分类号：O157.2　　单位代码：10335
密　级：　　学　　号：10706071

浙江大学

博士学位论文

中文论文题目：几类组合编码问题研究

英文论文题目：Combinatorial Constructions for Several Classes of Codes

申请人姓名：张　会
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

几类组合编码问题研究

论文作者签名：_____

指导教师签名：_____

论文评阅人 1：符方伟 \ 教授 \ 南开大学

评阅人 2：季利均 \ 教授 \ 苏州大学

评阅人 3：殷剑兴 \ 教授 \ 苏州大学

评阅人 4：李雨生 \ 教授 \ 同济大学

评阅人 5：常彦勋 \ 教授 \ 北京交通大学

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 Constructions for

Several Classes of Codes

Author's signature: _____

Supervisor's signature: _____

External Reviewers: Fangwei Fu\Professor\Nankai University

Lijun Ji\Professor\Soochow University

Jianxing Yin\Professor\Soochow University

Yusheng Li\Professor\Tongji University

Yanxun Chang\Professor\Beijing Jiaotong 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

摘　要

编码理论中的核心问题是构造各种最优码，但这一问题是非常困难的，甚至对于单个参数的构造都是不平凡的。我们将在本论文里延续前人相关的工作，提出一些新的组合思想和构造方法，用来构造最优的编码，具体包括常重码、常重复合码、常重覆盖码、认证码等。

第一部分由第 3 章和第 4 章组成，我们将利用广义Steiner系，构造重量为4、最小汉明距离为5的最优三元、四元常重码。

用广义Steiner系构造最优多元常重码是由以色列著名数学家Etizon最先提出的，此后很多组合学家都曾对此展开研究。著名组合学家殷剑兴教授等人把广义Steiner系推广到填充情况，用以构造一般参数的最优多元常重码。然而目前大部分的相关工作都集中在重量为3的情况，对重量为4的情况研究结果并不多，这主要是受限于新递归构造方法的缺乏以及短码字直接构造的困难。

在第 3 章中，我们研究了重量为4、最小汉明距离为5的最优三元常重码。此参数下，欧拉奖获得者朱烈教授和他的学生基本解决了长度$n \equiv 1 \pmod 3$时，广义Steiner系的构造问题。而我们建立了一些辅助设计与可分组码的联系，构造出其它长度时的最优码。可分组码这一概念是由Chee等人提出的，它类似于组合设计中的可分组设计，在常重码和常重复合码等的循环构造中具有重要作用。我们运用可分组码的构造方法，对除了8个不确定的长度以外的所有值，确定了重量为4、最小汉明距离为5的最优三元常重码的码字个数。

第 4 章中，我们研究了重量为4、最小汉明距离为5的最优四元常重码。对这类常重码，虽然之前已经有一些文章用广义Steiner系的方法给出了一些构造方法，和长度$n \equiv 0, 1 \pmod 4$时的一些无穷类，但是距离问题的完全解决还很远。我们改进了之前文章中的一类SIP方法，用可分组设计和超单正交表得到需要的广义Steiner系，使得在构造长度较小的码时更加有效。结合对一些长度较小的码和型不一致的辅助设计的直接构造，我们得到除了55个长度以外，所有长度的重量为4、最小汉明距离为5的最优四元常重码。

第二部分由第 5 章和第 6 章组成，我们将利用完全可约超单设计，构造重

量为4、最小汉明距离为6的最优三元、四元常重码。

在2007年，Chee等人提出了用不相交设计、大集等来构造重量为3的最优多元常重码的思想，并得到了一些完整的码类。在此基础上，我们在第 5 章中提出了用完全可约超单设计来构造最优多元常重码的方法，并结合完全可约超单可分组设计作为辅助，得到了除长度17外，所有长度的重量为4、最小汉明距离为6的最优三元常重码。

完全可约超单设计可以推出最优常重码，而完全可约超单可分组设计可以得到在递归构造中起重要作用的可分组码，这两种设计的构造也是组合设计理论中的重要问题。因此，在第 6 章中，我们专门研究了此类设计的构造问题，完全解决了区组大小为4、指数为3的完全可约超单设计，以及区组大小为4、指数为2的完全可约超单一致可分组设计和超单填充的存在性，并得到了一类新的重量为4、最小汉明距离为6的最优四元常重码。

第三部分由第 7 章和第 8 章组成，我们将研究两类特殊的最优多元常重码，即：线性大小的多元常重码和常重复合码。

对最优多元常重码的研究工作，多是考虑固定重量w和最小汉明距离d，而让长度n和码元q变动时，最优多元常重码的构造问题。目前已知具有完整结果的，只有当参数(d,w)取值$(3,2)$和$(4,3)$的情形。在第 7 章中，我们将对任意码长n和码元$q \geq 2$，都确定出重量为3、最小汉明距离为5的最优q元常重码的码字个数。这类参数的码也被称为是线性大小的。我们的方法是建立Hanani三元填充与此类码的联系。Hanani三元填充是组合设计中的Hanani三元系的推广，后者是著名组合学家Stinson和Colbourn（欧拉奖获得者）等人于1993年提出并解决的。我们还确定了任意阶数的Hanani三元填充的存在性。

在第 8 章中，我们将构造一类重量为4、最小汉明距离为6、型为$[2,2]$的最优三元常重复合码。常重复合码是常重码的一种特殊情况，它具有许多重要的应用。我们确定了当长度$n \not\equiv 5 \pmod 6$时，除了11个值以外的所有此类最优码的码字个数。而当$n \equiv 5 \pmod 6$时，也得到好的下界。我们所用的方法是第 3 章中给出的可分组码的循环构造方法，以及从斜Room frame构造可分组码的方法。

最后一个部分由第 9 章和第 10 章组成，我们将利用3-设计中的方法，构造最优常重覆盖码和具有分裂性质的认证码。

常重覆盖码不但在数据压缩算法中有重要应用，还在组合设计理论中具

有很多相似的结构，例如Turán设计、彩票方案和覆盖设计等。在过去的六十多年中，有很多数学家对这些组合结构进行过研究。在第 9 章中，我们建立了一类参数下的最优常重覆盖码与可分组覆盖之间的联系，并运用辅助设计H-frame，构造出除$(q,n)=(3,5)$以外，任意$n\geq 4$，$q\in\{3,4\}$或者$q=2^m+1$（$m\geq 2$）时，重量为4的最优q元常重覆盖码，使得其中任意重量为3的字都与至少一个码字的最小汉明距离为1。

在第 10 章中，我们考虑了具有分裂性质的认证码。利用Huber所建立的分裂认证码与分裂设计的等价性，我们将组合设计中的方法推广到构造分裂t-设计和分裂烛台设计，得到了两类新的无穷类。我们得到的$(3,2)$-分裂认证码是当$t>2$和$c>1$时，(t,c)-分裂认证码的第一个已知的无穷类。我们还证明了具有k个源状态和v个信息的$(2,c)$-分裂认证码对任意充分大的v（当k和c固定时）都是存在的。

关键词：
多元常重码，常重复合码，常重覆盖码，广义Steiner系，完全可约超单设计，可分组码，认证码

Abstract

A fundamental problem in coding theory is to constuct optimal codes. This problem turns out to be extremely difficult, even for a single code with affirmatory parameters. In this dissertation, we will concentrate on this topic and bring some new combinatorial construction methods to obtain several new classes of optimal codes. Our results will include constant-weight codes (CWCs), constant-composition codes (CCCs), constant-weight covering codes (CWCCs), and authentication codes (ACs).

The first part consists of Chapters 3 and 4. In which, we will construct optimal ternary or quaternary constant-weight codes with weight 4 and minimum Hamming distance 5 via generalized Steiner systems. It was the famous Israeli mathematician Etizon who first raised the idea of constructing optimal q-ary CWCs with generalized Steiner systems. Later, Yin generalized this idea to packing designs. Most of works in literature focused on the case of weight 3. For weight 4, only a few results are known due to limitation of methods.

In Chapter 3, we will study the case of ternary CWCs with weight 4 and minimum Hamming distance 5. For length $n \equiv 1 \pmod 3$, the existence of generalized Steiner system was determined by the Euler Medal owner Prof. Zhu and his students. We will establish a connection between some auxiliary designs and group divisible codes (GDCs), and construct the optimal codes with other lengths. The concept of group divisible codes was brought up by Chee et al. It is the analog of group divisible designs in combinatorial design theory and shows a great power in the recursive constructions of CWCs and CCCs. With the help of GDCs, we will construct the optimal ternary CWCs with weight 4 and distance 5 for all but 8 lengths.

In Chapter 4, we will construct the optimal quaternary CWCs with weight 4 and distance 5 for all length n except for 55 values. We will improve an SIP method in literature and obtain the desired generalized Steiner systems from group divisible designs and super simple orthogonal arrays. Before our work,

only some infinite classes of length $n \equiv 0, 1 \pmod 4$ are known.

The second part consists of Chapters 5 and 6, in which, we will investigate the constructions of optimal ternary or quaternary CWCs with weight 4 and distance 6 using completely reducible super simple (CRSS) designs. This idea is based on the work of Chee et al. in 2007, in which they obtained optimal q-ary CWCs from disjoint designs and large set of designs. In Chapter 5, we will use CRSS designs together with CRSS group divisible designs to get the optimal ternary CWCs with weight 4 and distance 6 for all length n, except for $n = 17$.

In view of the important applications of these two kind of designs with CRSS property, we will investigate the existence problems related to both designs in Chapter 6. As a byproduct, a new class of optimal quaternary CWCs with weight 4 and distance 6 is obtained as well.

The third part consists of Chapters 7 and 8. We will exploit two special classes of optimal q-ary CWCs and CCCs.

The researches on optimal CWCs with large alphabet usually focused on fixed weight w and distance d and let length n and alphabet size q vary. To the best of author's knowledge, the only complete solutions to this problem are when $(d, w) = (3, 2)$ or $(4, 3)$. In Chapter 7, we will construct optimal CWCs with $(d, w) = (5, 3)$ for all the length n and alphabet size $q \geq 2$. They are the so called linear size CWCs. Our main tool is the Hanani triple packings (HTPs), which can be regarded as the generalization of Hanani triple systems raised by the Euler Medal owner Prof. Colbourn in 1993. The existence of HTPs with all orders will be determined as well in this chapter.

In Chapter 8, optimal ternary CCCs with weight 4, distance 6, and type $[2, 2]$ will be constructed. When $n \not\equiv 5 \pmod 6$, optimal codes for all but 11 lengths will be obtained. For $n \equiv 5 \pmod 6$, near-optimal lower bounds on the code size will be derived from GDCs and skew Room frames.

The last part consists of Chapters 9 and 10. We will study the CWCCs and ACs with splitting property in these two chapters respectively.

Not only do CWCCs find itself having important applications in universal data compression algorithms, but also share similar structural properties with

several subjects in combinatorial design theory, such as Turán designs, lottery schemes, and covering designs. These topics are well investigated by numbers of mathematicians during the past sixty years. In Chapter 9, we will show a connection between optimal CWCCs with specific parameters and group divisible covering designs. Using the H-frame as auxiliary designs, we will obtain optimal q-ary CWCCs with weight 4 for all $n \geq 4$, $q \in \{3, 4\}$ or $q = 2^m + 1$ $(m \geq 2)$, excepting $(q, n) = (3, 5)$, such that every word with weight 3 is at distance 1 from at least one codewords.

In Chapter 10, we will consider the problem of constructing optimal ACs with splitting property. By the equivalence of splitting ACs and splitting designs established by Huber, we will generalize the methods in design theory to construct two new infinite classes of splitting ACs. The $(3, 2)$-splitting ACs we obtained are the first known infinite family of (t, c)-splitting ACs with $t > 2$ and $c > 1$. We also prove that a $(2, c)$-splitting AC with k source states and v messages exists for all sufficiently large v (with k and c fixed).

Keywords:
q-Ary constant-weight codes, constant-composition codes, constant-weight covering codes, generalized Steiner Systems, completely reducible super simple designs, group divisible codes, authentication codes

目　　录

Chapter 1

绪论

编码理论是主要研究在有噪信道中传输数据和恢复受损数据的一门学科。1948年，Claude Shannon发表了开创性的论文“A mathematical theory of communication”，以此为标志编码理论正式诞生。在短短的60多年中，编码理论蓬勃发展，取得了一系列的重要成果，并在实际生活中得到了广泛的应用，为互联网的兴起以及其它许多数据存储和传输技术的进步奠定了坚实的理论基础。

如何构造好的码一直是编码理论中的一个非常重要的问题。在编码理论的发展过程中人们使用了各种各样的方法来构造不同的码，所用到的知识几乎涉及到了数学的各个分支，包括分析、代数、数论、组合数学、几何等。为了检验构造出来的码是不是好的，人们计算出了许多码的界，即在一定条件下码的参数可能达到的最优值。通过码的参数与这些界的比较，人们可以判断构造出来的码是否有意义。编码理论中的一个重要问题就是构造出能达到这些界的码。

组合设计是组合数学的一个分支。它的理论和方法已渗透到许多学科和领域，特别是在编码学、密码学、计算机科学及实验设计等方面有着广泛应用。组合设计理论中最基本的问题是设计的存在性问题。近年来，组合设计理论研究的热点问题主要集中于经典组合设计和有着实际应用背景的组合设计的存在性问题上。本论文着重研究与编码学和计算机科学相关的组合问题，包括：常重码（constant-weight code）、常重复合码（constant composition codes）、常重覆盖码（constant weight covering code）、认证码（authentication code）等。

常重码

常重码是编码理论中一类重要的码[107]，它要求码中的每个码字的重量都是相同的。编码理论中研究的很多重要的码都是特殊的常重码，如光正交码、常重复合码、完美常重码、等距常重码等。历史上，由于常重码可以用来计算

一般纠错码的界，其一直有着重要的理论意义。近年来，常重码在现实生活中也得到了大量的应用，被用于CDMA系统、并行异步通讯、自动纠错系统等许多领域。另外，常重码的构造问题与组合学中的许多著名难题和猜想相联系。因为在理论研究和实际应用中的双重意义，常重码引起了人们广泛的研究。

对二元常重码，在确定长度为n，重量为w，最小汉明距离为d的码字个数，即$A(n,d,w)$的研究方面已经得到了很多结果。1990年Brouwer等在*IEEE Transactions on Information Theory*上发表的文章"A New Table of Constant Weight Codes"[19]只研究了长度n小于等于28的所有最优二元常重码的码字个数的准确值或下界。这篇文章已经成为编码理论研究中一个重要成果，有很多后续文章研究文中的方法，并改进其结果。由此可见这类问题不但是非常重要而且即使对单个值的确定都是十分困难的。

最近，由于非二元码的诸多应用，如有效带宽信道[46]、DNA计算中核苷酸序列的设计[101, 110]中的重要应用，非二元常重码逐渐引起了人们的重视，有越来越多的文章对其界及构造等方面的问题展开了研究，取得了很多重要的成果，如[15, 22, 23, 26, 59, 60, 102, 115, 131–133, 135, 159]等。

关于多元常重码，其核心问题是确定特定参数下最优多元常重码的码字个数，即$A_q(n,d,w)$，其中$A_q(n,d,w)$表示长度为n，最小汉明距离为d，重量为w的q元码，即$(n,d,w)_q$码的最大可能的码字个数。关于这类问题，一般从两个方面展开研究：一是$A_q(n,d,w)$上界的确定，二是构造出达到上界的最优的多元常重码。

关于多元常重码上界的确定，最初分别由Svanström[133]和Fu[60]给出了Johnson类型的递归界。虽然很多情况下可以证明这个界是紧的，但是在有些情况下它与已知的下界还有一定距离。而其他的更好的上界通常需要用一些特别的方法得到，比如计数、线性规划等方法或者对特定参数的码进行具体的分析。

而对最优多元常重码的构造，如果没有好的组合方法，人们只能对长度非常小的码逐个解决。在文[115]中，Östergård和Svanström仅在$n \leq 10$时，对任意的d，w给出了$A_3(n,d,w)$的准确值或界。目前，对最优多元常重码的组合构造主要有以下方法：

1）1997年由以色列著名数学家Etzion首先给出了一类最优多元常重码与组合结构的等价性，并把这种结构称为广义Steiner系（generalized Steiner

system）[56]，用来构造长度为n，重量为k，最小汉明距离为$2k-3$的最优$g+1$元常重码。随后国内外的组合学家引进了很多构造方法对其展开研究，得到了很多结果（如[10, 32, 33, 56, 62–64, 73, 116, 117, 151, 156]等）。Yin等把广义Steiner系推广到填充情况，来对n不满足广义Steiner系存在的必要条件时，构造一般参数的最优多元常重码[97, 156]。然而目前的研究工作多是集中在重量为3的情况，当重量为4时，由于方法的限制，研究结果不多。

对重量为4，最小汉明距离为5的最优三元常重码，即$(n, 5, 4)_3$码，Ji, Wu和Zhu（欧拉奖获得者）在文[97] 中，对所有$n \geq 10$，$n \equiv 1 \pmod 3$，$n \notin \{13, 52, 58\}$，研究了广义Steiner系的构造，从而确定了$A_3(n, 5, 4)$的准确值。在第3章中，我们研究了所有长度的最优$(n, 5, 4)_3$码，通过建立了一种辅助设计frame-GS与可分组码的联系，并运用可分组码的循环构造方法对任意$n \geq 4$，除了$n \in \{12, 13, 21, 27, 33, 39, 45, 52\}$ 以外的所有长度确定了$A_3(n, 5, 4)$的准确值。本章内容已发表于杂志*IEEE Transactions on Information Theory*。

但是这种方法当q变大时，由于需要构造的设计的组变大，无疑难度要增加很多。对重量为4，最小汉明距离为5的最优四元常重码，即$(n, 5, 4)_3$码，当长度$n \equiv 0, 1 \pmod 4$ 时，尽管在文[74, 75, 150, 165] 等中给出了一些构造方法和较少的无穷类，但是距离这个问题的完全解决还很远。在第4章中，我们改进原来文章中的SIP构造法，用可分组设计和超单正交表直接构造出广义Steiner系，使得在构造较小参数的码时更加有效。运用这个方法，再结合一些型不一致的辅助设计，frame-GS，我们对任意$n \geq 4$，除了55个不确定的长度以外，确定了$A_4(n, 5, 4)$的准确值。本章内容已发表于杂志*IEEE Transactions on Information Theory*。

2）2007年Chee等在文[26]中提出了组合设计中的不相交设计、大集与一些最优多元常重码的等价性，并对所有的q，n确定了$A_q(n, 3, 2)$和$A_q(n, 4, 3)$ 的值[23, 26]。在此基础上，在第5章中，我们建立了区组大小为4的完全可约超单设计（completely reducible super simple design）与最优$(n, 6, 4)_q$码的联系。结合一种辅助设计，完全可约超单可分组设计，这种设计可以看作构造此类码的可分组码，结合可分组码的递归构造方法，我们对任意长度n，完全确定了除$n = 17$以外的所有$A_3(n, 6, 4)$的准确值。此类常重码之前已知的结果只有Östergård 和Svanström在文[115] 中确定的长度10以内的值。本章内容已发

