcal{G}_{4,2}, \mathcal{C}_1)$ 是一个大小为 8、型为 2^4 的 $[3,1]$-GDC(5),其中 $\mathcal{C}_1$ 由以下向量组成:

$$\begin{array}{cccc} \langle 0,1,2,3\rangle & \langle 0,6,7,1\rangle & \langle 1,4,7,2\rangle & \langle 2,5,7,0\rangle \\ \langle 0,3,5,6\rangle & \langle 1,3,6,4\rangle & \langle 2,3,4,5\rangle & \langle 4,5,6,7\rangle \end{array}$$

$(\mathbb{Z}_{14}, \mathcal{G}_{7,2}, \mathcal{C}_2)$ 是一个大小为 28、型为 2^7 的 $[3,1]$-GDC(5),其中 $\mathcal{C}_2$ 由以下向量组成:

$$\begin{array}{cccc} \langle 0,1,2,3\rangle & \langle 2,3,6,8\rangle & \langle 4,9,12,1\rangle & \langle 0,12,13,8\rangle \\ \langle 0,3,4,5\rangle & \langle 2,7,8,5\rangle & \langle 5,7,13,4\rangle & \langle 1,10,12,0\rangle \\ \langle 0,5,6,1\rangle & \langle 2,4,5,10\rangle & \langle 5,8,10,6\rangle & \langle 1,11,13,5\rangle \\ \langle 0,8,9,4\rangle & \langle 3,7,11,9\rangle & \langle 5,9,11,8\rangle & \langle 2,10,13,1\rangle \\ \langle 1,3,5,7\rangle & \langle 3,9,13,0\rangle & \langle 6,7,12,3\rangle & \langle 2,11,12,6\rangle \\ \langle 1,4,6,2\rangle & \langle 4,7,10,8\rangle & \langle 6,8,11,0\rangle & \langle 3,8,12,11\rangle \\ \langle 1,7,9,6\rangle & \langle 4,8,13,3\rangle & \langle 0,10,11,2\rangle & \langle 6,9,10,11\rangle \end{array}$$

□

性质 5.30: *存在大小为 30、型为 3^5,和大小为 63、型为 3^7 的 $[3,1]$-GDC(5)。*

证明. $(\mathbb{Z}_{15}, \mathcal{G}_{5,3}, \mathcal{C}_1)$ 是一个大小为 30、型为 3^5 的 $[3,1]$-GDC(5),其中 $\mathcal{C}_1$ 由向量 $\langle 1,2,13,0\rangle$ 和 $\langle 3,9,11,0\rangle$ 的所有循环移位组成。

$(\mathbb{Z}_{21}, \mathcal{G}_{7,3}, \mathcal{C}_2)$ 是一个大小为 63、型为 3^7 的 $[3,1]$-GDC(5),其中 $\mathcal{C}_2$ 由向量 $\langle 1,2,4,0\rangle$、$\langle 3,8,18,0\rangle$ 和 $\langle 5,9,17,0\rangle$ 的所有循环位移组成。 □

性质 5.31: *存在一个大小为 32、型为 4^4 的 $[3,1]$-GDC(5)。*

证明. $(\mathbb{Z}_{16}, \mathcal{G}_{4,4}, \mathcal{C})$ 是一个大小为 32、型为 4^4 的 $[3,1]$-GDC(5),其中 $\mathcal{C}$ 由向量 $\langle 1,3,14,0\rangle$ 和 $\langle 5,6,15,0\rangle$ 的所有循环移位组成。 □

性质 5.32: *对于所有 $u \geq 4$,都存在一个型为 6^u 的 $[3,1]$-GDC(5)。*

证明. 当 $u \equiv 0,1 \pmod 4$ 且 $u \geq 4$ 时,由定理 5.15 知,存在一个成对平衡设计 PBD$(3u+1, \{4\})$。从这个设计中删除一个点,则我们得到一个型为 3^u 的 $\{4\}$-GDD。而当 $u \equiv 2,3 \pmod 4$ 且 $u \geq 7$ 时,由同一定理知存在一个 PBD$(3u+1, \{4, 7^\star\})$。我

们从 X 中删除掉大小 7 的区组之外的某一个点，可以得到型为 3^u 的 $\{4,7^\star\}$-GDD。总之，对于所有参数 $u \geq 4$ 且 $u \neq 6$，都存在一个型为 3^u 的 $\{4,7\}$-GDD。

将基本构造法应用于以上得到的型为 3^u 的 $\{4,7\}$-GDD，其中权重函数的值恒为 2，而需要的辅助码（型为 2^4 和 2^7 的 $[3,1]$-GDC(5)）由性质 5.29 保证。因此对于所有参数 $u \geq 4$，并且 $u \neq 6$，我们都可以得到一个型为 6^u 的 $[3,1]$-GDC(5)。

当 $u = 6$ 时，$(\mathbb{Z}_{36}, \mathcal{G}_{6,6}, \mathcal{C})$ 是一个大小为 180、型为 6^6 的 $[3,1]$-GDC(5)，其中 $\mathcal{C}$ 由第 5.5 节中表 5.4 内的向量组成。 □

性质 5.33：对于所有 $u \in [4,7]$，都存在一个型为 $6^u 2^1$ 的 $[3,1]$-GDC(5)，其含有 $2u(3u-1)$ 个码字；对于所有 $v \in [4,9]$，都存在一个型为 $6^v 4^1$ 的 $[3,1]$-GDC(5)，其含有 $2v(3v+1)$ 个码字。

证明. 对于 $u \in [4,7]$，令 $X_u = \mathbb{Z}_{6u} \cup \{\infty_0, \infty_1\}$，且 $\mathcal{H}_u = \mathcal{G}_{u,6} \cup \{\{\infty_0, \infty_1\}\}$。那么 $(X_u, \mathcal{H}_u, \mathcal{C}_u)$ 就是我们需要的大小为 $2u(3u-1)$、型为 $6^u 2^1$ 的 $[3,1]$-GDC(5)，其中 $\mathcal{C}_u$ 由第 5.5 节中表 5.5 内的向量按步长为 6 的拟循环（Quasi-Cyclic）移位得到。

对于 $v \in [4,9]$，令 $X_v = \mathbb{Z}_{6v} \cup \{\infty_0, \ldots, \infty_3\}$，且 $\mathcal{H}_v = \mathcal{G}_{v,6} \cup \{\{\infty_0, \ldots, \infty_3\}\}$。那么 $(X_v, \mathcal{H}_v, \mathcal{C}_v)$ 就是我们需要的大小为 $2v(3v+1)$、型为 $6^v 4^1$ 的 $[3,1]$-GDC(5)，其中 $\mathcal{C}_v$ 由第 5.5 节中表 5.6 内的向量按步长为 6 的拟循环移位得到。 □

5.3.2 长度 $n \equiv 0 \pmod 6$ 的情形

我们首先确定长度 $n \geq 11$ 且 $n \equiv 0 \pmod 6$ 时，$A_3(n, 5, [3,1])$ 的值。

性质 5.34：对于每个 $n \in \{12, 18, 24, 30, 36, 42, 54\}$，都存在一个含有 $U(n, 5, [3,1])$ 个码字的最优 $(n, 5, [3,1])_3$-码。

证明. 以下为最优 $(12, 5, [3,1])_3$-码的 20 个码字：

$$\begin{array}{lllll} \langle 0,1,2,3\rangle & \langle 1,3,5,7\rangle & \langle 2,4,8,9\rangle & \langle 1,8,11,4\rangle & \langle 5,8,10,3\rangle \\ \langle 0,3,4,5\rangle & \langle 1,4,6,2\rangle & \langle 2,5,9,6\rangle & \langle 3,6,10,9\rangle & \langle 6,7,11,3\rangle \\ \langle 0,5,6,1\rangle & \langle 1,7,9,0\rangle & \langle 6,8,9,7\rangle & \langle 3,9,11,1\rangle & \langle 2,10,11,0\rangle \\ \langle 0,7,8,2\rangle & \langle 2,3,7,4\rangle & \langle 0,9,10,4\rangle & \langle 4,7,10,1\rangle & \langle 4,5,11,10\rangle \end{array}$$

以下为最优 $(18,5,[3,1])_3$-码的 48 个码字：

$\langle 0,4,7,9\rangle$ $\langle 2,4,5,13\rangle$ $\langle 0,3,17,13\rangle$ $\langle 4,12,17,5\rangle$ $\langle 0,12,14,16\rangle$
$\langle 0,1,11,7\rangle$ $\langle 2,7,9,14\rangle$ $\langle 1,15,17,0\rangle$ $\langle 4,14,16,6\rangle$ $\langle 10,12,16,4\rangle$
$\langle 0,2,13,1\rangle$ $\langle 3,5,13,7\rangle$ $\langle 1,5,16,14\rangle$ $\langle 4,9,10,17\rangle$ $\langle 10,13,17,6\rangle$
$\langle 0,5,9,11\rangle$ $\langle 3,8,9,16\rangle$ $\langle 1,9,13,10\rangle$ $\langle 7,10,14,5\rangle$ $\langle 11,14,17,4\rangle$
$\langle 0,6,16,2\rangle$ $\langle 4,8,11,2\rangle$ $\langle 2,15,16,8\rangle$ $\langle 7,12,13,2\rangle$ $\langle 13,14,15,9\rangle$
$\langle 1,2,12,9\rangle$ $\langle 5,6,17,1\rangle$ $\langle 2,6,10,15\rangle$ $\langle 8,12,15,6\rangle$ $\langle 5,11,12,15\rangle$
$\langle 1,3,7,15\rangle$ $\langle 5,7,15,4\rangle$ $\langle 2,8,17,10\rangle$ $\langle 8,13,16,0\rangle$ $\langle 6,11,13,14\rangle$
$\langle 1,4,6,11\rangle$ $\langle 5,8,10,9\rangle$ $\langle 3,10,11,8\rangle$ $\langle 9,11,15,3\rangle$ $\langle 7,11,16,10\rangle$
$\langle 1,8,14,3\rangle$ $\langle 6,7,8,13\rangle$ $\langle 3,4,15,14\rangle$ $\langle 9,16,17,7\rangle$
$\langle 2,3,14,0\rangle$ $\langle 6,9,14,8\rangle$ $\langle 3,6,12,17\rangle$ $\langle 0,10,15,12\rangle$

大小为 204 的最优 $(36,5,[3,1])_3$-码的码字集合由下面的向量按步长为 12 的拟循环移位展开得到：

$\langle 6,7,1,4\rangle$ $\langle 15,5,26,8\rangle$ $\langle 6,17,29,0\rangle$ $\langle 12,21,15,3\rangle$ $\langle 22,3,30,10\rangle$
$\langle 1,8,25,0\rangle$ $\langle 16,0,14,3\rangle$ $\langle 7,11,27,1\rangle$ $\langle 12,27,25,4\rangle$ $\langle 23,10,35,3\rangle$
$\langle 4,28,7,3\rangle$ $\langle 17,0,32,4\rangle$ $\langle 7,19,25,8\rangle$ $\langle 13,10,24,5\rangle$ $\langle 24,9,18,11\rangle$
$\langle 7,3,26,5\rangle$ $\langle 17,3,21,9\rangle$ $\langle 8,16,34,6\rangle$ $\langle 13,26,2,10\rangle$ $\langle 25,28,29,2\rangle$
$\langle 7,8,0,10\rangle$ $\langle 18,16,1,5\rangle$ $\langle 8,31,22,9\rangle$ $\langle 14,18,15,9\rangle$ $\langle 4,27,35,10\rangle$
$\langle 8,13,9,2\rangle$ $\langle 19,0,28,6\rangle$ $\langle 8,4,21,11\rangle$ $\langle 14,20,17,8\rangle$ $\langle 6,35,13,11\rangle$
$\langle 9,23,7,0\rangle$ $\langle 2,20,23,9\rangle$ $\langle 9,15,20,5\rangle$ $\langle 14,34,28,7\rangle$ $\langle 10,34,17,11\rangle$
$\langle 0,35,24,9\rangle$ $\langle 2,21,18,0\rangle$ $\langle 9,35,16,8\rangle$ $\langle 15,27,22,2\rangle$ $\langle 12,32,30,11\rangle$
$\langle 10,0,31,1\rangle$ $\langle 20,30,6,1\rangle$ $\langle 1,17,15,10\rangle$ $\langle 16,21,26,1\rangle$ $\langle 14,19,22,11\rangle$
$\langle 11,1,10,6\rangle$ $\langle 21,10,9,4\rangle$ $\langle 10,16,30,2\rangle$ $\langle 16,29,23,4\rangle$ $\langle 14,21,24,10\rangle$
$\langle 11,30,2,8\rangle$ $\langle 21,31,6,2\rangle$ $\langle 10,25,33,9\rangle$ $\langle 17,22,24,1\rangle$ $\langle 15,16,25,11\rangle$
$\langle 13,5,11,4\rangle$ $\langle 21,5,23,7\rangle$ $\langle 11,24,15,7\rangle$ $\langle 18,23,31,8\rangle$ $\langle 32,11,20,10\rangle$
$\langle 15,30,4,0\rangle$ $\langle 5,16,32,9\rangle$ $\langle 12,13,14,0\rangle$ $\langle 19,26,17,7\rangle$
$\langle 15,32,7,6\rangle$ $\langle 5,33,19,3\rangle$ $\langle 12,18,17,2\rangle$ $\langle 20,26,22,3\rangle$

当 $n\in\{24,30,42,54\}$ 时，最优 $(n,5,[3,1])_3$-码的码字由第 5.5 节中表 5.7 内的向量按照步长为 6 的拟循移位环展开得到。 □

性质 5.35：对于所有 $t\geq 4$，都存在大小为 $24t(t-1)$、型为 12^t 的 $[3,1]$-GDC(5)。

证明. 当 $t>4$ 时，由定理 5.7 知存在一个型为 6^t 的 $\{4\}$-GDD，对其应用权重为 2 的基本构造，则可得到大小为 $24t(t-1)$、型为 12^t 的 $[3,1]$-GDC(5)，其中需要的 2^4 型辅助可分组码由性质 5.29 提供。

当 $t=4$ 时，使用横截设计 TD$(4,3)$ 对一个大小为 32、型为 4^4 的 $[3,1]$-GDC(5) 进行膨胀，就可以得到一个大小为 288、型为 12^4 的 $[3,1]$-GDC(5)。 □

性质 5.36：对于所有 $t\geq 1$，等式 $A_3(12t,5,[3,1])=U(12t,5,[3,1])$ 均成立。

证明. 当 $t \geq 4$ 时，向型为 12^t 的 $[3,1]$-GDC(5) 中每个组内填入一个大小为 20 的 $(12,5,[3,1])_3$-码，则我们可以得到一个大小为 $24t(t-1)+20t = 24t^2-4t$ 的 $(12t,5,[3,1])_3$-码，这正好达到了推论 5.28 中的上界，因此它是最优的。而当 $n = 24,36$ 时，我们在性质 5.34 中构造出的码达到了最优。 □

性质 5.37：对于所有 $t \geq 49$，均存在一个含有 $U(12t+6,5,[3,1])$ 个码字的最优 $(12t+6,5,[3,1])_3$-码。

证明. 由定理 5.9 知，对于所有 $u \geq 12$ 都存在横截设计 TD$(6,2u)$。如定理 5.10 中所示，我们将最后两个组截短，得到型为 $(2u)^4(2x)^13^1$ 的 $\{4,5,6\}$-GDD，其中 $x \in [0,u]$。对这个可分组设计使用权重为 6 的基本构造，填入型为 $6^4,6^5,6^6$ 的 $[3,1]$-GDC(5)，从而得到型为 $(12u)^4(12x)^118^1$ 的可分组码。向其组内添加进长度为 $12u,12x,18$ 的最优码。则生成的码具有长度 $n = 12t+6$，其中 $t = 4u+x+1$，而 $u \geq 12, x \in [0,u]$。当 x 跑遍 $[0,u]$ 时，t 的取值将包含整个区间 $[4u+1,5u+1]$。进一步，当 u 的取值从 12 逐渐增大到无穷时，区间 $[4u+1,5u+1]$ 将会产生重叠并覆盖所有不小于 49 的正整数。容易检查发现，这些常重复合码的码字个数恰为 $U(12t+6,5,[3,1])$，从而它们是最优的。 □

性质 5.38：对于所有 $t \in [17,48]$，均存在达到 Johnson 界的最优 $(12t+6,5,[3,1])_3$-码。

证明. 当 $17 \leq t \leq 33$ 时，我们将一个横截设计 TD$(9,8)$ 的最后五个组进行截短，得到一个型为 $8^4(2g_5)^1\ldots(2g_8)^13^1$ 的 $\{4,5,\ldots,9\}$-GDD，其中 $0 \leq g_i \leq 4 (i \in [5,8])$。利用型为 $6^u (u \in [4,9])$ 的辅助 $[3,1]$-GDC(5)，对其使用权重为 6 的基本构造，从而获得一个型为 $48^4(12g_5)^1\ldots(12g_8)^118^1$ 的 $[3,1]$-GDC(5)。最后再向组中填入长度为 $n \in \{12,24,36,48,18\}$ 的最优码，我们就可以得到需要的最优常重复合码。对横截设计 TD$(9,16)$ 使用相似的方法，我们可以得到长度为 $12t+6 (t \in [33,48])$ 的最优码。 □

性质 5.39：对于所有 $t \in [5,16]$，均存在最优 $(12t+6,5,[3,1])_3$-码，其含有的码字个数是 $U(12t+6,5,[3,1])$。

证明. 当时 $t=5,6,8$，对型为 $6^{t-1}9^1$ 的 $\{4\}$-GDD 使用基本构造法，辅助设计是型为 2^4 的 $[3,1]$-GDC(5)。再向其组内填入长度为 $12,18$ 的最优码，则可以得到长度为 $n=12t+6$ 的最优常重复合码。

当 $t=7,10$ 时，利用横截设计 TD$(4,3)$ 对型为 6^5 或 6^7 的 $[3,1]$-GDC(5) 进行膨胀，并在组中填入长度合适的最优码，则可以得到所需的最优常重复合码。

当 $t=9$ 时，截短横截设计 TD$(5,4)$ 得到一个型为 4^43^1 的 $\{4,5\}$-GDD，利用型为 6^4 或 6^5 的 $[3,1]$-GDC(5)，使用基本构造法得到型为 24^418^1 的 $[3,1]$-GDC(5)。最后向其组内填入合适的码即能得到要求的最优常重复合码。

当 $t=11,12$ 时，由横截设计 TD$(5,5)$ 得到型为 5^43^1 或 5^5 的 $\{4,5\}$-GDD。使用基本构造法（输入型为 6^4 或 6^5 的 $[3,1]$-GDC(5)）并向组内填入最优码，就等得到我们需要的结果。

当 $t=13,14$ 时，由横截设计 TD$(6,5)$ 得到型为 5^52^1 或 5^54^1 的 $\{5,6\}$-GDD。使用基本构造法（输入型为 6^5 或 6^6 的 $[3,1]$-GDC(5)）并向组内填入最优码，就等得到我们需要的结果。

当 $t=15$ 时，给型为 4^7 的 $\{4\}$-RGDD 中的三个平行类分别添加三个点，从而得到一个型为 4^73^1 的 $\{4,5\}$-GDD。再使用基本构造法，输入型为 6^4 和 6^5 的 $[3,1]$-GDC(5)，并向组内填入最优码，即可得到所需的结论。

当 $t=16$ 时，截短横截设计 TD$(6,7)$ 得到一个型为 $7^43^12^1$ 的 $\{4,5,6\}$-GDD，利用型为 6^4、6^5 和 6^6 的 $[3,1]$-GDC(5)，使用基本构造法得到型为 $42^518^112^1$ 的 $[3,1]$-GDC(5)。最后向其组内填入合适的码即能得到要求的最优常重复合码。 □

综合以上的结论，我们可以知道：

定理 5.40：对于所有 $t\geq 2$，等式 $A_3(6t,5,[3,1])=U(6t,5,[3,1])$ 均成立。

5.3.3 长度 $n\equiv 1 \pmod 6$ 的情形

性质 5.41：存在长度 $n=13$ 和 19 的最优 $(n,5,[3,1])_3$-码，其大小达到上界 $U(n,5,[3,1])$。

证明. 最优 $(13,5,[3,1])_3$-码的 26 个码字由向量 $\langle 0,1,4,2\rangle$ 和 $\langle 0,2,7,6\rangle$ 的所有循环移位产生。

最优 $(19,5,[3,1])_3$-码的 57 个码字由向量 $\langle 3,11,13,0\rangle$、$\langle 1,14,15,0\rangle$ 和 $\langle 2,5,9,0\rangle$ 的所有循环移位产生。 □

定理 5.42: 对于所有 $t\geq 2$, 等式 $A_3(6t+1,5,[3,1])=U(6t+1,5,[3,1])$ 均成立。

证明. 对于 $t=2,3$, 参见性质 5.41。当 $t\geq 4$ 时, 向型为 6^t 的 $[3,1]$-GDC(5) 中添加一个无穷点, 并向每个组和这个无穷点中填入最优 $(7,5,[3,1])_3$-码, 就可以得到长度为 $6t+1$ 的最优常重复合码。 □

5.3.4 长度 $n\equiv 2 \pmod 6$ 的情形

性质 5.43: 存在长度 $n=14$ 和 20 的最优 $(n,5,[3,1])_3$-码, 含有 $U(n,5,[3,1])$ 个码字。

证明. 最优 $(14,5,[3,1])_3$-码的 28 个码字由向量 $\langle 0,2,3,1\rangle$、$\langle 1,4,8,0\rangle$、$\langle 3,5,9,0\rangle$ 和 $\langle 4,9,10,1\rangle$ 按步长为 2 的拟循环移位组成。

最优 $(20,5,[3,1])_3$-码的 60 个码字有以下向量按步长为 4 的拟循环移位组成:

$$\begin{array}{cccc}\langle 0,1,2,3\rangle & \langle 1,5,12,0\rangle & \langle 3,14,8,1\rangle & \langle 0,17,12,2\rangle\\ \langle 0,4,7,1\rangle & \langle 1,7,13,2\rangle & \langle 3,4,15,2\rangle & \langle 5,10,15,3\rangle\\ \langle 3,7,6,0\rangle & \langle 2,5,18,1\rangle & \langle 4,2,14,0\rangle & \langle 6,17,19,3\rangle\end{array}$$

□

定理 5.44: 对于任意整数 $t\geq 2$, 均有 $A_3(6t+2,5,[3,1])=U(6t+2,5,[3,1])$ 成立。

证明. 当 $t=2$ 和 3 时, 所需的码在性质 5.43 中已经给出。当 $t\geq 4$ 时, 选取一个型为 6^t 的 $[3,1]$-GDC(5) 作为主码, 添加两个无穷点, 然后向每个组与这两个点中同时填入一个型为 2^4 的 $[3,1]$-GDC(5)。得到的可分组码的型为 2^{3t+1}。仔细计算这个可分组码的参数可发现, 它包含了 $8*t+6t(t-1)=6t^2+2t$ 个码字, 恰好等于 $U(6t+2,5,[3,1])$。因此这个可分组码就是一个所求的最优 $(6t+2,5,[3,1])_3$-码。 □

5.3.5 长度 $n \equiv 3 \pmod 6$ 的情形

性质 5.45：对于每个 $n \in \{15, 21, 27, 33, 39\}$，均存在含 $U(n, 5, [3, 1])$ 个码字的最优 $(n, 5, [3, 1])_3$ 码。

证明. 最优 $(n, 5, [3, 1])_3$-码包含的 $U(n, 5, [3, 1])$ 个码字分别由以下向量按步长为 3 的所有移位组成：

$n = 15$:

$$\langle 0, 1, 3, 2\rangle \quad \langle 5, 8, 9, 2\rangle \quad \langle 2, 4, 10, 0\rangle \quad \langle 3, 5, 12, 0\rangle \quad \langle 2, 7, 11, 1\rangle$$
$$\langle 0, 4, 5, 1\rangle \quad \langle 1, 6, 13, 0\rangle$$

$n = 21$：

$$\langle 5, 18, 1, 2\rangle \quad \langle 8, 3, 12, 0\rangle \quad \langle 5, 20, 17, 1\rangle \quad \langle 9, 20, 10, 0\rangle \quad \langle 8, 16, 7, 2\rangle$$
$$\langle 6, 19, 4, 2\rangle \quad \langle 0, 14, 15, 2\rangle \quad \langle 7, 12, 14, 1\rangle \quad \langle 13, 16, 11, 0\rangle \quad \langle 18, 15, 4, 1\rangle$$

$n = 27$：

$$\langle 7, 9, 6, 0\rangle \quad \langle 6, 20, 1, 2\rangle \quad \langle 11, 1, 25, 0\rangle \quad \langle 3, 24, 26, 1\rangle \quad \langle 15, 26, 22, 2\rangle$$
$$\langle 18, 3, 7, 2\rangle \quad \langle 8, 23, 5, 0\rangle \quad \langle 11, 13, 4, 1\rangle \quad \langle 7, 22, 23, 1\rangle \quad \langle 8, 14, 15, 1\rangle$$
$$\langle 5, 0, 10, 2\rangle \quad \langle 9, 0, 17, 1\rangle \quad \langle 12, 4, 25, 2\rangle$$

$n = 33$：

$$\langle 2, 7, 4, 0\rangle \quad \langle 3, 14, 10, 0\rangle \quad \langle 5, 21, 12, 0\rangle \quad \langle 9, 10, 17, 1\rangle \quad \langle 5, 15, 20, 1\rangle$$
$$\langle 6, 16, 5, 2\rangle \quad \langle 4, 18, 10, 2\rangle \quad \langle 6, 20, 26, 0\rangle \quad \langle 9, 15, 27, 0\rangle \quad \langle 8, 11, 32, 2\rangle$$
$$\langle 6, 2, 19, 1\rangle \quad \langle 4, 21, 23, 1\rangle \quad \langle 7, 18, 22, 1\rangle \quad \langle 11, 19, 31, 0\rangle \quad \langle 13, 22, 23, 2\rangle$$
$$\langle 0, 28, 30, 1\rangle$$

$n = 39$：

$$\langle 29, 0, 9, 2\rangle \quad \langle 29, 26, 5, 0\rangle \quad \langle 38, 16, 8, 0\rangle \quad \langle 14, 21, 18, 0\rangle \quad \langle 27, 10, 15, 2\rangle$$
$$\langle 1, 19, 34, 0\rangle \quad \langle 31, 6, 17, 2\rangle \quad \langle 4, 12, 13, 2\rangle \quad \langle 17, 15, 33, 1\rangle \quad \langle 31, 20, 21, 1\rangle$$
$$\langle 21, 8, 34, 2\rangle \quad \langle 32, 37, 5, 1\rangle \quad \langle 6, 10, 30, 0\rangle \quad \langle 22, 15, 20, 0\rangle \quad \langle 33, 31, 11, 0\rangle$$
$$\langle 25, 9, 37, 0\rangle \quad \langle 36, 5, 30, 2\rangle \quad \langle 13, 29, 23, 1\rangle \quad \langle 25, 26, 22, 2\rangle$$

□

性质 5.46：对于所有整数 $t \geq 94$，$A_3(6t + 3, 5, [3, 1])$ 的值均为 $U(6t + 3, 5, [3, 1])$。

证明. 截短横截设计 TD$(6,u)$($u \geq 23$)的最后两个组，可以得到一个型为 $u^4x^1y^1$ 的 $\{4,5,6\}$-GDD，其中 $x,y \in [0,u]$。对这个可分组设计使用基本构造，其中对大小为 u 和 x 的五个组中的点使用权重 6，对最后一个组中的点使用权重 2、4 或 6，则生成的是一个型为 $(6u)^4(6x)^1z^1$ 的 $[3,1]$-GDC(5)，其中 $x \in [0,u]$，并且 $z \in \{14,20,\ldots,38\}$。向这个可分组码添加一个无穷点，然后向每个组和这一无穷点填入一个长度为 $6u+1$、$6x+1$ 和 $z+1$ 的最优码，则得到一个长度为 $n=6t+3$ 的最优常重复合码，其中 $t \in [4u+2,5u+6]$。当 u 从 23 逐渐增加时，区间 $[4u+2,5u+6]$ 会产生重叠，并覆盖所有不小于 94 的正整数。 □

性质 5.47：对于每个整数 $22 \leq t \leq 93$，等式 $A_3(6t+3,5,[3,1]) = U(6t+3,5,[3,1])$ 均成立。

证明. 证明与性质 5.46 相类似。当 $t \in [22,29]$ 时，截短 TD$(6,5)$ 的最后两个组，得到一个型为 $5^4x^1y^1$ 的 $\{4,5,6\}$-GDD，其中 $x,y \in [0,5]$。对其使用基本构造，得到型为 $30^4(6x)^1z^1$ 的 $[3,1]$-GDC(5)，其中 $x \in [0,5]$，$z \in \{14,20,26\}$。添加一个无穷点，然后向每个组和这点中填入适当长度的最优码，就可以得到长度为 $n=6t+3$ 的最优常重复合码。当 $t \in [30,93]$ 时，将同样的方法应用到横截设计 TD$(8,7)$ 和 TD$(8,13)$，分别得到 $t \in [30,55]$ 和 $t \in [55,93]$ 时的结果。 □

性质 5.48：对于每个 $t \in [7,21]$，$A_3(6t+3,5,[3,1]) = U(6t+3,5,[3,1])$ 均成立。

证明. 对于 $t=12$ 和 17，由性质 5.30 知，存在型为 3^5 和 3^7 的可分组码，对其使用 TD$(4,5)$ 进行膨胀，得到型为 15^5 和 15^7 的 $[3,1]$-GDC(5)。向其组内填入最优 $(15,5,[3,1])_3$-码，就可以得到长度为 75 和 105 时的最优常重复合码。

对于其它的 $t \in [7,21]\backslash\{12,17\}$，最优 $(6t+3,5,[3,1])_3$-码的 $U(6t+3,5,[3,1]) = (2t+1)(3t+1)$ 个码字由文献[84] 中表 I 内的向量按步长为 3 的拟循环移位所组成。 □

综合上述结果，我们有如下结论：

定理 5.49：对于每个正整数 $t \geq 2$，等式 $A_3(6t+3,5,[3,1]) = U(6t+3,5,[3,1])$ 均成立。

表 5.2　最优 $(16,5,[3,1])_3$-码的 37 个码字

$\langle 0,3,8,9\rangle$	$\langle 0,6,7,12\rangle$	$\langle 8,9,11,2\rangle$	$\langle 3,5,13,12\rangle$	$\langle 9,13,15,1\rangle$
$\langle 1,4,7,6\rangle$	$\langle 1,3,15,5\rangle$	$\langle 0,9,12,13\rangle$	$\langle 4,10,13,9\rangle$	$\langle 0,10,15,11\rangle$
$\langle 3,6,9,7\rangle$	$\langle 1,6,11,8\rangle$	$\langle 1,5,14,11\rangle$	$\langle 5,11,15,7\rangle$	$\langle 4,12,15,10\rangle$
$\langle 4,6,8,0\rangle$	$\langle 1,8,12,3\rangle$	$\langle 1,9,10,14\rangle$	$\langle 5,6,10,15\rangle$	$\langle 8,10,14,12\rangle$
$\langle 5,7,9,0\rangle$	$\langle 2,3,7,11\rangle$	$\langle 2,10,11,1\rangle$	$\langle 6,12,14,1\rangle$	$\langle 11,13,14,15\rangle$
$\langle 0,1,13,2\rangle$	$\langle 2,4,9,12\rangle$	$\langle 2,12,13,6\rangle$	$\langle 7,11,12,4\rangle$	
$\langle 0,2,14,8\rangle$	$\langle 2,5,8,10\rangle$	$\langle 3,10,12,0\rangle$	$\langle 7,14,15,3\rangle$	
$\langle 0,4,5,14\rangle$	$\langle 2,6,15,9\rangle$	$\langle 3,4,11,13\rangle$	$\langle 7,8,13,14\rangle$	

5.3.6　长度 $n\equiv 4 \pmod 6$ 的情形

性质 5.50：对于每个整数 $u\in[3,11]\cup\{13,14,17,18,22\}$，都存在型为 $2^{3u}4^1$ 的 $[3,1]$-GDC(5)。

证明. 对于每个 $u\in[3,11]\cup\{13,14,17,18,22\}$，令 $X_u=\mathbb{Z}_{3u}\cup\{\infty_0,\ldots,\infty_3\}$，并令 $\mathcal{H}_u=\mathcal{G}_{3u,2}\cup\{\{\infty_0,\ldots,\infty_3\}\}$。假设是 $\mathcal{C}_u$ 所有文献[84] 中表 II 内的相应向量按步长为 2 的拟循环移位组成。则 $(X_u,\mathcal{H}_u,\mathcal{C}_u)$ 就是所求的型为 $2^{3u}4^1$ 的 $[3,1]$-GDC(5)，它含有 $6u(u+1)$ 个码字。 □