表于杂志*IEEE Transactions on Information Theory*。

由于完全可约超单设计对应最优多元常重码，而完全可约超单可分组设计对应在构造码时有重要应用的可分组码，而超单填充也与码有着密切联系，在第6章中，我们解决了区组大小为4，指数为3的完全可约超单设计，区组大小为4，指数为2的一致的完全可约超单可分组设计和超单填充的存在性问题，并且得到了一类新的最优$(n, 6, 4)_4$ 码。本章内容已发表于杂志*Designs, codes and Cryptography*。

3）对最优多元常重码的研究工作，多是考虑固定重量w和最小汉明距离d，而让长度n和码元q变动时，最优多元常重码的构造问题。目前已知具有完整结果的，只有当参数(d, w)取值$(3, 2)$和$(4, 3)$的情形。在文[24]中，Chee等对任意$q \geq 2$，得到了最优$(n, 2w-1, w)_q$码的渐近结果。他们称这种码是线性大小的，因为$A_q(n, 2w-1, w) = O(n)$。在第7章中，我们对所有长度n，$q \geq 2$，确定了$A_q(n, 5, 3)$的准确值。具体的，我们建立了这种码与Hanani三元填充的联系，而Hanani三元填充是组合设计中Hanani三元系的推广，后者是著名组合学家Stinson，Colbourn（欧拉奖获得者）等在1993年提出并解决的[140]。在本章中，我们不但建立了其与$(n, 5, 3)_q$码的联系，还将其推广到填充情况，并完全解决了Hanani三元填充的存在性。

常重复合码

常重复合码（constant-composition code）是一类特殊的常重码，它要求码中的每个码字的元素组成都是相同的。具有非常重要应用的置换码就是一种常重复合码。由于其在多址通信、DNA码、电力线通讯、跳频序列等许多方面的应用，上世纪九十年代末，对常重复合码就有了系统的研究[14, 17, 133]。人们为了确定常重复合码的最大可能的码字个数引入了各种各样的方法，如计算机搜索方法[16]，填充设计[38, 49, 50, 93, 144, 153, 154, 157]，竞赛设计[158]，多项式和非线性函数[38, 47, 48, 51, 52]，PBD闭包方法[25, 28] 和一些其他的方法[105, 106, 134, 149] 等。

在文[25]，Chee等提出了对其构造起重要作用的可分组码的概念以及与组合设计中类似的构造方法。在第8章中，我们建立了一类可分组码与重量为4，最小汉明距离为6的最优三元常重复合码，即$(n, 6, [2, 2])_3$码的联系。我们还给出了一个用斜Room frame构造此类可分组码的方法，结合一些长度较小的码，

和型不一致的可分组码的直接构造，我们对长度$n \neq 5 \pmod 6$，除了11个值外确定了此类码的码字个数，对$n \equiv 5 \pmod 6$，我们也给出了好的下界。

常重覆盖码

常重覆盖码（constant weight covering code）的主要应用是数据压缩算法[39, 80]。从数学方面而言，其码字容量下界的确定是也是一个基本的组合问题。在组合设计理论中，有一些和它等价的组合结构[41]，如Turán设计、彩票方案、覆盖设计等，在过去的六十多年中有许多研究者对其进行了研究。

令$K_q(n, w, t, d)$表示长度为n，重量为w，每个重量为t的字与至少一个码字的最小汉明距离为d的q元常重覆盖码的最小可能的码字个数。在第9章中，我们建立一类常重覆盖码和可分组覆盖的联系，结合一种辅助设计：H-frame，我们对任意整数$n \geq 4$，$q \in \{3, 4\}$或者$q = 2^m + 1$ （$m \geq 2$），除了$(q, n) = (3, 5)$以外，完全确定了$K_q(n, 4, 3, 1)$的值。本章内容已发表于杂志*Designs, codes and Cryptography*。

认证码

在认证码（authentication code）的标准模型中[122–124, 127]，一个发射器需要在一个不安全信道传送信息给一个接收器，而一个敌人访问这个信道并想欺骗接收器。在一个阶数为i的欺骗攻击[108]中，敌人在非安全信道中观察到由发射器发出的在相同编码规则下的i 个不同的信息，并加入一个与已发送的i个信息不同的新的信息，并希望被接收器认为是可信的。在这种框架下，当对认证码的身份模拟和身份替换攻击只是阶数为0和1的欺骗攻击时，已经有了很多研究工作，然而当阶数$i \geq 2$时，对分裂认证码的研究却很少。

在文[92]中，Huber建立了阶数$i \geq 2$时，分裂认证码与分裂设计的联系。在第10章中，我们通过构造分裂设计来构造具有分裂性质的最优认证码。具体的，我们定义了一些与组合设计理论中类似的辅助设计，如分裂t-GDD，分裂烛台设计等，并推广了组合设计中的递归方法，得到了一些新的无穷类。本章内容已发表于杂志*Advances in Mathematics of Communications*。

本论文中所应用的方法涉及组合设计理论中的多种不同的设计和构造方法。然而，组合设计用来构造码的方法非常广泛，文中所用的方法仅是九牛一毛。在以后的研究工作中，作者将继续探索编码理论中的组合设计方法。

本文收录了作者攻读博士学位期间的部分论文，发表和投稿的详细情况可参见文中附表。限于作者水平有限，文中难免有不当谬误之处，敬请诸位不吝批评和指正。

Chapter 2

基本定义和符号

在本章中，我们将介绍编码理论和组合设计中的一些基本定义符号和基本结果。

对整数$m \leq n$，令$[m,n]_a$表示集合$\{m, m+a, m+2a, \ldots, n\}$。当$a=1$时，我们将下标省略。我们把模$n$整数环，$\mathbb{Z}/n\mathbb{Z}$记为$\mathbb{Z}_n$，非负整数集记为$\mathbb{Z}_{\geq 0}$。对任意两个集合$X$和$Y$，$X \times Y$记为它们的笛卡尔积，即：$X \times Y = \{(x,y) : x \in X, y \in Y\}$。对一个有限集合$X$和整数$n \in [1, |X|]$，记

$$\binom{X}{n} = \{A \subseteq X : |A| = n\}。$$

2.1 码

令X和R是有限集，R^X表示一个长度为$|X|$的向量的集合，其中每个向量$\mathsf{u} \in R^X$在R中取值，并用X中的元素标记，即：$\mathsf{u} = (\mathsf{u}_x)_{x \in X}$，且对任意$x \in X$，$\mathsf{u}_x \in R$。

一个*长度为n的q元码*就是一个集合$\mathcal{C} \subseteq \mathbb{Z}_q^X$，其中$|X| = n$。$\mathcal{C}$中的元素称为*码字*。一个向量$\mathsf{u} \in \mathbb{Z}_q^X$的*汉明重量*定义为$\|\mathsf{u}\| = |\{x \in X : \mathsf{u}_x \neq 0\}|$。两个码字$\mathsf{u}, \mathsf{v} \in \mathbb{Z}_q^X$的*汉明距离*，记为$d_H$，就是$d_H(\mathsf{u}, \mathsf{v}) = \|\mathsf{u} - \mathsf{v}\|$。对任意向量$\mathsf{u} \in \mathbb{Z}_q^X$，定义$\mathsf{u}$的*支撑集*为$\mathrm{supp}(\mathsf{u}) = \{x \in X : \mathsf{u}_x \neq 0\}$。

我们说一个码$\mathcal{C}$具有（*最小汉明*）*距离*d，如果任意两个相异码字$\mathsf{u}, \mathsf{v} \in \mathcal{C}$，$d_H(\mathsf{u}, \mathsf{v}) \geq d$。因为在本文中我们研究的都是最小汉明距离，为了简便起见，当我们说一个码的距离，就是指的是它的最小汉明距离。如果对任意码字$\mathsf{u} \in \mathcal{C}$，$\|\mathsf{u}\| = w$，那么我们称$\mathcal{C}$具有（常）*重量*$w$。我们把一个长度为$n$，距离为$d$，重量为$w$的$q$元常重码，记为$(n,d,w)_q$码。一个$(n,d,w)_q$码中的码字个数被称为码的*大小*，并把它最大可能的码字个数记为$A_q(n,d,w)$。大小达到$A_q(n,d,w)$的码被称为是*最优的*。

Svanström 在文[133]中给出了$A_q(n,d,w)$的上界：

引理 2.1 (Svanström [133]).

$$A_q(n,d,w) \le \left\lfloor \frac{n}{n-w} A_q(n-1,d,w) \right\rfloor 。$$

引理 2.2 (Svanström [133]).

$$A_q(n,d,w) \le \left\lfloor \frac{n(q-1)}{w} A_q(n-1,d,w-1) \right\rfloor 。$$

一个码字$\mathsf{u} \in \mathcal{C}$的复合是一个向量$\overline{w} = [w_1, \cdots, w_{q-1}]$，使得$\mathsf{u}$包含$i \in \mathbb{Z}_q \setminus \{0\}$恰好$w_i$次。如果$\mathcal{C}$中的每个码字都有复合$\overline{w}$，那么就称$q$元码$\mathcal{C}$具有常复合$\overline{w}$。一个长度为$n$，距离为$d$，具有常复合$\overline{w}$的$q$元码记为$(n,d,\overline{w})_q$码。一个$(n,d,\overline{w})_q$码中的码字个数被称为码的大小，并把它最大可能的码字个数记为$A_q(n,d,\overline{w})$。大小达到$A_q(n,d,\overline{w})$的码被称为是最优的。一般，我们假设在$\overline{w} = [w_1, \cdots, w_{q-1}]$中，$w_1 \ge \cdots \ge w_{q-1}$。

Svanström等在文章[135]中给出了$A_q(n,d,\overline{w})$的一个上界。

引理 2.3 (Svanström等[135]).

$$A_q(n,d,[w_1,\ldots,w_{q-1}]) \le \left\lfloor \frac{n}{w_1} A_q(n-1,d,[w_1-1,\ldots,w_{q-1}]) \right\rfloor 。$$

2.2 设计

一个集合系统（set system）是一个二元组$(X,\mathcal{B})$，其中X是一个点集，$\mathcal{B}$是X的一个子集族，称为区组。一个集合系统的阶数就是X中点的个数。对一个非负整数集K，如果对任意$B \in \mathcal{B}$，都有$|B| \in K$，那么称$(X,\mathcal{B})$为K-一致的。

对一个非负整数集合K，一个成对平衡设计（$(v,K,1)$-PBD）就是一个阶数为v的K-一致的集合系统$(X,\mathcal{B})$，使得X中的任意相异点对恰好出现在$\mathcal{B}$的一个区组中。一个元素$k \in K$是"加星的"，记为$k^\star$，就是说这个PBD恰好有一个大小为k的区组。

引理 2.4 (Ling等[104]). *对任意整数$v \ge 10$，$v \notin [10,20] \cup [22,24] \cup [27,29] \cup [32,34]$，都存在一个$(v,\{5,6,7,8,9\},1)$-PBD。*

引理 2.5 (Ling等[104]，Colbourn等[44])．如果$v \geq 10$，$v \notin [10,30] \cup [32,41] \cup [45,47] \cup [93,95] \cup [98,101] \cup [138,139] \cup [142,150] \cup [152,155] \cup [160,161] \cup [166,167] \cup \{185\}$，那么存在一个$(v, \{6,7,8,9\}, 1)$-*PBD*。

引理 2.6 (Colbourn，Ling [45])．如果$v \geq 11$，$v \notin [11,56] \cup [58,63] \cup [66,71] \cup [75,79] \cup [101,109] \cup [111,113] \cup [115,119] \cup [126,127] \cup [133,135] \cup [155,160] \cup [166,167] \cup [173,231] \cup \{239\} \cup [247,287] \cup [290,295] \cup [299,343] \cup [346,351] \cup [355,399] \cup [403,407] \cup [411,423] \cup [426,431] \cup [435,439] \cup [443,448] \cup [452,455] \cup [472,497] \cup [499,503] \cup [507,511] \cup [580,582]$，那么存在一个$(v, \{8,9,10\}, 1)$-*PBD*。

引理 2.7 (Rees，Stinson [118])．一个$(v, \{4, w^\star\}, 1)$-*PBD*，$v > w$存在当且仅当$v \geq 3w+1$，且：

(i) $v \equiv 1$或$4 \pmod{12}$，$w \equiv 1$或$4 \pmod{12}$；或者

(ii) $v \equiv 7$或$10 \pmod{12}$，$w \equiv 7$或$10 \pmod{12}$。

令$(X, \mathcal{B})$是一个集合系统，$\mathcal{G} = \{G_1, \ldots, G_u\}$是集合$X$的一个划分，称为组。那么一个三元组$(X, \mathcal{G}, \mathcal{B})$被称为是一个可分组设计（group divisible design，GDD），如果X中不在同一个组的点对恰好出现在λ个区组中，且对任意$B \in \mathcal{B}$，$G \in \mathcal{G}$，$|B \cap G| \leq 1$。如果对任意$B \in \mathcal{B}$，$|B| \in K$，那么称$(X, \mathcal{G}, \mathcal{B})$为$(K, \lambda)$-GDD。如果$K = \{k\}$，简记为$(k, \lambda)$-GDD。如果$\lambda = 1$，简记为$K$-GDD或$k$-GDD。

一个GDD的型是一个多重集$\{|G| : G \in \mathcal{G}\}$。我们通常用“指数”符号来表示GDD的型：型为$g_1^{u_1} g_2^{u_2} \ldots g_t^{u_t}$表示对任意$i = 1, 2, \ldots, t$，有$u_i$个大小为$g_i$的组。一个型为$1^v$的$(k, \lambda)$-GDD（$k < v$）称为一个平衡不完全区组设计（balanced incomplete block design，BIBD），记为(v, k, λ)-BIBD。

引理 2.8 ([66])．一个型为g^u的$(4, \lambda)$-*GDD*存在当且仅当（*i*）$u \geq 4$；（*ii*）$\lambda(u-1)g \equiv 0 \pmod 3$，（*iii*）$\lambda u(u-1)g^2 \equiv 0 \pmod{12}$，除了两组确定的值$(g, u, \lambda) \in \{(2,4,1), (6,4,1)\}$外。在这两种情况下，不存在这样的*GDD*。

一个型为n^k的(k, λ)-GDD也称为一个横截设计（transversal design，TD），记为$\mathrm{TD}_\lambda(k, n)$。当$\lambda = 1$时，也记为$\mathrm{TD}(k, n)$。

引理 2.9 ([3]). 令m为一个正整数。那么：

i) 若$m \notin \{2, 6\}$，存在一个$TD(4, m)$；

ii) 若$m \notin \{2, 3, 6, 10\}$，存在一个$TD(5, m)$；

iii) 若$m \notin \{2, 3, 4, 6, 10, 14, 18, 22\}$，存在一个$TD(6, m)$；

iv) 若$m \notin \{2, 3, 4, 5, 6, 10, 14, 15, 18, 20, 22, 26, 30, 34, 38, 46, 60\}$，存在一个$TD(7, m)$；

v) 若$m \notin \{2, 3, 4, 5, 6, 10, 12, 14, 15, 18, 20, 21, 22, 26, 28, 30, 33, 34, 35, 38, 39, 42, 44, 46, 51, 52, 54, 58, 60, 62, 66, 68, 74\}$，存在一个$TD(8, m)$；

vi) 若m是一个素数幂，存在一个$TD(m + 1, m)$。

一个GDD称为一致的如果所有组的大小都相同。区组大小为3或4的一致的GDD的存在谱已经完全被确定（见[66]）。

对型为$g^u m^1$的非一致GDD，当区组大小为3时，它的存在性已经完全被Colbourn等解决[42]。当区组大小为4时，Ge等对它的存在性也做了很多研究工作，如[69, 70, 76–78]等。

研究GDD的主要工具是Wilson's基本构造法（WFC）（见[41]）。

构造 2.10. 令$(X, \mathcal{G}, \mathcal{B})$是一个*GDD*，$w : X \to \mathbb{Z}^+ \cup \{0\}$是$X$上的一个加权函数。假设对任意区组$B \in \mathcal{B}$，都存在一个型为$\{w(x) : x \in B\}$的$K$-*GDD*。那么存在一个型为$\{\sum_{x \in G} w(x) : G \in \mathcal{G}\}$的$K$-*GDD*。

一个双可分组设计（DGDD）是一个四元组$(X, \mathcal{H}, \mathcal{G}, \mathcal{B})$，其中$X$是一个点集，$\mathcal{H}$和$\mathcal{G}$都是$X$的划分（分别称为洞和组），$\mathcal{B}$是$X$中的一个子集族使得：

(i) 对任意区组$B \in \mathcal{B}$，和任意洞$H \in \mathcal{H}$，$|B \cap H| \leq 1$；

(ii) X中的不在同一组中，且不在同一洞中的任意点对都恰好出现在一个区组中，其余点对不出现在任何区组中。

每个区组大小是K中的元素，且有u_i个大小为g_i的组，且每个交v个洞h_i个点的DGDD记为一个型为$(g_1,h_1^v)^{u_1}(g_2,h_2^v)^{u_2}\ldots(g_s,h_s^v)^{u_s}$的$K$-DGDD。一个改进可分组设计，是一个型为$(g,1^g)^u$的$K$-DGDD，记为型为$g^u$的$K$-MGDD。

令$v\geq k$。一个(v,k,λ)-填充是一个阶数为v的$\{k\}$-一致集合系统$(X,\mathcal{B})$，使得X中的任意相异点对最多出现在$\mathcal{B}$的λ个区组中。填充数$D_\lambda(v,k,2)$就是一个(v,k,λ)-填充中最大可能的区组数。

引理 2.11 ([129]). （第一*Johnson*界） $D_\lambda(v,k,2)\leq U_\lambda(v,k,2)$，其中

$$U_\lambda(v,k,2)=\left\lfloor\frac{v}{k}\left\lfloor\frac{\lambda(v-1)}{k-1}\right\rfloor\right\rfloor。$$

一个阶数为v的$\{k\}$-一致集合系统的部分平行类（partial parallel class，PPC）就是一些点不相交的区组的集合，且称为最大的如果它包含$\lfloor v/k\rfloor$个区组（记为MPPC），否则称为非最大的。如果它恰好形成点集的一个划分，那么称之为一个平行类（parallel class，PC）。一个GDD被称为是可分解的 （resolvable），如果它的所有区组可以划分成平行类的集合。一个可分解的K-GDD，简记为K-RGDD。

引理 2.12 ([41]). 一个型为h^u的$\{3\}$-*RGDD*存在当且仅当$u\geq 3$，$h(u-1)$是偶数，$hu\equiv 0\pmod 3$且$(h,u)\notin\{(2,3),(2,6),(6,3)\}$。

Chapter 3

用广义Steiner系构造最优三元常重码

3.1 引言和主要结果

常重码在编码理论中有重要作用[107]。二元常重码已经被广泛研究[19, 128]。最近，由于非二元码的诸多应用，如有效带宽信道[46]、DNA计算中核苷酸序列的设计[101, 110]等，多元常重码的构造逐渐引起了人们的重视。其中，大部分工作是集中在$A_q(n,d,w)$的确定上。我们简要列举一下已有的一些研究工作：