定理 5.51：对于所有 $t\geq 2$，$A_3(6t+4,5,[3,1])=U(6t+4,5,[3,1])$ 均成立。

证明. 当 $t=2$ 时，最优 $(16,5,[3,1])_3$-码的 37 个码字列在表 5.2 中。

当 $t\geq 3$ 时，令 $K=[4,12]\cup\{14,15,18,19,23\}$。由定理 5.16 知，对于每个 $t\geq 3$ 都存在 PBD$(t+1,K)$。从这个成对平衡设计中删去一个点，得到一个 t 阶的 K-GDD，其组大小落在集合 $\{k-1\mid k\in K\}$ 中。对这个可分组设计使用基本构造，输入型为 6^u 的 $[3,1]$-GDC(5)，其中 $u\in K$。则得到的可分组码长度为 $6t$，并且组大小集合为 $\{6k-6\mid k\in K\}$。向这个码中添加四个无穷点，并填入型为 $2^{3s}4^1$ 的辅助码，$s+1\in K$，那么生成的码的型为 $2^{3t}4^1$。最后向大小为 4 的那个组中填入长度 4 的最优码（仅一个码字），从而得到长度为 $6t+4$ 的常重复合码。计算得知，这个码含有 $U(6t+4,5,[3,1])$ 个码字，因此它是最优的。 □

5.3.7　长度 $n\equiv 5 \pmod 6$ 的情形

引理 5.52：对于所有正整数 $n\equiv 5 \pmod 6$，均有 $A_3(n,5,[3,1])\leq U(n,5,[3,1])-1$。

证明. 令 $\mathcal{C} \subseteq \mathbb{Z}_3^X$ 是一个最优 $(n,5,[3,1])_3$-码，其长度 $|X| = n$ 满足条件 $n \equiv 5 \pmod 6$。对于每个码字，我们将其中为 "1" 的位置取出组成一个 X 的 3-子集。容易验证，以这些 $|\mathcal{C}|$ 个 3-子集为区组集，就构成了 X 上的一个 2-$(n,3,1)$ 填充设计。由定理 5.19 知，

$$\begin{aligned} A_3(n,5,[3,1]) &\leq D_1(n,3,2) \\ &= U_1(n,3,2) - 1 \\ &= \lfloor \frac{n}{3} \lfloor \frac{n-1}{2} \rfloor \rfloor - 1 \\ &= U(n,5,[3,1]) - 1 \text{。} \end{aligned}$$

□

性质 5.53：对于每个 $n \in \{11,17,23,29\}$，都存在大小为 $U(n,5,[3,1])-1$ 的最优 $(n,5,[3,1])_3$-码。

证明. 参见文献[84] 中的表 III。 □

性质 5.54：对于所有整数 $t \geq 93$，等式 $A_3(6t+5,5,[3,1]) = U(6t+5,5,[3,1]) - 1$ 均成立。

证明. 截短横截设计 TD$(6,u)$ 的组，得到型为 $u^4x^1y^1$ 的 $\{4,5,6\}$-GDD，其中 $x \in [0,u]$，而 $y \in [2,5]$。应用基本构造，其中大小为 y 的组中一个点的权重为 4，其它所有点的权重为 6，可得到一个型为 $(6u)^4(6x)^1z^1$ 的可分组码，其中 $z = 10,16,22,28$。添加一个无穷点，再向每个组和这个无穷点中填入合适长度的最优码，我们可以得到长度为 $6t+5$ 的最优常重复合码，其中 $t \in [4u+1, 5u+4]$。当 u 从 23 增大到无穷时，区间将会产生重叠并覆盖所有不小于 93 的正整数。 □

性质 5.55：对于每个整数 $17 \leq t \leq 92$，等式 $A_3(6t+5,5,[3,1]) = U(6t+5,5,[3,1])-1$ 都成立。

证明. 证明与性质 5.54 类似。当 $t \in [17,20]$ 时，截短 TD$(5,4)$ 的最后一个组得到型为 4^4x^1 的 $\{4,5\}$-GDD，其中 $x \in [1,4]$。应用权重为 6 的基本构造法，得到型为 $24^4(6x)^1$ 的可分组码。添加四个无穷点，并向每个组和这四个点中填入型为 6^44^1 的辅助码，得

到型为 $6^{16}(6x+4)^1$ 的 $[3,1]$-GDC(5)。最后再向这个码中添加一个无穷点，并填入长为 7 和 $6x+5$ 的最优码，就可以得到最优 $(6t+5,5,[3,1])_3$-码。

当 $t\in[21,29]$ 时，截短 TD$(6,5)$ 得到型为 $5^4x^1y^1$ 的 $\{4,5,6\}$-GDD，其中 $x\in[0,5]$，$y\in[2,5]$。应用基本构造，最后一个组中的一点权重为 4，其它所有点权重为 6，得到型为 $30^4(6x)^1z^1$ 的可分组码，其中 $z=10,16,22,28$。添加一个无穷点，并向每个组和这个无穷点中填入长度为 $6x+1$ 和 $z+1$ 的最优码，就可以得到长度 $6t+5$ 的最优常重复合码。

当 $t\in[29,92]$ 时，将相似的方法应用到横截设计 TD$(8,7)$ 和 TD$(10,9)$，就可以分别得到 $t\in[29,60]$ 和 $t\in[37,94]$ 时的结果。 □

性质 5.56：对于每个整数 $6\le t\le 16$，等式 $A_3(6t+5,5,[3,1])=U(6t+5,5,[3,1])-1$ 均成立。

证明. 当 $t\in\{6,8,10,12,14,16\}$ 时，最优 $(6t+5,5,[3,1])$ 码的码字由两部分组成。第一部分是一个基于点集 $\{\infty_0,\ldots,\infty_{10}\}$ 上的最优 $(11,5,[3,1])$ 码。第二部分由文献[84] 中表 IV 内的向量按照置换 $(0,1,\ldots,3t-4)(3t-3,\ldots,6t-7)(\infty_0)\cdots(\infty_{10})$ 的作用展开得到。

当 $t\in\{7,9,11,13,15\}$ 时，令 $s=3(t-1)/2$。最优 $(6t+5,5,[3,1])$ 码的码字将有以下三部分：第一部分是在点集 $\{\infty_0,\ldots,\infty_{10}\}$ 上的最优 $(11,5,[3,1])$ 码；第二部分是文献[84] 中表 V 内第一行的两个向量按照置换 $(0,1,\ldots,s-1)(s,\ldots,2s-1)(2s,\ldots,3s-1)(3s,\ldots,4s-1)(\infty_0)\cdots(\infty_{10})$ 作用展开生成；第三部分由表内剩下的向量按照置换 $(0,1,\ldots,2s-1)(2s,\ldots,4s-1)(\infty_0)\cdots(\infty_{10})$ 作用得到。 □

我们将这些结果合并起来。

定理 5.57：对于所有正整数 $t\ge 1$，等式 $A_3(6t+5,5,[3,1])=U(6t+5,5,[3,1])-1$ 均成立。

5.4 确定 $A_3(n,5,[2,2])$ 的值

在这一节中，我们将确定所有 $A_3(n,5,[2,2])$ 的值。其中当长度 $n\le 10$ 时，已经由 Svanström 等人确定[165]，见本章第 5.1 节中的表 5.1。

5.4.1 一些可分组码 [2,2]-GDC(5)

性质 5.58:对于 $u \in \{7,9,11\}$,存在大小为 $u(u-1)$、型为 2^u 的 $[2,2]$-GDC(5)。

证明. $(\mathbb{Z}_{14}, \mathcal{G}_{7,2}, \mathcal{C}_1)$ 是一个大小为 42、型为 2^7 的 [2,2]-GDC(5),其中 $\mathcal{C}_1$ 是由向量 $\langle 0,11,2,12\rangle$、$\langle 0,1,4,10\rangle$ 和 $\langle 0,5,11,13\rangle$ 的所有循环移位组成。

$(\mathbb{Z}_{18}, \mathcal{G}_{9,2}, \mathcal{C}_2)$ 是一个大小为 72、型为 2^9 的 [2,2]-GDC(5),其中是 $\mathcal{C}_2$ 由向量 $\langle 0,14,10,13\rangle$、$\langle 0,2,7,8\rangle$、$\langle 0,1,3,16\rangle$ 和 $\langle 0,8,1,12\rangle$ 的所有循环移位组成。

$(\mathbb{Z}_{22}, \mathcal{G}_{11,2}, \mathcal{C}_3)$ 是一个大小为 110、型为 2^{11} 的 [2,2]-GDC(5),其中 $\mathcal{C}_3$ 是由向量 $\langle 0,8,6,10\rangle$、$\langle 0,10,1,3\rangle$、$\langle 0,19,4,9\rangle$、$\langle 0,6,5,14\rangle$ 和 $\langle 0,2,18,19\rangle$ 的所有循环移位组成。 □

性质 5.59:对于 $u \in [4,7]$,都存在型为 4^u 的 $[2,2]$-GDC(5),其含有 $4u(u-1)$ 个码字。

证明. $(\mathbb{Z}_{16}, \mathcal{G}_{4,4}, \mathcal{C}_1)$ 是一个大小为 48、型为 4^4 的 [2,2]-GDC(5),其中的码字是由以下向量按步长为 4 的拟循环移位组成:

$$\begin{array}{ccccc} \langle 0,2,1,7\rangle & \langle 0,11,6,9\rangle & \langle 1,8,7,10\rangle & \langle 3,10,8,13\rangle & \langle 1,2,3,12\rangle \\ \langle 1,7,4,6\rangle & \langle 1,15,2,8\rangle & \langle 3,14,4,5\rangle & \langle 3,12,9,10\rangle & \langle 1,14,0,11\rangle \\ \langle 0,10,3,5\rangle & \langle 0,13,10,11\rangle & & & \end{array}$$

对于 $u \in [5,7]$,令 $X_u = \mathbb{Z}_{4u}$,$\mathcal{H}_u = \mathcal{G}_{u,4}$,并令 $\mathcal{C}_u$ 分别由以下向量的循环移位组成:

$u = 5$:

$$\langle 0,7,8,19\rangle \quad \langle 0,14,3,11\rangle \quad \langle 0,12,14,18\rangle \quad \langle 0,9,13,16\rangle$$

$u = 6$:

$$\begin{array}{ccc} \langle 0,16,15,17\rangle & \langle 0,9,11,16\rangle & \langle 0,14,10,19\rangle \\ \langle 0,1,14,22\rangle & \langle 0,5,8,9\rangle & \end{array}$$

$u = 7$:

$$\begin{array}{ccc} \langle 0,12,17,23\rangle & \langle 0,19,10,18\rangle & \langle 0,4,12,24\rangle \\ \langle 0,15,9,13\rangle & \langle 0,18,6,15\rangle & \langle 0,2,3,4\rangle \end{array}$$

则 $(X_u, \mathcal{H}_u, \mathcal{C}_u)$ 分别是我们所求的分组码。 □

性质 5.60:存在大小为 64、型为 $4^4 2^1$ 的,和大小为 100、型为 $4^5 2^1$ 的 $[2,2]$-GDC(5)。

证明. 对于 $u=4$ 和 5，令 $X_u=\mathbb{Z}_{4u}\cup\{\infty_0,\infty_1\}$，$\mathcal{H}_u=\mathcal{G}_{u,4}\cup\{\{\infty_0,\infty_1\}\}$。让 $\mathcal{C}_u$ 分别是由以下向量按步长为 2 的拟循环移位组成的集合：

$u=4$：

$$\begin{array}{cccc}\langle 0,2,9,15\rangle & \langle 0,13,3,10\rangle & \langle 1,10,12,15\rangle & \langle 1,15,2,8\rangle\\ \langle \infty_0,1,3,6\rangle & \langle \infty_1,0,1,6\rangle & \langle 2,1,0,\infty_1\rangle & \langle 7,6,1,\infty_0\rangle\end{array}$$

$u=5$：

$$\begin{array}{cccc}\langle 0,3,2,16\rangle & \langle 0,11,9,13\rangle & \langle 0,13,1,7\rangle & \langle 0,19,6,8\rangle\\ \langle 1,4,7,18\rangle & \langle 1,14,12,13\rangle & \langle \infty_0,1,2,5\rangle & \langle 17,8,0,\infty_0\rangle\\ \langle \infty_1,0,4,11\rangle & \langle 5,4,1,\infty_1\rangle & & \end{array}$$

则 $(X_u,\mathcal{H}_u,\mathcal{C}_u)$ 是所求的可分组码。 □

性质 5.61：存在一个型为 6^5 的 $[2,2]$-GDC(5)，含有 180 个码字。

证明. 令 $\mathcal{C}$ 是由以下向量在 $\mathbb{Z}_{30}$ 中的循环移位组成：

$$\begin{array}{cccc}\langle 0,12,6,8\rangle & \langle 0,22,9,23\rangle & \langle 0,24,7,28\rangle & \langle 0,9,21,27\rangle\\ \langle 0,11,14,22\rangle & \langle 0,13,2,29\rangle & & \end{array}$$

则 $(\mathbb{Z}_{30},\mathcal{G}_{5,6},\mathcal{C})$ 是一个所求的可分组码。 □

性质 5.62：当 $u=4$ 或 5 时，存在一个大小为 $16u(u-1)$、型为 8^u 的 $[2,2]$-GDC(5)。

证明. 令 $\mathcal{C}_4$ 和 $\mathcal{C}_5$ 分别是以下向量在 $\mathbb{Z}_{32}$ 和 $\mathbb{Z}_{40}$ 中的循环移位组成的集合：

$u=4$：

$$\begin{array}{cccc}\langle 0,11,5,10\rangle & \langle 0,31,22,29\rangle & \langle 0,6,17,19\rangle & \langle 0,2,9,27\rangle\\ \langle 0,3,6,21\rangle & \langle 0,13,14,15\rangle & & \end{array}$$

$u=5$：

$$\begin{array}{cccc}\langle 0,7,16,39\rangle & \langle 0,12,13,31\rangle & \langle 0,21,29,33\rangle & \langle 0,38,4,36\rangle\\ \langle 0,1,3,22\rangle & \langle 0,3,14,27\rangle & \langle 0,31,17,28\rangle & \langle 0,11,18,34\rangle\end{array}$$

则 $(\mathbb{Z}_{32},\mathcal{G}_{4,8},\mathcal{C}_4)$ 和 $(\mathbb{Z}_{40},\mathcal{G}_{5,8},\mathcal{C}_5)$ 分别是大小为 192、型为 8^4 和大小为 320、型为 8^5 的 $[2,2]$-GDC(5)。 □

性质 5.63：对于每个 $u\in[5,9]$，都存在一个大小为 $8u(2u+3)$、型为 8^u10^1 和一个大小为 $8u(2u+5)$、型为 8^u14^1 的 $[2,2]$-GDC(5)。

表 5.3　最优 $(12,5,[2,2])_3$-码的 30 个码字

$\langle 0,4,1,7\rangle$	$\langle 2,7,6,8\rangle$	$\langle 4,5,0,9\rangle$	$\langle 4,11,2,3\rangle$	$\langle 7,9,3,10\rangle$
$\langle 0,5,3,8\rangle$	$\langle 2,8,4,9\rangle$	$\langle 0,11,4,6\rangle$	$\langle 4,8,5,11\rangle$	$\langle 8,10,1,2\rangle$
$\langle 0,6,2,5\rangle$	$\langle 2,9,0,1\rangle$	$\langle 1,3,9,11\rangle$	$\langle 5,10,6,7\rangle$	$\langle 8,11,0,7\rangle$
$\langle 1,5,2,4\rangle$	$\langle 3,6,4,7\rangle$	$\langle 1,6,0,10\rangle$	$\langle 6,10,8,9\rangle$	$\langle 0,2,10,11\rangle$
$\langle 1,8,3,6\rangle$	$\langle 3,7,0,2\rangle$	$\langle 2,10,3,5\rangle$	$\langle 6,7,1,11\rangle$	$\langle 5,11,1,10\rangle$
$\langle 1,9,7,8\rangle$	$\langle 3,9,5,6\rangle$	$\langle 3,4,8,10\rangle$	$\langle 7,11,5,9\rangle$	$\langle 9,10,4,11\rangle$

证明. 当 $u\in[5,9]$ 时，令 $X_u=\mathbb{Z}_{8u}\cup\{\infty_0,\ldots,\infty_9\}$，并令 $\mathcal{H}_u=\mathcal{G}_{u,8}\cup\{\{\infty_0,\ldots,\infty_9\}\}$。假设 $\mathcal{C}_u$ 是由文献[84] 中表 VI 内的向量按照步长为 2 的拟循环移位展开得到的集合，那么 $(X_u,\mathcal{H}_u,\mathcal{C}_u)$ 就是所需的可分组码。

当 $v\in[5,9]$ 时，令 $X_v=\mathbb{Z}_{8v}\cup\{\infty_0,\ldots,\infty_{13}\}$，并令 $\mathcal{H}_v=\mathcal{G}_{v,8}\cup\{\{\infty_0,\ldots,\infty_{13}\}\}$。假设 $\mathcal{C}_v$ 是由文献[84] 中表 VII 的向量按照步长为 2 的拟循环移位展开得到的集合，那么 $(X_v,\mathcal{H}_v,\mathcal{C}_v)$ 就是所需的可分组码。 □

性质 5.64：*对于每个 $u\in[4,7]$，都存在大小为 $36u(u-1)$、型为 12^u 的 $[2,2]$-GDC(5)。*

证明. 对于每个 $4\le u\le 7$，利用横截设计 TD(4,3) 将型为 4^u 的 $[2,2]$-GDC(5) 进行权重为 3 的膨胀就可以得到结果，其中所需的可分组码由性质 5.59 保障。 □

5.4.2　长度 $n\not\equiv 3\pmod 4$ 的情形

性质 5.65：*对于每个 $n\in\{12,13,14,16,17,18,20,21,22\}$，都存在含有 $U(n,5,[2,2])$ 个码字的最优 $(n,5,[2,2])_3$-码。*

证明. 最优 $(12,5,[2,2])_3$-码的 30 个码字见表 5.3。

对于 $n\in\{13,14,17,18,21,22\}$，最优 $(n,5,[2,2])_3$-码的 $U(n,5,[2,2])$ 个码字由以下向量的循环移位组成：

$n=13$：　$\langle 0,2,7,10\rangle$、$\langle 0,1,3,12\rangle$ 和 $\langle 0,3,4,9\rangle$；

$n=14$：　$\langle 0,5,6,8\rangle$、$\langle 0,3,2,12\rangle$ 和 $\langle 0,1,5,11\rangle$；

$n=17$：　$\langle 0,9,6,8\rangle$、$\langle 0,14,7,15\rangle$、$\langle 0,10,2,13\rangle$ 和 $\langle 0,1,5,12\rangle$；

$n=18$：　$\langle 0,1,2,4\rangle$、$\langle 0,4,14,17\rangle$、$\langle 0,5,11,12\rangle$ 和 $\langle 0,8,5,16\rangle$；

$n=21$：　$\langle 0,12,13,15\rangle$、$\langle 0,11,10,18\rangle$、$\langle 0,2,11,14\rangle$、$\langle 0,20,5,16\rangle$ 和 $\langle 0,6,4,8\rangle$；

$n=22$： $\langle 0,1,2,4\rangle$、$\langle 0,2,7,8\rangle$、$\langle 0,4,14,19\rangle$、$\langle 0,3,12,20\rangle$ 和 $\langle 0,5,18,21\rangle$。

对于 $n=16$ 和 20，最优 $(n,5,[2,2])_3$-码的 $U(n,5,[2,2])$ 个码字由以下向量按步长为 2 的拟循环移位组成：

$n=16$：

$$\begin{array}{cccc}\langle 0,2,4,9\rangle & \langle 1,8,2,14\rangle & \langle 1,7,10,11\rangle & \langle 0,15,13,14\rangle\\ \langle 1,13,3,8\rangle & \langle 1,10,6,13\rangle & \langle 0,10,11,15\rangle & \end{array}$$

$n=20$：

$$\begin{array}{cccc}\langle 0,4,1,3\rangle & \langle 1,8,6,17\rangle & \langle 0,15,8,14\rangle & \langle 0,12,5,16\rangle\\ \langle 0,19,2,6\rangle & \langle 0,1,12,15\rangle & \langle 1,17,5,18\rangle & \langle 1,7,13,16\rangle\\ \langle 0,9,7,11\rangle & & & \end{array}$$

□

性质 5.66：对于每个正整数，都存在长度为 $n=4t$、$4t+1$ 和 $4t+2$ 的最优 $(n,5,[2,2])_3$-码。

证明. 由定理 5.16，对于所有 $t\geq 23$，都存在一个 PBD$(t+1,\{4,5,6\})$。删去其中一个点得到组大小为 3、4 或 5 的 t 阶 $\{4,5,6\}$-GDD。应用基本构造进行 4 加权，得到型为 4^4、4^5 和 4^6 的 $[2,2]$-GDC(5)，其组大小为 12、16 或 20，我们将其记为 $\mathcal{C}^\star$。

向 $\mathcal{C}^\star$ 的组中填入长度为 12、16 和 20 的最优常重复合码，就可以得到关于 $n=4t$ 的结果，其中 $t\geq 23$。

在 $\mathcal{C}^\star$ 中添加一个无穷点，并向每个组和这个无穷点填入长度为 13、17 和 21 的最优码，就得到关于长度 $n=4t+1$ 的结果。

在 $\mathcal{C}^\star$ 中添加两个无穷点，并向每个组和这两个无穷点填入型为 2^7、2^9 和 2^{11} 的 $[2,2]$-GDC(5)。通过计算得知，这个可分组码中恰好含有 $U(4t+2,5,[2,2])$ 个码字，因此它们就是长度为 $4t+2$ 的最优常重复合码。 □

性质 5.67：对于每个 $t\in\{8,10,12\}\cup[14,16]\cup[18,22]$，都存在长度为 $n=4t$ 和 $4t+1$ 的最优 $(n,5,[2,2])_3$-码。

证明. 对于 $t=8,10$，选取型为 8^4 和 8^5 的 $[2,2]$-GDC(5)。向其中添加 x 个无穷点，$x=0,1$，并向每个组和这些无穷点中填入最优码，就可以得到长度分别为 $32+x$ 和 $40+x$ 的最优常重复合码。

当 $t=12,14$ 时，由定理 5.7 知，存在型为 3^4 和 2^7 的 $\{4\}$-GDD。对其应用基本构造，选择权重为 4，就得到了型为 12^4 和 8^7 的 $[2,2]$-GDC(5)。然后向其中添加 x 个无穷点，$x=0,1$，并向每个组和这些无穷点中填入最优码，就可以得到长度分别为 $48+x$ 和 $56+x$ 的最优常重复合码。

对于 $t=15$，将权为 4 的基本构造应用到型为 3^5 的 $\{4\}$-GDD。然后向其中添加 x 个无穷点，$x=0,1$，并向每个组和这些无穷点中填入最优码，就可以得到长度为 $60+x$ 的最优常重复合码。

当 $t=16,18,19,20$ 时，截短 TD$(5,4)$ 得到型为 4^4y^1 的 $\{4,5\}$-GDD，其中 $y=0,2,3,4$。将权为 4 的基本构造应用到这个可分组设计，然后向其中添加 x 个无穷点，$x=0,1$。再向每个组和这些无穷点中填入最优码，就可以得到长度为 $4t+x$ 的最优常重复合码。

对于 $t=21$，将权为 4 的基本构造应用到型为 3^7 的 $\{4\}$-GDD。然后向其中添加 x 个无穷点，$x=0,1$，并向每个组和这些无穷点中填入最优码，就可以得到最优 $(84+x,5,[2,2])_3$-码。

当 $t=22$ 时，截短 TD$(5,5)$ 得到型为 5^42^1 的 $\{4,5\}$-GDD。将权为 4 的基本构造应用到这个可分组设计。然后向其中添加 x 个无穷点，$x=0,1$，并向每个组和这些无穷点中填入最优码，就可以得到长度为 $88+x$ 的最优常重复合码。 □

性质 5.68：*对于每个 $t\in\{12,15,16\}\cup[18,22]$，都存在大小为 $U(4t+2,5,[2,2])$ 的最优 $(4t+2,5,[2,2])_3$-码。*

证明. 当 $t\in\{12,15,18,21\}$ 时，向型为 12^u（$u\in[4,7]$）的 $[2,2]$-GDC(5) 中添加两个无穷点，然后向每个组和这些无穷点中填入型为 2^7 的辅助码。我们得到一个型为 2^{6u+1} 的可分组码，由于其大小等于 $U(4*(3u)+2,5,[2,2])$，因此是最优常重复合码。

当 $t=16,19,20$ 时，截短 TD$(5,4)$ 得到型为 4^4x^1（$x=0,3,4$）的 $\{4,5\}$-GDD。应用权重为 4 的基本构造，然后添加两个无穷点，并向每个组和这些无穷点中填入型为 2^7 和 2^9 的辅助码。我们就得到了要求的结果。

最后当 $t=22$ 时，对型为 6^5 的 $[2,2]$-GDC(5) 进行权重为 3 的膨胀，然后向每个组内填入长度为 18 的最优码就得到了长度为 90 的最优常重复合码。 □

性质 5.69:对于参数

1. $n=4t,4t+1$ 且 $t\in\{6,7,9,11,13,17\}$;和

2. $n=4t+2$ 且 $t\in[6,11]\cup\{13,14,17\}$,

等式 $A_3(n,5,[2,2])=U(n,5,[2,2])$ 均成立。

证明. 对于每个 $t\in\{6,7,9,11,13,17\}$,最优 $(4t,5,[2,2])_3$-码的码字由第 5.5 节中表 5.8 内的向量按步长为 2 的拟循环移位组成。

对于每个 $t\in\{6,7,9,11,13,17\}$,最优 $(4t+1,5,[2,2])_3$-码的码字由第 5.5 节中表 5.9 内的向量的循环移位组成。

对于每个 $t\in[6,11]\cup\{13,14,17\}$,最优 $(4t+2,5,[2,2])_3$-码的码字由第 5.5 节中表 5.10 内的向量的循环移位组成。 □

综上,我们有下面的结论。

定理 5.70:对于所有满足 $n\geq 12$ 和 $n\not\equiv 3\pmod 4$ 的长度 n,等式 $A_3(n,5,[2,2])=U(n,5,[2,2])$ 均成立。

5.4.3 长度 $n\equiv 3\pmod 4$ 的情形

在叙述下面的引理之前,我们需要引入残留图的概念。令 $G=(V_n,E)$ 是一个 n 阶有向完全图,其中顶点集为 $V_n=\{1,2,\ldots,n\}$,边集为 $E=\{i\to j:i\neq j\}$。给定一个 $(n,5,[2,2])_3$-码 $\mathcal{C}$,对于其中每个码字 $\mathtt{v}=\langle a,b,c,d\rangle$,我们将其与 G 的一个子图 $G(\mathtt{v})=(V_n,E(\mathtt{v}))$ 相对应,其中边集为 $E(\mathtt{v})=\{a\to c,a\to d,b\to c,b\to d\}$。容易验证,对于任意两个不同码字 $\mathtt{u}\neq\mathtt{v}$,均有 $E(\mathtt{u})\cap E(\mathtt{v})=\emptyset$,否则 $d_H(\mathtt{u},\mathtt{v})<5$ 违背了距离条件。我们将 G 的子图 $G(\mathcal{C})=(V_n,E(\mathcal{C}))$ 称为码 $\mathcal{C}$ 的残留图(Leave Graph),其中 $E(\mathcal{C})=E\backslash\bigcup_{\mathtt{v}\in\mathcal{C}}E(\mathtt{v})$。

引理 5.71:对于所有长度 $n\equiv 3\pmod 4$,均有 $A_3(n,5,[2,2])\leq U(n,5,[2,2])-1$。

证明. 记 $n=4t+3$。假设存在一个 $(4t+3,5,[2,2])_3$-码 $\mathcal{C}$,含有 $U:=U(4t+3,5,[2,2])=4t^2+5t+1$ 个码字。那么它的残留图 $G(\mathcal{C})=(V_{4t+3},E(\mathcal{C}))$ 中含有的边

数目为：

$$\begin{aligned} |E(\mathcal{C})| &= |E| - \left|\bigcup_{\mathrm{v}\in\mathcal{C}} E(\mathrm{v})\right| \\ &= (4t+3)(4t+2) - 4U \\ &= 2。 \end{aligned}$$

由于 $G(\mathcal{C})$ 的补图中每个顶点的出度和入度都为偶数，所有残留图上唯一可能的边排布形式只能是从某个顶点指向另一个顶点的具有两条重复的有向边。但这和残留图应该是一个简单有向图的事实产生了矛盾。因此 Johnson 界不可能达到。 □

性质 5.72：对于每个 $t \in \{0,1,2\}$，都存在最优 $(4t+11,5,[2,2])_3$-码，其大小为 $U(4t+11,5,[2,2])-1$。

证明. 见第 5.5 节中的表 5.11。 □

性质 5.73：对于所有 $t \geq 96$，都存在大小为 $U(4t+11,5,[2,2])-1$ 的最优 $(4t+11,5,[2,2])_3$-码。

证明. 由定理 5.9 知，对于所有 $u \geq 12$，都存在横截设计 TD$(6,2u)$。截短最后两个组，得到型为 $(2u)^4(2x)^15^1$ 或 $(2u)^4(2x)^17^1$ 的 $\{4,5,6\}$-GDD，其中 $x \in [0,u]$。应用基本构造法，其中前五个组的权重为 4，最后一个组的权重为 2，得到型为 $(8u)^4(8x)^110^1$ 或 $(8u)^4(8x)^114^1$ 的 $[2,2]$-GDC(5)。然后添加一个无穷点，并向每个组和这个无穷点中填入最优码，就可以生成长度为 $4t+11$ 的最优常重复合码，其中 $t \in [8u, 10u+1]$。当 u 从 12 增大时，区间 $[8u,10u+1]$ 将会产生重叠，并覆盖全部不小于 96 的整数。 □

性质 5.74：对于每个整数 $10 \leq t \leq 95$，都存在最优 $(4t+11,5,[2,2])_3$-码，含 $U(4t+11,5,[2,2])-1$ 个码字。

证明. 当 $10 \leq t \leq 19$ 时，由性质 5.63，对于每个 $u \in [5,9]$，存在型为 8^u10^1 和 8^u14^1 的 $[2,2]$-GDC(5)。添加一个无穷点并向每个组和这个点中填入最优的常重复合码，就得到了最优 $(4t+11,5,[2,2])_3$-码，其中 $10 \leq t \leq 19$。

对于 $20 \leq t \leq 27$，截短 TD$(6,5)$ 的最后两个组生成一个型为 $5^4x^1y^1$ 的 $\{4,5,6\}$-GDD，其中 $x \in \{0,2,3,4,5\}$，而 $y \in [3,5]$。对其应用基本构造法，其中选定最后一个

组中的某个点权重为 2，而其他所有点权重为 4，得到型为 $20^4(4x)^1 10^1$、$20^4(4x)^1 14^1$ 和 $20^4(4x)^1 18^1$ 的可分组码。添加一个无穷点，并向每个组和这一无穷点中填入长度为 $4(20+x)+11$、$4(21+x)+11$ 和 $4(22+x)+11$ 的最优码即得到结论。

当 $28 \le t \le 97$ 时，将同样的方法应用到横截设计 $\mathrm{TD}(6,u)$ 上，$u \in \{7,9,11,19\}$，就可以得到所需的结论。 □

性质 5.75：对于每个 $3 \le t \le 9$，都存在长度为 $n = 4t+11$ 的最优 $(n,5,[2,2])_3$-码，其大小为 $U(n,5,[2,2])-1$。

证明. 最优 $(23,5,[2,2])_3$-码的 125 个码字由以下向量按置换

$$(0,1,\ldots,4)(5,6,\ldots,9)(10,11,\ldots,14)(15,16,\ldots,19)(20)(21)(22)$$

作用生成：

$\langle 1,8,9,14\rangle$ $\langle 0,17,20,6\rangle$ $\langle 19,3,7,18\rangle$ $\langle 11,1,15,10\rangle$ $\langle 3,10,16,15\rangle$
$\langle 10,5,0,3\rangle$ $\langle 12,13,8,6\rangle$ $\langle 20,9,8,16\rangle$ $\langle 12,19,1,15\rangle$ $\langle 5,11,18,22\rangle$
$\langle 19,4,0,6\rangle$ $\langle 13,0,11,4\rangle$ $\langle 3,16,13,0\rangle$ $\langle 12,22,9,13\rangle$ $\langle 5,12,20,14\rangle$
$\langle 21,6,0,9\rangle$ $\langle 14,3,21,1\rangle$ $\langle 7,2,14,18\rangle$ $\langle 20,18,3,12\rangle$ $\langle 7,15,21,10\rangle$
$\langle 5,9,19,1\rangle$ $\langle 18,4,22,9\rangle$ $\langle 8,15,5,13\rangle$ $\langle 22,17,0,15\rangle$ $\langle 21,18,15,14\rangle$

最优 $(27,5,[2,2])_3$-码的 174 个码字由以下向量按步长为 9 的拟循环移位生成：

$\langle 5,6,8,9\rangle$ $\langle 0,2,14,15\rangle$ $\langle 5,25,2,10\rangle$ $\langle 1,18,17,21\rangle$ $\langle 5,20,12,15\rangle$
$\langle 0,6,4,11\rangle$ $\langle 0,23,8,21\rangle$ $\langle 6,10,2,18\rangle$ $\langle 1,25,11,18\rangle$ $\langle 5,23,18,25\rangle$
$\langle 1,2,6,23\rangle$ $\langle 0,26,7,16\rangle$ $\langle 6,22,7,17\rangle$ $\langle 2,12,10,17\rangle$ $\langle 6,18,13,24\rangle$
$\langle 2,16,0,8\rangle$ $\langle 1,14,2,13\rangle$ $\langle 7,16,3,22\rangle$ $\langle 2,19,22,26\rangle$ $\langle 6,20,10,16\rangle$
$\langle 2,23,5,7\rangle$ $\langle 1,19,3,25\rangle$ $\langle 8,11,0,10\rangle$ $\langle 2,22,16,20\rangle$ $\langle 6,23,15,19\rangle$
$\langle 2,3,9,12\rangle$ $\langle 3,13,2,21\rangle$ $\langle 8,21,9,13\rangle$ $\langle 2,24,11,13\rangle$ $\langle 6,25,14,26\rangle$
$\langle 4,25,7,8\rangle$ $\langle 3,23,4,13\rangle$ $\langle 8,23,2,24\rangle$ $\langle 3,12,14,20\rangle$ $\langle 8,18,11,20\rangle$
$\langle 6,14,1,3\rangle$ $\langle 3,25,0,15\rangle$ $\langle 0,11,12,13\rangle$ $\langle 3,18,16,19\rangle$ $\langle 8,24,12,18\rangle$
$\langle 6,7,5,25\rangle$ $\langle 3,5,23,26\rangle$ $\langle 0,13,10,19\rangle$ $\langle 3,22,10,24\rangle$ $\langle 8,25,19,22\rangle$
$\langle 7,9,6,14\rangle$ $\langle 4,22,0,23\rangle$ $\langle 0,19,17,23\rangle$ $\langle 3,26,17,25\rangle$ $\langle 8,26,14,21\rangle$
$\langle 8,13,4,6\rangle$ $\langle 4,24,3,14\rangle$ $\langle 1,12,15,16\rangle$ $\langle 4,16,11,21\rangle$
$\langle 8,19,1,5\rangle$ $\langle 4,8,15,17\rangle$ $\langle 1,16,19,24\rangle$ $\langle 4,19,13,18\rangle$

最优 $(31,5,[2,2])_3$-码的 231 个码字由以下向量按置换

$$(0,1,\ldots,6)(7,8,\ldots,13)(14,15,\ldots,20)(21,22,\ldots,27)(28)(29)(30)$$

作用生成：

$\langle 1,3,9,8\rangle$	$\langle 2,8,28,22\rangle$	$\langle 15,18,3,16\rangle$	$\langle 2,16,26,21\rangle$	$\langle 14,28,11,23\rangle$
$\langle 2,3,4,6\rangle$	$\langle 22,21,7,0\rangle$	$\langle 15,29,23,6\rangle$	$\langle 22,24,27,4\rangle$	$\langle 15,27,10,29\rangle$
$\langle 2,9,11,0\rangle$	$\langle 8,11,12,3\rangle$	$\langle 16,23,6,28\rangle$	$\langle 22,25,17,6\rangle$	$\langle 16,26,15,27\rangle$
$\langle 8,7,1,18\rangle$	$\langle 8,30,4,23\rangle$	$\langle 16,24,18,8\rangle$	$\langle 22,29,20,9\rangle$	$\langle 23,13,11,22\rangle$
$\langle 1,28,14,0\rangle$	$\langle 9,17,14,6\rangle$	$\langle 2,10,18,13\rangle$	$\langle 4,21,30,25\rangle$	$\langle 23,30,12,20\rangle$
$\langle 1,4,16,15\rangle$	$\langle 15,14,1,21\rangle$	$\langle 2,12,19,29\rangle$	$\langle 8,24,26,17\rangle$	
$\langle 2,7,27,24\rangle$	$\langle 15,17,11,8\rangle$	$\langle 2,13,25,12\rangle$	$\langle 9,19,30,15\rangle$	

对于每个 $n \in \{35,39,43,47\}$，最优 $(n,5,[2,2])_3$-码的 $U(n,5,[2,2])-1$ 个码字由两部分组成。第一部分是在点集 $\{n-11,n-10,\ldots,n-1\}$ 上的一个最优 $(11,5,[2,2])$-码。第二部分由第 5.5 节中表 5.12 内的向量分别按以下置换作用生成：

- 当 $n=35$ 时，置换为 $(0,1,\ldots,5)$ $(6,7,\ldots,11)$ $(12,13,\ldots,17)$ $(18,19,\ldots,23)$ $(24,25,\ldots,29)$ $(30,31)$ $(32,33)$ (34)；
- 当 $n \in \{39,43,47\}$ 时，置换为 $(0,1,\ldots,s-1)$ $(s,\ldots,2s-1)$ $(2s,\ldots,3s-1)$ $(3s,\ldots,4s-1)$ $(4s)(4s+1)\cdots(4s+10)$，其中 $s=(n-11)/4$。

□

综合上述结论，我们证明了下面的定理。

定理 5.76：对于每个正整数 t，都存在最优 $(4t+11,5,[2,2])_3$-码，其含有 $U(4t+11,5,[2,2])-1$ 个码字。

5.5 表格附录

表 5.4 6^6 型 $[3,1]$-GDC(5) 中的 180 个码字

$\langle 0,1,8,3\rangle$	$\langle 4,7,21,18\rangle$	$\langle 11,16,18,2\rangle$	$\langle 6,20,23,21\rangle$	$\langle 13,27,29,22\rangle$
$\langle 0,4,35,2\rangle$	$\langle 5,12,33,8\rangle$	$\langle 11,19,27,0\rangle$	$\langle 6,21,34,13\rangle$	$\langle 13,34,35,26\rangle$
$\langle 0,9,23,7\rangle$	$\langle 5,7,18,10\rangle$	$\langle 11,32,33,4\rangle$	$\langle 6,33,35,10\rangle$	$\langle 14,15,25,18\rangle$
$\langle 1,3,35,6\rangle$	$\langle 5,8,16,24\rangle$	$\langle 12,15,35,4\rangle$	$\langle 7,10,14,33\rangle$	$\langle 14,16,27,13\rangle$
$\langle 1,4,27,8\rangle$	$\langle 5,9,19,22\rangle$	$\langle 13,26,30,3\rangle$	$\langle 7,11,28,27\rangle$	$\langle 14,17,30,19\rangle$
$\langle 1,5,6,14\rangle$	$\langle 6,10,15,8\rangle$	$\langle 14,21,31,6\rangle$	$\langle 7,12,26,15\rangle$	$\langle 14,22,23,25\rangle$
$\langle 2,7,29,4\rangle$	$\langle 6,13,22,2\rangle$	$\langle 15,19,32,5\rangle$	$\langle 7,15,23,20\rangle$	$\langle 14,24,35,27\rangle$
$\langle 3,4,32,0\rangle$	$\langle 6,16,19,3\rangle$	$\langle 16,20,33,1\rangle$	$\langle 7,22,33,35\rangle$	$\langle 14,28,33,31\rangle$
$\langle 3,5,25,2\rangle$	$\langle 6,25,29,9\rangle$	$\langle 16,21,30,7\rangle$	$\langle 8,10,13,27\rangle$	$\langle 15,17,20,22\rangle$

$\langle 3,7,24,8\rangle$	$\langle 6,28,32,7\rangle$	$\langle 17,18,28,8\rangle$	$\langle 8,11,25,21\rangle$	$\langle 15,29,31,14\rangle$
$\langle 4,5,14,3\rangle$	$\langle 6,8,17,31\rangle$	$\langle 17,24,25,3\rangle$	$\langle 8,12,27,29\rangle$	$\langle 15,30,34,17\rangle$
$\langle 4,8,9,17\rangle$	$\langle 7,16,17,9\rangle$	$\langle 2,12,21,11\rangle$	$\langle 8,15,24,35\rangle$	$\langle 16,23,32,18\rangle$
$\langle 6,7,27,5\rangle$	$\langle 7,20,34,3\rangle$	$\langle 2,13,33,28\rangle$	$\langle 8,21,35,34\rangle$	$\langle 16,24,26,31\rangle$
$\langle 6,9,14,4\rangle$	$\langle 7,8,30,28\rangle$	$\langle 2,15,18,13\rangle$	$\langle 8,31,33,30\rangle$	$\langle 16,31,35,12\rangle$
$\langle 0,13,20,4\rangle$	$\langle 7,9,35,14\rangle$	$\langle 2,16,25,33\rangle$	$\langle 9,10,25,30\rangle$	$\langle 17,22,32,27\rangle$
$\langle 0,2,34,15\rangle$	$\langle 8,18,34,7\rangle$	$\langle 2,24,28,25\rangle$	$\langle 9,12,16,20\rangle$	$\langle 17,26,31,34\rangle$
$\langle 0,3,17,26\rangle$	$\langle 8,19,23,6\rangle$	$\langle 2,27,31,17\rangle$	$\langle 9,13,18,35\rangle$	$\langle 17,27,34,18\rangle$
$\langle 0,5,27,28\rangle$	$\langle 8,22,29,1\rangle$	$\langle 22,24,27,7\rangle$	$\langle 9,20,22,23\rangle$	$\langle 18,19,21,14\rangle$
$\langle 0,7,32,34\rangle$	$\langle 9,24,31,2\rangle$	$\langle 23,27,30,1\rangle$	$\langle 9,29,34,19\rangle$	$\langle 18,20,31,29\rangle$
$\langle 1,2,30,10\rangle$	$\langle 9,26,28,5\rangle$	$\langle 25,26,27,6\rangle$	$\langle 9,30,32,13\rangle$	$\langle 18,22,25,26\rangle$
$\langle 1,23,24,4\rangle$	$\langle 0,10,26,23\rangle$	$\langle 3,11,30,14\rangle$	$\langle 10,17,19,32\rangle$	$\langle 18,26,35,21\rangle$
$\langle 1,33,34,5\rangle$	$\langle 0,11,31,33\rangle$	$\langle 3,12,22,19\rangle$	$\langle 10,20,27,25\rangle$	$\langle 18,27,32,11\rangle$
$\langle 1,9,11,18\rangle$	$\langle 0,14,19,35\rangle$	$\langle 3,13,16,17\rangle$	$\langle 10,21,23,31\rangle$	$\langle 18,29,33,34\rangle$
$\langle 2,10,35,9\rangle$	$\langle 0,15,28,19\rangle$	$\langle 3,19,20,18\rangle$	$\langle 10,24,33,17\rangle$	$\langle 19,22,35,15\rangle$
$\langle 2,3,23,34\rangle$	$\langle 0,16,29,21\rangle$	$\langle 3,31,34,11\rangle$	$\langle 10,31,32,15\rangle$	$\langle 19,24,34,33\rangle$
$\langle 2,4,19,30\rangle$	$\langle 0,21,22,20\rangle$	$\langle 4,12,13,32\rangle$	$\langle 11,13,14,15\rangle$	$\langle 19,26,29,27\rangle$
$\langle 2,5,22,18\rangle$	$\langle 0,25,33,14\rangle$	$\langle 4,15,26,11\rangle$	$\langle 11,21,24,28\rangle$	$\langle 19,30,33,26\rangle$
$\langle 2,6,11,19\rangle$	$\langle 1,10,29,26\rangle$	$\langle 4,18,23,15\rangle$	$\langle 11,26,34,25\rangle$	$\langle 20,21,29,12\rangle$
$\langle 2,9,17,12\rangle$	$\langle 1,12,17,33\rangle$	$\langle 4,24,29,20\rangle$	$\langle 12,14,34,23\rangle$	$\langle 20,30,35,31\rangle$
$\langle 3,10,18,1\rangle$	$\langle 1,14,18,28\rangle$	$\langle 4,25,30,23\rangle$	$\langle 12,19,28,17\rangle$	$\langle 21,25,28,32\rangle$
$\langle 3,14,29,7\rangle$	$\langle 1,15,16,30\rangle$	$\langle 5,10,30,20\rangle$	$\langle 12,20,25,34\rangle$	$\langle 22,30,31,32\rangle$
$\langle 3,6,26,28\rangle$	$\langle 1,20,28,35\rangle$	$\langle 5,13,15,12\rangle$	$\langle 12,23,31,28\rangle$	$\langle 23,25,34,27\rangle$
$\langle 3,8,28,13\rangle$	$\langle 1,21,32,29\rangle$	$\langle 5,20,24,13\rangle$	$\langle 12,29,32,25\rangle$	$\langle 23,26,33,16\rangle$
$\langle 4,11,20,7\rangle$	$\langle 1,22,26,12\rangle$	$\langle 5,21,26,19\rangle$	$\langle 13,17,21,10\rangle$	$\langle 25,32,35,22\rangle$
$\langle 4,17,33,6\rangle$	$\langle 10,11,12,3\rangle$	$\langle 5,28,31,21\rangle$	$\langle 13,23,28,24\rangle$	$\langle 27,28,35,30\rangle$
$\langle 4,6,31,35\rangle$	$\langle 11,15,22,6\rangle$	$\langle 5,32,34,31\rangle$	$\langle 13,24,32,16\rangle$	$\langle 28,29,30,33\rangle$

表 5.5　6^u2^1 型 $[3,1]$-GDC(5) 的基础码字，$u\in[4,7]$

u	基础码字				
4	$\langle 0,18,7,9\rangle$	$\langle 3,0,10,5\rangle$	$\langle 2,12,23,5\rangle$	$\langle 5,20,11,22\rangle$	$\langle \infty_1,1,15,0\rangle$
	$\langle 1,8,19,2\rangle$	$\langle 3,2,16,1\rangle$	$\langle 3,4,17,14\rangle$	$\langle \infty_0,0,9,3\rangle$	$\langle \infty_0,4,19,17\rangle$
	$\langle 2,1,0,11\rangle$	$\langle 3,5,22,4\rangle$	$\langle 4,22,1,15\rangle$	$\langle \infty_0,2,5,8\rangle$	$\langle 1,16,11,18\rangle$
	$\langle 2,8,21,3\rangle$	$\langle 3,9,12,2\rangle$	$\langle 5,12,7,18\rangle$	$\langle \infty_1,2,4,7\rangle$	$\langle \infty_1,0,5,23\rangle$
	$\langle 2,9,7,16\rangle$	$\langle 4,6,5,19\rangle$			
5	$\langle 0,3,4,1\rangle$	$\langle 0,18,29,7\rangle$	$\langle 3,17,10,4\rangle$	$\langle 3,11,22,25\rangle$	$\langle \infty_0,5,13,1\rangle$
	$\langle 1,4,2,10\rangle$	$\langle 1,28,0,27\rangle$	$\langle 3,25,9,26\rangle$	$\langle 3,20,21,17\rangle$	$\langle \infty_1,0,14,2\rangle$
	$\langle 1,7,3,24\rangle$	$\langle 2,10,26,8\rangle$	$\langle 5,12,3,11\rangle$	$\langle 3,24,26,12\rangle$	$\langle \infty_1,1,22,0\rangle$
	$\langle 0,13,6,17\rangle$	$\langle 2,28,19,0\rangle$	$\langle 5,22,4,18\rangle$	$\langle 5,23,14,17\rangle$	$\langle \infty_1,3,29,10\rangle$
	$\langle 0,16,22,9\rangle$	$\langle 2,29,5,28\rangle$	$\langle 1,17,13,15\rangle$	$\langle \infty_0,2,6,9\rangle$	$\langle \infty_0,3,16,2\rangle$
	$\langle 0,17,19,8\rangle$	$\langle 3,14,6,27\rangle$	$\langle 2,13,20,21\rangle$		

6	$\langle 0,9,8,13\rangle$	$\langle 1,8,30,33\rangle$	$\langle 5,9,25,28\rangle$	$\langle 2,35,34,21\rangle$	$\langle \infty_1,1,2,6\rangle$
	$\langle 3,6,8,11\rangle$	$\langle 1,9,16,26\rangle$	$\langle 0,19,22,27\rangle$	$\langle 3,18,28,26\rangle$	$\langle \infty_0,3,7,35\rangle$
	$\langle 4,0,3,19\rangle$	$\langle 2,15,10,0\rangle$	$\langle 0,34,23,14\rangle$	$\langle 4,17,12,32\rangle$	$\langle \infty_0,5,22,7\rangle$
	$\langle 0,26,1,10\rangle$	$\langle 2,27,4,17\rangle$	$\langle 1,11,32,28\rangle$	$\langle 4,24,13,33\rangle$	$\langle \infty_1,0,11,7\rangle$
	$\langle 0,31,29,2\rangle$	$\langle 2,29,9,24\rangle$	$\langle 1,15,23,12\rangle$	$\langle 4,26,35,18\rangle$	$\langle \infty_0,0,20,15\rangle$
	$\langle 0,35,32,4\rangle$	$\langle 3,24,1,14\rangle$	$\langle 2,21,23,16\rangle$	$\langle 5,13,34,15\rangle$	$\langle \infty_1,3,22,23\rangle$
	$\langle 1,20,10,5\rangle$	$\langle 5,1,27,18\rangle$	$\langle 2,22,25,18\rangle$	$\langle 5,24,15,16\rangle$	
7	$\langle 0,2,1,6\rangle$	$\langle 0,38,19,2\rangle$	$\langle 4,15,0,27\rangle$	$\langle 2,20,17,32\rangle$	$\langle 5,23,22,41\rangle$
	$\langle 0,16,3,8\rangle$	$\langle 0,5,39,36\rangle$	$\langle 4,35,8,17\rangle$	$\langle 2,36,27,19\rangle$	$\langle 5,28,31,30\rangle$
	$\langle 2,5,24,1\rangle$	$\langle 1,14,16,4\rangle$	$\langle 5,30,36,3\rangle$	$\langle 3,15,40,14\rangle$	$\langle \infty_1,1,9,38\rangle$
	$\langle 3,32,2,5\rangle$	$\langle 1,41,35,3\rangle$	$\langle 0,26,31,37\rangle$	$\langle 3,19,29,28\rangle$	$\langle \infty_0,0,32,26\rangle$
	$\langle 3,5,1,39\rangle$	$\langle 2,33,39,7\rangle$	$\langle 0,27,18,17\rangle$	$\langle 4,20,14,15\rangle$	$\langle \infty_0,1,33,17\rangle$
	$\langle 4,26,3,9\rangle$	$\langle 3,23,27,4\rangle$	$\langle 0,40,13,39\rangle$	$\langle 4,22,10,19\rangle$	$\langle \infty_0,4,41,36\rangle$
	$\langle 5,6,35,2\rangle$	$\langle 3,7,25,26\rangle$	$\langle 1,13,18,21\rangle$	$\langle 4,27,17,30\rangle$	$\langle \infty_1,0,34,12\rangle$
	$\langle 0,30,10,4\rangle$	$\langle 4,1,37,41\rangle$	$\langle 2,10,19,41\rangle$	$\langle 5,14,25,37\rangle$	$\langle \infty_1,2,11,22\rangle$

表 5.6　6^v4^1 型 $[3,1]$-GDC(5) 的基础码字，$v\in[4,9]$

v	基础码字				
4	$\langle 4,2,5,7\rangle$	$\langle 0,5,23,14\rangle$	$\langle 0,13,15,10\rangle$	$\langle \infty_1,1,20,3\rangle$	$\langle \infty_3,2,16,15\rangle$
	$\langle 5,3,8,6\rangle$	$\langle 1,22,11,8\rangle$	$\langle 2,12,13,23\rangle$	$\langle \infty_2,0,7,21\rangle$	$\langle \infty_3,3,17,16\rangle$
	$\langle 2,8,17,3\rangle$	$\langle 2,19,1,20\rangle$	$\langle \infty_0,2,0,5\rangle$	$\langle \infty_2,2,3,12\rangle$	$\langle 0,11,18,17\rangle$
	$\langle 3,20,9,2\rangle$	$\langle 3,4,13,18\rangle$	$\langle \infty_1,0,9,6\rangle$	$\langle \infty_3,0,19,1\rangle$	$\langle \infty_0,5,7,18\rangle$
	$\langle 3,6,16,9\rangle$	$\langle 4,10,1,23\rangle$	$\langle \infty_0,4,21,2\rangle$	$\langle \infty_1,5,10,19\rangle$	$\langle \infty_2,4,11,22\rangle$
	$\langle 4,6,9,19\rangle$				
5	$\langle 1,7,9,3\rangle$	$\langle 5,4,8,12\rangle$	$\langle 2,18,24,16\rangle$	$\langle \infty_0,0,26,9\rangle$	$\langle \infty_1,5,18,21\rangle$
	$\langle 3,9,0,2\rangle$	$\langle 1,12,24,0\rangle$	$\langle 2,19,15,28\rangle$	$\langle \infty_1,3,16,4\rangle$	$\langle \infty_2,3,22,25\rangle$
	$\langle 1,4,28,2\rangle$	$\langle 1,18,19,7\rangle$	$\langle 2,23,11,19\rangle$	$\langle \infty_2,2,0,24\rangle$	$\langle \infty_3,0,29,11\rangle$
	$\langle 2,20,1,9\rangle$	$\langle 3,5,12,24\rangle$	$\langle 3,14,15,17\rangle$	$\langle \infty_3,2,16,8\rangle$	$\langle \infty_3,1,15,24\rangle$
	$\langle 2,9,5,26\rangle$	$\langle 4,26,2,25\rangle$	$\langle 4,13,11,17\rangle$	$\langle \infty_0,1,10,12\rangle$	$\langle \infty_2,5,1,4\rangle$
	$\langle 3,10,6,7\rangle$	$\langle 5,21,22,9\rangle$	$\langle 5,24,16,28\rangle$	$\langle \infty_0,3,11,14\rangle$	$\langle \infty_1,2,25,14\rangle$
	$\langle 4,22,6,3\rangle$	$\langle 1,17,23,15\rangle$			
6	$\langle 4,9,1,2\rangle$	$\langle 0,33,14,5\rangle$	$\langle 0,26,19,11\rangle$	$\langle 5,14,31,16\rangle$	$\langle \infty_2,3,8,16\rangle$
	$\langle 2,9,0,31\rangle$	$\langle 1,0,17,10\rangle$	$\langle 0,29,31,33\rangle$	$\langle 5,20,28,27\rangle$	$\langle \infty_0,3,13,17\rangle$
	$\langle 3,11,2,7\rangle$	$\langle 1,2,15,17\rangle$	$\langle 0,32,21,22\rangle$	$\langle \infty_3,0,3,1\rangle$	$\langle \infty_2,1,24,15\rangle$
	$\langle 3,5,1,12\rangle$	$\langle 1,32,34,0\rangle$	$\langle 1,10,21,11\rangle$	$\langle \infty_0,0,22,2\rangle$	$\langle \infty_2,4,11,13\rangle$
	$\langle 5,19,8,3\rangle$	$\langle 3,10,35,0\rangle$	$\langle 2,30,17,22\rangle$	$\langle \infty_0,2,5,18\rangle$	$\langle \infty_3,1,29,14\rangle$
	$\langle 5,4,6,19\rangle$	$\langle 4,26,13,9\rangle$	$\langle 3,16,24,13\rangle$	$\langle \infty_1,0,7,15\rangle$	$\langle \infty_3,2,34,15\rangle$
	$\langle 0,20,4,17\rangle$	$\langle 5,22,21,8\rangle$	$\langle 4,21,25,32\rangle$	$\langle \infty_1,3,29,2\rangle$	$\langle \infty_1,4,14,0\rangle$
	$\langle 0,27,5,32\rangle$	$\langle 0,25,10,20\rangle$	$\langle 5,10,30,33\rangle$		

7	$\langle 4,0,3,9\rangle$	$\langle 1,38,12,0\rangle$	$\langle 4,21,38,6\rangle$	$\langle 1,25,33,13\rangle$	$\langle \infty_3,1,10,7\rangle$
	$\langle 2,6,0,29\rangle$	$\langle 2,21,5,18\rangle$	$\langle 4,6,19,10\rangle$	$\langle 2,22,28,20\rangle$	$\langle \infty_3,2,17,0\rangle$
	$\langle 3,23,7,5\rangle$	$\langle 2,26,13,8\rangle$	$\langle 5,1,37,24\rangle$	$\langle 2,32,41,10\rangle$	$\langle \infty_0,1,27,11\rangle$
	$\langle 5,22,6,2\rangle$	$\langle 2,35,3,36\rangle$	$\langle 5,16,28,1\rangle$	$\langle 4,27,15,35\rangle$	$\langle \infty_0,2,40,34\rangle$
	$\langle 0,5,20,22\rangle$	$\langle 2,8,25,19\rangle$	$\langle 5,18,9,13\rangle$	$\langle 5,24,41,25\rangle$	$\langle \infty_1,3,36,28\rangle$
	$\langle 1,18,0,26\rangle$	$\langle 3,14,27,1\rangle$	$\langle 0,12,22,17\rangle$	$\langle \infty_0,0,11,3\rangle$	$\langle \infty_1,5,13,14\rangle$
	$\langle 1,21,24,9\rangle$	$\langle 3,16,40,6\rangle$	$\langle 0,27,32,16\rangle$	$\langle \infty_1,2,4,27\rangle$	$\langle \infty_2,4,41,22\rangle$
	$\langle 1,23,41,3\rangle$	$\langle 3,5,39,15\rangle$	$\langle 0,37,34,12\rangle$	$\langle \infty_2,0,8,31\rangle$	$\langle \infty_3,0,15,20\rangle$
	$\langle 1,34,2,33\rangle$	$\langle 4,17,5,23\rangle$	$\langle 1,16,13,40\rangle$	$\langle \infty_2,3,1,39\rangle$	
8	$\langle 0,2,1,45\rangle$	$\langle 4,23,24,3\rangle$	$\langle 1,26,39,29\rangle$	$\langle 4,33,22,47\rangle$	$\langle \infty_3,0,9,14\rangle$
	$\langle 0,4,3,15\rangle$	$\langle 4,29,39,8\rangle$	$\langle 1,37,46,43\rangle$	$\langle 4,40,45,33\rangle$	$\langle \infty_3,1,8,12\rangle$
	$\langle 2,3,32,4\rangle$	$\langle 5,2,27,23\rangle$	$\langle 1,43,29,31\rangle$	$\langle 4,41,30,26\rangle$	$\langle \infty_3,4,5,17\rangle$
	$\langle 0,17,20,6\rangle$	$\langle 5,20,3,10\rangle$	$\langle 2,13,31,16\rangle$	$\langle 4,47,27,18\rangle$	$\langle \infty_0,0,21,47\rangle$
	$\langle 0,46,43,5\rangle$	$\langle 5,24,1,36\rangle$	$\langle 2,16,44,25\rangle$	$\langle 5,18,32,39\rangle$	$\langle \infty_0,4,25,30\rangle$
	$\langle 0,5,31,20\rangle$	$\langle 5,43,9,34\rangle$	$\langle 2,19,17,14\rangle$	$\langle 5,22,39,41\rangle$	$\langle \infty_0,5,14,19\rangle$
	$\langle 1,3,21,18\rangle$	$\langle 0,19,45,38\rangle$	$\langle 3,44,39,14\rangle$	$\langle 5,23,17,18\rangle$	$\langle \infty_1,0,34,28\rangle$
	$\langle 1,42,12,5\rangle$	$\langle 0,26,13,39\rangle$	$\langle 4,14,26,25\rangle$	$\langle 5,46,44,31\rangle$	$\langle \infty_1,5,26,11\rangle$
	$\langle 2,46,7,29\rangle$	$\langle 0,36,15,34\rangle$	$\langle 4,17,42,16\rangle$	$\langle \infty_1,3,7,9\rangle$	$\langle \infty_2,0,41,23\rangle$
	$\langle 3,45,12,6\rangle$	$\langle 0,38,42,29\rangle$	$\langle 4,31,46,32\rangle$	$\langle \infty_2,4,19,9\rangle$	$\langle \infty_2,2,39,12\rangle$
9	$\langle 2,1,0,3\rangle$	$\langle 2,15,22,8\rangle$	$\langle 4,42,5,16\rangle$	$\langle 4,12,52,11\rangle$	$\langle \infty_3,1,11,5\rangle$
	$\langle 0,4,3,34\rangle$	$\langle 2,19,9,26\rangle$	$\langle 5,8,36,22\rangle$	$\langle 4,29,34,51\rangle$	$\langle \infty_3,3,28,0\rangle$
	$\langle 1,4,48,0\rangle$	$\langle 2,21,10,0\rangle$	$\langle 0,30,28,11\rangle$	$\langle 4,41,17,15\rangle$	$\langle \infty_0,0,49,26\rangle$
	$\langle 2,8,12,5\rangle$	$\langle 2,4,36,28\rangle$	$\langle 0,39,43,17\rangle$	$\langle 4,47,32,43\rangle$	$\langle \infty_0,2,34,18\rangle$
	$\langle 3,8,37,4\rangle$	$\langle 2,48,5,44\rangle$	$\langle 0,42,13,19\rangle$	$\langle 5,17,38,48\rangle$	$\langle \infty_0,3,23,22\rangle$
	$\langle 4,7,46,2\rangle$	$\langle 2,7,24,37\rangle$	$\langle 1,25,17,51\rangle$	$\langle 5,18,11,43\rangle$	$\langle \infty_1,0,51,32\rangle$
	$\langle 4,9,25,3\rangle$	$\langle 3,1,36,15\rangle$	$\langle 1,53,24,12\rangle$	$\langle 5,21,51,35\rangle$	$\langle \infty_1,5,25,10\rangle$
	$\langle 5,0,6,49\rangle$	$\langle 3,20,31,6\rangle$	$\langle 2,45,44,15\rangle$	$\langle 5,40,27,19\rangle$	$\langle \infty_2,4,43,24\rangle$
	$\langle 5,3,24,9\rangle$	$\langle 3,26,51,1\rangle$	$\langle 2,46,32,51\rangle$	$\langle \infty_1,2,40,7\rangle$	$\langle 4,37,11,6\rangle$
	$\langle 5,9,1,17\rangle$	$\langle 3,40,17,5\rangle$	$\langle 2,52,18,41\rangle$	$\langle \infty_2,3,42,8\rangle$	$\langle 3,47,25,28\rangle$
	$\langle 1,43,20,9\rangle$	$\langle 3,45,22,2\rangle$	$\langle 3,43,29,32\rangle$	$\langle \infty_2,5,20,7\rangle$	$\langle \infty_3,0,14,4\rangle$
	$\langle 1,8,49,39\rangle$				

表 5.7 最优 $(n,5,[3,1])_3$-码的基础码字，$n \in \{24,30,42,54\}$

n	基础码字				
24	$\langle 12,2,9,5\rangle$	$\langle 8,14,1,4\rangle$	$\langle 13,3,11,0\rangle$	$\langle 8,16,21,0\rangle$	$\langle 14,11,17,3\rangle$
	$\langle 17,3,1,5\rangle$	$\langle 8,9,13,1\rangle$	$\langle 16,2,17,1\rangle$	$\langle 9,15,22,2\rangle$	$\langle 18,19,20,5\rangle$
	$\langle 4,6,23,2\rangle$	$\langle 11,15,7,5\rangle$	$\langle 18,14,9,0\rangle$	$\langle 12,15,16,3\rangle$	$\langle 7,18,13,3\rangle$
	$\langle 7,22,4,1\rangle$	$\langle 11,2,22,4\rangle$	$\langle 6,12,11,1\rangle$	$\langle 12,21,23,4\rangle$	$\langle 13,16,23,5\rangle$
	$\langle 8,0,10,3\rangle$	$\langle 12,4,19,0\rangle$			