(i) 文[26, 56, 60]研究了$(n,d,w)_q$码的一般构造。

(ii) 文[15, 59, 115, 131, 133]对一般的d和w，研究了$A_3(n,d,w)$的值。

(iii) 文[10, 32, 33, 56, 62–64, 73, 116, 117, 151, 156]研究了$A_q(n,3,3)$。

(iv) 文[67, 74, 75, 97, 150, 152, 162, 165]研究了$A_q(n,5,4)$。

(v) 文[22, 56]研究了$A_3(n,3,4)$。

(vi) 文[23, 26]研究了$A_q(n,3,2)$和$A_q(n,4,3)$。

(vii) 文[24]研究了$A_q(n,2w-1,w)$。

(viii) 文[159]研究了$A_3(n,6,4)$。

在Östergård和Svanström的文章[115]中，他们给出了一些确定$A_3(n,d,w)$的上界和下界的方法，并得到了长度$n \leq 10$的码字个数的准确值或者界。我们在表10.18中列出了长度n不超过10时，$A_3(n,5,4)$的准确值。

广义Steiner系$\mathrm{GS}(2,k,n,g)$是由Etzion在文[56]中提出的，用来构造长度为n，重量为k，距离为$2k-3$的$g+1$元最优常重码。Yin等把广义Steiner 系推广到填充情况，对一般长度n构造最优多元常重码[97, 156]。人们对$\mathrm{GS}(2,k,n,g)$已

表 3.1: 当$n \leq 10$时，$A_3(n,5,4)$的值

n	4	5	6	7	8	9	10
$A_3(n,5,4)$	1	2	4	7	13	19	30

经做了很多研究工作，例如：[10, 32, 56, 62–64, 67, 73, 75, 97, 116, 117, 151, 156]等。在文[97]中，Ji，Wu和Zhu证明了如果$n \geq 10$，$n \equiv 1 \pmod 3$，$n \notin \{13, 52, 58\}$，那么存在一个GS$(2,4,n,2)$。由此我们得到：

引理 3.1. *对任意$n \geq 10$，$n \equiv 1 \pmod 3$，$n \notin \{13,52,58\}$，存在一个大小为$\frac{n(n-1)}{3}$的最优$(n,5,4)_3$码。*

可分组码，类似于组合设计中的可分组设计，是由Chee，Ge和Ling在文[25]中提出的。这种码可以用在常重码和常重复合码的递归构造中。在本章中，我们将用可分组码构造所有长度n的最优$(n,5,4)_3$码。我们对所有长度$n \geq 4$，除了8个不确定的值$n \in \{12,13,21,27,33,39,45,52\}$外，确定了所有长度的最优$(n,5,4)_3$码的码字个数。

众所周知，对$d > 2w$，$A_q(n,d,w) = 1$，因此由引理2.2，我们得到：

引理 3.2. $A_3(n,5,4) \leq \left\lfloor \frac{n}{2} \left\lfloor \frac{2(n-1)}{3} \right\rfloor \right\rfloor := U(n,3)$。

在本章中，我们记最优$(n,5,4)_3$码的上界为$U(n,3)$。

这一章的结构如下：在第3.2节中，我们将介绍一些基本概念和基本构造方法；在第3.3节中，我们将分情况构造最优$(n,5,4)_3$码；在第3.4节中，将对本章的主要结果进行总结。

3.2 准备知识和基本构造方法

如Etzion[56]和Yin等[156]在文中所述，一个$\mathbb{Z}_{g+1}$上的$(n,d,k)_{g+1}$码可以通过构造一个型为g^n的$\{k\}$-GDD，$(I_n \times I_g, \{\{i\} \times I_g : i \in I_n\}, \mathcal{B})$得到，其中$I_m = \{1,2,\ldots,m\}$，$d$是得到的码的距离。对任意区组$\{(i_1,a_1),(i_2,a_2),\ldots,(i_k,a_k)\} \in \mathcal{B}$，我们可以通过对任意$1 \leq j \leq k$，在第$i_j$位放$a_j$，其它位放零得到一个长度为$n$的码字。如果一个型为$g^n$的$\{k\}$-GDD可以形成一个距离为$2k-3$的码，那么就称它为一个广义*Steiner*系（generalized Steiner system，GS），记为GS$(2,k,n,g)$。

下面的frame广义Steiner系的定义是由Ji，Wu和Zhu在文[97]中给出的。

令$n = h_1u_1 + \cdots + h_tu_t$，$\mathcal{P}$是$I_n$的一个划分，其中有$u_i$个大小为$h_i$，$i = 1, 2, \ldots, t$。令$(I_n \times I_g, \{P \times I_g : P \in \mathcal{P}\}, \mathcal{B})$是一个型为$(h_1g)^{u_1} \ldots (h_tg)^{u_t}$的$\{k\}$-GDD。对任意一个区组$\{(i_1, a_1), (i_2, a_2), \ldots, (i_k, a_k)\} \in \mathcal{B}$，令$i_j$的位置为$a_j$，$1 \le j \le k$，其余位置为0，我们得到了一个长度为$n$的码字。如果从这个$\{k\}$-GDD得到的码达到距离$2k-3$，我们称之为一个型为$h_1^{u_1} \ldots h_t^{u_t}$的*frame*广义*Steiner*系（或者简称为*frame*），记为frame-GS$(2, k, (h_1^{u_1} \ldots h_t^{u_t}), g)$。我们称这个$\{k\}$-GDD的组为frame的组，记为$\mathcal{G}$，$\{\{i\} \times I_g : i \in I_n\}$为frame的洞，记为$\mathcal{H}$。与GDD类似，frame-GS的型就是多重集$\mathcal{T} = \{|P| : P \in \mathcal{P}\}$，用“指数”记为$h_1^{u_1} \ldots h_t^{u_t}$。显然，一个GS$(2, k, n, g)$就是一个frame-GS$(2, k, (1^n), g)$。

Chee，Ge和Ling在文[25]中提出了可分组码的概念，这种码在常重码和常重复合码的循环构造中起着重要作用。

给定$\mathsf{u} \in \mathbb{Z}_q^X$，$Y \subseteq X$，令$\mathsf{u}$在$Y$上的限制，记为$\mathsf{u}\,|_Y$，是一个向量$\mathsf{v} \in \mathbb{Z}_q^Y$，使得$\mathsf{v} = (\mathsf{u}_x)_{x \in Y}$。

相对地，令$\mathsf{v} \in \mathbb{Z}_q^Y$，$Y \subseteq X$，$\mathsf{v}$在$X$上的扩张，记为$\mathsf{v}|^X$，就是一个向量$\mathsf{u} \in \mathbb{Z}_q^X$，使得：

$$\mathsf{u}_x = \begin{cases} \mathsf{v}_x, & \text{若} x \in Y; \\ 0, & \text{若} x \in X \setminus Y。 \end{cases}$$

给定集合$\mathcal{C} \subseteq \mathbb{Z}_q^Y$，令$\mathcal{C}|^X = \{\mathsf{v}|^X : \mathsf{v} \in \mathcal{C}\}$。

一个距离为d的可分组码（Group divisible code，GDC）就是一个三元组$(X, \mathcal{G}, \mathcal{C})$，其中$\mathcal{G} = \{G_1, \ldots, G_t\}$是集合$X$（$|X| = n$）的一个划分，$\mathcal{C} \subseteq \mathbb{Z}_q^X$是一个长度为$n$的$q$元码，使得对任意两个相异向量$u, v \in \mathcal{C}$，$d_H(u, v) \ge d$，并且对任意的$u \in \mathcal{C}$，$1 \le i \le t$，$\|u|_{G_i}\| \le 1$。$\mathcal{G}$中的元素称为组。如果$\mathcal{C}$具有常重量$w$，我们把一个距离为$d$的GDC$(X, \mathcal{G}, \mathcal{C})$记为$w$-GDC$(d)$。如果任意$u \in \mathcal{C}$的形式是$\overline{w}$，我们把这个GDC记为$\overline{w}$-GDC$(d)$。GDC$(X, \mathcal{G}, \mathcal{C})$的型是一个多重集$\{|G| : G \in \mathcal{G}\}$。与GDD的表示类似，我们用“指数”表示GDC的型。GDC$(X, \mathcal{G}, \mathcal{C})$的大小是$|\mathcal{C}|$。注意到一个大小为$s$的$(n, d, w)_q$码等价与一个型为$1^n$，大小为$s$的$w$-GDC$(d)$。

由frame-GS的定义，我们有如下结果：

引理 3.3. *如果存在一个具有b个区组的frame-GS$(2, k, (h_1^{u_1} \ldots h_t^{u_t}), g)$，那么存在一个型为$h_1^{u_1} \ldots h_t^{u_t}$大小为$b$的$(g+1)$元$k$-GDC$(2k-3)$。*

推论 3.4. 分别存在型为3^5，大小为60；型为$3^5 6^1$，大小为120；型为2^u，大小为$\frac{4u(u-1)}{3}$，$u \in \{7, 13\}$；型为6^u，大小为$12u(u-1)$，$u \in \{4, 5\}$的4-$GDC(5)$。

我们对码或者GDC的直接构造是基于一般的差方法，即在一个有限群（通常是$\mathbb{Z}_n$）的作用下来得到码或者GDC的所有码字。因此，我们通常仅列出一个基码的集合，然后用加法群或者其它自同构群来得到所有码字。

为了节省空间，对一个GDC的码字$\mathsf{u} = (\mathsf{u}_x)_{x \in X}$，我们只列出集合$\mathrm{supp}(\mathsf{u})$，并用下标来表示对任意$x \in \mathrm{supp}(\mathsf{u})$，$\mathsf{u}_x$的值。在下文中，如果没有明确指出，我们用的自同构通常只是作用在基码的支撑集上，而保持下标不动。

例 3.5. 令$X = \mathbb{Z}_{20}$，组集为$\mathcal{G} = \{\{i, i+10\} : 0 \le i \le 9\}$。那么$(X, \mathcal{G}, \mathcal{C})$就是一个型为$2^{10}$，大小为120的三元4-$GDC(5)$，如果$\mathcal{C}$是由下面码字循环移位得到：

11000200020000000000	10020100000000002000	10010000000000020200
10000012100000000000	10200000010000001000	22000000000020020000

或者，等价地，我们也可以说$\mathcal{C}$是由下面码字在$\mathbb{Z}_{20}$中$+1 \pmod{20}$展开而保持下标不动得到：

$(0_1, 1_1, 5_2, 9_2)$ $(0_1, 5_1, 16_2, 3_2)$ $(0_1, 3_1, 15_2, 17_2)$ $(0_1, 6_1, 8_1, 7_2)$ $(0_1, 9_1, 16_1, 2_2)$ $(0_2, 1_2, 12_2, 15_2)$

显然，型为2^{10}的三元4-GDC(5)也是最优$(20, 5, 4)_3$码，因为它的码字个数达到了引理3.2中的上界。

例 3.6. 令$X = \mathbb{Z}_{16}$，$\mathcal{G} = \{\{i, i+4, i+8, i+12\} : 0 \le i \le 3\}$。那么$(X, \mathcal{G}, \mathcal{C})$就是一个型为$4^4$，大小为64的三元4-$GDC(5)$，如果$\mathcal{C}$是由如下码字在$\mathbb{Z}_{16}$上$+2 \pmod{16}$展开得到：

$(1_1, 8_1, 14_1, 7_2)$	$(0_1, 5_1, 7_1, 14_2)$	$(0_1, 1_1, 2_1, 3_2)$	$(1_1, 6_1, 11_2, 0_2)$
$(1_2, 3_2, 4_2, 14_2)$	$(1_1, 4_1, 15_2, 6_2)$	$(1_1, 7_1, 2_2, 4_2)$	$(0_1, 13_2, 6_2, 7_2)$

例 3.7. 令点集$X = \{0, 1, \ldots, 29\}$，组$\mathcal{G} = \{\{i\} : 0 \le i \le 23\} \cup \{\{24, 25, \ldots, 29\}\}$，那么$(X, \mathcal{G}, \mathcal{C})$就是一个型为$1^{24}6^1$，大小为276的三元4-$GDC(5)$，如果$\mathcal{C}$是由如下码字由自同构群$G = \langle (0\ 2\ 4\ \cdots\ 22)(1\ 3\ 5\ \cdots\ 23)\ (24\ 25\ 26)(27\ 28\ 29) \rangle$展开得到。

$(1_2, 2_2, 5_2, 7_2)$	$(0_1, 5_1, 25_1, 20_2)$	$(1_1, 5_2, 15_2, 28_2)$	$(0_1, 4_1, 16_2, 10_2)$	$(1_1, 5_1, 22_1, 23_1)$
$(0_1, 26_1, 9_2, 1_2)$	$(0_1, 6_1, 21_1, 13_2)$	$(1_1, 8_1, 10_2, 11_2)$	$(1_1, 2_1, 13_2, 20_2)$	$(1_1, 14_1, 16_1, 24_2)$
$(1_1, 28_1, 0_2, 2_2)$	$(1_1, 11_1, 9_2, 25_2)$	$(1_1, 8_2, 12_2, 19_2)$	$(0_1, 23_2, 4_2, 24_2)$	$(0_2, 13_2, 16_2, 26_2)$
$(1_1, 6_1, 27_1, 3_2)$	$(1_1, 12_1, 24_1, 7_2)$	$(1_1, 9_1, 22_2, 27_2)$	$(0_1, 17_2, 8_2, 27_2)$	$(1_1, 29_1, 6_2, 21_2)$
$(0_1, 14_1, 29_1, 5_2)$	$(1_1, 25_1, 4_2, 18_2)$	$(0_1, 16_1, 14_2, 28_2)$		

如下关于GDC的构造在文[25]中给出。

构造 3.8 (Chee等[25]). （基本构造法） 令$d \le 2(w-1)$，$(X, \mathcal{G}, \mathcal{B})$是一个$GDD$，$\omega : X \to \mathbb{Z}_{\ge 0}$是一个加权函数。对任意子集$S \subseteq X$，令$\widehat{S} = \cup_{x\in S}(\{x\} \times \mathbb{Z}_{\omega(x)})$。假设对任意$B \in \mathcal{B}$，存在一个型为$\{\omega(a) : a \in B\}$，大小为$c_B$的（输入）$q$元$w$-$GDC(d)$ $(\widehat{B}, \{\widehat{\{a\}} : a \in B\}, \mathcal{C}_B)$。那么$(\widehat{X}, \{\widehat{G} : G \in \mathcal{G}\}, \cup_{B\in\mathcal{B}}(\mathcal{C}_B|^{\widehat{X}}))$就是一个型为$\{\sum_{x\in G}\omega(x) : G \in \mathcal{G}\}$，大小为$\sum_{B\in\mathcal{B}} c_B$的$q$元$w$-$GDC(d)$。进一步，如果输入$GDC$有常复合$\overline{w}$，那么得到的码也有常复合$\overline{w}$。

例 3.9. 从引理*2.9*取一个$TD(4,5)$ $(X, \mathcal{G}, \mathcal{B})$，并用基本构造法对每个点加权4（即：对任意$x \in X$，$\omega(x) = 4$）。对任意$B \in \mathcal{B}$，由例*3.6*存在一个型为$4^4$，大小为64的三元4-$GDC(5)$（我们称之为输入$GDC$）。那么我们就得到了一个型为$20^4$，大小为1600的三元4-$GDC(5)$。

构造 3.10 (Chee等[25]). （填组） 令$d \le 2(w-1)$。假设$(X, \mathcal{G}, \mathcal{C})$是一个大小为$a$的$q$元$w$-$GDC(d)$。进一步假设，对任意$G \in \mathcal{G}$，都存在一个大小为$c_G$的$(|G|, d, w)_q$码$\mathcal{C}_G$。那么$\mathcal{C}' = \mathcal{C} \cup (\cup_{G\in\mathcal{G}}(\mathcal{C}_G|^X))$就是一个大小为$a + \sum_{G\in\mathcal{G}} c_G$的$(|X|, d, w)_q$码。特别的，如果$\mathcal{C}$和$\mathcal{C}_G$，$G \in \mathcal{G}$有常复合$\overline{w}$，那么得到的码也有常复合$\overline{w}$。

例 3.11. 从例*3.9*取一个型为20^4，大小为1600的三元4-$GDC(5)$。由例*3.5*，我们有一个最优$(20, 5, 4)_3$码。在型为20^4的4-$GDC(5)$的组上填入这个最优码，就得到了一个最优$(80, 5, 4)_3$码。

注意：构造3.10有一个显然的推广，就是在GDC的组上填入小的GDC，来得到大的GDC。例如，如果我们在例3.11中的型为20^4的三元4-GDC(5)的组上填入型为2^{10}，大小为120的三元4-GDC(5)，我们就得到了一个型为2^{40}，大小为2080的三元4-GDC(5)。

构造 3.12. （膨胀法） 令$d \le 2(w-1)$。假设$(X, \mathcal{G}, \mathcal{C})$是一个大小为$c$的$q$元$w$-$GDC(d)$。令$\widetilde{X} = X \times \mathbb{Z}_m$，$\widetilde{\mathcal{G}} = \{G \times \mathbb{Z}_m : G \in \mathcal{G}\}$。进一步假设，对任意码字$\mathsf{u} \in \mathcal{C}$，存在一个$TD(w, m)$，$(\mathrm{supp}(\mathsf{u}) \times \mathbb{Z}_m, \{\{x\} \times \mathbb{Z}_m : x \in \mathrm{supp}(\mathsf{u})\}, \mathcal{B}_\mathsf{u})$。对任意$B \in \mathcal{B}_\mathsf{u}$，构造一个码$\mathsf{v}_B \in \mathbb{Z}_q^{\widetilde{X}}$，$(\mathsf{v}_B)_{(x,i)} = \mathsf{u}_x$，$(x, i) \in B$，其它位置为零。那么$(\widetilde{X}, \widetilde{\mathcal{G}}, \cup_{\mathsf{u}\in\mathcal{C}} \cup_{B\in\mathcal{B}_\mathsf{u}} \mathsf{v}_B)$就是一个型为$\{m|G| : G \in \mathcal{G}\}$，大小为$cm^2$的$q$元$w$-$GDC(d)$。进一步，如果原始的$GDC$有常复合$\overline{w}$，那么得到的$GDC$也有常复合$\overline{w}$。

例 3.13. 由引理*2.9*存在一个$TD(4,4)$。从推论*3.4*取一个型为6^4，大小为144的三元4-$GDC(5)$。由构造*3.12*，我们得到了一个型为24^4，大小为2304的三元4-$GDC(5)$。我们也称这个过程为对型为6^4的4-$GDC(5)$用4膨胀。

构造 3.14 (Chee等[25]). （增加y个点） 令$y \in \mathbb{Z}_{\geq 0}$。假设$(X, \mathcal{G}, \mathcal{C})$是大小为$c$的（主）$q$元$w$-$GDC(d)$。令$Y$是一个大小为$y$的集合，并且与$X$不相交，令$X' = X \cup Y$。进一步假设存在如下的（输入）码：

i) 对一个组$G_0 \in \mathcal{G}$，存在一个大小为c_{G_0}的$(|G_0|+y, d, w)_q$码$\mathcal{C}_{G_0}$；

ii) 对任意组$G \in \mathcal{G} \setminus \{G_0\}$，存在一个型为$1^{|G|}y^1$，大小为$c_G$的$q$元$w$-$GDC(d)$ $(G \cup Y, \{\{x\} : x \in G\} \cup \{Y\}, \mathcal{C}_G)$。

那么，$(\mathcal{C}|^{X'}) \cup (\mathcal{C}_{G_0}|^{X'}) \cup (\cup_{G \in \mathcal{G} \setminus \{G_0\}} (\mathcal{C}_G|^{X'}))$就是一个大小为$c + c_{G_0} + \sum_{G \in \mathcal{G} \setminus \{G_0\}} c_G$的$(|X|+y, d, w)_q$码。进一步，如果主码和输入码都有常复合$\overline{w}$，那么得到的码也有常复合$\overline{w}$。

例 3.15. 这里我们构造一个最优$(30, 5, 4)_3$码。令点集为$\mathbb{Z}_{30}$，所有码字由如下基码在$\mathbb{Z}_{30}$上$+2 \pmod{30}$展开得到。

$(0_1, 1_1, 3_1, 24_1)$	$(1_1, 6_1, 8_2, 13_2)$	$(0_1, 5_1, 11_2, 19_2)$	$(0_2, 10_2, 13_2, 18_2)$	$(0_1, 22_1, 10_2, 16_2)$
$(1_1, 5_1, 15_1, 28_2)$	$(0_1, 2_1, 20_1, 23_2)$	$(0_1, 13_1, 26_1, 22_2)$	$(0_1, 16_1, 6_2, 17_2)$	$(1_1, 29_2, 6_2, 20_2)$
$(0_1, 23_1, 4_2, 8_2)$	$(1_1, 7_1, 27_2, 9_2)$	$(1_1, 11_2, 25_2, 4_2)$	$(1_1, 0_2, 2_2, 19_2)$	$(1_1, 2_1, 13_1, 17_2)$
$(1_1, 9_1, 12_1, 26_2)$	$(0_1, 25_2, 27_2, 28_2)$	$(0_1, 21_1, 12_2, 13_2)$	$(0_1, 29_2, 5_2, 9_2)$	

从例*3.13*取一个型为24^4，大小为2304的三元4-$GDC(5)$。增加6个无穷点，在前三个组上连同这6个无穷点填入例*3.7*中的型为$1^{24}6^1$，大小为276的4-$GDC(5)$，在最后一个组上连同无穷点填入上面的最优$(30, 5, 4)_3$码，我们就得到了一个最优$(102, 5, 4)_3$码。

在下文中我们将考虑重量为4，距离为5的三元常重码，因此，在本章中我们将把三元4-GDC(5)简记为GDC。

3.3 主要证明过程

a. 一些小的GDC和最优码

在本节中，我们将构造一些小的GDC和最优码，这些码我们将在下面的构造中用到。

引理 3.16. *对所有$u \in \{16, 19, 22, 28\}$，存在型为2^u，大小为$\frac{4u(u-1)}{3}$的GDC。*

证明. 对任意$u \in \{16, 19, 22, 28\}$，令点集为$X_u = \mathbb{Z}_{2u}$，组集为$\mathcal{G}_u = \{\{i, i+u\} : 0 \le i \le u-1\}$。那么$(X_u, \mathcal{G}_u, \mathcal{C}_u)$是一个型为$2^u$，大小为$\frac{4u(u-1)}{3}$的GDC，如果$\mathcal{C}_u$是由[162, 表 III]中的码字在$\mathbb{Z}_{2u}$中$+1 \pmod{2u}$展开得到。 □

引理 3.17. *存在一个型为4^7，大小为224的GDC。*

证明. 令点集$X = \mathbb{Z}_{28}$，组集为$\mathcal{G} = \{\{i, i+7, i+14, i+21\} : 0 \le i \le 6\}$。那么$(X, \mathcal{G}, \mathcal{C})$就是一个型为$4^7$，大小为224的GDC，如果$\mathcal{C}$是由如下码字在$\mathbb{Z}_{28}$中$+1 \pmod{28}$展开得到。

$$(0_1, 17_1, 4_2, 19_2) \quad (0_1, 12_2, 13_2, 17_2) \quad (0_1, 6_1, 8_1, 9_1) \quad (0_1, 10_1, 23_1, 11_2)$$
$$(0_1, 4_1, 10_2, 26_2) \quad (0_1, 18_2, 24_2, 27_2) \quad (0_1, 3_2, 5_2, 23_2) \quad (0_1, 16_1, 8_2, 25_2)$$

□

引理 3.18. *对所有$u \in [6, 10] \cup \{19\}$，存在型为$6^u$，大小为$12u(u-1)$的GDC。*

证明. 对任意$u \in \{6, 8, 9\}$，令点集$X_u = \mathbb{Z}_{6u}$，组集为$\mathcal{G}_u = \{\{i, i+u, \ldots, i+5u\} : 0 \le i \le u-1\}$。那么$(X_u, \mathcal{G}_u, \mathcal{C}_u)$就是型为$6^u$，大小为$12u(u-1)$的GDC，如果$\mathcal{C}_u$是由如下码字在$\mathbb{Z}_{6u}$上$+1 \pmod{6u}$展开得到。

$u = 6$:

$$(0_1, 2_2, 9_2, 10_2) \quad (0_1, 10_1, 19_1, 21_1) \quad (0_1, 28_1, 31_1, 29_2) \quad (0_1, 14_1, 17_2, 21_2) \quad (0_1, 14_2, 19_2, 28_2)$$
$$(0_1, 5_2, 8_2, 25_2) \quad (0_1, 13_2, 15_2, 26_2) \quad (0_1, 32_1, 16_2, 31_2) \quad (0_1, 13_1, 29_1, 4_2) \quad (0_1, 1_1, 23_2, 33_2)$$

$u = 8$:

$$(0_1, 2_1, 44_1, 1_2) \quad (0_1, 10_2, 27_2, 38_2) \quad (0_1, 28_1, 31_1, 41_1) \quad (0_1, 7_2, 11_2, 26_2) \quad (0_1, 25_1, 36_1, 42_2)$$
$$(0_1, 26_1, 27_1, 9_2) \quad (0_1, 12_2, 18_2, 19_2) \quad (0_1, 29_1, 34_1, 14_2) \quad (0_1, 22_2, 25_2, 35_2) \quad (0_1, 39_1, 34_2, 36_2)$$
$$(0_1, 30_1, 2_2, 23_2) \quad (0_1, 21_2, 39_2, 44_2) \quad (0_1, 33_1, 37_2, 46_2) \quad (0_1, 3_2, 15_2, 29_2)$$

$u = 9$:

$$(0_1, 5_2, 7_2, 8_2) \quad (0_1, 10_1, 51_1, 34_2) \quad (0_1, 26_2, 31_2, 42_2) \quad (0_1, 20_1, 42_1, 53_2) \quad (0_1, 26_1, 21_2, 41_2)$$
$$(0_1, 1_1, 7_1, 20_2) \quad (0_1, 10_2, 32_2, 47_2) \quad (0_1, 30_1, 35_1, 16_2) \quad (0_1, 17_2, 38_2, 46_2) \quad (0_1, 50_1, 39_2, 51_2)$$
$$(0_1, 2_1, 17_1, 33_1) \quad (0_1, 11_1, 25_1, 23_2) \quad (0_1, 46_1, 22_2, 48_2) \quad (0_1, 6_2, 25_2, 29_2) \quad (0_1, 4_2, 14_2, 28_2)$$
$$(0_1, 3_2, 44_2, 50_2)$$

对$u \in \{7, 10, 19\}$，分别对型为2^u的GDC（引理3.5，推论3.4和引理3.16）用3膨胀得到所需的GDC。 □

引理 3.19. *存在一个型为$3^6 6^1$，大小为162的GDC。*

证明. 令点集为$X=\{0,1,\ldots,23\}$，组集为$\mathcal{G}=\{\{i,i+6,i+12\}:0\le i\le 5\}\cup\{\{18,\ldots,23\}\}$。那么$(X,\mathcal{G},\mathcal{C})$是一个型为$3^6 6^1$，大小为162的GDC，如果$\mathcal{C}$是由如下码字由自同构群$G=\langle(0\ 2\ 4\ \cdots\ 16)(1\ 3\ 5\ \cdots\ 17)(18\ 19\ 20)\rangle$展开得到。

$(0_1,1_2,4_2,19_2)$ $(1_1,3_1,6_1,16_2)$ $(1_1,12_1,5_2,20_2)$ $(1_1,11_1,22_1,9_2)$ $(1_1,14_1,15_1,19_2)$
$(0_1,22_1,7_2,8_2)$ $(1_1,8_1,6_2,22_2)$ $(1_2,9_2,14_2,19_1)$ $(0_2,3_2,10_2,18_2)$ $(1_1,11_2,15_2,21_2)$
$(0_1,3_1,20_1,2_2)$ $(0_1,14_1,21_1,9_2)$ $(0_1,16_1,15_2,22_2)$ $(1_1,18_1,2_2,3_2)$ $(1_1,21_1,4_2,8_2)$
$(0_1,3_2,5_2,14_2)$ $(0_1,8_1,17_1,19_1)$ $(1_1,10_2,12_2,23_2)$

□

引理 3.20. *对任意$u\in\{4,5\}$，存在一个型为6^u3^1，大小为$12u^2$的GDC。*

证明. 对任意$u\in\{4,5\}$，令$X_u=\{0,1,\ldots,6u+2\}$，组集为$\mathcal{G}_u=\{\{i,i+u,\ldots,i+5u\}:0\le i\le u-1\}\cup\{\{6u,6u+1,6u+2\}\}$。那么$(X_u,\mathcal{G}_u,\mathcal{C}_u)$就是型为$6^u3^1$，大小为$12u^2$的GDC，如果$\mathcal{C}_u$是由如下码字由自同构群$G=\langle(0\ 1\ 2\ 3\ \cdots\ 6u-1)(6u\ 6u+1\ 6u+2)\rangle$展开得到。

$u=4$：

$(0_1,2_1,15_1,21_1)$ $(0_1,17_1,10_2,23_2)$ $(0_1,2_2,5_2,11_2)$ $(0_1,14_1,26_1,15_2)$
$(0_1,3_2,13_2,26_2)$ $(0_1,25_1,21_2,22_2)$ $(0_1,7_2,9_2,14_2)$ $(0_1,1_1,19_2,25_2)$

$u=5$：

$(0_1,4_1,3_2,27_2)$ $(0_1,1_1,14_2,30_2)$ $(0_1,9_1,12_1,28_1)$ $(0_1,8_1,31_1,26_2)$ $(0_1,11_2,28_2,31_2)$
$(0_1,4_2,6_2,22_2)$ $(0_1,30_1,2_2,21_2)$ $(0_1,12_2,16_2,19_2)$ $(0_1,7_1,24_1,1_2)$ $(0_1,8_2,9_2,17_2)$

□

引理 3.21. *对任意$u\ge 4$，存在一个型为12^u，大小为$48u(u-1)$的GDC。*

证明. 当$u\equiv 0$或$1\pmod 4$，$u\ge 4$时，由引理2.7，存在一个$(3u+1,\{4\},1)$-PBD。在这个PBD的点集去掉一个点得到型为3^u的$\{4\}$-GDD。当$u\equiv 2$或$3\pmod 4$，$u\ge 7$时，由引理2.7存在一个$(3u+1,\{4,7^\star\},1)$-PBD。从这个PBD的点集去掉一个不在大小为7的组中的点得到型为3^u的$\{4,7^\star\}$-GDD。因此，对任意$u\ge 4$，$u\ne 6$，我们总有一个型为3^u的$\{4,7\}$-GDD。

对这个型为3^u的$\{4,7\}$-GDD，用基本构造法加权4得到型为12^u的GDC。这里，输入的是型为4^4和4^7的GDC（例3.6和引理3.17）。

对$u=6$，取一个型为4^6的$\{5\}$-GDD（见文[71]），用基本构造法加权3得到所需的GDC。这里，输入的是型为3^5的GDC（推论3.4）。 □

引理 3.22. *对任意$u\in[4,9]$，存在一个型为12^u18^1，大小为$48u(u+2)$的GDC。*

证明. 对任意$u \in [4,9]$，令点集为$X_u = \{0,1,\ldots,12u+17\}$，组集为$\mathcal{G}_u = \{\{i, i+u, \ldots, i+11u\} : 0 \le i \le u-1\} \cup \{\{12u, \ldots, 12u+17\}\}$。那么$(X_u, \mathcal{G}_u, \mathcal{C}_u)$就是型为$12^u 18^1$，大小为$48u(u+2)$的GDC，如果$\mathcal{C}_u$是由[162, 表 IV]中的码字在如下自同构群$G$下展开得到。

当$u = 4$时，$G = \langle (0\ 2\ 4\ \cdots\ 46)(1\ 3\ 5\ \cdots\ 47)(48\ 51\ 54\ \cdots\ 63)(49\ 52\ 55\ \cdots\ 64)(50\ 53\ 56\ \cdots\ 65)\rangle$。

当$u \in \{5,7,8,9\}$时，$G = \langle (0\ 1\ 2\ \cdots\ 12u-1)(12u\ 12u+1\ 12u+2\ \cdots\ 12u+5)(12u+6\ 12u+7\ 12u+8\ \cdots\ 12u+17)\rangle$。

当$u = 6$时，$G = \langle (0\ 1\ 2\ \cdots\ 71)(72\ 73\ 74)(75\ 76\ 77)(78\ 79\ 80)(81\ 82\ 83)(84\ 85\ 86)(87\ 88\ 89)\rangle$。 □

引理 3.23. *存在一个型为$1^{12}4^1$，大小为72的GDC。*

证明. 令点集为$X = \{0,1,\ldots,15\}$，组为$\mathcal{G} = \{\{i\} : 0 \le i \le 11\} \cup \{\{12,\ldots,15\}\}$。那么$(X, \mathcal{G}, \mathcal{C})$就是型为$1^{12}4^1$，大小为72的GDC，如果$\mathcal{C}$是由如下码字由自同构群$G = \langle (0\ 4\ 8)(1\ 5\ 9)(2\ 6\ 10)(3\ 7\ 11)(12\ 13\ 14)(15)\rangle$展开得到。

$(0_1, 2_1, 7_1, 1_2)$	$(1_1, 2_1, 4_1, 12_2)$	$(3_1, 7_1, 0_2, 14_2)$	$(3_1, 12_1, 1_2, 2_2)$	$(3_1, 7_2, 10_2, 12_2)$	$(9_1, 14_1, 2_2, 6_2)$
$(1_1, 0_2, 2_2, 5_2)$	$(1_1, 4_2, 7_2, 13_2)$	$(0_1, 6_1, 2_2, 12_2)$	$(2_1, 5_1, 3_2, 15_2)$	$(2_1, 15_1, 9_2, 11_2)$	$(2_1, 14_1, 0_2, 4_2)$
$(2_1, 6_2, 7_2, 8_2)$	$(1_1, 6_1, 9_2, 14_2)$	$(0_1, 5_1, 11_1, 7_2)$	$(2_1, 3_1, 6_1, 13_1)$	$(1_2, 7_2, 11_2, 14_1)$	$(5_1, 1_1, 3_1, 14_1)$
$(0_1, 1_1, 15_1, 8_2)$	$(1_2, 4_2, 5_2, 14_2)$	$(0_1, 3_1, 6_2, 15_2)$	$(0_1, 4_1, 12_1, 9_2)$	$(0_1, 13_1, 4_2, 11_2)$	$(4_1, 7_2, 2_2, 14_2)$

□

当$n \equiv 1 \pmod 3$时，我们对$A_3(n,5,4)$有如下改进。

引理 3.24. $A_3(58,5,4) = U(58,3)$，$A_3(13,5,4) \ge U(13,3) - 4$，$A_3(52,5,4) \ge U(52,3) - 12$。

证明. 对$n = 58$，令点集为$\mathbb{Z}_{58}$。所需的码字由如下码字在$\mathbb{Z}_{58}$中$+2 \pmod{58}$展开得到。

$(1_1, 3_2, 5_2, 6_2)$	$(1_1, 24_1, 48_2, 4_2)$	$(0_1, 44_2, 19_2, 26_2)$	$(1_1, 13_1, 30_2, 7_2)$	$(0_1, 33_1, 49_1, 18_2)$
$(0_1, 4_1, 47_2, 5_2)$	$(1_1, 37_2, 8_2, 17_2)$	$(0_1, 57_2, 36_2, 42_2)$	$(0_1, 31_1, 39_1, 52_2)$	$(1_2, 10_2, 27_2, 48_2)$
$(0_1, 6_2, 9_2, 49_2)$	$(1_1, 45_1, 48_1, 2_2)$	$(1_1, 10_2, 20_2, 46_2)$	$(0_1, 30_2, 34_2, 17_2)$	$(1_1, 35_1, 50_1, 12_2)$
$(1_1, 2_1, 5_1, 34_1)$	$(1_1, 6_1, 22_1, 29_1)$	$(1_1, 11_1, 18_1, 57_2)$	$(0_1, 8_1, 28_1, 56_2)$	$(0_1, 8_2, 21_2, 32_2)$
$(0_1, 19_1, 53_2, 3_2)$	$(1_1, 7_1, 55_2, 32_2)$	$(1_1, 12_1, 27_1, 39_2)$	$(0_1, 27_1, 41_2, 22_2)$	$(1_1, 33_2, 38_2, 45_2)$
$(0_1, 1_1, 50_2, 31_2)$	$(0_1, 10_2, 11_2, 35_2)$	$(1_1, 14_1, 19_1, 27_2)$	$(0_1, 18_1, 15_2, 25_2)$	$(1_1, 24_2, 40_2, 52_2)$
$(0_1, 21_1, 54_2, 4_2)$	$(0_1, 13_1, 37_2, 23_2)$	$(1_1, 21_1, 23_1, 41_2)$	$(0_1, 2_2, 29_2, 33_2)$	$(0_1, 6_1, 46_2, 51_2)$
$(0_1, 2_1, 14_1, 24_1)$	$(0_1, 17_1, 14_2, 16_2)$	$(1_1, 23_2, 29_2, 51_2)$		