30	$\langle 2,0,1,3\rangle$	$\langle 1,8,25,0\rangle$	$\langle 0,29,24,1\rangle$	$\langle 6,14,16,0\rangle$	$\langle 8,27,23,4\rangle$
	$\langle 2,7,3,4\rangle$	$\langle 5,28,7,3\rangle$	$\langle 3,21,10,0\rangle$	$\langle 6,25,22,1\rangle$	$\langle 10,11,23,3\rangle$
	$\langle 4,0,3,5\rangle$	$\langle 6,2,18,5\rangle$	$\langle 4,16,20,3\rangle$	$\langle 6,28,19,2\rangle$	$\langle 10,27,12,5\rangle$
	$\langle 7,9,0,2\rangle$	$\langle 8,3,19,1\rangle$	$\langle 4,23,28,1\rangle$	$\langle 8,11,21,2\rangle$	$\langle 11,20,14,1\rangle$
	$\langle 1,17,6,4\rangle$	$\langle 9,11,1,5\rangle$	$\langle 5,12,29,4\rangle$	$\langle 8,16,26,5\rangle$	$\langle 8,18,15,3\rangle$
	$\langle 1,5,13,2\rangle$	$\langle 9,4,19,0\rangle$	$\langle 5,27,21,1\rangle$		
42	$\langle 21,2,1,4\rangle$	$\langle 3,19,13,5\rangle$	$\langle 16,13,15,0\rangle$	$\langle 23,10,14,3\rangle$	$\langle 30,32,17,1\rangle$
	$\langle 26,0,9,1\rangle$	$\langle 31,16,8,4\rangle$	$\langle 17,12,33,2\rangle$	$\langle 23,41,20,2\rangle$	$\langle 32,12,34,0\rangle$
	$\langle 26,8,1,2\rangle$	$\langle 31,24,1,0\rangle$	$\langle 20,10,40,1\rangle$	$\langle 24,34,37,5\rangle$	$\langle 35,33,25,3\rangle$
	$\langle 1,29,41,5\rangle$	$\langle 34,28,3,1\rangle$	$\langle 20,24,32,3\rangle$	$\langle 26,33,20,0\rangle$	$\langle 36,11,12,3\rangle$
	$\langle 13,37,8,1\rangle$	$\langle 34,6,29,4\rangle$	$\langle 21,16,24,1\rangle$	$\langle 26,36,40,5\rangle$	$\langle 36,30,31,2\rangle$
	$\langle 13,9,17,4\rangle$	$\langle 35,0,16,5\rangle$	$\langle 21,30,18,0\rangle$	$\langle 27,38,33,4\rangle$	$\langle 37,12,26,4\rangle$
	$\langle 27,0,15,2\rangle$	$\langle 4,25,39,5\rangle$	$\langle 21,41,40,3\rangle$	$\langle 28,10,37,2\rangle$	$\langle 38,29,35,0\rangle$
	$\langle 27,41,9,0\rangle$	$\langle 11,15,28,4\rangle$	$\langle 22,11,38,1\rangle$	$\langle 29,13,22,3\rangle$	$\langle 41,30,19,4\rangle$
54	$\langle 2,0,1,3\rangle$	$\langle 4,30,7,1\rangle$	$\langle 8,20,38,5\rangle$	$\langle 14,41,49,5\rangle$	$\langle 17,42,24,1\rangle$
	$\langle 3,7,2,4\rangle$	$\langle 9,11,1,5\rangle$	$\langle 8,36,51,2\rangle$	$\langle 14,48,31,1\rangle$	$\langle 18,48,37,4\rangle$
	$\langle 4,5,1,2\rangle$	$\langle 10,12,3,2\rangle$	$\langle 9,21,50,0\rangle$	$\langle 15,28,40,1\rangle$	$\langle 19,33,50,3\rangle$
	$\langle 5,0,6,1\rangle$	$\langle 13,11,4,0\rangle$	$\langle 9,24,40,4\rangle$	$\langle 15,43,23,2\rangle$	$\langle 20,23,26,4\rangle$
	$\langle 0,35,7,2\rangle$	$\langle 18,39,5,3\rangle$	$\langle 11,15,25,3\rangle$	$\langle 15,51,34,4\rangle$	$\langle 20,39,53,1\rangle$
	$\langle 1,6,17,4\rangle$	$\langle 19,28,6,2\rangle$	$\langle 11,40,48,2\rangle$	$\langle 16,22,32,0\rangle$	$\langle 21,22,42,2\rangle$
	$\langle 12,2,9,1\rangle$	$\langle 2,31,33,0\rangle$	$\langle 12,16,44,5\rangle$	$\langle 16,43,27,1\rangle$	$\langle 28,13,33,5\rangle$
	$\langle 18,6,2,5\rangle$	$\langle 5,16,11,4\rangle$	$\langle 12,26,37,3\rangle$	$\langle 16,53,30,2\rangle$	$\langle 29,10,44,0\rangle$
	$\langle 3,0,27,5\rangle$	$\langle 6,14,16,3\rangle$	$\langle 13,34,52,1\rangle$	$\langle 17,33,39,2\rangle$	$\langle 14,22,46,4\rangle$
	$\langle 3,29,8,1\rangle$	$\langle 7,20,13,3\rangle$	$\langle 13,45,35,4\rangle$	$\langle 17,40,26,5\rangle$	$\langle 17,41,53,0\rangle$
	$\langle 4,17,8,3\rangle$	$\langle 7,25,37,5\rangle$			

表 5.8 最优 $(4t,5,[2,2])_3$-码的基础码字，$t \in \{6,7,9,11,13,17\}$

t	基础码字				
6	$\langle 1,9,4,7\rangle$	$\langle 1,3,5,10\rangle$	$\langle 1,5,19,21\rangle$	$\langle 1,10,11,14\rangle$	$\langle 1,22,9,16\rangle$
	$\langle 0,4,9,23\rangle$	$\langle 0,9,14,20\rangle$	$\langle 0,10,13,17\rangle$	$\langle 1,20,18,22\rangle$	$\langle 0,18,10,15\rangle$
	$\langle 1,18,0,2\rangle$				
7	$\langle 0,11,1,6\rangle$	$\langle 1,3,8,16\rangle$	$\langle 0,1,23,26\rangle$	$\langle 0,13,17,24\rangle$	$\langle 1,19,21,27\rangle$
	$\langle 0,9,2,19\rangle$	$\langle 1,8,7,17\rangle$	$\langle 0,19,3,15\rangle$	$\langle 0,16,20,21\rangle$	$\langle 0,18,12,25\rangle$
	$\langle 1,14,2,4\rangle$	$\langle 1,9,0,18\rangle$	$\langle 0,2,10,13\rangle$		
9	$\langle 1,3,4,35\rangle$	$\langle 0,8,13,15\rangle$	$\langle 1,32,5,34\rangle$	$\langle 0,24,14,30\rangle$	$\langle 1,16,24,28\rangle$
	$\langle 0,2,22,31\rangle$	$\langle 1,25,6,27\rangle$	$\langle 0,13,23,24\rangle$	$\langle 0,27,10,21\rangle$	$\langle 1,12,10,16\rangle$
	$\langle 0,3,25,28\rangle$	$\langle 1,26,9,29\rangle$	$\langle 0,15,27,35\rangle$	$\langle 1,11,25,32\rangle$	$\langle 0,20,16,17\rangle$
	$\langle 0,31,1,11\rangle$	$\langle 1,31,8,30\rangle$			

11	$\langle 0,5,4,21\rangle$	$\langle 0,24,8,33\rangle$	$\langle 1,21,4,40\rangle$	$\langle 0,17,15,26\rangle$	$\langle 1,34,19,22\rangle$
	$\langle 0,6,1,16\rangle$	$\langle 0,28,3,41\rangle$	$\langle 1,35,8,27\rangle$	$\langle 0,23,20,34\rangle$	$\langle 0,1,35,36\rangle$
	$\langle 1,2,7,39\rangle$	$\langle 0,4,11,27\rangle$	$\langle 1,5,25,33\rangle$	$\langle 1,26,32,38\rangle$	$\langle 1,10,6,41\rangle$
	$\langle 1,3,5,15\rangle$	$\langle 0,9,17,24\rangle$	$\langle 0,12,14,30\rangle$	$\langle 1,30,11,24\rangle$	$\langle 0,13,42,43\rangle$
	$\langle 1,33,14,34\rangle$				
13	$\langle 0,44,8,9\rangle$	$\langle 0,43,3,49\rangle$	$\langle 1,32,5,42\rangle$	$\langle 0,18,37,38\rangle$	$\langle 0,49,40,51\rangle$
	$\langle 0,14,4,48\rangle$	$\langle 0,7,12,36\rangle$	$\langle 1,49,4,24\rangle$	$\langle 0,24,31,39\rangle$	$\langle 1,18,12,47\rangle$
	$\langle 0,19,5,27\rangle$	$\langle 1,15,2,29\rangle$	$\langle 1,7,17,51\rangle$	$\langle 0,29,14,47\rangle$	$\langle 1,21,43,46\rangle$
	$\langle 0,3,23,50\rangle$	$\langle 1,22,0,14\rangle$	$\langle 0,11,32,41\rangle$	$\langle 0,39,11,35\rangle$	$\langle 1,35,16,32\rangle$
	$\langle 0,30,2,21\rangle$	$\langle 1,3,20,37\rangle$	$\langle 0,12,13,18\rangle$	$\langle 0,45,28,33\rangle$	$\langle 1,40,10,33\rangle$
17	$\langle 0,1,7,17\rangle$	$\langle 0,41,1,13\rangle$	$\langle 0,14,37,66\rangle$	$\langle 0,56,46,50\rangle$	$\langle 1,45,44,52\rangle$
	$\langle 0,4,3,39\rangle$	$\langle 0,49,2,51\rangle$	$\langle 0,16,25,26\rangle$	$\langle 0,57,43,54\rangle$	$\langle 1,50,27,64\rangle$
	$\langle 1,5,6,30\rangle$	$\langle 0,9,19,32\rangle$	$\langle 0,23,38,47\rangle$	$\langle 0,66,22,28\rangle$	$\langle 1,52,13,20\rangle$
	$\langle 0,24,5,40\rangle$	$\langle 1,11,9,49\rangle$	$\langle 0,36,21,27\rangle$	$\langle 1,16,28,58\rangle$	$\langle 1,53,43,57\rangle$
	$\langle 0,27,8,20\rangle$	$\langle 1,55,4,19\rangle$	$\langle 0,40,33,55\rangle$	$\langle 1,37,14,15\rangle$	$\langle 1,66,54,61\rangle$
	$\langle 0,33,4,44\rangle$	$\langle 1,9,31,56\rangle$	$\langle 0,45,18,41\rangle$	$\langle 1,40,32,51\rangle$	$\langle 1,43,34,37\rangle$
	$\langle 0,37,6,57\rangle$	$\langle 0,13,48,65\rangle$	$\langle 0,55,31,64\rangle$		

表 5.9 最优 $(4t+1,5,[2,2])_3$-码的基础码字，$t \in \{6,7,9,11,13,17\}$

t	基础码字				
6	$\langle 0,4,1,3\rangle$	$\langle 0,16,5,6\rangle$	$\langle 0,17,9,19\rangle$	$\langle 0,3,16,23\rangle$	$\langle 0,11,4,21\rangle$
	$\langle 0,1,8,12\rangle$				
7	$\langle 0,1,2,4\rangle$	$\langle 0,3,19,25\rangle$	$\langle 0,7,18,27\rangle$	$\langle 0,14,21,26\rangle$	$\langle 0,11,10,17\rangle$
	$\langle 0,10,5,23\rangle$	$\langle 0,6,14,15\rangle$			
9	$\langle 0,5,9,22\rangle$	$\langle 0,28,6,35\rangle$	$\langle 0,34,2,29\rangle$	$\langle 0,19,30,31\rangle$	$\langle 0,30,27,33\rangle$
	$\langle 0,1,19,24\rangle$	$\langle 0,31,8,20\rangle$	$\langle 0,15,25,28\rangle$	$\langle 0,20,21,36\rangle$	
11	$\langle 0,2,9,43\rangle$	$\langle 0,16,1,20\rangle$	$\langle 0,31,34,42\rangle$	$\langle 0,40,16,33\rangle$	$\langle 0,39,23,26\rangle$
	$\langle 0,11,6,10\rangle$	$\langle 0,35,2,27\rangle$	$\langle 0,33,19,24\rangle$	$\langle 0,42,14,15\rangle$	$\langle 0,17,25,39\rangle$
	$\langle 0,15,5,28\rangle$				
13	$\langle 0,52,5,9\rangle$	$\langle 0,3,24,45\rangle$	$\langle 0,4,39,51\rangle$	$\langle 0,10,38,40\rangle$	$\langle 0,45,23,33\rangle$
	$\langle 0,12,7,44\rangle$	$\langle 0,32,4,22\rangle$	$\langle 0,6,14,19\rangle$	$\langle 0,26,29,52\rangle$	$\langle 0,34,46,49\rangle$
	$\langle 0,17,1,34\rangle$	$\langle 0,39,2,36\rangle$	$\langle 0,9,20,27\rangle$		
17	$\langle 0,67,5,8\rangle$	$\langle 0,8,52,65\rangle$	$\langle 0,22,14,33\rangle$	$\langle 0,38,59,64\rangle$	$\langle 0,68,15,50\rangle$
	$\langle 0,43,1,34\rangle$	$\langle 0,9,29,39\rangle$	$\langle 0,25,18,67\rangle$	$\langle 0,52,46,54\rangle$	$\langle 0,29,38,53\rangle$
	$\langle 0,58,6,45\rangle$	$\langle 0,10,22,68\rangle$	$\langle 0,27,31,55\rangle$	$\langle 0,57,23,37\rangle$	$\langle 0,63,13,66\rangle$
	$\langle 0,7,43,47\rangle$	$\langle 0,16,41,48\rangle$			

表 5.10　最优 $(4t+2, 5, [2,2])_3$-码的基础码字，$t \in [6,11] \cup \{13,14,17\}$

t	基础码字
6	$\langle 0,2,7,8\rangle$ $\langle 0,8,1,10\rangle$ $\langle 0,4,15,22\rangle$ $\langle 0,3,12,17\rangle$ $\langle 0,5,21,25\rangle$ $\langle 0,1,4,24\rangle$
7	$\langle 0,19,7,8\rangle$ $\langle 0,10,2,13\rangle$ $\langle 0,3,23,28\rangle$ $\langle 0,16,10,12\rangle$ $\langle 0,6,11,27\rangle$ $\langle 0,25,1,9\rangle$ $\langle 0,17,4,16\rangle$
8	$\langle 0,1,2,4\rangle$ $\langle 0,3,12,26\rangle$ $\langle 0,5,27,33\rangle$ $\langle 0,9,20,30\rangle$ $\langle 0,16,29,32\rangle$ $\langle 0,2,7,8\rangle$ $\langle 0,4,14,19\rangle$ $\langle 0,6,24,31\rangle$
9	$\langle 0,1,2,4\rangle$ $\langle 0,11,8,36\rangle$ $\langle 0,3,12,16\rangle$ $\langle 0,5,20,23\rangle$ $\langle 0,7,31,37\rangle$ $\langle 0,2,7,34\rangle$ $\langle 0,15,6,26\rangle$ $\langle 0,4,14,21\rangle$ $\langle 0,6,28,33\rangle$
10	$\langle 0,1,2,4\rangle$ $\langle 0,4,13,16\rangle$ $\langle 0,6,24,35\rangle$ $\langle 0,14,34,40\rangle$ $\langle 0,17,14,36\rangle$ $\langle 0,2,7,8\rangle$ $\langle 0,5,22,37\rangle$ $\langle 0,8,31,38\rangle$ $\langle 0,16,27,41\rangle$ $\langle 0,18,28,33\rangle$
11	$\langle 0,14,1,21\rangle$ $\langle 0,10,16,32\rangle$ $\langle 0,17,11,29\rangle$ $\langle 0,28,13,42\rangle$ $\langle 0,16,25,44\rangle$ $\langle 0,40,4,18\rangle$ $\langle 0,12,17,20\rangle$ $\langle 0,19,38,45\rangle$ $\langle 0,37,34,39\rangle$ $\langle 0,24,15,27\rangle$ $\langle 0,5,35,41\rangle$
13	$\langle 0,2,7,8\rangle$ $\langle 0,3,12,16\rangle$ $\langle 0,7,35,49\rangle$ $\langle 0,12,11,46\rangle$ $\langle 0,22,37,43\rangle$ $\langle 0,1,40,52\rangle$ $\langle 0,4,14,48\rangle$ $\langle 0,8,31,41\rangle$ $\langle 0,14,17,50\rangle$ $\langle 0,21,22,25\rangle$ $\langle 0,11,2,30\rangle$ $\langle 0,6,24,32\rangle$ $\langle 0,9,29,47\rangle$
14	$\langle 0,57,1,3\rangle$ $\langle 0,3,12,52\rangle$ $\langle 0,7,28,41\rangle$ $\langle 0,14,22,39\rangle$ $\langle 0,42,35,55\rangle$ $\langle 0,17,6,37\rangle$ $\langle 0,4,14,19\rangle$ $\langle 0,8,31,46\rangle$ $\langle 0,19,11,17\rangle$ $\langle 0,49,33,44\rangle$ $\langle 0,20,5,27\rangle$ $\langle 0,6,24,32\rangle$ $\langle 0,12,48,57\rangle$ $\langle 0,24,40,54\rangle$
17	$\langle 0,7,5,19\rangle$ $\langle 0,8,18,24\rangle$ $\langle 0,24,11,50\rangle$ $\langle 0,44,14,36\rangle$ $\langle 0,66,38,54\rangle$ $\langle 0,2,15,39\rangle$ $\langle 0,15,59,67\rangle$ $\langle 0,34,51,55\rangle$ $\langle 0,49,27,45\rangle$ $\langle 0,40,31,65\rangle$ $\langle 0,28,7,30\rangle$ $\langle 0,17,20,64\rangle$ $\langle 0,39,22,32\rangle$ $\langle 0,50,23,56\rangle$ $\langle 0,65,29,69\rangle$ $\langle 0,38,1,46\rangle$ $\langle 0,19,28,60\rangle$

表 5.11　最优 $(4t+11, 5, [2,2])_3$-码的码字，$t \in \{0,1,2\}$

t	码字集合
0	$\langle 0,1,2,9\rangle$ $\langle 2,3,1,6\rangle$ $\langle 5,6,2,8\rangle$ $\langle 1,2,4,10\rangle$ $\langle 7,10,3,5\rangle$ $\langle 0,4,3,8\rangle$ $\langle 2,4,0,5\rangle$ $\langle 6,7,0,9\rangle$ $\langle 2,10,7,8\rangle$ $\langle 8,10,1,9\rangle$ $\langle 0,8,5,7\rangle$ $\langle 2,5,3,9\rangle$ $\langle 6,9,1,5\rangle$ $\langle 3,10,0,2\rangle$ $\langle 4,9,2,6\rangle$ $\langle 1,3,5,8\rangle$ $\langle 3,6,4,7\rangle$ $\langle 7,9,4,8\rangle$ $\langle 3,4,9,10\rangle$ $\langle 0,7,1,10\rangle$ $\langle 1,8,0,6\rangle$ $\langle 4,5,1,7\rangle$ $\langle 0,10,4,6\rangle$ $\langle 5,9,0,10\rangle$ $\langle 6,8,3,10\rangle$ $\langle 1,9,3,7\rangle$

1	$\langle 0,2,5,8\rangle$	$\langle 1,4,9,11\rangle$	$\langle 4,10,0,6\rangle$	$\langle 0,1,10,12\rangle$	$\langle 10,12,5,14\rangle$
	$\langle 0,8,6,9\rangle$	$\langle 1,7,4,13\rangle$	$\langle 4,11,2,5\rangle$	$\langle 0,10,7,13\rangle$	$\langle 10,13,8,12\rangle$
	$\langle 1,6,2,8\rangle$	$\langle 1,9,7,14\rangle$	$\langle 5,14,8,9\rangle$	$\langle 0,14,1,11\rangle$	$\langle 11,13,3,10\rangle$
	$\langle 1,8,0,3\rangle$	$\langle 2,11,0,9\rangle$	$\langle 5,6,4,12\rangle$	$\langle 11,12,1,8\rangle$	$\langle 11,14,7,12\rangle$
	$\langle 2,6,3,7\rangle$	$\langle 2,4,1,12\rangle$	$\langle 5,7,2,14\rangle$	$\langle 12,13,7,9\rangle$	$\langle 12,14,3,13\rangle$
	$\langle 3,4,7,8\rangle$	$\langle 2,9,6,13\rangle$	$\langle 5,9,3,11\rangle$	$\langle 2,14,4,10\rangle$	$\langle 6,12,10,11\rangle$
	$\langle 5,8,1,7\rangle$	$\langle 3,10,2,9\rangle$	$\langle 7,10,1,3\rangle$	$\langle 2,3,11,14\rangle$	$\langle 8,11,13,14\rangle$
	$\langle 6,7,5,9\rangle$	$\langle 3,11,4,6\rangle$	$\langle 7,9,8,10\rangle$	$\langle 4,5,10,13\rangle$	$\langle 3,8,5,10\rangle$
	$\langle 0,13,2,4\rangle$	$\langle 3,6,1,13\rangle$	$\langle 8,9,2,12\rangle$	$\langle 6,13,0,14\rangle$	$\langle 9,13,1,5\rangle$
	$\langle 0,4,3,14\rangle$	$\langle 3,7,0,12\rangle$	$\langle 9,12,0,4\rangle$	$\langle 7,13,6,11\rangle$	$\langle 8,10,4,11\rangle$
	$\langle 1,14,5,6\rangle$				
2	$\langle 0,5,4,8\rangle$	$\langle 3,6,8,16\rangle$	$\langle 1,3,13,14\rangle$	$\langle 4,9,11,18\rangle$	$\langle 10,16,8,13\rangle$
	$\langle 1,9,2,7\rangle$	$\langle 3,7,5,15\rangle$	$\langle 10,15,3,6\rangle$	$\langle 5,11,3,16\rangle$	$\langle 10,17,5,11\rangle$
	$\langle 2,8,5,6\rangle$	$\langle 4,10,0,2\rangle$	$\langle 11,16,1,9\rangle$	$\langle 5,16,7,12\rangle$	$\langle 12,16,2,10\rangle$
	$\langle 2,9,3,8\rangle$	$\langle 4,5,1,15\rangle$	$\langle 11,18,2,8\rangle$	$\langle 6,11,0,10\rangle$	$\langle 13,14,7,10\rangle$
	$\langle 4,7,8,9\rangle$	$\langle 4,8,3,14\rangle$	$\langle 12,14,1,8\rangle$	$\langle 6,15,2,12\rangle$	$\langle 15,18,5,14\rangle$
	$\langle 6,9,1,4\rangle$	$\langle 5,6,9,18\rangle$	$\langle 13,16,4,6\rangle$	$\langle 6,8,11,13\rangle$	$\langle 2,16,14,18\rangle$
	$\langle 0,11,5,7\rangle$	$\langle 6,14,3,5\rangle$	$\langle 13,17,0,8\rangle$	$\langle 7,11,6,18\rangle$	$\langle 4,18,12,13\rangle$
	$\langle 0,18,1,6\rangle$	$\langle 7,13,2,3\rangle$	$\langle 14,15,4,9\rangle$	$\langle 7,12,4,14\rangle$	$\langle 5,15,10,13\rangle$
	$\langle 1,13,5,9\rangle$	$\langle 8,17,1,2\rangle$	$\langle 17,18,3,7\rangle$	$\langle 7,15,1,11\rangle$	$\langle 6,17,14,15\rangle$
	$\langle 1,5,6,11\rangle$	$\langle 0,10,9,14\rangle$	$\langle 2,13,1,12\rangle$	$\langle 7,9,13,16\rangle$	$\langle 9,18,10,15\rangle$
	$\langle 1,7,0,12\rangle$	$\langle 0,12,3,11\rangle$	$\langle 2,17,4,13\rangle$	$\langle 8,10,7,15\rangle$	$\langle 10,14,16,17\rangle$
	$\langle 1,8,4,10\rangle$	$\langle 0,14,2,13\rangle$	$\langle 2,3,10,11\rangle$	$\langle 8,14,0,18\rangle$	$\langle 11,12,13,15\rangle$
	$\langle 2,12,0,9\rangle$	$\langle 0,7,10,17\rangle$	$\langle 3,10,1,18\rangle$	$\langle 8,18,9,17\rangle$	$\langle 11,13,14,17\rangle$
	$\langle 2,6,7,17\rangle$	$\langle 0,8,12,16\rangle$	$\langle 3,17,9,12\rangle$	$\langle 9,14,6,12\rangle$	$\langle 12,17,16,18\rangle$
	$\langle 3,12,6,7\rangle$	$\langle 1,15,8,18\rangle$	$\langle 4,12,5,17\rangle$	$\langle 9,15,0,17\rangle$	$\langle 13,18,11,16\rangle$
	$\langle 3,18,0,4\rangle$	$\langle 1,16,3,17\rangle$	$\langle 4,15,7,16\rangle$	$\langle 0,13,15,18\rangle$	$\langle 14,16,11,15\rangle$
	$\langle 3,5,2,17\rangle$	$\langle 1,2,15,16\rangle$	$\langle 4,17,6,10\rangle$	$\langle 10,11,4,12\rangle$	

表 5.12 最优 $(n,5,[2,2])_3$-码的基础码字，$n \in \{35,39,43,47\}$

n	基础码字				
35	$\langle 2,26,6,1\rangle$	$\langle 25,20,2,8\rangle$	$\langle 11,4,23,34\rangle$	$\langle 20,18,27,7\rangle$	$\langle 9,24,14,18\rangle$
	$\langle 33,0,4,3\rangle$	$\langle 27,2,9,11\rangle$	$\langle 12,10,32,3\rangle$	$\langle 22,11,28,6\rangle$	$\langle 11,20,12,24\rangle$
	$\langle 5,9,7,24\rangle$	$\langle 27,4,20,5\rangle$	$\langle 12,17,7,25\rangle$	$\langle 22,33,7,13\rangle$	$\langle 13,30,21,14\rangle$
	$\langle 1,0,27,16\rangle$	$\langle 3,12,5,27\rangle$	$\langle 12,27,19,0\rangle$	$\langle 23,24,16,0\rangle$	$\langle 14,10,31,16\rangle$
	$\langle 10,8,2,28\rangle$	$\langle 6,32,9,22\rangle$	$\langle 12,6,28,23\rangle$	$\langle 3,14,23,26\rangle$	$\langle 17,24,11,21\rangle$
	$\langle 11,31,0,7\rangle$	$\langle 8,28,17,7\rangle$	$\langle 17,21,1,31\rangle$	$\langle 3,34,20,15\rangle$	$\langle 18,12,10,29\rangle$
	$\langle 13,0,32,6\rangle$	$\langle 0,23,18,30\rangle$	$\langle 19,5,13,27\rangle$	$\langle 30,19,0,22\rangle$	$\langle 23,18,13,22\rangle$
	$\langle 17,34,0,8\rangle$	$\langle 1,20,32,22\rangle$	$\langle 2,11,31,13\rangle$	$\langle 31,5,10,12\rangle$	$\langle 27,15,12,14\rangle$
	$\langle 21,9,0,32\rangle$	$\langle 10,26,0,14\rangle$	$\langle 20,12,4,34\rangle$	$\langle 7,25,21,20\rangle$	$\langle 32,13,17,19\rangle$

39	$\langle 2,3,32,4\rangle$	$\langle 5,37,8,21\rangle$	$\langle 16,20,4,14\rangle$	$\langle 5,19,38,22\rangle$	$\langle 18,26,35,10\rangle$
	$\langle 2,4,28,9\rangle$	$\langle 5,8,35,15\rangle$	$\langle 16,35,23,1\rangle$	$\langle 5,22,24,33\rangle$	$\langle 18,27,30,26\rangle$
	$\langle 5,34,2,1\rangle$	$\langle 7,38,4,11\rangle$	$\langle 18,36,27,8\rangle$	$\langle 5,33,13,11\rangle$	$\langle 18,28,22,14\rangle$
	$\langle 18,30,9,1\rangle$	$\langle 9,13,33,1\rangle$	$\langle 23,24,2,31\rangle$	$\langle 9,30,27,22\rangle$	$\langle 19,22,37,12\rangle$
	$\langle 25,30,6,2\rangle$	$\langle 10,36,14,3\rangle$	$\langle 23,25,21,5\rangle$	$\langle 10,12,20,33\rangle$	$\langle 19,28,24,18\rangle$
	$\langle 3,0,14,15\rangle$	$\langle 11,28,5,23\rangle$	$\langle 23,37,18,6\rangle$	$\langle 11,26,27,12\rangle$	$\langle 23,35,14,10\rangle$
	$\langle 5,12,30,3\rangle$	$\langle 11,34,10,9\rangle$	$\langle 26,34,8,18\rangle$	$\langle 11,31,16,20\rangle$	$\langle 24,19,36,14\rangle$
	$\langle 5,13,32,9\rangle$	$\langle 12,19,34,1\rangle$	$\langle 4,38,25,20\rangle$	$\langle 12,14,27,18\rangle$	$\langle 24,21,33,17\rangle$
	$\langle 5,30,23,7\rangle$	$\langle 13,23,38,8\rangle$	$\langle 5,10,36,27\rangle$	$\langle 16,14,30,10\rangle$	$\langle 26,32,23,20\rangle$
	$\langle 5,31,4,18\rangle$	$\langle 16,17,3,34\rangle$	$\langle 5,11,37,25\rangle$	$\langle 18,25,31,13\rangle$	
43	$\langle 11,0,9,2\rangle$	$\langle 8,2,21,24\rangle$	$\langle 24,5,30,21\rangle$	$\langle 7,34,12,13\rangle$	$\langle 25,22,15,29\rangle$
	$\langle 37,7,5,3\rangle$	$\langle 9,1,28,34\rangle$	$\langle 25,36,27,6\rangle$	$\langle 8,18,30,39\rangle$	$\langle 26,35,15,19\rangle$
	$\langle 8,3,6,10\rangle$	$\langle 11,14,38,6\rangle$	$\langle 27,32,13,5\rangle$	$\langle 9,21,17,39\rangle$	$\langle 27,25,33,28\rangle$
	$\langle 20,7,37,4\rangle$	$\langle 12,14,9,32\rangle$	$\langle 29,16,6,21\rangle$	$\langle 11,35,29,31\rangle$	$\langle 28,16,12,41\rangle$
	$\langle 23,36,0,3\rangle$	$\langle 12,31,42,6\rangle$	$\langle 3,19,42,17\rangle$	$\langle 12,40,22,27\rangle$	$\langle 28,27,37,18\rangle$
	$\langle 25,4,5,36\rangle$	$\langle 14,5,18,23\rangle$	$\langle 32,7,25,30\rangle$	$\langle 14,30,35,15\rangle$	$\langle 32,30,17,18\rangle$
	$\langle 27,4,39,3\rangle$	$\langle 15,29,3,41\rangle$	$\langle 33,12,8,23\rangle$	$\langle 15,33,28,22\rangle$	$\langle 33,27,21,10\rangle$
	$\langle 3,5,13,39\rangle$	$\langle 17,39,18,0\rangle$	$\langle 39,31,28,2\rangle$	$\langle 17,20,28,32\rangle$	$\langle 40,16,23,15\rangle$
	$\langle 5,33,25,9\rangle$	$\langle 21,1,16,32\rangle$	$\langle 40,11,4,10\rangle$	$\langle 20,27,14,26\rangle$	$\langle 42,17,12,30\rangle$
	$\langle 5,34,8,17\rangle$	$\langle 21,19,11,0\rangle$	$\langle 40,19,28,5\rangle$	$\langle 21,14,41,31\rangle$	$\langle 25,16,13,32\rangle$
	$\langle 6,1,41,30\rangle$	$\langle 22,7,16,36\rangle$	$\langle 42,12,18,1\rangle$		
47	$\langle 1,7,3,28\rangle$	$\langle 13,36,35,2\rangle$	$\langle 4,11,28,39\rangle$	$\langle 10,16,22,17\rangle$	$\langle 27,32,22,38\rangle$
	$\langle 18,1,8,44\rangle$	$\langle 17,22,18,8\rangle$	$\langle 4,15,23,46\rangle$	$\langle 10,21,35,44\rangle$	$\langle 28,37,24,14\rangle$
	$\langle 32,26,8,5\rangle$	$\langle 17,32,1,26\rangle$	$\langle 4,24,37,17\rangle$	$\langle 14,18,19,38\rangle$	$\langle 30,44,23,19\rangle$
	$\langle 4,5,43,10\rangle$	$\langle 19,4,14,27\rangle$	$\langle 4,30,44,22\rangle$	$\langle 15,21,27,33\rangle$	$\langle 31,13,27,28\rangle$
	$\langle 5,44,31,0\rangle$	$\langle 20,42,22,5\rangle$	$\langle 4,33,41,13\rangle$	$\langle 15,22,37,26\rangle$	$\langle 31,29,41,33\rangle$
	$\langle 6,10,42,0\rangle$	$\langle 22,36,33,5\rangle$	$\langle 4,40,15,32\rangle$	$\langle 15,44,17,35\rangle$	$\langle 32,44,33,13\rangle$
	$\langle 6,2,22,14\rangle$	$\langle 25,33,45,5\rangle$	$\langle 42,4,19,18\rangle$	$\langle 18,17,16,43\rangle$	$\langle 35,12,39,17\rangle$
	$\langle 6,25,23,3\rangle$	$\langle 27,44,2,11\rangle$	$\langle 43,28,2,13\rangle$	$\langle 18,36,31,10\rangle$	$\langle 45,26,27,20\rangle$
	$\langle 7,38,20,8\rangle$	$\langle 31,11,14,8\rangle$	$\langle 44,9,25,28\rangle$	$\langle 19,26,16,35\rangle$	$\langle 46,32,23,31\rangle$
	$\langle 7,44,29,6\rangle$	$\langle 31,26,1,38\rangle$	$\langle 45,13,10,0\rangle$	$\langle 21,34,12,46\rangle$	$\langle 6,19,38,13\rangle$
	$\langle 11,10,5,40\rangle$	$\langle 32,1,35,30\rangle$	$\langle 5,13,45,26\rangle$	$\langle 24,40,23,11\rangle$	$\langle 25,34,22,43\rangle$
	$\langle 12,46,4,16\rangle$	$\langle 34,41,13,5\rangle$			