对$n=13$，令点集为$\{0,1,2,\ldots,12\}$。所需的48个码字直接构造如下：

$(0_1,7_2,4_1,6_1)$	$(10_1,1_2,8_1,6_1)$	$(8_1,0_1,11_2,5_2)$	$(4_2,5_1,9_1,8_2)$	$(7_2,5_2,8_2,10_1)$	$(0_1,10_1,11_1,6_2)$
$(1_2,0_1,3_2,8_2)$	$(11_2,5_1,7_2,1_2)$	$(8_1,4_1,10_2,3_1)$	$(3_2,9_2,1_1,4_1)$	$(7_1,2_1,10_1,4_1)$	$(10_1,1_1,12_2,4_2)$
$(1_2,0_2,9_1,7_1)$	$(11_2,6_1,1_1,2_2)$	$(8_1,6_2,12_1,4_2)$	$(3_1,5_2,2_1,11_1)$	$(6_1,2_1,10_2,9_1)$	$(10_2,11_1,1_1,8_2)$
$(2_1,1_1,8_1,0_2)$	$(12_1,9_1,2_2,5_2)$	$(9_1,4_1,6_2,11_2)$	$(0_2,7_2,11_1,2_2)$	$(0_2,4_1,12_2,5_2)$	$(10_2,12_1,0_1,7_1)$
$(2_1,5_1,0_1,9_2)$	$(12_1,9_2,6_1,0_2)$	$(9_2,11_1,7_1,4_2)$	$(5_2,7_1,1_1,6_2)$	$(6_2,1_2,2_1,12_2)$	$(11_1,1_2,4_1,12_1)$
$(2_2,1_2,4_2,3_1)$	$(1_1,3_1,7_2,12_1)$	$(3_2,9_1,8_1,11_1)$	$(8_2,9_2,2_2,6_2)$	$(12_2,3_2,11_2,7_1)$	$(4_2,0_2,10_2,11_2)$
$(3_1,5_1,0_2,6_2)$	$(1_2,10_2,5_2,9_2)$	$(7_2,8_1,9_2,12_2)$	$(8_1,2_2,7_1,5_1)$	$(12_2,5_1,6_1,11_1)$	$(8_2,2_1,12_1,11_2)$
$(3_1,6_1,7_1,8_2)$	$(3_1,0_1,9_1,12_2)$	$(7_2,6_2,10_2,3_2)$	$(6_1,3_2,4_2,5_2)$	$(12_1,5_1,10_1,3_2)$	$(9_2,10_1,11_2,3_1)$

对$n=52$，由引理3.21存在型为12^4的GDC。增加4个无穷点，并在前3个组上连同无穷点填入引理3.23中的型为$1^{12}4^1$的GDC，在最后一个组上连同无穷点填入最优$(16,5,4)_3$码就得到了所需的码。 □

b. 当长度$n\equiv 0 \pmod 6$时

在本节中，我们将确定当$n\equiv 0 \pmod 6$时，$A_3(n,5,4)$的值。当$n=12$时，我们有如下的界。

引理 3.25. $A_3(12,5,4)\geq U(12,3)-1$。

证明. 令点集为$\{0,1,2,\ldots,11\}$，所需41个码字如下：

$(0_2,1_1,4_1,7_1)$	$(9_1,0_2,5_2,6_1)$	$(5_1,9_2,4_2,0_1)$	$(5_2,9_2,10_1,2_2)$	$(5_1,0_2,3_1,10_2)$	$(5_2,10_2,11_2,1_2)$
$(1_1,5_2,8_1,0_1)$	$(9_1,2_2,3_1,1_1)$	$(5_1,9_1,7_2,1_2)$	$(6_2,10_2,4_2,8_1)$	$(11_2,1_1,6_1,9_2)$	$(4_2,9_1,11_2,10_1)$
$(1_2,2_1,4_1,8_1)$	$(9_2,0_2,1_2,3_2)$	$(4_2,8_2,0_2,2_2)$	$(6_2,1_1,7_2,10_1)$	$(11_2,0_2,7_2,2_1)$	$(7_1,10_2,2_2,11_1)$
$(1_2,2_2,0_1,6_2)$	$(0_1,10_2,9_1,2_1)$	$(8_1,2_2,6_1,5_1)$	$(1_1,3_2,8_2,10_2)$	$(11_1,3_1,1_2,4_2)$	$(10_1,8_1,11_1,0_2)$
$(3_1,8_1,9_2,7_1)$	$(0_1,11_2,3_1,8_2)$	$(6_2,9_2,2_1,8_2)$	$(11_2,6_2,5_1,7_1)$	$(7_2,9_2,10_2,4_1)$	$(11_1,2_1,5_1,1_1)$
$(3_2,6_1,4_2,7_2)$	$(0_1,6_1,4_1,11_1)$	$(6_1,7_1,1_2,8_2)$	$(3_1,6_1,2_1,10_1)$	$(9_1,11_1,6_2,3_2)$	$(7_1,0_1,10_1,3_2)$
$(4_1,6_2,3_1,5_2)$	$(10_1,5_1,4_1,8_2)$	$(4_2,2_1,7_1,5_2)$	$(3_2,11_2,4_1,2_2)$	$(11_1,5_2,7_2,8_2)$	

□

引理 3.26. *对任意*$n\equiv 0 \pmod 6$，$18\leq n\leq 66$*或*$n=78$，$A_3(n,5,4)=U(n,3)$。

证明. 对$n=30$，所需码在例3.15中构造。对其它的n，令点集为$\mathbb{Z}_n$，所需的码字由[162, 表 V]中的码字在$\mathbb{Z}_n$中$+2 \pmod n$展开得到。 □

引理 3.27. *存在型为*$1^{66}18^1$，*大小为*2211*的*GDC。*

证明. 令$X = \{0, 1, \ldots, 83\}$，组集为$\mathcal{G} = \{\{i\} : 0 \le i \le 65\} \cup \{\{66, 67, \ldots, 83\}\}$。那么$(X, \mathcal{G}, \mathcal{C})$是型为$1^{66}18^1$，大小为2211的GDC，如果$\mathcal{C}$是由[162, 表 VI]中的码字由自同构群$G = \langle(0\ 2\ 4\ \cdots\ 64)(1\ 3\ 5\ \cdots\ 65)(66\ 67\ 68)(69\ 70\ 71)(72\ 73\ 74)(75\ 76\ 77)(78\ 79\ 80)(81\ 82\ 83)\rangle$展开得到。 □

引理 3.28. *对任意$u \ge 4$，存在一个型为18^u，大小为$108u(u-1)$的GDC。*

证明. 对$u \ge 4$，$u \ne 6$，证明与引理3.21的证明类似。这里输入的GDC为型为6^4和6^7的GDC（推论3.4和引理3.18）。对$u = 6$，取引理3.18中的型为6^6的GDC，用3膨胀得到所需的GDC。 □

推论 3.29. *对任意$u \ge 4$，$A_3(18u, 5, 4) = U(18u, 3)$。*

证明. 取引理3.28中的型为18^u的GDC。在组上填入最优$(18, 5, 4)_3$码（引理3.26），就对任意$u \ge 4$得到了最优$(18u, 5, 4)_3$码。 □

引理 3.30. *对任意$u \in \{3, 4\}$，$A_3(18u + 30, 5, 4) = U(18u + 30, 3)$。*

证明. 当$u = 3$，从引理3.27取型为$1^{66}18^1$的GDC。在长度为18的组上填入最优$(18, 5, 4)_3$码就得到了所需的码。对$u = 4$，所需的码在例3.15中给出。 □

引理 3.31. *对任意$u \ge 31$，$m \in \{24, 30\}$，存在一个型为$18^u m^1$，大小为$108u(u-1) + 12um$的GDC。*

证明. 从引理2.9取一个TD$(6, 3t)$，用基本构造法对前4个组的所有点，第5个组的$3x$个点，最后一个组的y个点加权6，其中$x = 0$或$3 \le x \le t$，$y \in \{1, 2\}$。其余点加权0。这里输入的是型为6^4，6^5和6^6的GDC（推论3.4和引理3.18）。我们就得到了型为$(18t)^4(18x)^1(6y)^1$的GDC。增加18个无穷点，在前5个组连同无穷点填入型为18^{t+1}或18^{x+1}的GDC就得到了型为$18^{4t+x}(6y + 18)^1$的GDC。令$u = 4t + x$，$m = 6y + 18$，我们就得到了型为$18^u m^1$的GDC，其中$m \in \{24, 30\}$，$u = 4t + x$可以取不小于31的任何值。 □

推论 3.32. *对任意$u \ge 31$，$m \in \{24, 30\}$，$A_3(18u + m, 5, 4) = U(18u + m, 3)$。*

证明. 取引理3.31中的型为$18^u m^1$的GDC，其中$u \ge 31$，$m \in \{24, 30\}$。在组上填入适当长度的最优码（引理3.26）就得到了所需的码。 □

引理 3.33. 对任意$u \equiv 0 \pmod 3$，$12 \leq u \leq 27$，$m \in \{24, 30, 42, 48, 60, 66\}$，存在一个型为$18^u m^1$，大小为$108u(u-1)+12um$的*GDC*。

证明. 从引理2.9取一个TD$(10, 9)$，用基本构造法对前4个组的所有点，最后一个组的y个点，剩余i个组的$3x_i$个点，$1 \leq i \leq 5$，加权6，其余点加权0。我们得到了型为$54^4(18x_1)^1 \cdots (18x_5)^1(6y)^1$，$x_i \in \{0, 3\}$，$y \in \{1, 2, 4, 5, 7, 8\}$的GDC。这里，输入码为型为$6^s$，$s \in [4, 10]$（推论3.4和引理3.18）的GDC。增加18个无穷点，在除了大小为$6y$外的所有组上连同无穷点填入型为18^4的GDC，我们得到型为$18^{12+\sum x_i}(6y+18)^1$的GDC，其中$x_i \in \{0, 3\}$，$y \in \{1, 2, 4, 5, 7, 8\}$。令$u = 12 + \sum x_i$，$m = 6y + 18$，我们就得到了型为$18^u m^1$的GDC，其中$u \equiv 0 \pmod 3$，$12 \leq u \leq 27$，$m \in \{24, 30, 42, 48, 60, 66\}$。 □

推论 3.34. 对任意$12 \leq u \leq 29$，$m \in \{24, 30\}$，$A_3(18u+m, 5, 4) = U(18u+m, 3)$。

证明. 从引理3.33取型为$18^u m^1$的GDC，其中$u \equiv 0 \pmod 3$，$12 \leq u \leq 27$，$m \in \{24, 30, 42, 48, 60, 66\}$。在组上填入适当长度的最优码（引理3.26）就得到了所需的码。 □

引理 3.35. 如下*GDC*都存在：

i) 型为24^u，大小为$192u(u-1)$，$u \in \{4, 5, 7, 8\}$；

ii) 型为30^u，大小为$300u(u-1)$，$u \in \{5, 7, 19\}$；

iii) 型为$24^u 36^1$，大小为$192u(u+2)$，$u \in \{4, 5, 7, 8, 22\}$；

iv) 型为$24^u 18^1$，大小为$96u(2u+1)$，$u \in \{4, 5, 7\}$；

v) 型为$24^8 30^1$，大小为14592；

vi) 型为$30^5 24^1$，大小为8400。

证明. 型为24^u，$u \in \{4, 5, 7, 8\}$的GDC是由型为6^u的GDC（推论3.4和引理3.18）用4膨胀得到。

型为30^u，$u \in \{5, 7, 19\}$的GDC是由型为6^u的GDC（推论3.4和引理3.18）用5膨胀得到。

型为24^u36^1，$u \in \{4,5,7,8,22\}$的GDC是对型为6^u9^1的$\{4\}$-GDD（见[77, 定理 1.6]）用基本构造法加权4得到。

对型为24^u18^1，$u \in \{4,5,7\}$的GDC，从引理2.9取一个TD$(5,u)$，去掉一个点得到型为$4^u(u-1)^1$的$\{5,u\}$-GDD。用基本构造法对大小为4的组的所有点，大小为$u-1$的组的3个点加权6，其余点加权0，就得到了型为24^u18^1的GDC。

对型为24^830^1的GDC，取一个TD$(5,8)$，去掉一个点得到型为4^87^1的$\{5,8\}$-GDD。用基本构造法对大小为4的组的所有点，和大小为7的组的5个点加权6，其余点加权0，就得到了型为24^830^1的GDC。

对型为30^524^1的GDC，取一个TD$(6,5)$，用基本构造法对前5个组的所有点，最后一个组的4个点加权6，其余点加权0就得到了型为30^524^1的GDC。 □

推论 3.36. *对任意$u \in [5,11] \cup \{30\}$，$m \in \{24,30\}$或$(u,m) = (4,24)$，$A_3(18u+m,5,4) = U(18u+m,3)$。*

证明. 取引理3.35中的GDC。在组上填入适当长度的最优码（引理3.26），就得到了需要的码。 □

结合引理3.25，3.26和3.30，推论3.29–3.36的结果，我们得到：

定理 3.37. *对任意$n \equiv 0 \pmod 6$，$n \geq 18$，$A_3(n,5,4) = U(n,3)$；$A_3(12,5,4) \geq U(12,3)-1$。*

c. 当长度$n \equiv 2 \pmod 6$时

在本节中，我们将确定当$n \equiv 2 \pmod 6$时，$A_3(n,5,4)$的值。显然，如果存在一个型为2^u，大小为$\frac{4u(u-1)}{3}$，$u \equiv 1 \pmod 3$的GDC，那么就存在一个最优$(2u,5,4)_3$码。

引理 3.38. *对任意$u \equiv 1 \pmod 3$，$7 \leq u \leq 34$或$u \in \{40,43,52\}$，存在一个型为2^u，大小为$\frac{4u(u-1)}{3}$的GDC。*

证明. 对$u \in \{7,10,13,16,19,22,28,40\}$，所需GDC在例3.5，例3.11和推论3.4，引理3.16中分别给出。

对$u \in \{25,31,43\}$，从引理3.21取型为12^s，$s \in \{4,5,7\}$的GDC。增加2个无穷点，并在组上连同无穷点填入型为2^7的GDC就得到了所需GDC。

对$u \in \{34, 52\}$，从引理3.22取型为$12^s 18^1$，$s \in \{4, 7\}$的GDC。增加2个无穷点，并在组上连同无穷点填入型为2^7或2^{10}的GDC就得到了所需GDC。 □

引理 3.39. *对任意$u \equiv 1 \pmod 3$，$u \in \{37, 46, 49\}$或$u \geq 55$，存在一个型为2^u，大小为$\frac{4u(u-1)}{3}$的GDC。*

证明. 取引理3.28和引理3.31–3.35中型为$g^t m^1$的GDC，其中$g \in \{18, 24, 30\}$，$m \in \{18, 24, 30, 42, 48, 60, 66\}$。增加2个无穷点，并在大小为$g$或$m$的组上连同无穷点填入型为$2^{\frac{g}{2}+1}$或$2^{\frac{m}{2}+1}$的GDC（引理3.38），就得到了型为$2^{\frac{gt+m}{2}+1}$的GDC。对任意$u = \frac{gt+m}{2} + 1$，所需的GDC的型和来源列在表3.2中。 □

表 3.2: 引理3.39中所需GDC的型和来源

u	GDC的型	来源
$9s+1$，$s \geq 4$	$18^{s-1}18^1$，$s \geq 4$	引理3.28
$9s+4$或$9s+7$，$s \geq 32$	$18^{s-1}m^1$，$s \geq 32$，$m \in \{24, 30\}$	引理3.31
$9s+4$或$9s+7$，$s \in [13, 30]$	$18^{s-1}m^1$，$s \equiv 0 \pmod 3$，$13 \leq s \leq 28$，$m \in \{24, 30, 42, 48, 60, 66\}$	引理3.33
$49, 61, 85, 97$	$24^s 24^1$，$s \in \{3, 4, 6, 7\}$	引理3.35
$76, 106, 286$	$30^s 30^1$，$s \in \{4, 6, 18\}$	引理3.35
$67, 79, 103, 115, 283$	$24^s 36^1$，$s \in \{4, 5, 7, 8, 22\}$	引理3.35
$58, 70, 94$	$24^s 18^1$，$s \in \{4, 5, 7\}$	引理3.35
112	$24^8 30^1$	引理3.35
88	$30^5 24^1$	引理3.35

结合引理3.38和3.39，我们得到如下结果：

定理 3.40. *对任意整数$n \equiv 2 \pmod 6$，$n \geq 14$，$A_3(n, 5, 4) = U(n, 3)$。*

d. 当长度$n \equiv 5 \pmod 6$时

在本节中，我们将确定$n \equiv 5 \pmod 6$时，$A_3(n, 5, 4)$的值。

引理 3.41. *$A_3(11, 5, 4) = U(11, 3)$。*

证明. 令点集为$\{0, 1, 2, \ldots, 10\}$，所需的33个码字如下：

$(9_1, 5_2, 8_1, 10_1)$ $(0_1, 8_1, 2_2, 7_1)$ $(3_2, 8_1, 9_2, 7_2)$ $(0_2, 2_1, 10_1, 1_1)$ $(3_1, 5_2, 0_1, 7_2)$ $(2_1, 6_2, 9_1, 7_2)$
$(0_1, 10_2, 8_2, 3_2)$ $(0_2, 5_1, 8_1, 1_2)$ $(5_1, 6_2, 8_2, 7_1)$ $(10_1, 4_1, 6_2, 0_1)$ $(3_1, 6_1, 8_2, 2_1)$ $(9_1, 4_2, 8_2, 0_2)$
$(8_1, 2_1, 10_2, 4_1)$ $(1_1, 3_2, 5_1, 9_1)$ $(6_1, 0_1, 9_1, 1_2)$ $(10_1, 5_1, 3_1, 2_2)$ $(9_2, 1_2, 4_1, 5_2)$ $(8_1, 3_1, 4_2, 1_1)$
$(7_2, 1_2, 10_1, 8_2)$ $(1_1, 7_2, 6_1, 4_1)$ $(6_1, 2_2, 4_2, 9_2)$ $(1_1, 7_1, 9_2, 10_2)$ $(9_2, 0_1, 5_1, 2_1)$ $(3_1, 4_1, 9_1, 7_1)$
$(6_1, 7_1, 10_1, 3_2)$ $(1_1, 8_2, 5_2, 2_2)$ $(6_2, 3_1, 0_2, 9_2)$ $(5_1, 7_2, 10_2, 4_2)$ $(2_2, 0_2, 3_2, 4_1)$ $(5_2, 10_2, 0_2, 6_1)$
$(6_2, 1_2, 2_2, 10_2)$ $(2_1, 4_2, 7_1, 1_2)$ $(6_2, 3_2, 5_2, 4_2)$

□

引理 3.42. 对任意$n \equiv 5 \pmod 6$，$17 \le n \le 71$或$n \in \{83, 89\}$，$A_3(n, 5, 4) = U(n, 3)$。

证明. 令点集为$\mathbb{Z}_n$，所需码字由[162, 表 VII]中的码字在$\mathbb{Z}_n$中$+1 \pmod n$展开得到。 □

引理 3.43. 对任意$u \in \{9, 12, 15\}$，存在一个型为2^u5^1，大小为$\frac{4u(u+4)}{3}$的GDC。

证明. 对任意$u \in \{9, 12, 15\}$，令点集$X_u = \{0, 1, \ldots, 2u+4\}$，组集为$\mathcal{G}_u = \{\{i, i+u\} : 0 \le i \le u-1\} \cup \{\{2u, 2u+1, \ldots, 2u+4\}\}$。那么$(X_u, \mathcal{G}_u, \mathcal{C}_u)$就是型为$2^u5^1$，大小为$\frac{4u(u+4)}{3}$的GDC，如果$\mathcal{C}$是由[162, 表 VIII]中的码字由自同构群$G = \langle(0\ 3\ 6\ \cdots\ 2u-3)(1\ 4\ 7\ \cdots\ 2u-2)(2\ 5\ 8\ \cdots\ 2u-1)(2u)(2u+1)(2u+2)(2u+3)(2u+4)\rangle$展开得到。 □

引理 3.44. 对任意$u = 12$或$u \ge 15$，$A_3(6u+5, 5, 4) = U(6u+5, 3)$。

证明. 对$u = 17$，从引理2.9取一个TD$(5, 4)$，用基本构造法对前4个组的所有点，最后一个组的1个点加权6，其余点加权0，得到了一个型为24^46^1的GDC。增加5个无穷点，并在大小为24的组上连同无穷点填入型为$2^{12}5^1$的GDC，在大小为6的组上连同无穷点填入最优$(11, 5, 4)_3$码得到所需的码。

对$u \in \{12, 15, 16\}$或$u \ge 18$，证明与引理3.39中的证明类似。取引理3.28，引理3.31–3.35中构造的型为g^tm^1的GDC，其中$g \in \{18, 24, 30\}$，$m \in \{18, 24, 30, 42, 48, 60, 66\}$。增加5个无穷点，并在大小为$g$的组上连同无穷点填入型为$2^{\frac{g}{2}}5^1$的GDC（引理3.43），在大小为$m$的组上连同无穷点填入长度为$m+5$的最优码（引理3.42），就得到了长度为$gt+m+5$的最优码。 □

结合引理3.41，3.42和3.44，我们得到如下结果：

定理 3.45. 对任意正整数$n \equiv 5 \pmod 6$，$n \ge 11$，$A_3(n, 5, 4) = U(n, 3)$。

e. 当长度$n \equiv 3 \pmod 6$时

在本节中，我们将确定当$n \equiv 3 \pmod 6$时，$A_3(n, 5, 4)$的值。

引理 3.46. $A_3(15, 5, 4) = U(15, 3)$。

证明. 令点集为$\mathbb{Z}_{15}$，我们所需要的67个码字由两部分组成。第一部分包含两个码字$(0_1, 3_2, 6_1, 12_1)$，$(0_2, 6_2, 9_1, 12_2)$。第二部分包含如下65个码字。如下13个码字中的每一个将在f_s，$s \in [0,4]$的作用下生成5个码字，其中：

$$f_s(a_i) = b_{1+\lfloor j/15 \rfloor},$$

$$b \in [0,14], \quad b \equiv a + 6s \pmod{15},$$

$$j \in [0,29], \quad j \equiv a + 15i + 6s \pmod{30}。$$

$(0_1, 1_1, 4_1, 7_2)$ $(3_1, 8_2, 11_2, 0_1)$ $(3_1, 13_2, 4_1, 14_2)$ $(2_1, 3_2, 7_1, 11_2)$ $(0_1, 9_1, 11_1, 13_1)$
$(3_1, 4_2, 2_1, 1_2)$ $(4_1, 6_1, 11_1, 8_2)$ $(4_1, 12_2, 2_1, 14_1)$ $(1_1, 2_1, 5_1, 10_2)$ $(2_1, 11_1, 12_1, 13_2)$
$(0_1, 10_1, 6_2, 2_1)$ $(0_1, 10_2, 12_2, 7_1)$ $(5_1, 13_1, 14_2, 6_2)$

□

引理 3.47. *存在一个型为*$1^{42}15^1$，*大小为*987*的*GDC。*

证明. 令点集$X = \{0, 1, \ldots, 56\}$，组$\mathcal{G} = \{\{i\} : 0 \le i \le 41\} \cup \{\{42, 43, \ldots, 56\}\}$。那么$(X, \mathcal{G}, \mathcal{C})$就是型为$1^{42}15^1$，大小为987的GDC，如果$\mathcal{C}$是由[162, 表 IX]中的码字由自同构群$G = \langle(0\ 2\ 4\ \cdots\ 40)(1\ 3\ 5\ \cdots\ 41)(42\ 43\ 44)(45\ 46\ 47)(48\ 49\ 50)(51\ 52\ 53)(54\ 55\ 56)\rangle$展开得到。 □

引理 3.48. *对所有*$n \in \{15, 21, 27, 33, 39, 45\}$，*存在型为*$1^{n-3}3^1$，*大小为*$\frac{(n-3)(2n+3)}{6}$*的*$GDC$，*因此*$A_3(n, 5, 4) \ge U(n, 3) - 1$。

证明. 对任意$n \in \{15, 21, 27, 33, 39, 45\}$，令点集为$X_n = \{0, 1, \ldots, n-1\}$，组集为$\mathcal{G}_n = \{\{i\} : 0 \le i \le n-4\} \cup \{\{n-3, n-2, n-1\}\}$。那么$(X_n, \mathcal{G}_n, \mathcal{C}_n)$就是型为$1^{n-3}3^1$，大小为$\frac{(n-3)(2n+3)}{6}$的GDC，如果$\mathcal{C}_n$是由[162, 表 X]中的码字由如下自同构群$G$展开得到。

当$n = 15$时，$G = \langle(0\ 4\ 8)(1\ 5\ 9)(2\ 6\ 10)(3\ 7\ 11)(12\ 13\ 14)\rangle$。当$n \in \{21, 27, 33, 39, 45\}$时，$G = \langle(0\ 2\ 4\ \cdots\ n-5)(1\ 3\ 5\ \cdots\ n-4)(n-3\ n-2\ n-1)\rangle$。 □

引理 3.49. *对任意*$n \equiv 3 \pmod{12}$，$n \ge 51$，$A_3(n, 5, 4) = U(n, 3)$。

证明. 对任意n，从引理3.21取一个型为12^u的GDC，增加3个无穷点，并在前$u-1$个组连同无穷点填入型为$1^{12}3^1$的GDC，在最后一个组连同无穷点填入最优$(15, 5, 4)_3$码就得到了所需的码。 □

引理 3.50. *对任意*$n \equiv 9 \pmod{12}$，$n \ge 57$，$A_3(n, 5, 4) = U(n, 3)$。

证明. 对$n = 57$，从引理3.47取一个型为$1^{42}15^1$的GDC，在长度为15的组上填入最优$(15, 5, 4)_3$码就得到所需的码。

对任意$n \in \{69, 81, 93, 105, 117, 129\}$，从引理3.22取一个型为$12^u18^1$，$4 \leq u \leq 9$的GDC。增加3个无穷点，在一个大小为12的组上连同无穷点填入最优$(15, 5, 4)_3$码，在其它的组上连同无穷点填入型为$1^{12}3^1$或$1^{18}3^1$的GDC就得到了所需的码。

对$n = 141$，取一个型为2^95^1的$\{4\}$-GDD（见文[69]），用基本构造法对所有点加权6就得到了一个型为12^930^1的GDC。增加3个无穷点，在一个大小为12的组上连同无穷点填入最优$(15, 5, 4)_3$码，并在其它组上连同无穷点填入型为$1^{12}3^1$或$1^{30}3^1$的GDC就得到了所需的码。

对$n = 177$，取一个型为$2^85^18^1$的$\{4\}$-GDD（见文[66]），用基本构造法对所有点加权6得到了一个型为$12^830^148^1$的GDC。增加3个无穷点，并在大小为48的组连同无穷点填入最优$(51, 5, 4)_3$码，在其它组上连同无穷点填入型为$1^{12}3^1$或$1^{30}3^1$的GDC得到所需的码。

对$n = 189$，从引理2.9取一个TD$(7, 8)$。用基本构造法对前5个组的所有点和第6个组的6个点加权3，对最后一个组的所有点加权6，其余点加权0就得到一个型为$24^518^148^1$的GDC。这里，输入的是型为3^56^1和3^66^1的GDC（推论3.4和引理3.19）。增加3个无穷点，在大小为48的组上连同无穷点填入最优$(51, 5, 4)_3$码，在其余的组上填入型为$1^{24}3^1$或$1^{18}3^1$的GDC就得到所需的码。

对$n \in \{153, 165\}$或$n \geq 201$，从引理2.9取一个TD$(6, t)$。用基本构造法对前4个组的所有点，第5个组的x个点，最后一个组的2个点加权6，对最后一个组的一个点加权3，其余点加权0，我们就得到了一个型为$(6t)^4(6x)^115^1$的GDC，其中$x = 0$或$3 \leq x \leq t$。在每个组上填入长度为$6t$，$6x$（定理3.37）或15（引理3.46）的最优码就得了长度为$6(4t + x) + 15$的最优码，这里$4t + x$可以取到23，25或任何不小于31的奇数。 □

综合如上引理，我们得到：

定理 3.51. 对任意$n = 15$或$n \equiv 3 \pmod 6$，$n \geq 51$，$A_3(n, 5, 4) = U(n, 3)$；对任意$n \in \{21, 27, 33, 39, 45\}$，$A_3(n, 5, 4) \geq U(n, 3) - 1$。

3.4 结论

在本章中，我们几乎完全确定了重量为4，最小距离为5的最优三元常重码的码字个数。我们把主要结果总结如下：

定理 3.52. 对任意正整数$n \geq 4$，

$$A_3(n,5,4) = \begin{cases} 1, & \text{当} n = 4\text{时} \\ 2, & \text{当} n = 5\text{时} \\ 4, & \text{当} n = 6\text{时} \\ 7, & \text{当} n = 7\text{时} \\ 13, & \text{当} n = 8\text{时} \\ 19, & \text{当} n = 9\text{时} \\ \left\lfloor \frac{n}{2} \left\lfloor \frac{2(n-1)}{3} \right\rfloor \right\rfloor, & \text{当} n \geq 10,\ n \notin \{12,13,21,27,33,39,45,52\}\text{时} \end{cases}$$

$$A_3(n,5,4) \in \left[\left\lfloor \frac{n}{2} \left\lfloor \frac{2(n-1)}{3} \right\rfloor \right\rfloor - 1,\ \left\lfloor \frac{n}{2} \left\lfloor \frac{2(n-1)}{3} \right\rfloor \right\rfloor \right],$$

对任意$n \in \{12,21,27,33,39,45\}$；$A_3(13,5,4) \in [48,52]$；$A_3(52,5,4) \in [872,884]$。

Chapter 4

用广义Steiner系构造最优四元常重码

4.1 引言和主要结果

Etzion在文[56]中首先提出了广义Steiner系GS$(2,k,n,g)$的概念，并用来构造长度为n，重量为k，距离为$2k-3$的最优$g+1$元常重码。

关于GS$(2,k,n,g)$的大部分工作都集中在$k=3$的情况（见文[10, 32, 33, 56, 62–64, 73, 116, 117, 151, 156]），对其它k的结果却不多。在前一章中，我们证明了当$k=4$，$g=2$时，GS$(2,4,n,2)$的必要条件除了$n\in\{7,13,52\}$外都是充分的（也见文[67, 97, 152, 162]）。当$k=4$，$g=3$时，GS$(2,4,n,3)$也有一些研究结果（见文[74, 75, 150, 165]）。尽管文章中已经得到了一些GS$(2,4,n,3)$的构造方法和无穷类，但是距离这个问题的完全解决还很远。文[75]中给出GS$(2,4,n,3)$存在的必要条件是$n\geq 8$，$n\equiv 0,1 \pmod 4$。

引理 4.1 (Ge，Wu [75]). *所有素数*$n\equiv 1 \pmod 4$，$n>13$，*存在*$GS(2,4,n,3)$。

引理 4.2 (Ge，Wu [74]). *如果*$m\equiv 0,1 \pmod 4$，$m\geq 8$，$n\equiv 1 \pmod 4$*是素数，*$n>13$，*那么存在一个*$GS(2,4,mn,3)$*和一个*$GS(2,4,m(n-1)+1,3)$。

引理 4.3 (Zhu，Ge [165]). *如果*$m\geq 14$，$2n+1\equiv 1 \pmod 4$*是素数，*$2n+1>13$，*那么存在一个*$GS(2,4,2mn+1,3)$*和一个*$GS(2,4,m(2n+1),3)$。

在本章中，我们将对所有长度的n，研究最优$(n,5,4)_4$码的构造。我们除了55个不确定的长度外，确定了所有长度的最优$(n,5,4)_4$码的码字个数。特别的，当$n\equiv 0,1 \pmod 4$时，我们只有7个不确定的值，也就是说除了7个不确定的值以外，GS$(2,4,n,3)$存在的必要条件也是充分的。

由引理2.2，我们得到：

推论 4.4. $A_4(n,5,4)\leq \left\lfloor \frac{3n(n-1)}{4} \right\rfloor := U(n,4)$。

这一章的结构如下：在第4.2节中，我们将介绍一些基本概念和基本构造方法；在第4.3节中，我们将给出一个SDP构造方法；在第4.4节中，我们将分情况构造最优$(n,5,4)_4$ 码；在第4.5节中，将对本章的主要结果进行总结。

4.2 准备知识和基本构造方法

令$N = I_n \times I_g$。在下面构造中，我们将使用上一章frame定义中的符号。Ji等在文[97]中提出了如下构造方法。

构造 4.5 (Ji等[97]). （填组） 假设$(N,\mathcal{G},\mathcal{H},\mathcal{B})$是一个*frame-GS*$(2,k,\mathcal{T},g)$。进一步假设对任意$P\in\mathcal{P}$，都存在一个$GS(2,k,|P|,g)$ $(P\times I_g,\{\{i\}\times I_g : i\in P\},\mathcal{B}_P)$。那么，$(N,\{\{i\}\times I_g : i\in I_n\},\mathcal{B}\cup(\cup_{P\in\mathcal{P}}\mathcal{B}_P))$是一个$GS(2,k,n,g)$。

构造 4.6 (Ji等[97]). （增加s个点） 假设$(N,\mathcal{G},\mathcal{H},\mathcal{B})$是一个*frame-GS*$(2,k,\mathcal{T},g)$。令$S$是一个大小为$s$且与$I_n$不相交的集合。进一步假设：

i) 对任意$P_0\in\mathcal{P}$，都存在一个$GS(2,k,|P_0|+s,g)$ $((P_0\cup S)\times I_g,\{\{i\}\times I_g : i\in P_0\cup S\},\mathcal{B}_{P_0})$；

ii) 对任意$P\in\mathcal{P}\setminus\{P_0\}$，都存在一个*frame-GS*$(2,k,(1^{|P|}s^1),g)$，$((P\cup S)\times I_g,\{\{i\}\times I_g : i\in P\}\cup\{S\times I_g\},\{\{i\}\times I_g : i\in P\cup S\},\mathcal{B}_P)$。

那么，$((I_n\cup S)\times I_g,\{\{i\}\times I_g : i\in I_n\cup S\},B\cup(\cup_{P\in\mathcal{P}}B_P))$是一个$GS(2,k,n+s,g)$。

构造 4.7 (Ji等[97]). （基本构造法） 令$(X,\mathcal{G},\mathcal{B})$是一个*GDD*，$\omega : X\to\mathbb{Z}_{\geq 0}$是一个加权函数。对任意$S\subseteq X$，令$\widehat{S}=\cup_{x\in S}((\{x\}\times\mathbb{Z}_{\omega(x)})\times I_g)$。假设对任意$B\in\mathcal{B}$，都存在一个*frame-GS*$(2,k,\{\omega(x) : x\in B\},g)$ $(\widehat{B},\{\widehat{\{x\}} : x\in B\},\{\{(x,y)\}\times I_g : (x,y)\in B\times\mathbb{Z}_{\omega(x)}\},\mathcal{B}_B)$。那么$(\widehat{X},\{\widehat{G} : G\in\mathcal{G}\},\{\{(x,y)\}\times I_g : (x,y)\in X\times\mathbb{Z}_{\omega(x)}\},\cup_{B\in\mathcal{B}}\mathcal{B}_B)$是一个*frame-GS*$(2,k,\{\sum_{x\in G}\omega(x) : G\in\mathcal{G}\},g)$。

构造 4.8 (Ji等[97]). （膨胀法） 假设$(N,\mathcal{G},\mathcal{H},\mathcal{B})$是一个*frame-GS*$(2,k,\mathcal{T},g)$。令$\widetilde{N}=(I_n\times\mathbb{Z}_m)\times I_g$，$\widetilde{\mathcal{G}}=\{(P\times\mathbb{Z}_m)\times I_g : P\in\mathcal{P}\}$，$\widetilde{\mathcal{H}}=\{\{(i,l)\}\times I_g : (i,l)\in I_n\times\mathbb{Z}_m\}$。进一步假设存在$TD(k,m)$，$(\{(i,l,\alpha) : (i,\alpha)\in B,l\in\mathbb{Z}_m\},\{\{(i,l,\alpha) : l\in\mathbb{Z}_m\} : (i,\alpha)\in B\},\mathcal{B}_B)$，$B\in\mathcal{B}$。那么$(\widetilde{N},\widetilde{\mathcal{G}},\widetilde{\mathcal{H}},\cup_{B\in\mathcal{B}}\mathcal{B}_B)$是一个*frame-GS*$(2,k,(m\mathcal{T}),g)$。

我们说一个K-GDD具有"星"性质，记为K-*GDD，如果任意两个区组最多交于两个公共的组。K-*GDD的定义首先在文[33]中提出，被用来构造广义Steiner系。

引理 4.9 (Ge，Wu [74]). *对任意$v \equiv 0, 1 \pmod 4$，$v \geq 8$，存在一个型为3^v的$\{4\}$-*GDD。*

结合引理2.5和引理2.6中的结果，我们得到：

推论 4.10. *对任意$v \geq 11$，$v \notin [11, 30] \cup [32, 41] \cup [45, 47] \cup \{101, 155, 160, 166, 167, 185\}$，存在一个$(v, \{6, 7, 8, 9, 10\}, 1)$-PBD。*

4.3　一个SDP构造法

在文[74]中，Ge和Wu给出了一些SIP构造，并在广义Steiner系的构造中发挥了重要作用。在本节中，我们将给出一个与[74, 构造SIP-3]类似的构造方法。首先，我们需要超单正交表的概念。

令$X = \{1, 2, \ldots, v\}$，L是一个X上的$v^2 \times k$矩阵。我们称L是一个正交表，记为OA(k, v)，如果对L的任意$v^2 \times 2$子矩阵，$X \times X$中的任意有序点对都恰好出现一次。假设$L = (e_{ij})$是一个OA(k, v)，$1 \leq i \leq v^2$，$1 \leq j \leq k$。$R_i = (e_{i1}, \ldots, e_{ik})$称为$L$的一个向量。假设$L_1, L_2, \ldots, L_r$是相同集合上的$r$个OA$(k, v)$。这$r$个OA$(k, v)$被称为是超单的，如果$L_1, L_2, \ldots, L_r$中的任意两个向量都最多有两个位置相同。

引理 4.11 (Ge [65]). *对任意$w \geq 4$，$w \neq 2 \pmod 4$，存在w个超单的$OA(4, w)$。*

构造 4.12. *令g，w，r，h，u和s为非负整数，$1 \leq r \leq w$。假设如下设计都存在：*

(1) 一个型为$(gh)^u$的$\{4\}$-GDD，并且所有的区组可以分成r个集合S_0，S_1，$\ldots$，S_{r-1}，每个组可以分成h个大小为g的子组，使得对任意$0 \leq a \leq r-1$，由S_a得到的码在子组上的最小距离都是5；