6 可分码上下界的研究

6.1 可分码简介

为了抵抗多媒体内容的合谋犯罪中最常见的平均攻击，Trappe 等人在 2003 年提出了 t-弹性与抗合谋码（t-Resilient AND Anti-Collusion Code，t-AND-ACC）的概念用来配合编码调制，达到检测最多 t 个恶意用户参与的平均攻击[173]。关于 t-AND-ACC 的构造方法可以在诸多文献中找到[36,66,117,173]。但遗憾的是，t-AND-ACC 所支持的授权用户数目在实用的多媒体指纹系统中仍显不足。

为了克服 t-AND-ACC 所支持的授权用户数目不足的劣势，Cheng 与 Miao 在 2011 年提出了 t-弹性逻辑抗合谋码（t-Resilient Logical Anti-Collusion Code，t-LACC）和与之相关的 $\bar{t}$-可分码（$\bar{t}$-Separable Code，$\bar{t}$-SC）等新概念[36]。事实上，一个二元 $\bar{t}$-可分码等价于一个 t-LACC。此外，多元可分码也可以用于递归构造二元的情形。作者证明了，t-LACC 与 t-AND-ACC 具有相同的追踪能力，但前者的要求更弱。基于一类特殊的 t-LACC，他们提出了一个高效的检测算法，可以在一个大的多媒体指纹系统中指认出至多 t 个参与平均攻击的恶意用户。

在后续的工作中，可分码的存在性问题成为关注的重点。Cheng 等人提出了一些上下界估计，并构造出长度为 2 和 3 时，部分参数的最优 $\bar{2}$-可分码[35]。在本章中，我们会继续研究 $\bar{2}$-可分码的上下界问题。具体内容安排如下。第 6.2 节将用来回顾相关的概念和已知结果。在第 6.3 节中，我们将大幅改进 $\bar{2}$-可分码已知的上界，同时还将考虑可分码是一个线性码时的情况。最后在第 6.4 节中，我们将会分别利用随机方法或确定性构造方法，得到任意长度可分码的存在性结果。

6.2 预备知识

首先回忆一下码的定义。设 n，M 和 q 是三个正整数，并且 Q 是一个大小为 $|Q| = q$ 的字母表，通常取 $Q = \{0, 1, \ldots, q-1\}$。我们将向量集合 $\mathcal{C} = \{\mathtt{c}_1, \mathtt{c}_2, \ldots, \mathtt{c}_M\} \subseteq Q^n$

称为一个(n, M, q)-码，其中的每个向量叫做一个码字。当 $Q = \{0, 1\}$ 时，我们也将一个 $(n, M, 2)$-码称为二元码。

定义 6.1. 假设 $\mathcal{C}$ 是字母表 $Q = \{0, 1\}$ 上的一个 $(n, M, 2)$-码，并设 $t \geq 2$ 是一个整数。

- 若对于任意两个码字集合 $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$，满足 $|\mathcal{C}_1| \leq t, |\mathcal{C}_2| \leq t$，并且 $\mathcal{C}_1 \neq \mathcal{C}_2$，下面的不等式都成立

$$\bigwedge_{\mathtt{c} \in \mathcal{C}_1} \mathtt{c} \neq \bigwedge_{\mathtt{c} \in \mathcal{C}_2} \mathtt{c}\,,$$

  其中 $\bigwedge$ 表示逐位（Bitwise）逻辑“与”（AND）运算。那么我们称 $\mathcal{C}$ 是一个t-AND-ACC$(n, M, 2)$。

- 若对于任意两个码字集合 $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$，满足 $|\mathcal{C}_1| \leq t, |\mathcal{C}_2| \leq t$，并且 $\mathcal{C}_1 \neq \mathcal{C}_2$，下面两个不等式中至少有一个成立：

$$\bigvee_{\mathtt{c} \in \mathcal{C}_1} \mathtt{c} \neq \bigvee_{\mathtt{c} \in \mathcal{C}_2} \mathtt{c}\,, \quad \text{或} \quad \bigwedge_{\mathtt{c} \in \mathcal{C}_1} \mathtt{c} \neq \bigwedge_{\mathtt{c} \in \mathcal{C}_2} \mathtt{c}\,,$$

  其中 $\bigvee$ 表示逐位逻辑“或”（OR）运算。那么我们就将 $\mathcal{C}$ 称为一个t-LACC$(n, M, 2)$。

对于整数 $i, 1 \leq i \leq n$，我们用 $\mathtt{c}(i)$ 表示向量 $\mathtt{c} \in Q^n$ 第 i 个位置上的值。而对于一个向量集合 $\mathcal{C} \subseteq Q^n$，我们同样称 $\mathcal{C}$ 的第 i 位为集合：

$$\mathcal{C}(i) = \{\mathtt{c}(i) \in Q \mid \mathtt{c} \in \mathcal{C}\}\,。$$

我们再定义：

$$\begin{aligned} \mathtt{desc}(\mathcal{C}) &= \{\mathtt{x} \in Q^n \mid \mathtt{x}(i) \in \mathcal{C}(i), 1 \leq i \leq n\} \\ &= \mathcal{C}(1) \times \cdots \times \mathcal{C}(n)\,。 \end{aligned}$$

即集合 $\mathtt{desc}(\mathcal{C})$ 是所有可以由 $\mathcal{C}$ 中的码字通过合谋所产生的 n 长向量组成的集合。

定义 6.2. 假设 $\mathcal{C}$ 是一个 (n, M, q)-码，并且整数 $t \geq 2$。

- 如果对于任意两个码字集合 $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$，满足条件 $|\mathcal{C}_1| = |\mathcal{C}_2| = t$，并且 $\mathcal{C}_1 \neq \mathcal{C}_2$，均有 $\mathtt{desc}(\mathcal{C}_1) \neq \mathtt{desc}(\mathcal{C}_2)$，即至少存在一个坐标位置 $i, 1 \leq i \leq n$，使得 $\mathcal{C}_1(i) \neq \mathcal{C}_2(i)$。那么我们就称 $\mathcal{C}$ 是一个t-**可分码**，记作 t-SC(n, M, q)。

- 如果对于任意两个码字集合 $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$，满足条件 $|\mathcal{C}_1| \leq t, |\mathcal{C}_2| \leq t$，并且 $\mathcal{C}_1 \neq \mathcal{C}_2$，都有 $\mathtt{desc}(\mathcal{C}_1) \neq \mathtt{desc}(\mathcal{C}_2)$，即至少存在一个位置 $i, 1 \leq i \leq n$，使得 $\mathcal{C}_1(i) \neq \mathcal{C}_2(i)$。那么我们就称 $\mathcal{C}$ 是一个**$\bar{t}$-可分码**，记作 $\bar{t}$-SC(n, M, q)。

- 如果对于任意一个码字集合 $\mathcal{C}_1 \subseteq \mathcal{C}$，满足条件 $|\mathcal{C}_1| \leq t$，都有 $\mathtt{desc}(\mathcal{C}_1) \cap \mathcal{C} = \mathcal{C}_1$，即对于任意 $\mathtt{c} \in \mathcal{C} \setminus \mathcal{C}_1$，都至少存在一个坐标 $i, 1 \leq i \leq n$，使得 $\mathtt{c}(i) \notin (\mathtt{desc}(\mathcal{C}_1))(i) = \mathcal{C}_1(i)$。那么我们就称 $\mathcal{C}$ 是一个**t-防诬陷码**（Frameproof Code，FPC），记作 t-FPC(n, M, q)。

这些码之间有如下的一些关系。

引理 6.3 (Cheng 等[35])：*一个 (n, M, q)-码 $\mathcal{C}$ 是 $\bar{t}$-可分码，当且仅当 $\mathcal{C}$ 同时是 $(t-1)$-防诬陷码和 t-可分码。另一方面，所有 t-防诬陷码都是 $\bar{t}$-可分码。*

引理 6.4：*如果同时存在一个 $\bar{t}$-$\mathtt{SC}(n_1, M, q)$ 和一个 $\bar{t}$-$\mathtt{SC}(n_2, q, 2)$，那么存在一个 $\bar{t}$-$\mathtt{SC}(n_1 n_2, M, 2)$。*

直观地看，一个 t-可分码中任意 t 个人合谋产生的向量集合都不同于另外 t 个人合谋产生的；$\bar{t}$-可分码中任意两个不超过 t 人的集体合谋所能够得到的向量集合是不同的；而 t-防诬陷码里，任意不超过 t 人的合谋集团都不能诬陷他们之外的某个用户。

还有一类被广泛研究的相关概念是分离哈希族（Separating Hash Family，SHF），也有学者将其称为分离码（Separating Code）[9,141,159]。

定义 6.5. 设 n, m, w_1, w_2 为正整数，并且 $n \geq w_1, n \geq w_2$。令 X 和 Y 为有限集，使得 $|X| = n$ 且 $|Y| = m$。设 $\mathcal{F}$ 是一些函数 $f : X \to Y$ 组成的集合。若对于 X 中任意两个不相交的子集 $X_1, X_2 \subseteq X$，其中 $|X_1| = w_1$ 且 $|X_2| = w_2$，都存在至少一个函数 $f \in \mathcal{F}$，使得 $\{f(x) \mid x \in X_1\} \cap \{f(x) \mid x \in X_2\} = \emptyset$。那么我们就将函数集合 $\mathcal{F}$ 称为一个**$(n, m, \{w_1, w_2\})$-分离哈希族**，记作 SHF$(N; n, m, \{w_1, w_2\})$，其中 $N = |\mathcal{F}|$。

文献中常常采用阵列的观点研究哈希函数族。设 $\mathcal{F}$ 是如上定义的一个 SHF$(N; n, m, \{w_1, w_2\})$，那么我们可以建立一个阵列 $\mathtt{A} \in Y^{N \times n}$ 来表示这个 SHF。矩阵的行标是 $\mathcal{F}$ 中的函数，而列标是 X 中的元素。对于任意 $f \in \mathcal{F}$ 和 $x \in X$，阵列 A

在 (f,x) 位置上的值是 $\mathtt{A}(f,x)=f(x)\in Y$。将这个阵列中的列向量作为码字集合，我们就得到了**分离码**的概念。

分离哈希族与防诬陷码之间具有如下广为所知的联系。

引理 6.6：*存在一个* $\mathtt{SHF}(n;M,q,\{1,t\})$，*当且仅当存在一个* t-$\mathtt{FPC}(n,M,q)$。

由于 $\bar{t}$-可分码的长度 n 与多媒体内容中正交基信号的数目相关，而码字个数则和可以分配到数字指纹的授权用户数目相关，我们应该努力构造具有更多码字的 $\bar{t}$-可分码，同时保持码长相对较小。这促使我们研究 $\bar{t}$-SC(n,M,q) 的码字个数的理论上界。令 $M(\bar{t},n,q)$ 表示所有长度为 n 的 q 元 $\bar{t}$-可分码中最大的码字个数。我们将一个含有 $M=M(\bar{t},n,q)$ 个码字的可分码 $\bar{t}$-SC(n,M,q) 称为是**最优的**。

我们可以利用 $\bar{t}$-可分码与 t-防诬陷码，以及与分离哈希族之间的关系，获得关于 $M(\bar{t},n,q)$ 的上界信息。

引理 6.7 (Blackburn **与** Wild[14], Staddon **等**[153])：*设正整数* $t\geq 2$。*如果存在一个* $\mathtt{SHF}(n;M,q,\{1,t\})$，*那么* $M\leq t(q^{\lceil\frac{n}{t}\rceil}-1)$。

引理 6.8 (Blackburn[13])：*设正整数* t,n,M,q *满足* $t\geq 2,n\geq 2$，*并且* $M>q$。*如果存在一个防诬陷码* t-$\mathtt{FPC}(n,M,q)$，*那么*

$$M\leq \max\left\{q^{\lceil\frac{n}{t}\rceil},r(q^{\lceil\frac{n}{t}\rceil}-1)+(t-r)(q^{\lfloor\frac{n}{t}\rfloor}-1)\right\}\ ,$$

其中整数 $r\in\{0,1,\ldots,t-1\}$，*使得* $n\equiv r\pmod t$。

注意到，对于几乎所有参数，上式右侧中的第二项都较大一些。

我们已经知道，如果存在一个可分码 $\bar{t}$-SC(n,M,q)，那么就存在一个防诬陷码 $(t-1)$-FPC(n,M,q)，或者等价的，一个分离哈希族 SHF$(n;M,q,\{1,t-1\})$。下面的结论直接来自于前面两个引理。

定理 6.9：*如果存在一个* $\bar{t}$-$\mathtt{SC}(n,M,q)$，*那么*

$$M\leq (t-1)(q^{\lceil\frac{n}{t-1}\rceil}-1)\ 。$$

特别的，如果 $M>q$，*并且整数* $r\in\{0,1,\ldots,t-2\}$ *使得* $n\equiv r\pmod{t-1}$，*那么*

$$M\leq \max\{q^{\lceil\frac{n}{t-1}\rceil},r(q^{\lceil\frac{n}{t-1}\rceil}-1)+(t-1-r)(q^{\lfloor\frac{n}{t-1}\rfloor}-1)\}\ 。$$

Cheng 等人认为，上述从防诬陷码得到的上界通常不是紧的，我们还应该可以从可分码的定义出发得到关于 $M(\bar{t},n,q)$ 上界更好的估计。

引理 6.10 (Cheng 等[35])：如果存在一个可分码 $\bar{t}$-SC(n,M,q)，那么 $M \leq q^{n-1} + \frac{q(q-1)}{2}$。

我们可以看到，这一上界中并没有用到参数 t 的信息。通过简单计算就能发现，当 $t=2$ 的时候，这一由定义直接得到的上界比之前从防诬陷码或分离哈希族得到的上界要更紧。但当 t 变大时，这一结论不再成立。

对于 $t=2$ 并且 $n=2$ 的特殊情况，这一直接上界可以被进一步的改进。

引理 6.11 (Cheng 等[35])：设 $t=2$，并且 $n=2$。那么

$$M(\overline{2},2,q) \leq qk+s\ ,$$

其中

$$\begin{aligned} k &= \left\lfloor \frac{1+\sqrt{4q-3}}{2} \right\rfloor , \\ s &= \begin{cases} 0 & \text{若 } k^2-k+1=q \\ \left\lfloor \frac{q(q-1-k^2+k)}{2k} \right\rfloor & \text{若 } k^2-k+2 \leq q \leq k^2 \\ \left\lfloor \frac{qk}{(k+1)^2-q} \right\rfloor & \text{若 } k^2+1 \leq q \leq k^2+k\ 。 \end{cases} \end{aligned}$$

定理 6.12：当 $n=2$，并且 $\frac{1+\sqrt{4q-3}}{2}$ 是一个素数幂时，存在一个到达引理 6.11 中上界的可分码 $\overline{2}$-SC$(2,M,q)$。当 $n=3$ 时，对于任意 q，都存在一个到达引理 6.10 中上界的可分码 $\overline{2}$-SC$(3,M,q)$。

6.3 改进 $\overline{2}$-可分码的上界

6.3.1 坐标分组法

通过下面的“坐标分组”方法，我们可以将可分码的长度进行缩短，但付出的代价是字母表的变大。这一想法的证明非常简单，但我们将会看到它非常有用。

引理 6.13：假设整数 $c \geq 2$。如果存在一个可分码 $\bar{t}$-SC(n, M, q)，那么就存在一个可分码 $\bar{t}$-SC$(\lceil \frac{n}{c} \rceil, M, q^c)$。

证明. 设 $\mathcal{C} = \{\mathtt{c}_1, \ldots, \mathtt{c}_M\}$ 是一个 $\bar{t}$-SC(n, M, q)。通过向 $\mathcal{C}$ 中每个码字的后面添加上任意 $n' \geq 0$ 个字母，我们就可以得到一个 $(n+n', M, q)$-码 $\mathcal{C}'$。容易验证，如果 $\mathcal{C}'$ 也是一个 $\bar{t}$-可分码。因此我们不妨假设 $c \mid n$，否则设置 n 为 $c \cdot \lceil \frac{n}{c} \rceil$。

令 $d := \lceil \frac{n}{c} \rceil$。考虑坐标集合 $[n] := \{1, 2, \ldots, n\}$ 的 d 个子集 $A_1, \ldots, A_d$，使得每个集合的大小都是 $|A_u| = c, u \in [d]$，并且 $A_1 \cup \cdots \cup A_d = \{1, 2, \ldots, n\}$，即 $A_1, \ldots, A_d$ 是 $[n]$ 的一个平均划分。我们定义字母表 Q^c 上的一个 (d, M, q^c)-码 $\mathcal{C}' = \{\mathtt{c}'_1, \ldots, \mathtt{c}'_M\}$，其中任意一个码字 $\mathtt{c}'_i$ 第 u 位上的取值是 $\mathtt{c}'_i(u) = (\mathtt{c}_i(j) \mid j \in A_u) \in Q^c$，其中 $i \in [M]$，$u \in [d]$。

设 $\mathcal{C}'$ 中任意两个码字集合 $\mathcal{C}'_1, \mathcal{C}'_2 \subseteq \mathcal{C}'$，满足 $\mathcal{C}'_1 \leq t, \mathcal{C}'_2 \leq t$，并且 $\mathcal{C}'_1 \neq \mathcal{C}'_2$。令 $\mathcal{C}_1 = \{\mathtt{c} \in \mathcal{C} \mid \mathtt{c}' \in \mathcal{C}'_1\}$，并令 $\mathcal{C}_2 = \{\mathtt{c} \in \mathcal{C} \mid \mathtt{c}' \in \mathcal{C}'_2\}$。容易验证 $\mathcal{C}_1 \leq t, \mathcal{C}_2 \leq t$，并且 $\mathcal{C}_1 \neq \mathcal{C}_2$。由于 $\mathcal{C}$ 是一个 $\bar{t}$-可分码，根据定义，存在一个坐标 $i \in \{1, 2, \ldots, n\}$，使得 $\mathcal{C}_1(i) \neq \mathcal{C}_2(i)$。不妨假设 i 在某个集合 A_u 内，其中 $1 \leq u \leq d$。此时，我们有不等式 $\mathcal{C}'_1(u) \neq \mathcal{C}'_2(u)$ 成立，即 $\mathcal{C}'$ 也是一个 $\bar{t}$-可分码。 □

Cheng 等人在文章中提问，是否可以从可分码 $\bar{t}$-SC(n, M, q) 的定义本身出发，得到更多关于 $M(\bar{t}, n, q)$ 的上界信息。在此，我们就给出一个 $t = 2$ 时的改进方法。通过在引理 6.13 中选取 $c = \lceil \frac{n}{3} \rceil$，我们就可以得到下面的结果。我们选择 c 的这一值是由于此时长度为 $\lceil \frac{n}{c} \rceil = 3$ 的最优可分码 $\bar{2}$-SC$(3, M, q)$ 对于任意的 q 都是存在的，它含有 $M = M(\bar{2}, 3, q) = q^2 + \frac{q(q-1)}{2}$ 个码字。

定理 6.14：如果存在一个可分码 $\bar{2}$-SC(n, M, q)，那么其中的码字个数

$$\begin{aligned} M &\leq q^{2 \cdot \lceil n/3 \rceil} + \frac{q^{\lceil n/3 \rceil}(q^{\lceil n/3 \rceil} - 1)}{2} \\ &= \frac{1}{2}\left(3q^{2 \cdot \lceil n/3 \rceil} - q^{\lceil n/3 \rceil}\right) 。 \end{aligned}$$

我们同样可以将引理 6.13 应用到引理 6.11 中。

定理 6.15：令 $c = \lceil n/2 \rceil$，那么

$$M(\bar{2}, n, q) \leq q^c \cdot k + s \,,$$

其中

$$k = \left\lfloor \frac{1+\sqrt{4q^c-3}}{2} \right\rfloor ,$$

并且

$$s = \begin{cases} 0 & \text{若 } k^2-k+1 = q^c \\ \left\lfloor \frac{q^c(q^c-1-k^2+k)}{2k} \right\rfloor & \text{若} k^2-k+2 \le q^c \le k^2 \\ \left\lfloor \frac{q^c k}{(k+1)^2-q^c} \right\rfloor & \text{若} k^2+1 \le q^c \le k^2+k \text{。} \end{cases}$$

6.3.2 线性 $\overline{2}$-可分码的上界

在这一小节之中，我们将考虑一类特殊的可分码的上界，这就是线性可分码。我们将假设 q 是一个素数幂，而将字母表 Q 取为有限域 $\mathbb{F}_q$。如果一个可分码 $\overline{t}$-SC(n,M,q) 同时也构成了向量空间 $\mathbb{F}_q^n$ 中的一个 m-维线性子空间，那么我们就称它是一个**线性可分码**，此时码字个数 $M = q^m$。

令 $\mathcal{C}$ 是一个线性 $\overline{t}$-SC(n,M,q)。不失一般性的，我们可以假设不存在坐标 i，$1 \le i \le n$，使得每个码字在这一位都取“0”。否则，我们可以将所有码字中的这一位都删去，得到仍然是一个 $\overline{t}$-SC$(n-1,M,q)$。此时，线性码 $\mathcal{C}$ 的生成矩阵 $\mathtt{G}$ 可以具有分块形式：

$$\mathtt{G} = [\mathtt{I} \mid \mathtt{A}]_{m\times n} ,$$

其中 $\mathtt{I}$ 是 m 阶单位矩阵，而 $\mathtt{A}$ 是 $\mathbb{F}_q$ 上的一个 $m \times (n-m)$ 阶矩阵。

对于任意集合 $Z \subseteq [m]$，我们定义一个 $k = n-m$ 阶方阵 $\mathtt{I}(Z)$ 为：

$$\mathtt{I}(Z)(i,j) := \begin{cases} 1 & \text{若 } i = j \in Z \\ 0 & \text{其它情况，} \end{cases}$$

其中 $i,j \in [k]$。

引理 6.16：设 $\mathcal{C} \subseteq \mathbb{F}_q^n$ 是一个大小为 q^m 的线性码，它的生成矩阵是 $\mathtt{G} = [\mathtt{I} \mid \mathtt{A}]_{m\times n}$。如果存在集合 $Z \subseteq [n-m]$，以及两个非零向量 $\mathtt{v}_1, \mathtt{v}_2 \in \mathbb{F}_q^m$，使得 $\mathtt{supp}(\mathtt{v}_1) \cap \mathtt{supp}(\mathtt{v}_2) = \emptyset$，并且

$$\mathtt{v}_1^T \cdot \mathtt{A} \cdot \mathtt{I}(Z) = \mathtt{v}_2^T \cdot \mathtt{A} \cdot \mathtt{I}(\overline{Z}) = 0 ,$$

其中 $\overline{Z}=[n-m]\backslash Z$ 表示 Z 的补集。那么 $\mathcal{C}$ 不是一个线性可分码 $\overline{2}$-$\mathtt{SC}(n,q^m,q)$。

证明. 将长度为 m 的全零向量记作 $\mathtt{0}$。我们考虑如下两个不相交的码字集合 $\mathcal{C}_1=\{\mathtt{0}^T\cdot\mathtt{G},(\mathtt{v}_1+\mathtt{v}_2)^T\cdot G\}$ 和 $\mathcal{C}_2=\{\mathtt{v}_1^T\cdot\mathtt{G},\mathtt{v}_2^T\cdot\mathtt{G}\}$。分别计算其中的码字，我们得到：

$$(\mathtt{v}_1^T\cdot\mathtt{G})(i) = \begin{cases}\mathtt{v}_1(i) & \text{若 } i\in\mathtt{supp}(\mathtt{v}_1)\\ (\mathtt{v}_1^T\cdot\mathtt{A}\cdot\mathtt{I}(\overline{Z}))(i-m) & \text{若 } i-m\in\overline{Z}\\ 0 & \text{其它情况;}\end{cases}$$

$$(\mathtt{v}_2^T\cdot\mathtt{G})(i) = \begin{cases}\mathtt{v}_2(i) & \text{若 } i\in\mathtt{supp}(\mathtt{v}_2)\\ (\mathtt{v}_2^T\cdot\mathtt{A}\cdot\mathtt{I}(Z))(i-m) & \text{若 } i-m\in Z\\ 0 & \text{其它情况;}\end{cases}$$

$$((\mathtt{v}_1+\mathtt{v}_2)^T\cdot\mathtt{G})(i) = \begin{cases}\mathtt{v}_1(i) & \text{若 } i\in\mathtt{supp}(\mathtt{v}_1)\\ \mathtt{v}_2(i) & \text{若 } i\in\mathtt{supp}(\mathtt{v}_2)\\ (\mathtt{v}_1^T\cdot\mathtt{A}\cdot\mathtt{I}(\overline{Z}))(i-m) & \text{若 } i-m\in\overline{Z}\\ (\mathtt{v}_2^T\cdot\mathtt{A}\cdot\mathtt{I}(Z))(i-m) & \text{若 } i-m\in Z\\ 0 & \text{其它情况。}\end{cases}$$

从而我们得知 $\mathtt{desc}(\mathcal{C}_1)=\mathtt{desc}(\mathcal{C}_2)$，即 $\mathcal{C}$ 不是一个 $\overline{2}$-可分码。 □

定理 6.17：设 $\mathcal{C}\subseteq\mathbb{F}_q^n$ 是一个大小为 q^m 的线性码，它的生成矩阵是 $\mathtt{G}=[\mathtt{I}\mid\mathtt{A}]_{m\times n}$。如果 $\mathtt{rank}(\mathtt{A})<m-1$，那么 $\mathcal{C}$ 不是一个线性 $\overline{2}$-可分码。

证明. 由于 $\mathtt{rank}(\mathtt{A})<m-1$，存在非零向量 $\mathtt{v}_1\in\mathbb{F}_q^m$，使得 $1\le|\mathtt{supp}(\mathtt{v}_1)|\le m-1$，并且 $\mathtt{v}_1^T\cdot\mathtt{A}=\mathtt{0}$。选取 $Z=[k]$，并令 $\mathtt{v}_2$ 为 $\mathbb{F}_q^m$ 中任意一个满足条件 $\mathtt{supp}(\mathtt{v}_1)\cap\mathtt{supp}(\mathtt{v}_2)=\emptyset$ 非零向量。容易检查，这样选取的集合 Z 与向量 $\mathtt{v}_1,\mathtt{v}_2$ 满足前一引理中的条件。因此 $\mathcal{C}$ 不是一个线性可分码 $\overline{2}$-$\mathtt{SC}(n,M,q)$。 □

推论 6.18：对于任意正整数 m，如果存在线性可分码 $\overline{2}$-$\mathtt{SC}(n,q^m,q)$，那么 $m\le(n+1)/2$。

证明. 如果 $m > (n+1)/2$，那么生成矩阵 $\mathtt{G} = [\mathtt{I} \mid \mathtt{A}]$ 中 $\mathtt{A}$ 的大小为 $m \times k$，其中 $k = n - m < m - 1$。此时必然有 $\mathtt{rank}(\mathtt{A}) < m - 1$，因此不存在这样的线性可分码 $\overline{2}$-SC(n, q^m, q)。 □

需要指出的是，定理 6.17 和推论 6.18 都要严格弱于引理 6.16，参见下面的这个例子。

例 6.19. 令 $m = k = 2, n = m + k = 4, q = 2$。设 $\mathtt{I}$ 是一个 m 阶单位矩阵。如果我们选取 $Z = \{2\}$，和 $\mathtt{v}_1 = (10), \mathtt{v}_2 = (01)$。那么对于任意 $m \times k$ 阶矩阵 $\mathtt{A}$，都有 $\mathtt{v}_1^T \cdot \mathtt{A} \cdot \mathtt{I}(Z) = \mathtt{v}_2^T \cdot \mathtt{A} \cdot \mathtt{I}(\overline{Z}) = \mathtt{0}$。特别的，我们让 $\mathtt{A} = \mathtt{I}$，那么由引理 6.16 得知，以生成矩阵 $[\mathtt{I} \mid \mathtt{I}]$ 的行空间为码字的线性码不是一个 $\overline{2}$-可分码。这一事实也可以通过直接验证得到：选择两个不交的码字集合 $\mathcal{C}_1 = \{(0000), (1111)\}$ 和 $\mathcal{C}_2 = \{(1010), (0101)\}$，则 $\mathtt{desc}(\mathcal{C}_1) = \{0,1\}^4 = \mathtt{desc}(\mathcal{C}_2)$。但是定理 6.17 和推论 6.18 都不能直接排除这个例子。

事实上，推论 6.18 中的上界在下面定理的意义上紧的。

定理 6.20：设正整数 d 满足条件 $2d + 1 \leq q + 1$，那么存在一个最优线性可分码 $\overline{2}$-SC$(2d+1, q^{d+1}, q)$。

证明. 记 $M = q^{d+1}$。令 $\mathcal{F} = \{f_1, \ldots, f_M\}$ 是有限域 $\mathbb{F}_q$ 上所有次数不超过 d 的多项式全体所组成的集合。令集合 $R \subseteq \mathbb{F}_q \cup \{\infty\}$，使得 $|R| = 2d + 1 \leq q + 1$。定义一个向量集合 $\mathcal{C} \subseteq \mathbb{F}_q^{|R|}$，其中的向量用集合 $\mathcal{F}$ 中的函数标记，而每个向量的坐标用 R 中的元素标记。对于任意 $f \in \mathcal{F}$，向量 $\mathtt{v}_f$ 在第 r 位，$1 \leq r \leq 2d+1$，上的取值是：

$$\mathtt{v}_f(r) = \begin{cases} f(r) & \text{若 } r \in R \setminus \{\infty\} \\ a_d & \text{若 } r = \infty \end{cases},$$

其中 a_d 是多项式 $f(x) = \sum_{i=0}^{d} a_i x^i$ 中 d 次项的系数。容易看出，这样得到的集合 $\mathcal{C}$ 是向量空间 $\mathbb{F}_q^{2d+1}$ 的一个线性子空间。

我们断言：$\mathcal{C}$ 是一个防诬陷码 2-FPC$(2d+1, q^{d+1}, q)$。事实上，由于 $\mathcal{F}$ 中函数的次数不超过 d，所以 $\mathcal{C}$ 中任意两个不同码字至多只在 d 个位置上的取值相同，进而 $\mathcal{C}$ 中不含重复的码字，即 $|\mathcal{C}| = q^{d+1}$。并且，对于任意三个两两不同的码字 $\mathtt{x}, \mathtt{v}_1, \mathtt{v}_2$，都

至少存在一个位置 $r \in R$，使得 $\mathtt{x}(r) \notin \{\mathtt{v}_1(r), \mathtt{v}_2(r)\}$。根据定义，$\mathcal{C}$ 就是一个防诬陷码 2-FPC$(2d+1, q^{d+1}, q)$。

我们已经知道每个 t-FPC(n, M, q) 就是一个 $\bar{t}$-SC(n, M, q)，所以 $\mathcal{C}$ 这样一个 $\bar{2}$-SC$(2d+1, q^{d+1}, q)$ 的码字个数达到了推论 6.18 中的上界，因此它是最优线性可分码。 □

6.4 可分码的构造

定义 6.21. 设 $\mathcal{C}$ 是一个 (n, M, q)-码。如果对于任意两个码字集合 $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$，其中 $|\mathcal{C}_1| = a, |\mathcal{C}_2| = b$，并且 $|\mathcal{C}_1 \cap \mathcal{C}_2| = c$，均有性质 $\mathtt{desc}(\mathcal{C}_1) \neq \mathtt{desc}(\mathcal{C}_2)$ 成立。那么我们就称 $\mathcal{C}$ 是$(a, b; c)$-**可分的**，记作 $(a, b; c)$-SC(n, M, q)，

利用这一定义，一个 (n, M, q)-码 $\mathcal{C}$ 是 t-可分码当且仅当对于每个 $s = 0, 1, \ldots, t-1$，它都是 $(t, t; s)$-可分的。$\mathcal{C}$ 是 $\bar{t}$-可分码当且仅当对于任意 $1 \leq a < b \leq t$ 且 $0 \leq c \leq a$，和任意 $1 \leq a = b \leq t$ 且 $0 \leq c \leq a-1$，它都是 $(a, b; c)$-可分的。特别的，对于 $t = 2$，下面的引理将说明 $\mathcal{C}$ 是一个 $\bar{2}$-可分码当且仅当它同时是 $(1, 1; 0)$-可分的和 $(2, 2; 0)$-可分的，而不用考虑 $(2, 2; 1)$-可分性。