(2) r个超单的$OA(4, w)$。

那么存在一个frame-GS$(2, 4, ((hw)^u), g)$。若还存在一个frame-GS$(2, 4, (1^{hw}s^1), g)$和一个GS$(2, 4, hw + s, g)$，那么存在一个GS$(2, 4, uhw + s, g)$。

证明. 令$(X_0, \mathcal{G}_0, \mathcal{B}_0)$是一个满足如上条件的型为$(gh)^u$的$\{4\}$-GDD，其中

$$X_0 = (\mathbb{Z}_u \times \mathbb{Z}_h) \times \mathbb{Z}_g,$$

$$\mathcal{G}_0 = \{(\{i\} \times \mathbb{Z}_h) \times \mathbb{Z}_g : i \in \mathbb{Z}_u\},\ \mathcal{B}_0 = \bigcup_{a=0}^{r-1} S_a。$$

$\mathcal{G}_0$的子组是$\mathcal{H}_0 = \{\{(i,j)\} \times \mathbb{Z}_g : (i,j) \in \mathbb{Z}_u \times \mathbb{Z}_h\}$。对任意区组$B = \{[i_1, j_1, \alpha_1], [i_2, j_2, \alpha_2], [i_3, j_3, \alpha_3], [i_4, j_4, \alpha_4]\} \in \mathcal{B}_0$，不妨假设$i_1 < i_2 < i_3 < i_4$。

令L_0，L_1，$\ldots$，L_{r-1}是$\mathbb{Z}_w$上的r个超单的OA$(4, w)$。现在，我们用如下方式构造新的区组。令$\mathcal{B} = \bigcup_{a=0}^{r-1} V_a$，其中：

$$V_a = \{\{[i_1, j_1, l_1, \alpha_1], [i_2, j_2, l_2, \alpha_2], \ldots, [i_4, j_4, l_4, \alpha_4]\} : \{[i_1, j_1, \alpha_1], \ldots, [i_4, j_4, \alpha_4]\} \in S_a, (l_1, \ldots, l_4) \in L_a\}。$$

令

$$X = (\mathbb{Z}_u \times (\mathbb{Z}_h \times \mathbb{Z}_w)) \times \mathbb{Z}_g,\ \mathcal{G} = \{(\{i\} \times (\mathbb{Z}_h \times \mathbb{Z}_w)) \times \mathbb{Z}_g : i \in \mathbb{Z}_u\}。$$

那么，不难看出$(X, \mathcal{G}, \mathcal{B})$是一个型为$(hwg)^u$的$\{4\}$-GDD。

下面，我们将说明$(X, \mathcal{G}, \mathcal{H}, \mathcal{B})$也是一个洞集为

$$\mathcal{H} = \{\{(i,j,l)\} \times \mathbb{Z}_g : (i,j,l) \in \mathbb{Z}_u \times (\mathbb{Z}_h \times \mathbb{Z}_w)\}$$

的frame-GS$(2, 4, (hw)^u), g)$。

否则，假设存在两个区组$A, A' \in \mathcal{B}$的距离小于5。假设$A = \{[i_1, j_1, l_1, \alpha_1], \ldots, [i_4, j_4, l_4, \alpha_4]\}$，$A' = \{[i'_1, j'_1, l'_1, \alpha'_1], \ldots, [i'_4, j'_4, l'_4, \alpha'_4]\}$。如果$A$和$A'$的距离小于5，那么至少满足下面两种情况之一：

(1) A和A'只有一个公共点，且至少交于3个公共的子组。那么$|\{[i_1, j_1, l_1], \ldots, [i_4, j_4, l_4]\} \cup \{[i'_1, j'_1, l'_1], \ldots, [i'_4, j'_4, l'_4]\}| \geq 3$。我们可以假设$A$ 和A'的前三位坐标分别为$\{[i_1, j_1, l_1], [i_2, j_2, l_2], [i_3, j_3, l_3], [i_4, j_4, l_4]\}$，$\{[i_1, j_1, l_1], [i_2, j_2, l_2], [i_3, j_3, l_3], [i'_4, j'_4, l'_4]\}$，且$\alpha_1 = \alpha'_1$。我们知道$\{[i_1, j_1, \alpha_1], [i_2, j_2, \alpha_2], [i_3, j_3, \alpha_3], [i_4, j_4, \alpha_4]\}$和$\{[i_1, j_1, \alpha_1], [i_2, j_2, \alpha'_2], [i_3, j_3, \alpha'_3], [i'_4, j'_4, \alpha'_4]\}$距离最多为4，它们一定是用不同的OA膨胀。因此，我们有$l_i = l'_i$，$i = 1, 2, 3$，这与超单条件相矛盾。

(2) A和A'没有公共点，但是交于4个公共的子组。$\{[i_1,j_1,l_1],\ldots,[i_4,j_4,l_4]\}=\{[i'_1,j'_1,l'_1],\ldots,[i'_4,j'_4,l'_4]\}$。因为$i_1<i_2<i_3<i_4$，$i'_1<i'_2<i'_3<i'_4$，我们有对任意$1\le i\le 4$，$l_i=l'_i$。然而，$\{[i_1,j_1,\alpha_1],\ldots,[i_4,j_4,\alpha_4]\}$和$\{[i_1,j_1,\alpha'_1],\ldots,[i_4,j_4,\alpha'_4]\}$的距离为4，它们一定是分别用不同的OA膨胀。也就是说$(l_1,\ldots,l_4)$和$(l'_1,\ldots,l'_4)$ 一定是两个不同OA的向量，这与$1\le i\le 4$，$l_i=l'_i$矛盾。

令$S=\{\infty_1,\infty_2,\ldots,\infty_s\}$。假设$(X_i,\mathcal{G}_i,\mathcal{H}_i,\mathcal{B}_i)$，$i\in\{0,1\ldots,u-2\}$是frame-GS$(2,4,(1^{hw}s^1),g)$，其中：$X_i=((\{i\}\times(\mathbb{Z}_h\times\mathbb{Z}_w))\times\mathbb{Z}_g)\cup(S\times\mathbb{Z}_g)$，$\mathcal{G}_i=\{\{(i,j,l)\}\times\mathbb{Z}_g:(j,l)\in\mathbb{Z}_h\times\mathbb{Z}_w\}\cup\{S\times\mathbb{Z}_g\}$，$\mathcal{H}_i=\{\{(i,j,l)\}\times\mathbb{Z}_g:(j,l)\in\mathbb{Z}_h\times\mathbb{Z}_w\}\cup\{\{m\}\times\mathbb{Z}_g:m\in S\}$。

再假设$(X_{u-1},\mathcal{G}_{u-1},\mathcal{B}_{u-1})$是一个GS$(2,4,hw+s,g)$，其中：$X_{u-1}=((\{u-1\}\times(\mathbb{Z}_h\times\mathbb{Z}_w))\times\mathbb{Z}_g)\cup(S\times\mathbb{Z}_g)$，$\mathcal{G}_{u-1}=\{\{(u-1,j,l)\}\times\mathbb{Z}_g:(j,l)\in\mathbb{Z}_h\times\mathbb{Z}_w\}\cup\{\{m\}\times\mathbb{Z}_g:m\in S\}$。那么$(X',\mathcal{G}',\mathcal{B}')$是一个GS$(2,4,uhw+s,g)$，其中：

$$X'=((\mathbb{Z}_u\times(\mathbb{Z}_h\times\mathbb{Z}_w))\times\mathbb{Z}_g)\cup(S\times\mathbb{Z}_g),$$

$$\mathcal{G}'=\{\{(i,j,l)\}\times\mathbb{Z}_g:(i,j,l)\in\mathbb{Z}_u\times(\mathbb{Z}_h\times\mathbb{Z}_w)\}\cup\{\{m\}\times\mathbb{Z}_g:m\in S\},$$

$$\mathcal{B}'=\mathcal{B}\cup(\bigcup_{i\in\mathbb{Z}_u}\mathcal{B}_i)。$$

□

这里当GDD是一般的组型时，证明与构造4.12相同，但是表述更复杂，所以我们把下面构造的证明省略。

构造 4.13. 设g，w，r，s和g_i，u_i，h_i，$i=1,2,\ldots,t$是非负整数，使得对任意$i=1,2,\ldots,t$，$1\le r\le w$，$g_i=h_ig$。假设如下设计都存在：

(1) 一个型为$g_1^{u_1}g_2^{u_2}\ldots g_t^{u_t}$的$\{4\}$-*GDD*具有如下性质，所有区组可以划分成$r$个集合$S_0$，$S_1$，…，$S_{r-1}$，每个大小为$g_i$的组可以划分成$h_i$个大小为$g$ 的子组，使得对任意$0\le a\le r-1$，S_a得到的码在子组上的最小距离都是5；

(2) r个超单的$OA(4,w)$。

那么存在一个*frame-GS*$(2,4,((h_1w)^{u_1}(h_2w)^{u_2}\dots(h_tw)^{u_t}),g)$。进一步，如果对任意$1\le i\le t-1$，都存在一个*frame-GS*$(2,4,(1^{h_iw}s^1),g)$，且存在一个$GS(2,4,h_tw+s,g)$，那么就存在一个$GS(2,4,\sum_{i=1}^{t}u_ih_iw+s,g)$。

在构造4.12取$h=1$，我们得到如下结果：

定理 4.14. 令g，w，r，s和u都是非负整数，$1\le r\le w$。假设下列设计都存在：

(1) 一个型为g^u的$\{4\}$-*GDD*具有如下性质：所有的区组可以划分成r个集合S_0，S_1，$\dots$，S_{r-1}，使得对任意$0\le a\le r-1$，S_a得到的码的最小距离都是5；

(2) r个超单的$OA(4,w)$。

那么存在一个*frame-GS*$(2,4,(w^u),g)$。进一步，若存在*frame-GS*$(2,4,(1^ws^1),g)$和$GS(2,4,w+s,g)$，那么就存在$GS(2,4,uw+s,g)$。

4.4 主要证明过程

a. 一些小的frame-GS和最优码

引理 4.15. 对任意$u\in[6,10]$，存在一个*frame-GS*$(2,4,(4^u),3)$。

证明. 对任意$u\in\{6,7,10\}$，点集为$\{0,1,2,\dots,12u-1\}$，组集为$\{\{0,u,2u,\dots,11u\}+i:0\le i\le u-1\}$，洞集为$\{\{0,4u,8u\}+i:0\le i\le 4u-1\}$。所需区组由下面的基区组通过自同构群$G=\langle(0\ 1\ 2\ \cdots\ 4u-1)(4u\ 4u+1\ 4u+2\ \cdots\ 8u-1)(8u\ 8u+1\ 8u+2\ \cdots\ 12u-1)\rangle$展开得到。

$u=6$：

$\{0,4,5,69\}$	$\{0,7,9,53\}$	$\{0,13,28,50\}$	$\{0,55,56,59\}$	$\{0,25,32,51\}$	$\{24,63,65,56\}$
$\{0,63,71,52\}$	$\{0,3,46,47\}$	$\{0,8,41,57\}$	$\{0,27,31,58\}$	$\{24,32,34,69\}$	$\{0,37,34,62\}$
$\{0,29,38,67\}$	$\{24,35,68,58\}$	$\{0,10,26,45\}$			

$u=7$：

$\{0,1,6,52\}$	$\{0,11,15,59\}$	$\{0,53,62,64\}$	$\{0,2,29,67\}$	$\{0,16,33,38\}$	$\{28,68,76,79\}$
$\{0,54,30,48\}$	$\{0,3,82,60\}$	$\{0,36,61,80\}$	$\{28,31,48,74\}$	$\{0,8,74,58\}$	$\{0,44,71,75\}$
$\{0,39,68,69\}$	$\{28,40,41,73\}$	$\{0,9,41,43\}$	$\{0,40,31,81\}$	$\{28,62,75,80\}$	$\{0,10,47,83\}$

$u = 10$：

$\{0,1,7,94\}$	$\{0,2,55,111\}$	$\{40,44,56,93\}$	$\{40,43,116,91\}$	$\{0,69,74,56\}$	$\{40,108,112,86\}$
$\{0,5,77,46\}$	$\{0,78,64,99\}$	$\{40,61,63,69\}$	$\{0,66,105,107\}$	$\{0,45,52,119\}$	$\{0,83,95,106\}$
$\{0,9,23,58\}$	$\{0,44,82,89\}$	$\{0,43,112,85\}$	$\{0,16,108,102\}$	$\{0,4,65,117\}$	$\{0,13,101,104\}$
$\{0,3,57,42\}$	$\{0,22,73,97\}$	$\{0,15,63,118\}$	$\{40,106,97,98\}$	$\{0,62,116,81\}$	$\{40,41,84,103\}$
$\{0,8,29,76\}$	$\{0,12,71,96\}$	$\{0,67,98,114\}$			

对$u \in \{8,9\}$，取型为3^u的$\{4\}$-*GDD（引理4.9），和三个超单的OA$(4,4)$（引理4.11），并应用定理4.14，就可以得到所需的frame-GS$(2,4,(4^u),3)$。 □

引理 4.16. *对任意$m \in \{6,8\}$，存在一个frame-GS$(2,4,(4^5m^1),3)$。*

证明. 令点集为$\{0,1,2,\ldots,59+3m\}$，组集为$\{\{(20+m)k,(20+m)k+5,(20+m)k+10,(20+m)k+15 : 0 \le k \le 2\}+i : 0 \le i \le 4\} \cup \{\{20+(20+m)k,20+(20+m)k+1,\ldots,20+(20+m)k+m-1 : 0 \le k \le 2\}\}$，洞集为$\{\{0,20+m,40+2m\}+i : 0 \le i \le 20+m-1\}$。所需区组由下面基区组通过如下自同构群$G$展开得到。

$m = 6$：$G = \langle$(0 3 6 9 12 15 18 27 30 33 36 39 42 45 54 57 60 63 66 69)(1 4 7 10 13 16 19 28 31 34 37 40 43 52 55 58 61 64 67 70)(2 5 8 11 14 17 26 29 32 35 38 41 44 53 56 59 62 65 68 71)(20 21 22 23 24)(25)(46 47 48 49 50)(51)(72 73 74 75 76)(77)$\rangle$。

$\{0,1,7,14\}$	$\{0,11,18,46\}$	$\{1,10,43,75\}$	$\{0,2,6,49\}$	$\{0,13,23,27\}$	$\{2,46,10,14\}$
$\{1,26,46,61\}$	$\{0,22,4,28\}$	$\{0,16,44,56\}$	$\{1,33,41,74\}$	$\{1,4,23,59\}$	$\{0,37,38,77\}$
$\{0,17,34,63\}$	$\{1,47,52,54\}$	$\{2,3,25,58\}$	$\{0,29,58,76\}$	$\{2,20,11,41\}$	$\{2,5,29,72\}$
$\{2,4,15,51\}$	$\{0,30,33,72\}$	$\{2,21,27,39\}$			

$m = 8$：$G = \langle$(0 3 6 9 12 15 18 29 32 35 38 41 44 47 58 61 64 67 70 73)(1 4 7 10 13 16 19 30 33 36 39 42 45 56 59 62 65 68 71 74)(2 5 8 11 14 17 28 31 34 37 40 43 46 57 60 63 66 69 72 75)(20 21 22 23 24)(25 26)(27)(48 49 50 51 52)(53 54)(55)(76 77 78 79 80)(81 82)(83)$\rangle$。

$\{0,7,59,77\}$	$\{0,19,26,74\}$	$\{1,38,46,83\}$	$\{1,2,24,61\}$	$\{0,23,62,70\}$	$\{2,43,57,76\}$
$\{1,47,48,59\}$	$\{1,4,71,77\}$	$\{0,29,51,73\}$	$\{2,10,49,59\}$	$\{1,5,21,65\}$	$\{1,22,40,66\}$
$\{0,34,36,82\}$	$\{2,11,26,47\}$	$\{2,9,51,66\}$	$\{0,42,72,81\}$	$\{2,16,52,75\}$	$\{0,18,67,80\}$
$\{0,11,12,21\}$	$\{0,45,55,60\}$	$\{2,34,64,77\}$	$\{0,13,54,63\}$	$\{1,12,14,27\}$	$\{2,41,42,54\}$

□

引理 4.17. *对任意$m \in \{6,8,10\}$，存在一个frame-GS$(2,4,(4^6m^1),3)$。*

证明. 令点集为$\{0,1,2\ldots,71+3m\}$，组集为$\{\{(24+m)k,(24+m)k+6,(24+m)k+12,(24+m)k+18 : 0 \le k \le 2\}+i : 0 \le i \le 5\} \cup \{\{24+(24+$

$m)k, 24+(24+m)k+1, \ldots, 24+(24+m)k+m-1 : 0 \le k \le 2\}\}$，洞集为$\{\{0, 24+m, 48+2m\}+i : 0 \le i \le 24+m-1\}$。所需区组由下面基区组通过如下自同构群$G$展开得到。

$m=6$：$G=\langle(0\ 1\ 2\ \cdots\ 23)(24\ 25)(26\ 27)(28\ 29)(30\ 31\ 32\ \cdots\ 53)(54\ 55)(56\ 57)(58\ 59)(60\ 61\ 62\ \cdots\ 83)(84\ 85)(86\ 87)(88\ 89)\rangle$。

$\{0,1,62,86\}$	$\{0,33,47,49\}$	$\{0,74,65,89\}$	$\{0,3,37,58\}$	$\{0,35,39,79\}$	$\{30,58,75,62\}$
$\{30,25,82,63\}$	$\{0,4,32,63\}$	$\{0,38,31,54\}$	$\{30,27,33,68\}$	$\{0,5,24,46\}$	$\{0,11,57,75\}$
$\{0,40,45,88\}$	$\{30,28,64,67\}$	$\{0,7,29,50\}$	$\{0,51,76,80\}$	$\{30,31,56,77\}$	$\{0,70,77,85\}$
$\{0,8,10,81\}$	$\{0,53,44,84\}$	$\{30,41,80,87\}$	$\{0,9,27,67\}$	$\{0,55,68,69\}$	$\{30,71,73,81\}$

$m=8$：$G=\langle(0\ 1\ 2\ \cdots\ 23)(24\ 25\ 26\ 27\ 28\ 29)(30\ 31)(32\ 33\ 34\ \cdots\ 55)(56\ 57\ 58\ 59\ 60\ 61)(62\ 63)(64\ 65\ 66\ \cdots\ 87)(88\ 89\ 90\ 91\ 92\ 93)(94\ 95)\rangle$。

$\{0,8,9,77\}$	$\{0,30,66,71\}$	$\{0,75,84,92\}$	$\{0,2,45,57\}$	$\{0,31,35,48\}$	$\{0,52,47,89\}$
$\{0,87,74,94\}$	$\{0,3,10,29\}$	$\{0,33,86,90\}$	$\{32,24,33,80\}$	$\{0,4,53,91\}$	$\{0,28,39,67\}$
$\{0,34,36,56\}$	$\{32,26,36,87\}$	$\{0,5,58,83\}$	$\{0,37,40,95\}$	$\{32,40,49,65\}$	$\{64,58,66,80\}$
$\{0,13,54,62\}$	$\{0,42,79,88\}$	$\{32,46,57,68\}$	$\{0,24,55,72\}$	$\{0,46,85,65\}$	$\{32,66,67,91\}$
$\{32,63,74,77\}$	$\{0,27,73,80\}$	$\{0,51,60,81\}$			