引理 6.22：一个 (n, M, q)-码 $\mathcal{C}$ 是 $\bar{2}$-可分码的充要条件是：

1. $\mathcal{C}$ 中不含重复的码字，即 $\mathcal{C}$ 是 $(1, 1; 0)$-可分的；并且
2. 对于任意两个不相交的码字集合 $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$，满足条件 $\mathcal{C}_1 \cap \mathcal{C}_2 = \emptyset$ 和 $|\mathcal{C}_1| = |\mathcal{C}_2| = 2$，均有 $\mathtt{desc}(\mathcal{C}_1) \neq \mathtt{desc}(\mathcal{C}_2)$；即 $\mathcal{C}$ 是 $(2, 2; 0)$-可分的。

证明. 由引理 6.3，必要性是显然的。下面证明充分性。

假设码 $\mathcal{C}$ 满足条件 1 和 2，但不是一个 $\bar{2}$-可分码。那么存在两个不同的码字子集合 $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$，$\mathcal{C}_1 \neq \mathcal{C}_2$ 并且 $|\mathcal{C}_1| \leq |\mathcal{C}_2| \leq 2$，使得 $\mathtt{desc}(\mathcal{C}_1) = \mathtt{desc}(\mathcal{C}_2)$。我们将一一分析 $\mathcal{C}_1$ 和 $\mathcal{C}_2$ 中码字的选取情况。（以下假设码字 $\mathtt{x}, \mathtt{y}, \mathtt{z}, \mathtt{v}$ 两两不同。）

- 若 $\mathcal{C}_1 = \{\mathtt{x}\}, \mathcal{C}_2 = \{\mathtt{y}\}$。那么由 $\mathtt{desc}(\mathcal{C}_1) = \mathtt{desc}(\mathcal{C}_2)$ 得出 $\mathtt{x} = \mathtt{y}$，这和我们的假设矛盾。

- 若 $\mathcal{C}_1=\{\mathtt{x}\},\mathcal{C}_2=\{\mathtt{x},\mathtt{y}\}$。那么由 $\mathtt{desc}(\mathcal{C}_1)=\mathtt{desc}(\mathcal{C}_2)$ 得出 $\mathtt{x}=\mathtt{y}$，这和条件 1 矛盾。

- 若 $\mathcal{C}_1=\{\mathtt{x}\},\mathcal{C}_2=\{\mathtt{y},\mathtt{z}\}$。那么由 $\mathtt{desc}(\mathcal{C}_1)=\mathtt{desc}(\mathcal{C}_2)$ 推出 $\mathtt{x}=\mathtt{y}=\mathtt{z}$，这也和条件 1 矛盾。

- 若 $\mathcal{C}_1=\{\mathtt{x},\mathtt{y}\},\mathcal{C}_2=\{\mathtt{x},\mathtt{z}\}$。那么由 $\mathtt{desc}(\mathcal{C}_1)=\mathtt{desc}(\mathcal{C}_2)$ 知道 $\mathtt{y}=\mathtt{z}$，这和假设 $\mathcal{C}_1\neq\mathcal{C}_2$ 矛盾。

- 若 $\mathcal{C}_1=\{\mathtt{x},\mathtt{y}\},\mathcal{C}_2=\{\mathtt{z},\mathtt{v}\}$。那么 $\mathtt{desc}(\mathcal{C}_1)=\mathtt{desc}(\mathcal{C}_2)$ 和条件 2 相矛盾。

因此，满足条件 1 和 2 的码 $\mathcal{C}$ 是一个 $\overline{2}$-可分码。 □

6.4.1 删除法

对于整数 a,b,c，我们假设 $a\geq 1,b\geq 1$，并且 $0\leq c\leq\min\{a,b\}$。我们用 $P_q(a,b;c)$ 表示向量空间 Q^{a+b-c} 中满足条件 $\{\mathtt{v}(i)\mid 1\leq i\leq a\}=\{\mathtt{v}(i)\mid a-c+1\leq i\leq a+b-c\}$ 的向量 $\mathtt{v}\in Q^{a+b-c}$ 的数目，其中 $q=|Q|$。我们还定义 $p_q(a,b;c):=P_q(a,b;c)/q^{a+b-c}$。例如，$P_q(1,1;0)=q,p_q(1,1;0)=1/q;P_q(2,2;0)=q(2q-1),p_q(2,2;0)=(2q-1)/q^3$。

我们将利用概率方法（Probabilistic Method）中著名的“删除法”（Deletion Method，或 Expurgation Method），来构造可分码 $\overline{2}$-SC(n,M,q)。读者可以参考相关文献中关于删除法在其它组合结构中的应用[158,159]。

定理 6.23：*存在一个 $\overline{2}$-$\mathtt{SC}(n,M,q)$，使得码字个数*

$$M\leq(\alpha-2^{n-3}\,\alpha^4)\,q^{\frac{2}{3}n}-2^{-1}\,\alpha^2\,q^{\frac{n}{3}}\ ,$$

其中 $0<\alpha<2^{1-\frac{n}{3}}$ 是一个常数。

证明. 假设 $\mathcal{C}$ 是一个随机的 (n,M,q)-码，其中每个码字在所有位置上的值都是互相独立且均匀的从字母表 Q 中随机选取的。对于两个码字集合 $\mathcal{C}_1,\mathcal{C}_2\subseteq\mathcal{C}$，我们定义一个随机变量

$$X(\mathcal{C}_1,\mathcal{C}_2)=\begin{cases}0 & \text{若 } \mathtt{desc}(\mathcal{C}_1)\neq\mathtt{desc}(\mathcal{C}_2)\\ 1 & \text{其它情况。}\end{cases}$$

对于非负整数 a,b,c，其中 $c \le \min\{a,b\}$，我们再定义另外一个随机变量 $X(a,b;c)$ 为

$$X(a,b;c) := \sum_{\mathcal{C}_1,\mathcal{C}_2 \subseteq \mathcal{C}} X(\mathcal{C}_1,\mathcal{C}_2)\ ,$$

其中的求和是对于所有满足条件 $|\mathcal{C}_1| = a, |\mathcal{C}_2| = b$，并且 $|\mathcal{C}_1 \cap \mathcal{C}_2| = c$ 的子集合 $\mathcal{C}_1$ 和 $\mathcal{C}_2$。

这两个随机变量的期望分别是

$$E[X(\mathcal{C}_1,\mathcal{C}_2)] = (p_q(a,b;c))^n$$

和

$$E[X(a,b;c)] = \begin{cases} \frac{1}{2}\cdot \binom{M}{a-c,a-c,c} \cdot (p_q(a,a;c))^n & \text{若 } a=b \\ \binom{M}{a-c,b-c,c} \cdot (p_q(a,b;c))^n & \text{其它情况。} \end{cases}$$

由于 $\mathcal{C}$ 是一个 $\overline{2}$-可分码的充要条件是 $\mathcal{C}$ 同时是 $(1,1;0)$-可分的和 $(2,2;0)$-可分的，我们令 $X = X(1,1;0) + X(2,2;0)$。那么

$$\begin{aligned} E[X] &= E[X(1,1;0)] + E[X(2,2;0)] \\ &= \frac{1}{2}\cdot \binom{M}{1,1} \cdot (p_q(1,1;0))^n + \frac{1}{2}\cdot \binom{M}{2,2} \cdot (p_q(2,2;0))^n \\ &\le \frac{1}{2}\cdot M^2 \cdot \left(\frac{1}{q}\right)^n + \frac{1}{2}\cdot \frac{M^4}{(2!)^2} \cdot \left(\frac{2q-1}{q^3}\right)^n \\ &\le \frac{M^2}{2}\cdot q^{-n} + \frac{M^4}{8}\cdot \left(\frac{q^2}{2}\right)^{-n} \ 。 \end{aligned}$$

现在，我们选取常数 α，使得 $0 < \alpha < 2^{1-\frac{n}{3}}$。并且我们总可以选择这样的 M 使得下面的不等式成立：

$$M \le \alpha\, q^{\frac{2}{3}n}\ 。$$

容易验证，此时

$$E[X] \ \le\ 2^{-1}\,\alpha^2\, q^{n/3} + 2^{n-3}\,\alpha^4\, q^{2n/3}\ 。$$

因此，我们总可以从 $\mathcal{C}$ 中删除至多 $E[X]$ 个码字，使得剩下的所有码字组成的集合是一个可分码 $\overline{2}$-SC(n,M',q)，其码字个数 M' 满足：

$$\begin{aligned} M' &\ge M - E[X] \\ &\ge (\alpha - 2^{n-3}\,\alpha^4)\, q^{\frac{2}{3}n} - 2^{-1}\,\alpha^2\, q^{\frac{n}{3}}\ 。 \end{aligned}$$

这正是我们需要的结果。 □

推论 6.24: 当常数 $\alpha = 2^{(1-n)/3}$ 时, 系数 $\alpha - 2^{n-3}\alpha^4$ 达到最大值 $3 \cdot 2^{-(n+5)/3}$。因此

$$M(\overline{2}, n, q) \geq 3 \cdot 2^{-(n+5)/3} q^{2n/3} - 2^{-(2n+1)/3} q^{n/3} \text{ 。}$$

将上面的结果和定理 6.14 中的上界相比较。对于给定的码字长度 n, 当字母表大小 q 趋向无穷时, 通过删除法得到的可分码下界码率 $R_{\overline{2},n} := \left(\log_q M\right)/n = 2/3$。这一结果和定理 6.14 中的码率相一致, 即通过删除法得到的可分码码类是渐近最优的。

6.4.2 Stein–Lovász 定理

在这一小节中, 我们将通过 Stein–Lovász 定理给出 $\overline{t}$-SC(n, M, q) 的一个确定性构造方法。这个定理最初是由 Stein 和 Lavász 在研究组合覆盖问题时独立提出的[123,154]。在 1996 年, Cohen 等人将这一定理应用到编码问题之中[47]。不同于传统的概率方法, Stein–Lovász 定理采用了构造性的方法, 获得组合结构的存在性结论[55,115]。我们现将定理陈述如下。

定理 6.25 (Cohen 等[47]): 设 A 是一个 $N \times M$ 阶二元矩阵。若矩阵 A 中的每一行至少含有 v 个“1”, 并且每列至多含有 a 个“1”。那么存在 A 的一个 $N \times K$ 阶子矩阵 S, 其中

$$\begin{aligned} K &\leq N/a + (M/v)\ln a \\ &\leq (M/v)(1 + \ln a)\text{ ,} \end{aligned}$$

使得 S 中的每一行都至少含有一个“1”。

我们将展示两个从 Stein–Lovász 定理构造可分码的方法, 第一个是由定义直接构造 $\overline{2}$-可分码, 第二个方法则是通过构造分离哈希族来导出一般 $\overline{t}$-可分码的存在性结论。

定理 6.26: 存在一个可分码 $\overline{2}$-SC(n, M, q), 使得

$$n \leq \frac{q^3}{q^3 - 2q + 1}\left(1 + \ln\left(\frac{1}{2}\binom{M}{1,1} + \frac{1}{2}\binom{M}{2,2}\right)\right) \text{ 。}$$

证明. 我们将构造一个适当的二元矩阵 A，从而利用 Stein–Lovász 定理获得我们需要的结论。

令 $r_1 = \binom{M}{1,1}/2$，和 $r_2 = \binom{M}{2,2}/2$。那么在自然数 $1, 2, \ldots, r_1$ 与 $[M] := \{1, 2, \ldots, M\}$ 的 2-子集 $\{c_1, c_2 \in [M] \mid c_1 \neq c_2\}$ 之间有着自然的一一对应，并且在自然数 $r_1 + 1, r_1 + 2, \ldots, r_1 + r_2$ 与集合 $[M]$ 中的无序不交 2-子集对 $\{B_1, B_2 \subseteq [M] \mid |B_1| = |B_2| = 2, B_1 \cap B_2 = \emptyset\}$ 之间也是一一对应的。另一方面，自然数 $1, 2, \ldots, q^M$ 也与向量空间 Q^M 中的所有向量存在一一对应关系。我们将构造的矩阵 A 的行数就是 $r_1 + r_2$，而列数就是 q^M。

对于矩阵 A 中的任意一行 $i, 1 \leq i \leq r_1 + r_2$，和任意一列 $j, 1 \leq j \leq q^M$，矩阵元素 $\mathtt{A}(i, j)$ 按下面的方式取值。我们不妨设列标 j 对应的 Q^M 中的向量是 v。如果 $1 \leq i \leq r_1$，我们假设行标对应的 $[M]$ 中的 2-子集是 $\{c_1, c_2\}$，此时 $\mathtt{A}(i, j) = 1$ 当且仅当 $\mathtt{v}(c_1) \neq \mathtt{v}(c_2)$。而如果 $r_1 + 1 \leq i \leq r_1 + r_2$，记 i 对应的 $[M]$ 中的无序 2-子集对是 (B_1, B_2)，那么定义 $\mathtt{A}(i, j) = 1$ 当且仅当 $\{\mathtt{v}(k) \mid k \in B_1\} \neq \{\mathtt{v}(k) \mid k \in B_2\}$。

显然，在矩阵 A 中的前 r_1 行中，每行都含有 $v_1 = q^M - P_q(1, 1; 0) \cdot q^{M-2} = (q-1)\, q^{M-1}$ 个“1”，而在矩阵的后 r_2 行中，每行都含有 $v_2 = q^M - P_q(2, 2; 0) \cdot q^{M-4} = (q^3 - 2q + 1)\, q^{M-3}$ 个“1”。由于对应任意正整数 q，v_1 都不大于 v_2，所以矩阵 A 中每一行都至少含有 $v = \max\{v_1, v_2\} = v_2$ 个“1”。另一方面，矩阵每一列中“1”的数目不会多于所有行数 $a = r_1 + r_2$。根据 Stein–Lovász 定理，我们知道存在 A 的一个 $(r_1 + r_2) \times n$ 阶子矩阵 S，使得其中每一行至少含有一个“1”，这里

$$\begin{aligned} n &\leq \frac{q^M}{v}\,(1 + \ln a) \\ &= \frac{q^3}{q^3 - 2q + 1}\left(1 + \ln\left(\frac{1}{2}\binom{M}{1,1} + \frac{1}{2}\binom{M}{2,2}\right)\right) 。 \end{aligned}$$

接着，我们将从矩阵 S 中构造一个 (n, M, q)-码 $\mathcal{C}$。为此，我们先从 S 出发构造另外一个 $n \times M$ 阶矩阵 H，方法如下。由于矩阵 S 的每一列都是从 A 中提取的，我们将 S 的所有列（在 A 中）对应的那些 M 长 q 元向量集合记作 $\mathcal{B} \subseteq Q^M$，$|\mathcal{B}| = n$。那么矩阵 H 就是以这些 $\mathcal{B}$ 中的向量作为行向量形成的 $n \times M$ 阶 q 元矩阵。我们需要的 (n, M, q)-码 $\mathcal{C}$ 就是由矩阵 H 的所有列向量组成的集合。

最后我们说明，这样得到的 $\mathcal{C}$ 确实是一个 $\overline{2}$-$\mathrm{SC}(n, M, q)$。根据引理 6.22，码 $\mathcal{C}$ 是 $\overline{2}$-可分码当且仅当它同时 $(1, 1; 0)$-可分的和 $(2, 2; 0)$-可分的。对于 $\mathcal{C}$ 中任意两个码字

$\mathtt{c}_1, \mathtt{c}_2$，它们对应于矩阵 H 中的两列 $1 \le h_1, h_2 \le M$，而集合 $\{h_1, h_2\}$ 标记了 S 中的某一行 r，$1 \le r \le r_1$。由于 S 的每行中至少含有一个“1”，我们假设第 r 行的“1”出现在第 s 列，而这一列对应的 Q^M 中的向量是 v。那么 v 是矩阵 H 中的某一行 r_h。根据这些矩阵的定义，这一行中第 h_1 列和第 h_2 列位置上的元素是不同的，即码字 $\mathtt{c}_1$ 和 $\mathtt{c}_2$ 在第 r_h 位上的值不同。所以码 $\mathcal{C}$ 中没有重复的码字，即是 $(1,1;0)$-可分的。同理可以证明 $\mathcal{C}$ 也是 $(2,2;0)$-可分的。因此，$\mathcal{C}$ 确实一个 $\overline{2}$-SC(n,M,q)。 □

第二个由 Stein–Loveász 定理获得的可分码下界是通过将其应用于分离哈希族得到的。为此，我们需要定义图的染色多项式的概念。

定义 6.27. 设 $G=(V,E)$ 是一个简单图，m 是一个正整数。我们用 $\Pi(G,m)$ 表示用 m 种颜色为图 G 中顶点染色的方法数，使得图中任意一条边上两个顶点的颜色都不相同。这样得到的 $\Pi(G,m)$ 被称之为图 G 的**染色多项式**（Chromatic Polynomial），它是关于 m 的 $|V|$ 次多项式。

定理 6.28 (Deng 等[55])：*存在一个分离哈希族* $\mathtt{SHF}(n;M,q,\{w_1,w_2\})$，*使得*

$$n \le \frac{q^{w_1+w_2}}{\Pi(K_{w_1,w_2},q)}\left(1+\ln\binom{M}{w_1,w_2}\right),$$

其中 K_{w_1,w_2} *表示两个部分分别含有* w_1 *和* w_2 *个顶点的完全二部图。*

由于我们可以从分离哈希族 SHF$(n;M,q,\{1,t\})$ 中导出可分码 $\bar{t}$-SC(n,M,q)，而容易计算二部图 $K_{1,t}$ 的染色多项式是 $\Pi(K_{1,t},q)=q\,(q-1)^t$。所以我们可以有下面的结论。

推论 6.29：*存在一个可分码* $\bar{t}$-$\mathtt{SC}(n,M,q)$ *使得*

$$n \le \frac{q^t}{(q-1)^t}\left(1+\ln\binom{M}{1,t}\right)。$$

7 压缩感知矩阵的构造

7.1 压缩感知理论简介

压缩感知(Compressed Sensing,CS)是近年来快速发展的一个信息学领域,其主要目的是使用尽量少的检测次数来获取一个信号的性质。对于一个离散时间信号 $x \in \mathbb{R}^n$,我们希望利用 m 个线性投影来测量 x。我们将由这 m 个线性投影组成的 $m \times n$ 阶矩阵 Φ 称为**感知矩阵**(Sensing Matrix),并把结果 $y = \Phi x$ 称为**测量向量**(Measurement Vector)。我们关心的问题是,给定一个测量向量 y,我们如何可以将原始信号 x 从 $y = \Phi x$ 这一结果中恢复出来?我们都知道,当 $m < n$ 时,这样的恢复问题通常是病态的。但 Donoho[67] 和 Candés 等[27] 的工作充分利用了稀疏信号的性质,使得我们能用次数很少的测量就能得到关于原来的稀疏信号的信息。这一问题可以描述成如下的寻找线性方程 $y = \Phi x$ 稀疏解的问题:

$$\min_{x \in \mathbb{R}^n} \|x\|_0 \quad \text{s.t.:}\ \Phi x = y\,。 \tag{7.1}$$

这样的 ℓ_0-最小化问题是一个组合问题,其求解通常是 NP-困难的[128]。但是,压缩感知理论提供了一个强大的方法,可以利用高效的算法恢复出稀疏信号 x,并且所用到的测量次数 m 远小于 n。

如果一个信号 x 中至多有 k 个非零分量,那么我们称 x 是**k-稀疏的**。选择一个 $m \times n$ 阶的随机 Gauss 矩阵 Φ 作为感知矩阵,其中每个位置上的值都相互独立的,并且服从相同参数的 Gauss 分布。压缩感知理论在本质上有两种方式来恢复一个 k-稀疏的信号 x。第一种方法是考虑对式子(7.1)中的问题进行**凸松弛**(Convex Relaxation)。令 $m \geq Ck\log(n/m)$,其中 C 是一个常数,我们可以利用求解如下的 ℓ_1-最小化问题来以非常高的概率完全恢复出 x[29]:

$$\min_{x \in \mathbb{R}^n} \|x\|_1 \quad \text{s.t.:}\ \Phi x = y。 \tag{7.2}$$

第二种方法是寻找贪婪算法求解 ℓ_0-最小化问题(7.1)。这类方法中最具有代表性的是正交匹配追踪(Orthogonal Matching Pursuit,OMP)算法。如果测量的次数

$m \geq C'k\log(n/\delta)$，其中 C' 是一个常数，并且 $\delta \in (0, 0.36)$，那么 OMP 算法能以超过 $1-2\delta$ 的概率从式（7.1）中恢复出信号 x。如果读者想了解更多关于 OMP 算法及其各种改进，或其和它类似的贪婪算法，可以参见相关文献[52,129,130,174]。总而言之，我们可以通过选取适当的感知矩阵，将稀疏信号恢复问题转换为一个具有高效求解算法的优化问题。

为了确定什么样的矩阵更适合作为感知矩阵，我们需要一些判断标准。Candés 和 Tao[28] 深刻洞察了传感矩阵的本质，提出了现在被广泛接受的判断标准：受限等距性（Restricted Isometry Property，RIP）。

定义 7.1. 设 Φ 是一个 $m \times n$ 阶矩阵。如果存在一个常数 $0 \leq \delta_k < 1$，使得对于任意 k-稀疏的信号 $x \in \mathbb{R}^n$，均有如下不等式成立：

$$(1-\delta_k)\|x\|_2^2 \leq \|\Phi x\|_2^2 \leq (1+\delta_k)\|x\|_2^2 \text{。}$$

则我们称矩阵 Φ 满足k 阶受限等距性。我们还将满足上式的最小非负实数 δ_k 称为k 阶受限等距常数（Restricted Isometry Constant，RIC）。

换句话说，如果矩阵 Φ 满足 k 阶受限等距性，那么矩阵中的任意 k 个列向量表现出来的性质，都非常接近于一个正交系统（Orthogonal System）。我们指出，受限等距性是保证稀疏信号可以通过求解 ℓ_1-最小化问题完全恢复的一个充分条件[26]。如果一个感知矩阵满足受限等距性，并且其受限等距常数足够小，那么 OMP 算法就可以准确恢复出稀疏信号[53]。

感知矩阵的构造是压缩感知理论中的核心问题。假设一个 k-稀疏信号 $x \in \mathbb{R}^n$ 可以通过 m 次测量被完全恢复，那么关于稀疏性的一个上界是：

$$k \leq C \cdot \frac{m}{\log(n/m)} \text{，}$$

其中 C 是一个常数[44]。研究者们已经构造出达到这一上界的随机感知矩阵，它们能够以很高概率恢复出 k-稀疏的信号[29]。事实上，如果矩阵的每个元素都随机的从一个给定的概率分布中选取，那么得到的矩阵以很高的概率满足 k 阶受限等距性，使得 $k \leq Cm/\log(n/m)$，其中 C 是某个常数[8]。但同时，随机矩阵也有一些缺点。首先，保存一个随机感知矩阵需要耗费巨大的存储空间。其次，我们还没有有效的算法来

检验一个随机矩阵是否满足受限等距性，甚至不能确认它能以很高的概率满足 RIP 性质。与随机感知矩阵相比，确定性构造方法可以摆脱这些不足之处。确定性感知矩阵可以在使用的时候再由算法生成，从而节省了存储空间。另一方面，通过研究确定性矩阵中的具体结构，我们可以针对性的设计出更加高效的快速恢复算法。

对于一个由列向量 $\mathtt{a}_1, \mathtt{a}_2, \ldots, \mathtt{a}_n$ 组成的矩阵 Φ，我们定义 Φ 的**相关性**（Coherence）为：

$$\mu(\Phi) = \max_{i \neq j} \frac{|\langle \mathtt{a}_i, \mathtt{a}_j \rangle|}{\|\mathtt{a}_i\| \cdot \|\mathtt{a}_j\|}, \quad \text{对于所有 } 1 \leq i, j \leq n。$$

由于低相关性可以导出受限等距性，所以这一性质在压缩感知矩阵的确定性构造方法研究中扮演核心角色。

引理 7.2 (Bourgain 等[22])：假设矩阵 Φ 的相关性为 μ。那么对于所有 $k < 1/\mu + 1$，矩阵 Φ 都满足 k 阶受限等距性，其受限等距常数 $\delta_k \leq \mu(k-1)$。

对于任意 $m \times n$ 阶（复）矩阵 Φ，它的相关性 $\mu(\Phi)$ 必须满足著名的 Welch 界：

$$\mu(\Phi) \geq \sqrt{\frac{n}{m(n-m)}}。$$

这说明，所有基于相关性的确定性构造方法得到的感知矩阵，都只能满足阶为 $k = O(m^{1/2})$ 的受限等距性。

近几年中，有一些使用受限等距性作为判定标准的确定性构造方法被提出，其中大部分都是基于相关性的。DeVore 使用有限域 $\mathbb{F}_p$ 上不大于 r 次的多项式来构造大小为 $p^2 \times p^{r+1}$ 的二元感知矩阵[56]。这些矩阵的相关性为 r/p，它们满足 $k < p/r + 1$ 阶受限等距性。Amini 和 Marvasti 则使用最小距离很大的 BCH 码作为工具[4]，构造了相关性为 $\mu \leq (2^{l-j} - 1)/(2^l - 1)$ 的两极矩阵（Bipolar Matrix），其中含有 $2^l - 1$ 行和 $2^{O(2^{(l-j)}(\ln j)/j)}$ 列，其 RIP 阶数是 $k \leq 2^j + 1$。之后，这一方法被推广到使用 p 元 BCH 码构造出复数域上的感知矩阵[5]。Bourgain 等人使用加法组合学（Additive Combinatorics）中的技巧构造出大小为 $m \times n$ 的感知矩阵，使得其受限等距性的阶是 $k \geq m^{1/2+\epsilon}$，并且 $n^{1-\epsilon} \leq m \leq n$，其中 $\epsilon > 0$ 是任意选定的实数[22]。值得一提的是，这一方法突破了基于相关性构造中的天然屏障 $k = O(m^{1/2})$。此外，还有研究者得到了相关性 $\mu = O(\frac{\log n \log\log n}{m})^{1/3}$ 的感知矩阵，它的 RIP 阶数是 $k = \Omega(\frac{m}{\log n \log\log n})^{1/3}$。

另一方面，同样有不基于受限等距性的确定性构造方法被提出。Applebaum 等人使用线性调频脉冲序列（Chirp Sequence）构造了复数域上的感知矩阵，并提出了一个快速恢复算法[7]。Howard 等人利用压缩感知和编码理论间的联系，使用二阶 Reed–Muller 码及其子码构造了实数域上的感知矩阵[98]。而 Calderbank 等人总结了以上两种方法，提出了感知矩阵的统计受限等距性（Statistical RIP）[25]。这一性质比 RIP 弱，它保证了除指数小（Exponentially Small）的部分之外，几乎所有稀疏信号的可恢复性。Berinde 等人从非平衡扩展图（Unbalanced Expander Graph）这样一类具有良好扩展性质的二部图出发，构造出二元的感知矩阵并设计了一个组合的恢复算法[11]。Indyk 利用哈希函数（Hash Functions）和提取图（Extractor Graph）也得到了二元的感知矩阵[100]。

在本章中，我们将着眼于利用有限域上的代数曲线来构造确定性的感知矩阵。这一构造方法可以看作是 DeVore 工作的推广[56]。我们的想法来源于 Goppa，他曾经使用有限域上的代数曲线构造出性能优异的线性码[91]。他的这一想法后来得到充分发展，人们将这些从代数曲线中构造出来的纠错码称为**代数几何码**（Algebraic Geometry Code）[15,175,184]。关于代数曲线和函数域的知识将为我们构造感知矩阵提供巨大的灵活性[131,156]。通过选取合适的曲线，我们能够得到比 DeVore 的方法中更好的感知矩阵。

本章余下的部分组织顺序如下。第 7.2 节中，我们将介绍有限域上的代数曲线及其代数函数域的背景知识。特别的，我们将会介绍 Goppa 是如何把 Reed–Solomon 码推广成为代数几何码的，这正是我们思想的出发点。在第 7.3 节中，我们首先回顾了 DeVore 的构造方法。随后我们将详细说明如何利用代数曲线来构造感知矩阵。最后，我们会在第 7.4 节中展示一些例子，以说明其性能。

7.2 准备知识

7.2.1 代数曲线简介

在本章中，我们将遵循 Xing 等人文章中关于代数曲线与代数函数域的记号[184]。令 $\mathbb{F}_q$ 表示含有 q 个元素的有限域，其中 q 是一个素数幂。我们将有限域 $\mathbb{F}_q$ 上的一个**绝对不可约**（Absolute Irreducible）代数曲线 $\mathcal{X}$ 写为 $\mathcal{X}/\mathbb{F}_q$，将曲线 $\mathcal{X}$ 的**亏格**（Genus）

记作 $g = g(\mathcal{X})$。我们把曲线上那些坐标都落在有限域 $\mathbb{F}_{q^r}$ 中的点称为$\mathbb{F}_{q^r}$-**有理点**，$r \geq 1$。一般的，我们将 $\mathbb{F}_q$-有理点简称为 $\mathcal{X}/\mathbb{F}_q$ 上的**有理点**。

曲线 $\mathcal{X}$ 的**除子**（Divisor）D 指的是这样的形式和

$$D = \sum_{P \in \mathcal{X}} n_P P,$$

其中对于每个点 P，系数 n_P 都是整数，并且所有这些系数中只有有限个的取值不为零。如果每一个系数 n_P 都是非负的，那么我们称除子 D 是一个**有效除子**，记为 $D \geq 0$。除子 D 的**支撑集**（Support Set）是形式和中所有那些系数 n_P 不等于零的点 P 构成的集合，记成 $\mathtt{supp}(D)$。除子 D 的**度数**（Degree）由下式给出

$$\deg(D) = \sum_{P \in \mathcal{X}} n_P \deg(P)。$$

注意到，所有有理点 $P \in \mathcal{X}$ 的度数都等于 1。

我们用记号 $\mathbb{F}_q(\mathcal{X})$ 表示曲线 $\mathcal{X}$ 的函数域，将其中的每个元素称为**函数**（Function）。对于一个函数 $x \in \mathbb{F}_q(\mathcal{X})$，它对应的**主除子**（Principal Divisor）是

$$\mathtt{div}(x) = \sum_{P \in \mathcal{X}} \nu_P(x)\, P,$$

其中 ν_P 是对应于点 P 的**正规化离散赋值**（Normalized Discrete Valuation）。可以证明，对于任意函数 x，这些赋值函数在 x 的值 $\nu_P(x)$ 只有有限个是非零的。另外，赋值 $\nu_P(x) \geq 0$ 意味着 $x(P) \in \overline{\mathbb{F}}_q$，其中 $\overline{\mathbb{F}}_q$ 表示有限域 $\mathbb{F}_q$ 的**代数闭包**（Algebraic Closure）。特别的，如果 P 是一个有理点，那么 $x(P) \in \mathbb{F}_q$。

给定代数曲线 $\mathcal{X}/\mathbb{F}_q$ 的一个除子 G，我们定义 G 的 Riemann–Roch **空间**为

$$\mathcal{L}(G) = \{x \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\} \mid \mathtt{div}(x) + G \geq 0\} \cup \{0\}。$$

这样定义的 $\mathcal{L}(G)$ 是有限域 $\mathbb{F}_q$ 上的一个有限维向量空间，我们将它的维数记作 $\ell(G)$。

定理 7.3 (Riemann–Roch **定理**):

$$\ell(G) \geq \deg(G) - 1 + g\ 。$$

并且当 $\deg(G) \geq 2g - 1$ 时，等号成立。

7.2.2 代数几何码

我们将遵循 Stichtenoth 书中关于代数几何码的表述方式[156]。假设集合 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 是有限域 $\mathbb{F}_q$ 中的一个 n 元子集。令 $\mathcal{P}_k$ 表示由 $\mathbb{F}_q$ 上所有度数不超过 $k-1$ 的多项式构成的集合：

$$\mathcal{P}_k = \{f \in \mathbb{F}_q[X] \mid \deg f \leq k-1\}。$$

容易验证，这样定义的 $\mathcal{P}_k$ 是 $\mathbb{F}_q$ 上的一个 k-维向量空间。

定义一个赋值映射 $\phi : \mathcal{P}_k \to \mathbb{F}_q^n$

$$\phi(f) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \in \mathbb{F}_q^n。$$

那么 ϕ 的象空间就是一个长度为 n，维数为 k 的 q 元线性码 $\mathcal{C}_k$

$$\mathcal{C}_k = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f \in \mathcal{P}_k\}。$$

这就是著名的 Reed–Solomon 码。由于 $f \in \mathcal{P}_k$ 最多只有 $k-1$ 个零点，$\mathcal{C}$ 的最小距离 $d \geq n+1-k$。另一方面，线性码的 Singleton 界告诉我们 $d \leq n+1-k$。因此，Reed–Solomon 码是一类极大距离可分（Maximum Distance Separable，MDS）码。

代数几何码是 Reed–Solomon 码的自然推广。我们只需对上面的构造方法做出适当的调整，就能得到代数几何码。具体说来，我们将把有限域中的子集合换成代数曲线上的一些有理点，并用某个除子 G 的 Riemann–Roch 空间 $\mathcal{L}(G)$ 来代替向量空间 $\mathcal{P}_k$。

考虑一条亏格为 g 的代数曲线 $\mathcal{X}/\mathbb{F}_q$。令 $P_1, P_2, \ldots, P_n$ 是它上面的 n 个不同的有理点。假设除子 G 满足条件 $g \leq \deg(G) < n$，并且 $\mathtt{supp}(G) \cap \{P_1, P_2, \ldots, P_n\} = \emptyset$。那么对于所有 $f \in \mathcal{L}(G)$ 和 $1 \leq i \leq n$，均有赋值 $\nu_{P_i}(f) \geq 0$，因此 $f(P_i) \in \mathbb{F}_q$。我们定义一个赋值映射 $\psi : \mathcal{L}(G) \to \mathbb{F}_q^n$

$$\psi(f) = (f(P_1), f(P_2), \ldots, f(P_n)) \in \mathbb{F}_q^n。$$

我们把 ψ 的象空间记作 $\mathcal{C}(P_1, P_2, \ldots, P_n; G)$，这就是一个代数几何码。下面的定理描述了这个码的参数。

定理 7.4 (Tsfasman 与 Vladut[175]): 如上构造的 $\mathcal{C}(P_1, P_2, \ldots, P_n; G)$ 是有限域 $\mathbb{F}_q$ 上的一个 $[n, k, d]_q$ 线性码，它的参数满足下面的不等式：

$$\begin{aligned} k &\geq \deg(G) + 1 - g, \quad \text{并且} \\ d &\geq n - \deg(G)。 \end{aligned}$$

特别的，当 $\deg(G) \geq 2g - 1$ 时，码的维数 $k = \deg(G) + 1 - g$。

7.3 主要结果

7.3.1 回顾 DeVore 的构造法

在 DeVore 的文章中，有限域上的多项式被用来构造感知矩阵[56]。为了表述的简便，我们用素数阶的有限域作为例子说明他的方法。对于素数幂的情形，方法是完全类似的。令 $\mathbb{F}_p$ 为 p 阶有限域，其中 p 是一个素数。用 $\mathcal{P}_r$ 表示 $\mathbb{F}_p$ 上所有次数不超过 $r-1$ 的多项式组成的集合，$|\mathcal{P}_r| = p^r$。

我们将笛卡儿积 $\mathbb{F}_p \times \mathbb{F}_p$ 中的所有元素按照字母顺序进行排列：$(0,0)$, $(0,1), \ldots, (p-1, p-1)$。对于 $\mathcal{P}_r$ 中的任意一个多项式 f，我们定义一个二元列向量 v_f，它的行用 $\mathbb{F}_p \times \mathbb{F}_p$ 中的元素标记。这个二元列向量 v_f 的形式是：

$$(f_{0,0}, \ldots, f_{0,p-1}, f_{1,0}, \ldots, f_{1,p-1}, \ldots, f_{p-1,0}, \ldots, f_{p-1,p-1})^T,$$

其中

$$f_{i,j} = \begin{cases} 1 & \text{若 } f(i) = j \\ 0 & \text{其它情况}, \end{cases}$$

这里 $0 \leq i, j \leq p-1$。此时，对于任意一个多项式 $f \in \mathcal{P}_r$，二元列向量 v_f 中都恰好含有 p 个“1”。事实上，我们可以将 f 看成从 $\mathbb{F}_p$ 到 $\mathbb{F}_p$ 的映射，那么 v_f 就是将 f 的象表示成了二元列向量的形式。我们将所有这些列向量 $\{\mathrm{v}_f \mid f \in \mathcal{P}_r\}$ 排在一起，组成了一个 $p^2 \times p^r$ 阶的矩阵 Φ_0。

定理 7.5 (DeVore[56]): 令 $\Phi = \frac{1}{\sqrt{p}}\Phi_0$，那么 Φ 是一个相关性为 $\mu(\Phi) \leq (r-1)/p$ 的感知矩阵。

显然，DeVore 的这个构造方法也适用于一般的有限域 $\mathbb{F}_q$ 的情形，其中 q 是一个素数幂。在这个构造中，每个多项式提供了感知矩阵中的一列。而在 Reed–Solomon 码的构造中，每个多项式提供了一个码字。这样的相似性促使我们去寻找感知矩阵新的构造方法。同 Reed–Solomon 码的推广类似，我们将在下一小节中给出一个基于有限域上代数曲线构造感知矩阵的方法。

7.3.2 我们的构造方法

假设 q 是一个素数幂，而 $\mathcal{X}$ 是有限域 $\mathbb{F}_q$ 上的一条代数曲线。令集合 $\mathcal{P}$ 由一些曲线 $\mathcal{X}/\mathbb{F}_q$ 上有理点构成。选择一个除子 G，使得它满足条件 $\deg(G) < |\mathcal{P}|$ 和 $\mathrm{supp}(G) \cap \mathcal{P} = \emptyset$。那么 G 的 Riemann–Roch 空间 $\mathcal{L}(G)$ 是 $\mathbb{F}_q$ 上的一个 $\ell(G)$-维向量空间。由于 $\mathrm{supp}(G) \cap \mathcal{P} = \emptyset$，所以对于任意有理点 $P \in \mathcal{P}$ 和函数 $f \in \mathcal{L}(G)$，我们均有 $f(P) \in \mathbb{F}_q$。与 DeVore 构造方法类似的，我们也可以将函数 f 表示成一个二元列向量 v_f，它的行用集合 $\mathcal{P} \times \mathbb{F}_q$ 中的元素标记。对于位置 $(P, a) \in \mathcal{P} \times \mathbb{F}_q$，向量 v_f 在这一位置上的取值是

$$f_{P,a} = \begin{cases} 1 & \text{若 } f(P) = a \\ 0 & \text{其它情况。} \end{cases}$$

注意到，对于每个 $f \in \mathcal{L}(G)$，向量 v_f 中都有 $|\mathcal{P}|$ 个非零元。

令 $m = |\mathcal{P}| \times q, n = q^{\ell(G)}$。所有的这些列向量 $\{\mathrm{v}_f \mid f \in \mathcal{L}(G)\}$ 构成了一个 $m \times n$ 阶的矩阵 Φ_0。我们有如下的定理。

定理 7.6：令 $\Phi = \frac{1}{\sqrt{|\mathcal{P}|}}\Phi_0$。那么 Φ 是一个相关性为 $\mu(\Phi) \leq \deg(G)/|\mathcal{P}|$ 的感知矩阵。

证明. 对于 $\mathcal{L}(G)$ 中任意两个不同的函数 f 和 g，列向量 $\frac{1}{\sqrt{|\mathcal{P}|}}\mathrm{v}_f$ 和 $\frac{1}{\sqrt{|\mathcal{P}|}}\mathrm{v}_g$ 是 Φ 中的两个单位长度的列向量。令 z 为向量 v_f 和 v_g 的内积：

$$\begin{aligned} z &= |\langle \mathrm{v}_f, \mathrm{v}_g \rangle| \\ &= |\{P \in \mathcal{P} \mid f(P) = g(P)\}| \\ &= |\{P \in \mathcal{P} \mid (f-g)(P) = 0\}|。 \end{aligned}$$

对于函数 $f - g \in \mathcal{L}(G)$，假设它在 $\mathcal{P}$ 中的 z 个零点是 $P_{i_1}, P_{i_2}, \ldots, P_{i_z}$。那么我们

有

$$0 \neq f - g \in \mathcal{L}(G - P_{i_1} - \cdots - P_{i_z}) \text{ 。}$$

这意味着

$$\deg(G - P_{i_1} - \cdots - P_{i_z}) = \deg(G) - z \geq 0 \text{ 。}$$

所以，

$$\frac{1}{\sqrt{|\mathcal{P}|}} \mathrm{v}_f \cdot \frac{1}{\sqrt{|\mathcal{P}|}} \mathrm{v}_g = \frac{z}{|\mathcal{P}|} \leq \frac{\deg(G)}{|\mathcal{P}|} \text{ 。}$$

即感知矩阵 Φ 的相关性 $\mu(\Phi)$ 满足 $\mu(\Phi) \leq \deg(G)/|\mathcal{P}|$。 □

从以下的角度出发，我们的这个定理可以看作是 DeVore 构造法的一个自然推广。如果选取代数曲线 $\mathcal{X}$ 为 $\mathbb{F}_q$ 上的**射影直线**（Projective Line），那么函数域 $\mathbb{F}_q(\mathcal{X})$ 就同构于有理函数域 $\mathbb{F}_q(x)$。在曲线 $\mathcal{X}$ 上共有 $q+1$ 个有理点，它们分别是一个无穷点 ∞ 和 q 个有限点，后者与有限域 $\mathbb{F}_q$ 中的 q 个元素之间存在自然的一一对应关系。设置除子 $G = (r-1) \cdot \infty$，那么 Riemann–Roch 空间 $\mathcal{L}(G) = \mathcal{L}((r-1)\infty)$ 将与第 7.3.1 节中的向量空间 $\mathcal{P}_r$ 正好相同。这时，我们的方法得到的矩阵和 DeVore 的一模一样。

我们还可以注意到，DeVore 的构造方法可以从有限域 $\mathbb{F}_q$ 扩展到它的有限次扩域 $\mathbb{F}_{q^r}$ 上，$r \geq 1$，即用域 $\mathbb{F}_{q^r}$ 上的元素和多项式来标记行列。这样得到的感知矩阵具有更大的规模。类似的，我们也可以使用代数曲线的语言来说明这一推广。我们可以在构造中将有理点换成 $\mathbb{F}_{q^r}$-有理点，并将 Riemann–Roch 空间看作是有限域 $\mathbb{F}_{q^r}$ 上的向量空间。具体的例子我们将在下节中介绍。

我们的构造方法需要用到代数曲线上有理点的信息，还需要对于给定除子的 Riemann–Roch 空间的详细刻画。关于前者，许多数学软件中都已经内置了相关函数可以明确的给出这些有理点，例如 `Magma` 和 `Sage` 等。另一方面，Hess 提出过一个简单高效的算法，可以确定出给定除子的 Riemann–Roch 空间[97]。总之，我们构造方法中所需要用到的这些信息都可以简单的获取到，并且构造的实现也非常容易。

7.4 一些例子

7.4.1 椭圆曲线的例子

有限域上的椭圆曲线由于其在构造简洁优雅的密码系统中的应用而为大家所熟知[109]。对于一条椭圆曲线 $\mathcal{X}/\mathbb{F}_q$，我们用 N_r 表示曲线上 $\mathbb{F}_{q^r}$-有理点的数目。利用 Schoof 算法[144]，N_1 可以很容易的计算出来。而对于一般 N_r，我们可以利用下面的引理就简单的推得。

引理 7.7 (Washington[181])：*设 a 是一个整数，使得 $N_1 = q+1-a$。如果二次方程 $X^2 - aX + q$ 在复数域上的分解式为*

$$X^2 - aX + q = (X-\alpha)(X-\beta) \ ,$$

其中 $\alpha, \beta \in \mathbb{C}$。那么 $N_r = q^r + 1 - (\alpha^r + \beta^r)$。

正如在上一节最后所指出，我们可以利用曲线上的 $\mathbb{F}_{q^r}$-有理点来代替 $\mathbb{F}_q$-有理点，从而构造出更大规模的感知矩阵。例如，给定一条有限域 $\mathbb{F}_2$ 上的椭圆曲线

$$y^2 + y = x^3 + x \ , \tag{7.3}$$

这条曲线的亏格 $g = g(\mathcal{X}) = 1$。曲线上的 $\mathbb{F}_{2^r}$-有理点数目 N_r 已经在 Stichtenoth 的书中被计算出来[156]：

$$N_r = \begin{cases} 2^r + 1 & \text{若 } r \equiv 2, 6 \pmod 8 \\ 2^r + 1 + 2\cdot 2^{r/2} & \text{若 } r \equiv 4 \pmod 8 \\ 2^r + 1 - 2\cdot 2^{r/2} & \text{若 } r \equiv 0 \pmod 8 \\ 2^r + 1 + 2^{(r+1)/2} & \text{若 } r \equiv 1, 7 \pmod 8 \\ 2^r + 1 - 2^{(r+1)/2} & \text{若 } r \equiv 3, 5 \pmod 8 \ 。 \end{cases}$$

我们用 ∞ 表示椭圆曲线 $\mathcal{X}$ 在无穷远处的有理点，并用 $\mathcal{P}$ 表示剩下的有限处的所有有理点组成的集合，那么 $|\mathcal{P}| = N_r - 1$。对于一个整数 $s, 1 = 2g-1 \le s < N_r - 1$，我们令 $G = s\cdot\infty$。由定理 7.6，我们可以得到一个大小为 $m_0 \times n_0$ 的感知矩阵 Φ_0，其中

$$m_0 = 2^r \cdot (N_r - 1), \quad n_0 = 2^{r\ell(G)} = 2^{rs} \ 。$$

由于 Φ_0 相关性为 $\mu(\Phi_0) \leq s/(N_r-1)$，所以它满足阶为 $k_0 < (N_r-1)/s+1$ 的受限等距性。

特别的，当 $r \equiv 4 \pmod 8$ 时，我们得到的 $m \times n$ 阶感知矩阵 Φ 的参数为：

$$m = 2^r(2^r + 2^{1+r/2})\,, \quad n = 2^{rs}\,, \quad \mu(\Phi) \leq s/(2^r + 2^{1+r/2})\,,$$

其中 s 是满足 $1 \leq s < 2^r + 2^{1+r/2}$ 的任意一个整数。Φ 满足的受限等距性阶数为 $k < (2^r+2^{1+r/2})/s+1$。注意到 $\log_2 m = 3r/2 + \log_2(2^{r/2}+2) \approx 2r$，并且 $\log_2 n = rs$，感知矩阵 Φ 可以被用来准确恢复的信号的稀疏度为

$$k \leq \frac{(\sqrt{m} + 2\sqrt[4]{m})\log m}{2\log n}\,。$$

同时注意到 DeVore 构造出的感知矩阵可以恢复的信号的稀疏度是

$$k \leq \frac{\sqrt{m}\log m}{2\log(n/m)}\,。$$

对于给定相同的测量次数 m，当信号长度 n 足够大时，我们构造出的感知矩阵对于完全恢复条件下信号的稀疏度要求更低。与此同时，我们可以通过适当的调节 r 和 s 的选取值，得到一组不同的感知矩阵。

现在，我们再来通过数值模拟，比较一下椭圆曲线构造的感知矩阵和 Gauss 随机矩阵之间的信号恢复能力。对于一个信号 x，我们选用 OMP 算法求解 ℓ_0-最小化问题（7.1），并将得到的解记作 $x^\star$。定义信号 x 的恢复信噪比（Signal-to-Noise Ratio，SNR）为

$$\mathrm{SNR}(x) = 10 \cdot \log_{10}\left(\frac{\|x\|_2}{\|x - x^*\|_2}\right)\ \mathrm{dB}\,。$$

如果信噪比 $\mathrm{SNR}(x)$ 不小于 100 dB，那么我们就称信号 x 被完美恢复出来了。

将式子（7.3）表示的椭圆曲线写成如下的射影形式：

$$y^2z + yz^2 = x^3 + xz^2。 \tag{7.4}$$

令 $r=2$，曲线（7.4）上的所有有限的 $\mathbb{F}_4$-有理点组成了集合

$$\{[0,0,1],[0,1,1],[1,0,1],[1,1,1]\},$$

而唯一一个无穷远点 ∞ 的坐标是 $[0,1,0]$。假如我们选取 $s=3$，那么 Riemann–Roch 空间 $\mathcal{L}(3\cdot\infty)$ 将是有限域 $\mathbb{F}_4$ 上的一个 3-维向量空间，它的一组基是 $\{1,x,y\}$。由定

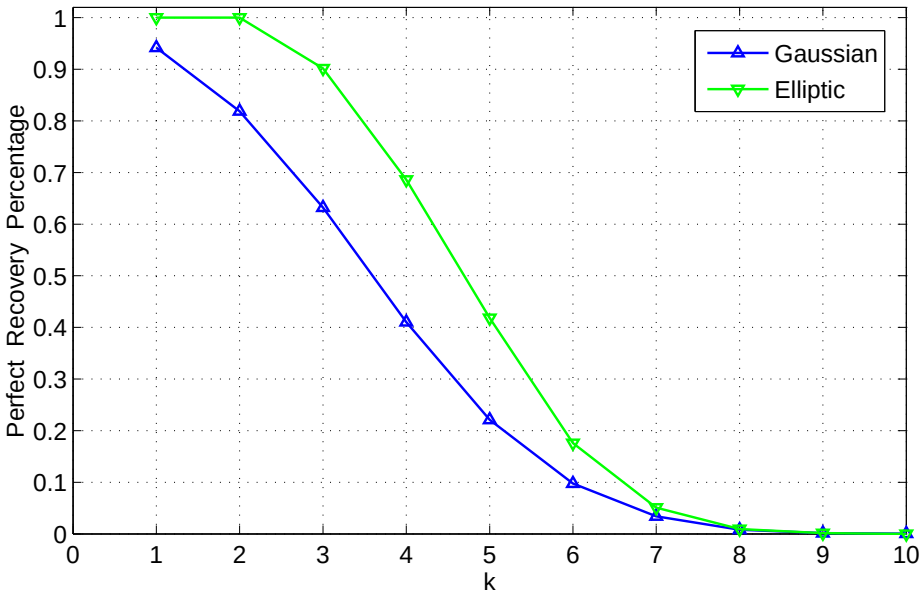

图 7.1　16×64 阶感知矩阵的完美恢复率比较

图中为大小是 16×64 的 Gauss 随机矩阵和椭圆曲线 $y^2 + y = x^3 + x$ 导出矩阵的完美恢复率对比。对于每个稀疏度 k，我们都模拟了 5000 次输入信号来计算比例。

理 7.6，我们得到一个大小为 16×64 的感知矩阵。图 7.1 展示了对于不同稀疏度的信号，这个矩阵与 Gauss 随机矩阵的完美恢复比例的对比情况。对于每个稀疏度 k，我们都随机选取了 5000 个信号进行模拟，从而得到完美恢复的比例。可以看到，由椭圆曲线（7.3）生成的矩阵比 Gauss 矩阵具有更高的完美恢复率。

类似的，通过选取 $r = 3$ 和 $s = 3$，我们可以得到一个 32×512 阶的感知矩阵。图 7.2 中展示了这个矩阵和一个同样大小的 Gauss 随机矩阵的完美恢复率的对比。此时，由椭圆曲线（7.3）得到的矩阵和 Gauss 矩阵的恢复率基本相同。考虑到确定性构造方法对比随机构造的优势，椭圆曲线构造的感知矩阵比 Gauss 矩阵具有更大的实用性。

7.4.2　Hermite 曲线的例子

由定理 7.6，我们可以得到相关性为 $\mu \leq \deg(G)/|\mathcal{P}|$ 的感知矩阵，其中 $\mathcal{P}$ 是曲线 $\mathcal{X}$ 中的一些有理点组成的集合。因此，我们我们关心那些具有很多有理点的曲线。

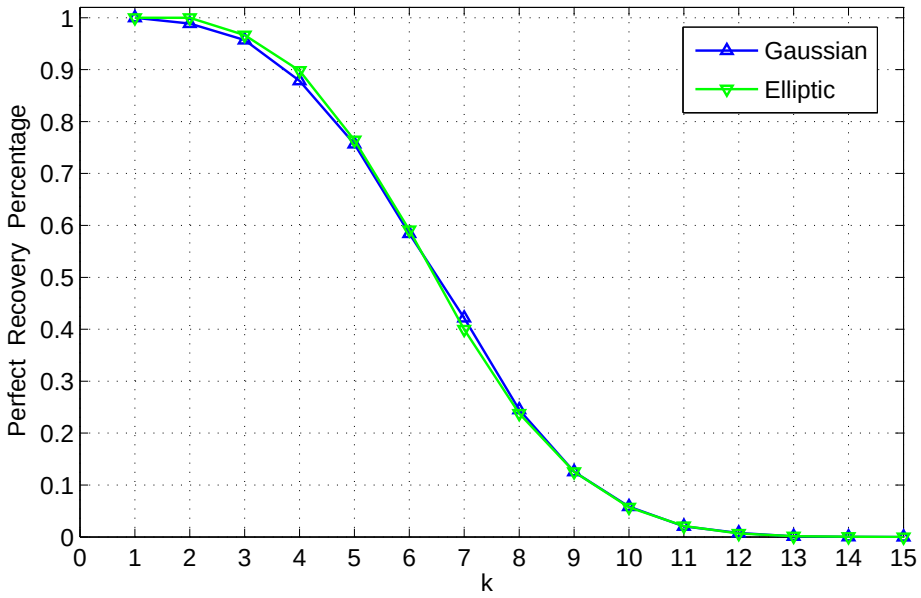

图 7.2　32×512 阶感知矩阵的完美恢复率比较

图中为大小是 32×512 的 Gauss 随机矩阵和椭圆曲线 $y^2 + y = x^3 + x$ 导出矩阵的完美恢复率对比。对于每个稀疏度 k，我们都模拟了 5000 次输入信号来计算比例。

此时相关性的上界就能尽可能的小。但一般来说，一条曲线上有理点的数目是有一定限制的。

定理 7.8 (Hasse–Weil **定理**)：令 $\mathcal{X}$ 是有限域 $\mathbb{F}_q$ 上一条亏格为 g 的代数曲线。那么 $\mathcal{X}$ 上的有理点的数目 $N(\mathcal{X})$ 满足不等式

$$|N(\mathcal{X}) - q - 1| \leq 2\,g\,\sqrt{q}\,。$$

Hermite 曲线就是一类达到上述定理中的上界的代数曲线。令 q 是一个素数幂的平方，那么有限域 $\mathbb{F}_q$ 上的 Hermite 曲线 H_q 可以由以下的仿射方程给出：

$$y^{\sqrt{q}} + y = x^{\sqrt{q}+1}\,。$$

这条曲线的亏格是 $g = g(H_q) = (q - q^{1/2})/2$，并且曲线上有理点的个数是 $N(H_q) = q^{3/2} + 1$，详见相关文献[156]。我们可以注意到，$N(H_q)$ 达到了 Hasse–Weil 定理中的上界。

令 Q 是曲线 H_q 上由 $\mathbb{F}_q(x)$ 的无穷远点扩张生成的一个有理点。将 H_q 上其它所有有理点组成的集合记为 $\mathcal{P}$，那么 $|\mathcal{P}| = N(H_q) - 1 = q^{3/2}$。对于整数 s，

$q-q^{1/2}-1=2g-1\leq s<q^{3/2}$，我们设置 $G=s\cdot Q$。根据定理 7.6，我们得到一个 $m\times n$ 阶感知矩阵 Φ，其中

$$m=q^{5/2}\ ,\quad n=q^{s+1-(q-q^{1/2})/2}\ 。$$

矩阵 Φ 的相关性是 $\mu(\Phi)\leq s/q^{3/2}$，所以它满足阶为 $k<q^{3/2}/s+1$ 的受限等距性。即，感知矩阵 Φ 可以用来准确恢复的信号的稀疏度是

$$k\leq\frac{m^{3/5}}{\log_q n+(m^{2/5}-m^{1/5})/2}。$$

接下来，我们将把 Hermite 曲线得到的感知矩阵和 DeVore 构造的矩阵进行比较。假设 p 是一个素数幂，而 $q=p^4$。我们可以从 Hermite 曲线 H_q 出发，构造一个 $m_H\times n_H$ 阶的感知矩阵 Φ_H，使得

$$m_H=p^{10}\ ,\quad n_H=p^{4(s+1-g)}\ ,\quad \mu_H=s/p^6\ ,$$

其中亏格 $g=(p^4-p^2)/2$，而整数 s 满足 $p^4-p^2-1\leq s<p^6$。矩阵 Φ_H 的相关性 $\mu(\Phi_H)\leq\mu_H$。而通过 DeVore 的方法，我们可以得到一个 $m_D\times n_D$ 阶的感知矩阵 Φ_D，使得

$$m_D=p^{10}\ ,\quad n_D=p^{5(t+1)}\ ,\quad \mu_D=t/p^5\ ,$$

其中整数 t 满足 $1\leq t<p^5$。矩阵 Φ_D 的相关性 $\mu(\Phi_D)\leq\mu_D$。我们可以适当选取参数 s 和 t，使得

$$4(s+1-g)=5(t+1)\ 。$$

此时两个矩阵 Φ_H 和 Φ_D 具有相同的大小。我们将比较两个矩阵的相关性的上界，即 μ_H 和 μ_D：

$$\begin{aligned}\frac{\mu_H}{\mu_D}&=\frac{1}{p}\cdot\frac{s}{t}\\&=\begin{cases}\Theta(p^{3-\eta}) & 若\ t=\Theta(p^{\eta}),0\leq\eta<3\\ \frac{1}{2c} & 若\ t=\Theta(p^3)=cp^3+o(p^3),c\neq 0\\ \Theta(p^{-\epsilon}) & 若\ t=\Theta(p^{3+\epsilon}),0<\epsilon\leq 2\ 。\end{cases}\end{aligned}$$

从相关性的角度看来，当 $t = \Theta(p^{3+\epsilon})$ 时，我们的矩阵在渐近意义下优于 DeVore 的。事实上，Amini 与 Marvasti 已经证明了，对于二元矩阵，当 $t = o(p^{2.5})$ 时 DeVore 构造的矩阵在渐近意义下是最优的[4]。而我们构造出来的二元矩阵在参数 $t > p^3/2$ 时比 DeVore 的更加好。

8 讨论与展望

本文总结了作者在攻读博士学位期间的大部分工作。这些工作的共同特色是从组合数学的观点出发，考察在现代通信理论和信息学中具有重要理论和应用价值的几类编码问题。

在第 2 章中，我们追寻 Ding 等人关于差集导出循环码，以及 Lander 等人关于对称矩阵导出子模码的想法，研究了从差集的轨道矩阵构造线性码码链的问题。正如我们的例子所展示的，这样的方法可以得到很多最优线性码。虽然受限于计算能力，得到的这些最优码还没有新的参数。但是，我们依然相信这一方法是获得新参数最优码的一个不错的候选。

另一方面，正如 Lander 指出子模码链可以看作对称设计的不变量，我们的想法也可以在研究差集的同构问题中发挥作用。例如我们可以将五类不等价的 $(511, 255, 127)$-循环 Hadamard 差集根据它们导出的码序列进行进一步的分类。我们希望这一从码的反馈可以在今后差集的理论研究中得到应用。

第 3 章中研究了具有快速迭代译码算法的 LDPC 码。利用循环群上的差矩阵，我们得到的 LDPC 码同时具有正则性和拟循环性，可以进一步降低编码译码过程中的时间复杂度。与文献中从其它组合结构得到的码进行数值比较后发现，我们的方案在性能上与前人结果非常接近，但具有更大的灵活性，可以选择的参数更广。

受限于软件模拟的精度，我们还不能很好地考察所得到的 LDPC 码所具有的最低误码率等性质，而国际上领先团队已经拥有专门的硬件来对 LDPC 码进行精确的模拟分析。下一阶段可行的方向是，进一步从组合结构的性质出发，通过理论研究 LDPC 码的陷阱集（Trapping Set）和停止集（Stopping Set）等影响差错平底的子结构，并改进现有的组合构造方法。

在第 4 章里，我们通过将置换码对应到 Cayley 图上的顶点独立集，从而利用图论中的方法对置换码的下界进行估计。我们的结果不但改进了一些小参数时的已知结果，还在渐近意义下将传统的 Gilbert–Varshamov 型下界提高了 $\Omega(\ln(n))$ 倍。

虽然码和独立集间具有自然的关联，但问题的难点在于选取合适的图论参数进

行分析和计算。因此,我们也可以考虑从图的其它性质入手,继续改进置换码的上下界估计。另一个有意思的研究课题是考虑其它度量下的置换码。这一问题具有实际的工程学背景,并且相关的工作才刚刚起步,是一个很好的话题。

第 5 章中,我们探讨了一类参数的最优常重复合码构造问题。2008 年,Chee 等人确定了重量为 3 时,所有长度和距离的最优三元常重复合码所含的码字个数。而我们在这章中,构造出了重量为 4 且最小距离为 5 时,所有长度的最优三元常重复合码。这里用到的主要工具是三类,即短码字的直接构造,可分组码,和大量的组合递归方法。

除了我们的工作以外,也有学者考虑了其它参数的情况,但整个问题距离完全解决还很遥远。事实上,每一类参数下最优码的确定都是极其困难的。这一方面是由于递归方法的缺乏,另一方面是受限于短码字直接构造所需的巨大计算量。因此,无论是新方法的提出,还是新码类的构造,都将是十分有意义的。

第 6 章讨论了 $\overline{2}$-可分码的存在性问题。我们首先利用坐标分组法,大幅改进了上界。接着,我们进一步降低了线性可分码的上界,并且利用正交表构造出了达到最优的无穷码类。最后我们分别使用随机方法和确定性方法获得了可分码的一些下界结果。其中,删除法构造的码和我们改进后的上界具有相同的渐近阶。

这一章中的内容和之前 Cheng 等人的工作仅仅只是数字指纹组合构造系列问题的一个引子,还有许多课题需要做更加深入的研究。可分码的几个有意思的前进方向是:一般长度和字母表上最优 $\overline{2}$-可分码的确定和构造;当 $t \geq 3$ 时,$\overline{t}$-可分码的上下界估计;配合可分码追踪罪犯的算法研究等。当然,更有意义的问题还包括从防合谋的要求出发,导出其它的组合结构与相关追踪算法。

在第 7 章中,我们介绍了一个利用有限域上的代数曲线构造二元感知矩阵的新方法,这可以看成是 DeVore 构造方法的自然推广。历史上,Goppa 开创了代数几何码研究的先河,很多好参数的线性码被发掘出来。我们相信,我们的构造方法还有巨大的潜力。一般来说,由于二元矩阵中所有元素都是非负的,这类矩阵在压缩感知领域中并不是最好的候选方案。Amini 等人已经迈出了从 p 元 BCH 码产生非二元感知矩阵的步伐。因此,利用代数曲线构造非二元感知矩阵将是一个有趣的问题,可以作为未来的研究方向。

另一方面，代数曲线和它们的代数函数域的种类繁多，这对于构造感知矩阵可以提供更大的灵活性。Candés 与 Tao 曾建议利用压缩感知的框架来设计加密方案[29]，其中每个感知矩阵被用作一个加密密钥。而由于不同的曲线可以产生不同的感知矩阵，我们的构造方法可以看作是提供了加密体系中加密密钥的更多选择。这一点在感知矩阵的密码学应用中具有很高的潜在价值。

除了上述收录在论文中的几类编码问题，作者还想借此机会简单介绍另一项纯组合设计的工作。问题的起源是农业和工业中的试验设计所用到的部分平衡不完全区组（Partially Balanced Incomplete Block，PBIB）设计。自 1973 年 Clatworthy 编著的关于两个结合类的 PBIB 设计（记为 PBIBD(2)）的参考手册[43] 发表以来，人们对其研究进展缓慢。对于 PBIBD(2) 中最重要的**可分组型**，Fu 等人解答了区组长度是 3 的情况[80,81]，而当区组长度为 4 时所知甚少[95,96,138]，其中的最困难点是组数目小于区组长度时的情况。我们的工作推广了组合设计理论中的 Wilson 基本构造法和双可分组设计构造法，获得了组数为 3 区组长为 4 时可分组型 PBIBD(2) 的一般性结果。这一工作已经发表在 SCI 期刊《SIAM Journal on Discrete Mathematics》。

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！

参 考 文 献

[1] ABEL R J R, BENNETT F E, MALCOLM G. PBD-Closure[G]// COLBOURN C J, DINITZ J H. Handbook of combinatorial designs. 2nd ed. Boca Raton: Chapman & Hall/CRC, Boca Raton, FL, 2007: 247–255.

[2] ABEL R J R, COLBOURN C J, DINITZ J H. Mutually Orthogonal Latin Squares (MOLS)[G]// COLBOURN C J, DINITZ J H. Handbook of combinatorial designs. 2nd ed. Boca Raton: Chapman & Hall/CRC, Boca Raton, FL, 2007: 160–193.

[3] ALON N, SPENCER J H. The probabilistic method[M]. Thirdth ed. Hoboken, NJ: John Wiley & Sons Inc., 2008.

[4] AMINI A, MARVASTI F. Deterministic construction of binary, bipolar and ternary compressed sensing matrices[J]. IEEE Trans. Inform. Theory, 2011, 57(4):2360–2370.

[5] AMINI A, MONTAZERHODJAT V, MARVASTI F. Matrices with small coherence using p-ary block codes[J]. IEEE Trans. Signal Process., 2012, 60(1):172–181.

[6] AMMAR B, HONARY B, KOU Y, et al. Construction of low-density parity-check codes based on balanced incomplete block designs[J]. IEEE Trans. Inform. Theory, 2004, 50(6):1257–1268.

[7] APPLEBAUM L, HOWARD S, SEARLE S, et al. Chirp sensing codes: deterministic compressed sensing measurements for fast recovery[J]. Appl. Comput. Harmon. Anal., 2009, 26(2):283–290.

[8] BARANIUK R, DAVENPORT M, DEVORE R, et al. A simple proof of the restricted isometry property for random matrices[J]. Constr. Approx., 2008, 28(3): 253–263.

[9] BARG A, BLAKLEY G R, KABATIANSKY G A. Digital fingerprinting codes:

problem statements, constructions, identification of traitors[J]. IEEE Trans. Inform. Theory, 2003, 49(4):852–865.

[10] BAUMERT L D, FREDRICKSEN H. The cyclotomic numbers of order eighteen with applications to difference sets[J]. Math. Comp., 1967, 21:204–219.

[11] BERINDE R, GILBERT A, INDYK P, et al. Combining geometry and combinatorics: a unified approach to sparse signal recovery[C]// Proc. 46th Annu. Allerton Conf. Commun., Control, Comput. 2008: 798–805.

[12] BETH T, JUNGNICKEL D, LENZ H. Design theory[M]. Mannheim: Bibliographisches Institut, 1985.

[13] BLACKBURN S R. Frameproof codes[J]. SIAM J. Discrete Math., 2003, 16(3): 499–510 (electronic).

[14] BLACKBURN S R, WILD P R. Optimal linear perfect hash families[J]. J. Combin. Theory Ser. A, 1998, 83(2):233–250.

[15] BLAKE I, HEEGARD C, HøHOLDT T, et al. Algebraic-geometry codes[J]. IEEE Trans. Inform. Theory, 1998, 44(6):2596–2618.

[16] BLAKLEY G R, MEADOWS C, PURDY G B. Fingerprinting long forgiving messages[G]// Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985). vol 218. Berlin: Springer, 1986: 180–189.

[17] BOGDANOVA G T, KAPRALOV S N. Enumeration of optimal ternary constant-composition codes[J]. Probl. Inf. Transm., 2003, 39:346–351.

[18] BOGDANOVA G T. Bounds for the maximum size of ternary constant-composition codes[C]// Proc. of the International Workshop on Optimal Codes. Sozopol: 1998: 15–18.

[19] BOGDANOVA G T, OCETAROVA D S. Some ternary constant-composition codes[C]// Proc. Sixth Int. Workshop "Algebraic and Combinatorial Coding Theory". Pskov, Russia: 1998: 41–45.

[20] BOGDANOVA G T, TODOROV T, YORGOVA T. New ternary and quaternary constant-weight equidistant codes[J]. Discrete Math. Algorithms Appl., 2010, 2(1): 89–97.

[21] BONEH D, SHAW J. Collusion-secure fingerprinting for digital data[J]. IEEE Trans. Inform. Theory, 1998, 44(5):1897–1905.

[22] BOURGAIN J, DILWORTH S, FORD K, et al. Explicit constructions of RIP matrices and related problems[J]. Duke Math. J., 2011, 159(1):145–185.

[23] BROUWER A E, SCHRIJVER A, HANANI H. Group divisible designs with block-size four[J]. Discrete Math., 1977/78, 20(1):1–10.

[24] BURATTI M. Recursive constructions for difference matrices and relative difference families[J]. J. Combin. Des., 1998, 6(3):165–182.

[25] CALDERBANK R, HOWARD S, JAFARPOUR S. Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property[J]. IEEE Trans. Inform. Theory, 2010, 4(2):358–374.

[26] CANDÈS E. The restricted isometry property and its implications for compressed sensing[J]. C. R. Math. Acad. Sci. Paris, 2008, 346(9–10):589–592.

[27] CANDÈS E, ROMBERG J, TAO T. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information[J]. IEEE Trans. Inform. Theory, 2006, 52(2):489–509.

[28] CANDÈS E, TAO T. Decoding by linear programming[J]. IEEE Trans. Inform. Theory, 2005, 51(12):4203–4215.

[29] CANDÈS E, TAO T. Near-optimal signal recovery from random projections: universal encoding strategies[J]. IEEE Trans. Inform. Theory, 2006, 52(12):5406–5425.

[30] CHEE Y M, DAU S H, LING A C H, et al. Linear size optimal q-ary constant-weight codes and constant-composition codes[J]. IEEE Trans. Inform. Theory, 2010, 56(1): 140–151.

[31] CHEE Y M, GE G, LING A C H. Group divisible codes and their application in the construction of optimal constant-composition codes of weight three[J]. IEEE Trans. Inform. Theory, 2008, 54(8):3552–3564.

[32] CHEE Y M, LING A C H, LING S, et al. The PBD-closure of constant-composition codes[J]. IEEE Trans. Inform. Theory, 2007, 53(8):2685–2692.

[33] CHEE Y M, LING S. Constructions for q-ary constant-weight codes[J]. IEEE Trans. Inform. Theory, 2007, 53(1):135–146.

[34] CHEN Y, PARHI K. Overlapped message passing for quasi-cyclic low-density parity check codes[J]. IEEE Trans. Circuits Syst. I. Regul. Pap., 2004, 51(6):1106–1113.

[35] CHENG M, JI L, MIAO Y. Separable codes[J]. IEEE Trans. Inform. Theory, 2012, 58(3):1791–1803.

[36] CHENG M, MIAO Y. On anti-collusion codes and detection algorithms for multimedia fingerprinting[J]. IEEE Trans. Inform. Theory, 2011, 57(7):4843–4851.

[37] CHENG U. Exhaustive construction of $(255, 127, 63)$-cyclic difference sets[J]. J. Combin. Theory Ser. A, 1983, 35(2):115–125.

[38] CHIEN R. Cyclic decoding procedure for the Bose-Chaudhuri-Hocquenghem codes[J]. IEEE Trans. Information Theory, 1964, 10:357–363.

[39] CHU W, COLBOURN C J, DUKES P. Constructions for permutation codes in powerline communications[J]. Des. Codes Cryptogr., 2004, 32(1-3):51–64.

[40] CHU W, COLBOURN C J, DUKES P. Tables for constant composition codes[J]. J. Combin. Math. Combin. Comput., 2005, 54:57–65.

[41] CHU W, COLBOURN C J, DUKES P. On constant composition codes[J]. Discrete Appl. Math., 2006, 154(6):912–929.

[42] CHUNG S Y, FORNEY JR G D, RICHARDSON T, et al. On the design of low-density parity-check codes within 0.0045 db of the Shannon limit[J]. IEEE Commun. Lett., 2001, 5.

[43] CLATWORTHY W H. Tables of two-associate-class partially balanced designs[M]. U. S. Department of Commerce, Washington, D. C.: National Bureau of Standards, 1973.

[44] COHEN A, DAHMEN W, DEVORE R. Compressed sensing and best k-term approximation[J]. J. Amer. Math. Soc., 2009, 22(1):211–231.

[45] COHEN D M, DALAL S R, FREDMAN M L, et al. The AETG system: an approach to testing based on combinatorial design[J]. IEEE Trans. Software Eng., 1997, 23:437–444.

[46] COHEN D M, DALAL S R, PARELIUS J, et al. The combinatorial design approach to automatic test generation[J]. IEEE Software, 1996, 13:83–88.

[47] COHEN G D, LITSYN S, ZÉMOR G. On greedy algorithms in coding theory[J]. IEEE Trans. Inform. Theory, 1996, 42(6, part 1):2053–2057.

[48] COLBOURN C J, DINITZ J H. Handbook of combinatorial designs[M]. 2nd ed. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[49] COLBOURN C J, KLøVE T, LING A C H. Permutation arrays for powerline communication and mutually orthogonal Latin squares[J]. IEEE Trans. Inform. Theory, 2004, 50(6):1289–1291.

[50] COLBOURN M J, COLBOURN C J. Recursive constructions for cyclic block designs[J]. J. Statist. Plann. Inference, 1984, 10(1):97–103.

[51] CSISZÁR I, KÖRNER J. Information theory: Coding theorems for discrete memoryless systems[M]. New York: Academic Press, 1981.

[52] DAI W, MILENKOVIC O. Subspace pursuit for compressive sensing signal reconstruction[J]. IEEE Trans. Inform. Theory, 2009, 55(5):2230–2249.

[53] DAVENPORT M, WAKIN M. Analysis of orthogonal matching pursuit using the restricted isometry property[J]. IEEE Trans. Inform. Theory, 2009, 56(9):4395–4401.

[54] DE LA TORRE D R, COLBOURN C J, LING A C H. An application of permutation arrays to block ciphers[C]// Proceedings of the Thirty-first Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 2000). vol 145. 2000: 5–7.

[55] DENG D, LI P C, VAN REES G H J, et al. The Stein-Lovász theorem and its applications to some combinatorial arrays[J]. J. Combin. Math. Combin. Comput., 2011, 77:17–31.

[56] DEVORE R. Deterministic constructions of compressed sensing matrices[J]. J. Complexity, 2007, 23(4–6):918–925.

[57] DEZA M, VANSTONE S A. Bounds for permutation arrays[J]. J. Statist. Plann. Inference, 1978, 2(2):197–209.

[58] DING C. Optimal constant composition codes from zero-difference balanced functions[J]. IEEE Trans. Inform. Theory, 2008, 54(12):5766–5770.

[59] DING C. Cyclic codes from the two-prime sequences[J]. IEEE Trans. Inform. Theory, 2012, 58(6):3881–3891.

[60] DING C, FU F W, KLøVE T, et al. Constructions of permutation arrays[J]. IEEE Trans. Inform. Theory, 2002, 48(4):977–980.

[61] DING C, YIN J. Algebraic constructions of constant composition codes[J]. IEEE Trans. Inform. Theory, 2005, 51(4):1585–1589.

[62] DING C, YIN J. Combinatorial constructions of optimal constant-composition codes[J]. IEEE Trans. Inform. Theory, 2005, 51(10):3671–3674.

[63] DING C, YIN J. A construction of optimal constant composition codes[J]. Des. Codes Cryptogr., 2006, 40(2):157–165.

[64] DING C, YUAN J. A family of optimal constant-composition codes[J]. IEEE Trans. Inform. Theory, 2005, 51(10):3668–3671.

[65] DING Y. A construction for constant-composition codes[J]. IEEE Trans. Inform. Theory, 2008, 54(8):3738–3741.

[66] DITTMANN J, SCHMITT P, SAAR E, et al. Combining digital watermarks and collusion secure fingerprints for digital images[J]. SPIE J. Electron, Imag., 2000, 9(4):456–467.

[67] DONOHO D. Compressed sensing[J]. IEEE Trans. Inform. Theory, 2006, 52(4): 1289–1306.

[68] DRAKE D A. Partial λ-geometries and generalized Hadamard matrices over groups[J]. Canad. J. Math., 1979, 31(3):617–627.

[69] DREIER R, SMITH K. Exhaustive determination of $(511, 255, 127)$ cyclic difference sets[M]. unpublished:. 1994.

[70] DUARTE M, DAVENPORT M, TAKHAR D, et al. Single-pixel imaging via compressive sampling[J]. IEEE Trans. Signal Process, 2008, 25(2):83–91.

[71] DUKES P, SAWCHUCK N. Bounds on permutation codes of distance four[J]. J. Algebraic Combin., 2010, 31(1):143–158.

[72] D'YACHKOV A G. Random constant composition codes for multiple access channels[J]. Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform., 1984, 13(6):357–369.

[73] ERICSON T, ZINOVIEW V. Spherical codes generated by binary partitions of symmetric pointsets[J]. IEEE Trans. Inform. Theory, 1995, 41(1):107–129.

[74] EVANS A B. On orthogonal orthomorphisms of cyclic and non-abelian groups. II[J]. J. Combin. Des., 2007, 15(3):195–209.

[75] EVANS R, HOLLMANN H D L, KRATTENTHALER C, et al. Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets[J]. J. Combin. Theory Ser. A, 1999, 87(1): 74–119.

[76] FERREIRA H C, VINCK A J H. Inference cancellation with permutation trellis arrays[C]// Proc. IEEE Vehicular Technology Conf. Boston, MA: 2000: 2401–2407.

[77] FORNEY J, G. On decoding BCH codes[J]. IEEE Trans. Information Theory, 1965, 11:549–557.

[78] FRANKL P, DEZA M. On the maximum number of permutations with given maximal or minimal distance[J]. J. Combinatorial Theory Ser. A, 1977, 22(3):352–360.

[79] FU F W, KLøVE T. Two constructions of permutation arrays[J]. IEEE Trans. Inform. Theory, 2004, 50(5):881–883.

[80] FU H L, RODGER C A. Group divisible designs with two associate classes: $n = 2$ or $m = 2$[J]. J. Combin. Theory Ser. A, 1998, 83(1):94–117.

[81] FU H L, RODGER C A, SARVATE D G. The existence of group divisible designs with first and second associates, having block size 3[J]. Ars Combin., 2000, 54:33–50.

[82] GAAL P, GOLOMB S W. Exhaustive determination of $(1023, 511, 255)$-cyclic difference sets[J]. Math. Comp., 2001, 70(233):357–366.

[83] GALLAGER R G. Low-density parity-check codes[J]. IRE Trans., 1962, IT-8:21–28.

[84] GAO F, GE G. Supporting information for the paper: Optimal ternary constant-composition codes of weight four and distance five[J]. arXiv, 2010.

[85] GE G. On $(g, 4; 1)$-difference matrices[J]. Discrete Math., 2005, 301(2-3):164–174.

[86] GE G. Construction of optimal ternary constant weight codes via Bhaskar Rao designs[J]. Discrete Math., 2008, 308(13):2704–2708.

[87] GE G, LING A C H. Asymptotic results on the existence of 4-RGDDs and uniform 5-GDDs[J]. J. Combin. Des., 2005, 13(3):222–237.

[88] GE G, REES R. On group-divisible designs with block size four and group-type $6^u m^1$[J]. Discrete Math., 2004, 279(1-3):247–265.

[89] GOLOMB S W. Shift register sequences[M]. San Francisco, Calif.: Holden-Day Inc., 1967.

[90] GOLOMB S. Two-valued sequences with perfect periodic autocorrelation[J]. IEEE Trans. Aerospace Electron. Systems, 1992, 28(2):383–386.

[91] GOPPA V D. Codes on algebraic curves[J]. Dokl. Akad. Nauk SSSR, 1981, 259(6): 1289–1290.

[92] GRASSL M. Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de 2007.

[93] HANANI H. Balanced incomplete block designs and related designs[J]. Discrete Math., 1975, 11:255–369.

[94] HARADA M, TONCHEV V D. Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms[J]. Discrete Math., 2003, 264(1-3):81–90.

[95] HENSON D, SARVATE D G, HURD S P. Group divisible designs with three groups and block size four[J]. Discrete Math., 2007, 307(14):1693–1706.

[96] HENSON D, SARVATE D G. A family of group divisible designs of block size four and three groups with $\lambda_1 = 2$ and $\lambda_2 = 1$ using MOLS[J]. Ars Combin., 2006, 78:123–125.

[97] HESS F. Computing Riemann-Roch spaces in algebraic function fields and related topics[J]. J. Symbolic Comput., 2002, 33(4):425–445.

[98] HOWARD S, CALDERBANK A, SEARLE J. A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes[C]// IEEE Conf. Inform. Sciences and Systems (CISS2008). 2008: 11–15.

[99] HUCZYNSKA S. Equidistant frequency permutation arrays and related constant composition codes[J]. Des. Codes Cryptogr., 2010, 54(2):109–120.

[100] INDYK P. Explicit constructions for compressed sensing matrices[C]// Proc. 19th Annu. ACM-SIAM Symp. Discrete Algorithms (SODA). 2008: 30–33.

[101] JIANG A, MATEESCU R, SCHWARTZ M, et al. Rank modulation for flash memories[C]// Proc. IEEE Int. Symp. Information Theory. 2008: 1731–1735.

[102] JIANG A, SCHWARTZ M, BRUCK J. Error-correcting codes for rank modulation[C]// Proc. IEEE Int. Symp. Information Theory. 2008: 1736–1740.

[103] JIANG T, VARDY A. Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes[J]. IEEE Trans. Inform. Theory, 2004, 50(8):1655–1664.

[104] JUNGNICKEL D. On difference matrices, resolvable transversal designs and generalized hadamard matricies[J]. Math. Zeitschr., 1979, 167:49–60.

[105] KIM J H. On the Binary Sequences of Period 511 with Ideal Autocorrelation[D]. M.s. thesis. Korea: Yonsei University, 1998.

[106] KING O D. Bounds for DNA codes with constant GC-content[J]. Electron. J. Combin., 2003, 10(1):#R33 13pp.

[107] KLøVE T. Lower bounds on the size of spheres of permutations under the Chebychev distance[J]. Des. Codes Cryptogr., 2011, 59(1-3):183–191.

[108] KLøVE T, LIN T T, TSAI S C, et al. Permutation arrays under the Chebyshev distance[J]. IEEE Trans. Inform. Theory, 2010, 56(6):2611–2617.

[109] KOBLITZ N, MENEZES A, VANSTONE S. The state of elliptic curve cryptography[J]. Des. Codes Cryptogr., 2000, 19(2–3):173–193.

[110] KORNER J, LUCERTINI M. Compressing inconsistent data[J]. IEEE Trans. Inform. Theory, 1994, 40:706–715.

[111] KOU Y, LIN S, FOSSORIER M P C. Low-density parity-check codes based on finite geometries: a rediscovery and new results[J]. IEEE Trans. Inform. Theory, 2001, 47(7):2711–2736.

[112] LAN L, TAI Y Y, LIN S, et al. New constructions of quasi-cyclic LDPC codes based on two classes of balanced incomplete block designs: for AWGN and binary erasure channels[G]// Applied algebra, algebraic algorithms and error-correcting codes. vol 3857. Berlin: Springer, 2006: 275–284.

[113] LAN L, ZENG L, TAI Y Y, et al. Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: a finite field approach[J]. IEEE Trans. Inform. Theory, 2007, 53(7):2429–2458.

[114] LANDER E S. Symmetric designs: an algebraic approach[M]. Cambridge: Cambridge University Press, 1983.

[115] LEE G S. An extension of Stein-Lovász theorem and some of its applications[J]. J. Comb. Optim., 2013, 25(1):1–18.

[116] LI C, LI Q, LING S. On the constructions of constant-composition codes from perfect nonlinear functions[J]. Sci. China Ser. F, 2009, 52(6):964–973.

[117] LI Q, WANG X, LI Y, et al. Construction of anti-collusion codes based on cover-free families[C]// Proc. 6th Int. Conf. Inf. Tech. New Generat., Las Vegas, NV: 2009: 362–365.

[118] LI Y, ROUSSEAU C C. On book-complete graph Ramsey numbers[J]. J. Combin. Theory Ser. B, 1996, 68(1):36–44.

[119] LI Y, ROUSSEAU C C, ZANG W. Asymptotic upper bounds for Ramsey functions[J]. Graphs Combin., 2001, 17(1):123–128.

[120] LI Z W, CHEN L, ZENG L Q, et al. Efficient encoding of quasi-cyclic low-density parity-check codes[J]. IEEE Trans. Comm., 2006, 54(1):71–81.

[121] LIN S, CHEN L, XU J, et al. Near shannon limit quasicyclic low-density parity-check codes[C]// Proc. 2003 IEEE GLOBECOM Conf. San Francisco, CA: 2003.

[122] LIN S, JR D J C. Error Constrol Coding: Fundamentals and Applications[M]. 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2004.

[123] LOVÁSZ L. On the ratio of optimal integral and fractional covers[J]. Discrete Math., 1975, 13(4):383–390.

[124] LUO Y, FU F W, VINCK A J H, et al. On constant-composition codes over Z_q[J]. IEEE Trans. Inform. Theory, 2003, 49(11):3010–3016.

[125] MACKAY D J C. Good error-correcting codes based on very sparse matrices[J]. IEEE Trans. Inform. Theory, 1999, 45(2):399–431.

[126] MACKENZIE-FLEMING K, SMITH K W. $(27, 13, 6)$ designs with an automorphism of order 3[J]. J. Combin. Math. Combin. Comput., 1996, 22:241–253.

[127] MILENKOVIC O, KASHYAP N. On the design of codes for DNA computing[G]// Coding and cryptography. vol 3969. Berlin: Springer, 2006: 100–119.

[128] NATARAJAN B K. Sparse approximate solutions to linear systems[J]. SIAM J. Comput., 1995, 24(2):227–234.

[129] NEEDELL D, TROPP J. CoSaMP: iterative signal recovery from incomplete and inaccurate samples[J]. Appl. Comput. Harmon. Anal., 2009, 26(3):301–321.

[130] NEEDELL D, VERSHYNIN R. Uniform uncertainty principle and signal recovery via regularized orthogonal matching pursuit[J]. Found. Comput. Math., 2009, 9(3): 317–334.

[131] NIEDERREITER H, XING C. Rational points on curves over finite fields: theory and applications[M]. Cambridge: Cambridge University Press, 2001.

[132] PAVLIDOU N, VINCK A J H, YAZDANI J, et al. Power line communications: State of the art and future trends[J]. IEEE Commun. Mag., 2003, 41:34–40.

[133] PLESS V S, TONCHEV V D. Self-dual codes over GF(7)[J]. IEEE Trans. Inform. Theory, 1987, 33(5):723–727.

[134] POTT A, KUMAR P V, HELLESETH T, et al. Difference sets, sequences and their correlation properties[C]. vol 542. Dordrecht: Kluwer Academic Publishers Group, 1999.

[135] REES R, STINSON D R. On the existence of incomplete designs of block size four having one hole[J]. Utilitas Math., 1989, 35:119–152.

[136] RICHARDSON T J, SHOKROLLAHI M A, URBANKE R L. Design of capacity-approaching irregular low-density parity-check codes[J]. IEEE Trans. Inform. Theory, 2001, 47(2):619–637.

[137] RICHARDSON T J, URBANKE R L. The capacity of low-density parity-check codes under message-passing decoding[J]. IEEE Trans. Inform. Theory, 2001, 47(2): 599–618.

[138] RODGER C, ROGERS J. Generalizing Clatworthy group divisible designs[J]. J. Statist. Plann. Inference, 2010, 140(9):2442 – 2447.

[139] RYAN W E, LIN S. Channel Codes: Classical and Modern[M]. Cambridge, UK: Cambridge University Press, 2009.

[140] S. Y. CHUNG G, JR D F, RICHARDSON T, et al. On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit[J]. IEEE Commun. Lett., 2001, 5.

[141] SAGALOVICH Y L. Separating systems[J]. Problemy Peredachi Informatsii, 1994, 30(2):14–35.

[142] SCHMIDT B, WHITE C. All two-weight irreducible cyclic codes?[J]. Finite Fields Appl., 2002, 8(1):1–17.

[143] SCHOLTZ R A, WELCH L R. GMW sequences[J]. IEEE Trans. Inform. Theory, 1984, 30(3):548–553.

[144] SCHOOF R. Elliptic curves over finite fields and the computation of square roots mod p[J]. Math. Comp., 1985, 44(170):483–494.

[145] SCHUSTER E, GE G. On uniformly resolvable designs with block sizes 3 and 4[J]. Des. Codes Cryptogr., 2010, 57:45–69.

[146] SHANNON C E. A mathematical theory of communication[J]. Bell System Tech. J., 1948, 27:379–423, 623–656.

[147] SHRIKHANDE S S. Generalized hadamard matrices and orthogonal arrays of strength 2[J]. Canad. J. Math., 1964, 16:131–141.

[148] SIMON M, OMURA J, SCHOLTZ R, et al. Spread Spectrum Comrnunications[M]. Rockville, MD.: Computer Science Press, 1985.

[149] SIPSER M, SPIELMAN D A. Expander codes[J]. IEEE Trans. Inform. Theory, 1996, 42(6, part 1):1710–1722.

[150] SLEPIAN D. Permutation modulation[J]. Proc. IEEE, 1965, 53(3):228–236.

[151] SMELTZER D L. Properties of codes from difference sets in 2-groups[J]. Des. Codes Cryptogr., 1999, 16(3):291–306.

[152] SMITH D H, MONTEMANNI R. A new table of permutation codes[J]. Des. Codes Cryptogr., 2012, 63(2):241–253.

[153] STADDON J N, STINSON D R, WEI R. Combinatorial properties of frameproof and traceability codes[J]. IEEE Trans. Inform. Theory, 2001, 47(3):1042–1049.

[154] STEIN S K. Two combinatorial covering problems[J]. J. Combin. Theory Ser. A, 1974, 16:391–397.

[155] STEIN W, OTHERS. Sage Mathematics Software (Version 5.1)[S]. The Sage Development Team. 2012.

[156] STICHTENOTH H. Algebraic Function Fields and Codes[M]. Secondth ed. Berlin: Springer, 2009.

[157] STINSON D R. Combinatorial characterizations of authentication codes[J]. Des. Codes Cryptogr., 1992, 2(2):175–187.

[158] STINSON D R, VAN TRUNG T, WEI R. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures[J]. J. Statist. Plann. Inference, 2000, 86(2):595–617.

[159] STINSON D R, WEI R, CHEN K. On generalized separating hash families[J]. J. Combin. Theory Ser. A, 2008, 115(1):105–120.

[160] STINSON D R, WEI R, YIN J. Packings[G]// COLBOURN C J, DINITZ J H. Handbook of combinatorial designs. 2nd ed. Boca Raton: Chapman & Hall/CRC, Boca Raton, FL, 2007: 550–556.

[161] SUN X, GE G. Resolvable group divisible designs with block size four and general index[J]. Discrete Math., 2009, 309:2982–2989.

[162] SVANSTRÖM M. Ternary Codes With Weight Constraints[D]. Ph.d. dissertation. Linköpings Universitet, 1999.

[163] SVANSTRÖM M. A lower bound for ternary constant weight codes[J]. IEEE Trans. Inform. Theory, 1997, 43(5):1630–1632.

[164] SVANSTRÖM M. Constructions of ternary constant-composition codes with weight three[J]. IEEE Trans. Inform. Theory, 2000, 46(7):2644–2647.

[165] SVANSTRÖM M, ÖSTERGåRD P R J, BOGDANOVA G T. Bounds and constructions for ternary constant-composition codes[J]. IEEE Trans. Inform. Theory, 2002, 48(1):101–111.

[166] TANG H, XU J, KOU Y, et al. On algebraic construction of Gallager and circulant low-density parity-check codes[J]. IEEE Trans. Inform. Theory, 2004, 50(6):1269–1279.

[167] TANNER R M. A recursive approach to low complexity codes[J]. IEEE Trans. Inform. Theory, 1981, 27(5):533–547.

[168] TANNER R M. Spectral graphs for quasi-cyclic LDPC codes[C]// Proc. 2001 Int. Symp. Information Theory. Washington, DC: 2001: 226.

[169] TANNER R M, SRIDHARA D, FUJA T. A class of group-structured LDPC codes[C]// Proc. 6th Int. Symp. Communications Theory and Applications. Ambleside, U.K.: 2001.

[170] TELATAR I E, GALLAGER R G. Zero error decision feedback capacity of discrete memoryless channels[C]// ARIKAN E. BILCON ’90: Proc. 1990 Bilkent Int. Conf. on New Trends in Communication, Control, and Signal Processing. Bilkent University. Amsterdam, The Netherlands: Elsevier, 1990: 228–233.

[171] TONCHEV V D. Hadamard matrices of order 28 with automorphisms of order 7[J]. J. Combin. Theory Ser. A, 1985, 40(1):62–81.

[172] TONCHEV V D. Codes and designs[G]// Handbook of coding theory, Vol. I, II. Amsterdam: North-Holland, 1998: 1229–1267.

[173] TRAPPE W, WU M, WANG Z J, et al. Anti-collusion fingerprinting for multimedia[J]. IEEE Trans. Signal Process., 2003, 51(4):1069–1087.

[174] TROPP J, GILBERT A. Signal recovery from random measurements via orthogonal matching pursuit[J]. IEEE Trans. Inform. Theory, 2007, 53(12):4655–4666.

[175] TSFASMAN M A, VLĂDUŢ S G. Algebraic-geometric codes[M]. Dordrecht: Kluwer, 1991.

[176] VASIC B, MILENKOVIC O. Combinatorial constructions of low-density parity-check codes for iterative decoding[J]. IEEE Trans. Inform. Theory, 2004, 50(6): 1156–1176.

[177] VINCK A J H. Coded modulation for powerline communications[J]. A.E.Ü. Int. J. Electron. Commun., 2000, 54:45–49.

[178] VU V, WU L. Improving the Gilbert-Varshamov bound for q-ary codes[J]. IEEE Trans. Inform. Theory, 2005, 51(9):3200–3208.

[179] WACHTER-ZEH A, BEZZATEEV S. Decoding cyclic codes up to a new bound on the minimum distance[J]. IEEE Trans. Inform. Theory, 2012, 58:3951–3960.

[180] WANG Z, CUI Z. Low-complexity high-speed decoder design for quasi-cyclic ldpc codes[J]. IEEE Trans. VLSI, 2007, 15(1):104 –114.

[181] WASHINGTON L C. Elliptic curves: Number theory and cryptography[M]. Secondth ed. Boca Raton, FL: Chapman & Hall/CRC, 2008.

[182] WELDON E J, JR. Difference-set cyclic codes[J]. Bell System Tech. J., 1966, 45:1045–1055.

[183] WU D, GE G, ZHU L. Generalized Steiner triple systems with group size $g = 7, 8$[J]. Ars Combin., 2000, 57:175–191.

[184] XING C P, NIEDERREITER H, LAM K Y. Constructions of algebraic-geometry codes[J]. IEEE Trans. Inform. Theory, 1999, 45(4):1186–1193.

[185] YAN J, WANG C. Constructions of a class of optimal constant composition codes[J]. Far East J. Appl. Math., 2009, 34(1):73–81.

[186] YAN J, YIN J. A class of optimal constant composition codes from GDRPs[J]. Des. Codes Cryptogr., 2009, 50(1):61–76.

[187] YIN J, TANG Y. A new combinatorial approach to the construction of constant composition codes[J]. Sci. China Ser. A, 2008, 51(3):416–426.

[188] ZHANG H, GE G. Optimal ternary constant-weight codes of weight four and distance six[J]. IEEE Trans. Inform. Theory, 2010, 56(5):2188–2203.

[189] ZHANG H, ZHANG X, GE G. Optimal ternary constant-weight codes with weight 4 and distance 5[J]. IEEE Trans. Inform. Theory, 2012, 58(5):2706–2718.

[190] ZHANG L, HUANG Q, LIN S, et al. Quasi-cyclic LDPC codes: An algebraic construction, rank analysis, and codes on latin squares[J]. IEEE Trans. Comm., 2010, 58(11):3126–3139.

[191] ZHANG X, ZHANG H, GE G. Optimal constant weight covering codes and nonuniform group divisible 3-designs with block size four[J]. Des. Codes Cryptogr., 2012, 62(2):143–160.

[192] ZHAO S M, XIAO Y, ZHU Y, et al. New class of quantum codes constructed from cyclic difference set[J]. Int. J. Quantum Inf., 2012, 10(1):1250015, 12.

[193] ZHU M, GE G. 4-$^{*}GDD(6^n)s$ and related optimal quaternary constant-weight codes[J]. J. Combin. Des., 2012, 20(12):509–526.

[194] ZHU M, GE G. Quaternary constant-composition codes with weight 4 and distances 5 or 6[J]. IEEE Trans. Inform. Theory, 2012, 58(9):6012–6022.

攻读博士学位期间主要研究成果

已经发表的论文：

[1] GAO F, GE G. Optimal ternary constant-composition codes of weight four and distance five[J]. IEEE Trans. Inform. Theory, 2011, 57(6): 3742–3757.

[2] GAO F, GE G. A complete generalization of Clatworthy group divisible designs[J]. SIAM J. Discrete Math., 2011, 25(4): 1547–1561.

[3] LI S, GAO F, GE G, et al. Deterministic construction of compressed sensing matrices via algebraic curves[J]. IEEE Trans. Inform. Theory, 2012, 58(8): 5035–5041.

[4] GAO F, YANG Y, GE G. An improvement on the Gilbert–Varshamov bound for permutation codes[J]. IEEE Trans. Inform. Theory, 2013, 59(5): 3059–3063.

其它已完成的工作：

[5] GAO F, GE G. Combinatorial constructions of low-density parity-check codes. In manuscript.

[6] GAO F, GE G. An improvement to the upper and lower bounds of separable codes. In preparation.

[7] FENG T, GAO F, GE G, LI S. More optimal linear codes from combinatorial designs. In preparation.

作者简历

基本情况

高斐，男，浙江大学数学系在读博士研究生。

教育经历

2004 年 9 月至 2008 年 7 月，浙江大学理学院，本科，专业：数学与应用数学。

2008 年 9 月至 2013 年 7 月，浙江大学数学系，博士，专业：应用数学。

研究兴趣

组合设计，编码理论，密码学。

联系方式

通讯地址：浙江大学数学系。邮编：310027

E-mail: feigao.chn@gmail.com