$m=10$：$G=\langle(0\ 1\ 2\ \cdots\ 23)(24\ 25\ 26\ 27\ 28\ 29)(30\ 31\ 32\ 33)(34\ 35\ 36\ \cdots\ 57)(58\ 59\ 60\ 61\ 62\ 63)(64\ 65\ 66\ 67)(68\ 69\ 70\ \cdots\ 91)(92\ 93\ 94\ 95\ 96\ 97)(98\ 99\ 100\ 101)\rangle$。

$\{0,2,3,66\}$	$\{0,28,37,48\}$	$\{0,63,78,71\}$	$\{34,36,61,83\}$	$\{0,31,45,75\}$	$\{0,53,73,93\}$
$\{34,24,69,89\}$	$\{0,9,29,79\}$	$\{0,33,87,88\}$	$\{34,30,37,79\}$	$\{0,10,32,41\}$	$\{68,67,73,83\}$
$\{0,35,59,72\}$	$\{0,7,51,62\}$	$\{0,11,76,98\}$	$\{0,36,69,96\}$	$\{0,27,56,82\}$	$\{34,42,90,95\}$
$\{0,16,39,95\}$	$\{0,43,65,84\}$	$\{34,43,44,67\}$	$\{0,20,81,94\}$	$\{0,5,38,101\}$	$\{0,60,90,77\}$
$\{34,70,73,98\}$	$\{0,24,49,42\}$	$\{0,50,54,58\}$	$\{34,85,87,97\}$	$\{0,25,83,91\}$	$\{34,39,77,100\}$

□

引理 4.18. *存在一个frame-GS*$(2,4,(4^7 10^1),3)$。

证明. 令点集为$\{0,1,2\ldots,113\}$，组集为$\{\{38k, 38k+7, 38k+14, 38k+21 : 0 \le k \le 2\}+i : 0 \le i \le 6\} \cup \{\{28+38k, 29+38k, \ldots, 37+38k : 0 \le k \le 2\}\}$，洞集为$\{\{0,38,76\}+i : 0 \le i \le 37\}$。所需区组由下面基区组通过自同构群$G=\langle(0\ 1\ 2\ \cdots\ 27)(28\ 29\ 30\ 31\ 32\ 33\ 34)(35\ 36)(37)(38\ 39\ 40\ \cdots\ 65)(66\ 67\ 68\ 69\ 70\ 71\ 72)(73\ 74)(75)(76\ 77\ 78\ \cdots\ 103)(104\ 105\ 106\ 107\ 108\ 109\ 110)(111\ 112)(113)\rangle$展开得到。

$\{0,1,87,92\}$	$\{0,5,39,109\}$	$\{0,3,63,111\}$	$\{38,67,89,92\}$	$\{0,50,51,79\}$	$\{38,77,88,111\}$
$\{0,6,28,54\}$	$\{38,29,53,80\}$	$\{0,56,64,96\}$	$\{38,32,85,86\}$	$\{0,68,95,82\}$	$\{42,76,78,109\}$
$\{0,8,71,88\}$	$\{38,36,43,84\}$	$\{0,11,15,66\}$	$\{0,31,101,81\}$	$\{38,48,64,71\}$	$\{0,73,84,103\}$
$\{0,2,12,32\}$	$\{0,37,65,100\}$	$\{0,19,36,89\}$	$\{0,94,78,105\}$	$\{0,41,85,106\}$	$\{0,55,58,110\}$
$\{0,33,40,44\}$	$\{38,72,81,91\}$	$\{0,47,75,77\}$	$\{0,53,102,113\}$	$\{38,30,99,103\}$	$\{0,93,99,108\}$
$\{0,43,49,67\}$	$\{0,57,46,107\}$	$\{0,42,61,74\}$			

□

b. 长度$n \equiv 0, 1 \pmod 4$时

通过计算机搜索可以很容易确定最优$(5, 5, 4)_4$码只有3个码字，例如：$\{30122, 12011, 21230\}$。

引理 4.19. *对任意$n \in \{17, 29, 37, 41, 53, 61, 73, 89, 101, 109, 149, 157\}$，存在一个$GS(2, 4, n, 3)$。*

证明. 所需设计由引理4.1得到。 □

引理 4.20. *对任意$n \in [16, 60]_4 \cup \{72, 92\}$，存在一个$GS(2, 4, n, 3)$。*

证明. 令点集为$\{0, 1, 2, \ldots, 3n-1\}$，组集为$\{\{0, n, 2n\} + i : 0 \le i \le n-1\}$。所需区组由[161, 表 I]中的基区组通过自同构群$G = \langle (0\ 1\ 2\ \cdots\ n-2)(n-1)(n\ n+1\ n+2\ \cdots\ 2n-2)(2n-1)(2n\ 2n+1\ 2n+2\ \cdots\ 3n-2)(3n-1)\rangle$展开得到。 □

引理 4.21. *对任意$n \in \{21, 25, 33, 45, 49, 57, 69\}$，存在一个$GS(2, 4, n, 3)$。*

证明. 令点集为$\{0, 1, 2, \ldots, 3n-1\}$，组集为$\{\{0, n, 2n\} + i : 0 \le i \le n-1\}$。所需区组由[161, 表 II]中的基区组通过自同构群$G = \langle (0\ 1\ 2\ \cdots\ n-1)(n\ n+1\ n+2\ \cdots\ 2n-1)(2n\ 2n+1\ 2n+2\ \cdots\ 3n-1)\rangle$展开得到。 □

显然，当$s \in \{0, 1\}$时，一个frame-GS$(2, 4, (1^w s^1), 3)$就是GS$(2, 4, w+s, 3)$。应用定理4.14和引理4.11，我们得到如下结果。

引理 4.22. *对任意$n \in \{64, 68, 76, 80, 84, 100, 116, 148, 156\} \cup \{65, 77, 81, 85, 93\}$，存在一个$GS(2, 4, n, 3)$。*

证明. 因为一个型3^4的$\{4\}$-GDD有9个区组，一个型为3^5的$\{4\}$-GDD有15个区组，我们可以把区组集划分成每个部分一个区组。取$g = 3$，和表4.1中的参数(u, w, s)，可以得到相应的GS$(2, 4, n, 3)$。 □

引理 4.23. *下列frame-GS均存在：*

i) frame-GS$(2, 4, (16^u), 3)$，$u \in [6, 10]$；

ii) frame-GS$(2, 4, (20^u), 3)$，$u \in \{7, 9\}$；

表 4.1: 引理4.22中的参数(u,w,s)

n	(u,w,s)	n	(u,w,s)	n	(u,w,s)	n	(u,w,s)
64	$(4,16,0)$	65	$(4,16,1)$	68	$(4,17,0)$	76	$(5,15,1)$
77	$(4,19,1)$	80	$(5,16,0)$	81	$(4,20,1)$	84	$(4,21,0)$
85	$(5,17,0)$	93	$(4,23,1)$	100	$(5,20,0)$	116	$(5,23,1)$
148	$(4,37,0)$	156	$(5,31,1)$				

iii) *frame-GS*$(2,4,(16^5 24^1),3)$；

iv) *frame-GS*$(2,4,(16^7 40^1),3)$；

v) *frame-GS*$(2,4,(40^{10}),3)$。

证明. i)，从引理4.15取frame-GS$(2,4,(4^u),3)$，$u\in[6,10]$用4膨胀，得到需要的frame-GS。ii)，取frame-GS$(2,4,(4^u),3)$，$u\in\{7,9\}$，用5膨胀得到所需设计。iii)，从引理4.16取frame-GS$(2,4,(4^5 6^1),3)$并用4膨胀。iv)，从引理4.18取frame-GS$(2,4,(4^7 10^1),3)$并用4膨胀。v)取frame-GS$(2,4,(4^{10}),3)$并用10膨胀。 □

推论 4.24. *对任意$n\in\{96,104,112,128,140,144,152,160,180,400\}$，分别存在一个$GS(2,4,n,3)$和一个$GS(2,4,n+1,3)$。*

证明. 取引理4.23中的frame-GS。如果在组上填入GS$(2,4,m,3)$，$m\in\{16,20,24,40\}$（引理4.20），我们得到需要的GS$(2,4,n,3)$。如果增加一个无穷点，并在组上连同无穷点填入GS$(2,4,m+1,3)$（引理4.19和4.21），我们得到需要的GS$(2,4,n+1,3)$。 □

引理 4.25. *对任意$n\in\{124,132,136,176,184\}$，存在一个$GS(2,4,n,3)$和一个$GS(2,4,n+1,3)$。*

证明. 从引理2.9中取一个TD$(6,t)$，$t\in\{5,7\}$，用基本构造法对前5个组的所有点，最后一个组的x个点加权4，最后一个组的y个点加权8，其中$x+y=t$。这里输入设计为frame-GS$(2,4,(4^6),3)$和frame-GS$(2,4,(4^5 8^1),3)$（引理4.15和4.16）。我们得到了frame-GS$(2,4,((4t)^5(4x+8y)^1),3)$。

如果在这些frame-GS的组上填入GS$(2,4,4t,3)$和GS$(2,4,4x+8y,3)$（引理4.20），我们得到了GS$(2,4,n,3)$，其中$n=20t+4x+8y$。若$(t,x,y)=(5,4,1)$，我们有GS$(2,4,124,3)$；若$(t,x,y)=(5,2,3)$，我们有GS$(2,4,132,3)$；

若$(t,x,y) = (5,1,4)$，我们有GS$(2,4,136,3)$；若$(t,x,y) = (7,5,2)$，我们得到GS$(2,4,176,3)$；若$(t,x,y) = (7,3,4)$，我们有GS$(2,4,184,3)$。

如果增加一个无穷点，并在组上连同无穷点填入GS$(2,4,4t+1,3)$和GS$(2,4,4x+8y+1,3)$（引理4.19和4.21），取上面相同的三元组(t,x,y)，我们可以得到相应的GS$(2,4,n+1,3)$。 □

引理 4.26. *对任意$n \in \{616,636,660,664,736\}$，存在一个$GS(2,4,n,3)$和一个$GS(2,4,n+1,3)$。*

证明. 从引理2.9取一个TD$(8,24)$，用基本构造法对前6个组的所有点，第7个组的x个点，最后一个组的y个点加权4，其余点加权0。这里输入设计为frame-GS$(2,4,(4^u),3)$，$u \in \{6,7,8\}$。我们得到了frame-GS$(2,4,(96^6(4x)^1(4y)^1),3)$。

如果我们在这些frame-GS的组上分别填入GS$(2,4,96,3)$，GS$(2,4,4x,3)$或者GS$(2,4,4y,3)$（引理4.20，引理4.22，推论4.24），我们得到了GS$(2,4,576+4x+4y,3)$。若$(x,y) = (10,0)$，我们有GS$(2,4,616,3)$；若$(x,y) = (15,0)$，我们有GS$(2,4,636,3)$；若$(x,y) = (15,6)$，我们有GS$(2,4,660,3)$；若$(x,y) = (15,7)$，我们有GS$(2,4,664,3)$；若$(x,y) = (24,16)$，我们有GS$(2,4,736,3)$。

如果增加一个无穷点，并在组上连同无穷点填入GS$(2,4,97,3)$，GS$(2,4,4x+1,3)$或者GS$(2,4,4y+1,3)$ （引理4.19，4.20和4.22），取上面相同的三元组(t,x,y)，我们可以得到相应的GS$(2,4,n+1,3)$。 □

令$P = [10,29] \cup [31,40] \cup [44,46] \cup \{100,154,159,165,166,184\}$。

引理 4.27. *对任意$t \geq 10$，$t \notin P$，存在一个$GS(2,4,4t,3)$和一个$GS(2,4,4t+1,3)$。*

证明. 对任意$t \geq 10$，$t \notin P$，由引理4.10，存在一个$(t+1,\{6,7,8,9,10\},1)$-PBD。从这个PBD的点集去掉一个点，得到型为$5^i6^j7^k8^l9^m$的$\{6,7,8,9,10\}$-GDD，其中$5i+6j+7k+8l+9m = t$。用基本构造法加权4得到frame-GS$(2,4,(20^i24^j28^k32^l36^m),3)$。这里，输入设计为frame-GS$(2,4,(4^u),3)$，$u \in [6,10]$（引理4.15）。

如果在这些frame-GS的组上填入GS$(2,4,m,3)$，$m \in \{20,24,28,32,36\}$（引理4.20），我们得到所需GS$(2,4,4t,3)$。如果增加一个无穷点并在这些frame-GS的组上连同无穷点填入GS$(2,4,m+1,3)$（引理4.19 和4.21），我们得到所需GS$(2,4,4t+1,3)$。 □

综合引理4.19–4.22，推论4.24和引理4.25–4.27中的结果，我们得到：

定理 4.28. *对任意*$n \equiv 0,1 \pmod 4$，$n \geq 8$，$n \notin \{8,9,12,13,88,108,117\}$，*存在一个*$GS(2,4,n,3)$。

c. 长度$n \equiv 2,3 \pmod 4$**时**

令g和n为正整数。一个*带洞填充*（holey packing），记为型为g^n的K-HP，是一个三元组$(X,\mathcal{G},\mathcal{B})$，其中$X$是一个大小为$gn$的集合（*点集*）。$\mathcal{G}$是一个$X$的划分，称为*洞*（或者*组*），将$X$划分成$n$个部分，每部分$g$个点。$\mathcal{B}$是$X$的一个子集族（*区组*），对任意$B \in \mathcal{B}$，$|B| \in K$，并且任意两个不同组的点对最多包含在一个区组中，同一个组的点对不包含在任何区组中。

令$\mathrm{PN}(2,k,n,g)$为*填充数*，即：型为g^n的$\{k\}$-HP的最大可能的区组个数。文[156]中给出了$\mathrm{PN}(2,k,n,g) \leq BN(2,k,n,g)$，其中：

$$BN(2,k,n,g) = \begin{cases} \left\lfloor \frac{ng}{k} \left\lfloor \frac{(n-1)g}{k-1} \right\rfloor \right\rfloor - 1, & \text{若} (n-1)g \equiv 0 \pmod{k-1}, \\ & \quad n(n-1)g^2 \not\equiv 0 \pmod{k(k-1)}; \\ \left\lfloor \frac{ng}{k} \left\lfloor \frac{(n-1)g}{k-1} \right\rfloor \right\rfloor, & \text{否则。} \end{cases}$$

显然，若$n \equiv 2,3 \pmod 4$，$A_4(n,5,4) \leq PN(2,4,n,3) \leq BN(2,4,n,3) = U(n,4)-1$。因此，如果有一个frame-GS$(2,4,(1^{n-2}2^1),3)$，就有最优$(n,5,4)_4$码。这本节中，我们将构造frame-GS$(2,4,(1^{n-2}2^1),3)$，$n \equiv 2,3 \pmod 4$。

引理 4.29. $A_4(6,5,4) = 9$，$A_4(7,5,4) \in [15,21]$。

证明. 由引理2.1，$A_4(6,5,4) \leq 9$。通过计算机搜索，我们找到最优$(6,5,4)_4$码：$\{333300, 310033, 031011, 003132, 100321, 201203, 122002, 012220, 220110\}$。

由引理2.1，$A_4(7,5,4) \leq 21$。通过计算机搜索，我们找到有15个码字的$(7,5,4)_4$码：$\{2102003, 3001201, 0120301, 0211002, 1300102, 1010031, 2013300, 2320010, 0033013, 0200233, 0101110, 0002322, 0332200, 3030120, 1203020\}$。 □

引理 4.30. *对任意*$n \in [19,83]_4 \cup \{91,99\}$，*存在一个*$\mathit{frame\text{-}GS}(2,4,(1^{n-2}2^1),3)$。

证明. 令点集为$\{0,1,2,\ldots,3n-1\}$，组集为$\{\{0,n,2n\}+i : 0 \leq i \leq n-3\} \cup \{\{n-2,n-1,2n-2,2n-1,3n-2,3n-1\}\}$，洞集为$\{\{0,n,2n\}+i : 0 \leq i \leq$

$n-1\}$。所需设计的区组可以由[161, 表 IV]和[161, 表 V]中的基区组通过自同构群$G=\langle(0\ 1\ 2\ \cdots\ n-3)(n-2)(n-1)(n\ n+1\ n+2\ \cdots\ 2n-3)(2n-2)(2n-1)(2n\ 2n+1\ 2n+2\ \cdots\ 3n-3)(3n-2)(3n-1)\rangle$展开得到。□

对$u\in\{4,5\}$，我们把型为3^u的{4}-*GDD的区组集划分成每个部分只有一个区组。对$u\in\{8,9\}$，由引理4.9存在一个型为3^u的{4}-*GDD。因为型为g^u的{4}-*GDD的区组集可以最多划分成g个部分，使得每个部分得到的码的最小距离是5。在定理4.14中，令$g=3$，$s=2$，与引理4.22 的证明类似，我们可以得到如下结果：

引理 4.31. *对任意$n\in\{87,107,127,147,155,167\}\cup\{70,86,102,118,134,138,150,166,170,182,198,202,206,214,230,234,246,254,262,294,298,302,402\}$，存在一个frame-GS$(2,4,(1^{n-2}2^1,3)$。*

证明. 对$n\in\{87,107,127,147,167\}$，分别取$u=5$，$w\in\{17,21,25,29,33\}$。对$n=155$，取$u=9$，$w=17$。对$n\in\{70,86,102,118,134,150,166,182,198,214,230,246,262,294\}$，分别取$u=4$，$w\in\{17,21,25,29,33,37,41,45,49,53,57,61,65,73\}$。对$n\in\{138,170,202,234,298\}$，分别取$u=8$，$w\in\{17,21,25,29,37\}$。对$n\in\{206,254,302\}$，分别取$u=12$，$w\in\{17,21,25\}$。对$n=402$，取$u=16$，$w=25$。□

引理 4.32. *对任意$n\in\{123,131,135,139,171,175,179,183\}$，存在一个frame-GS$(2,4,(1^{n-2}2^1),3)$。*

证明. 从引理2.9取一个TD$(6,t)$，$t\in\{5,7\}$，用基本构造法对前5个组的所有点加权4，对最后一个组的x,y,z个点分别加权$4,6,8$，其中$x+y+z=t$。这里输入设计为frame-GS$(2,4,(4^6),3)$（引理4.15）和frame-GS$(2,4,(4^5m^1),3)$，$m\in\{6,8\}$（引理4.16）。我们得到了frame-GS$(2,4,((4t)^5(4x+6y+8z)^1),3)$。增加一个无穷点，在此frame-GS的组上连同无穷点填入GS$(2,4,4t+1,3)$和frame-GS$(2,4,(1^{4x+6y+8z-1}2^1),3)$，就得到frame-GS$(2,4,(1^{20t+4x+6y+8z-1}2^1),3)$。令$n=20t+4x+6y+8z+1$。构造$n$所需的参数$(t,x,y,z)$列在表4.2中。□

令$Q=\{10,14,15,18,20,22,26,30,34,38,46,60\}\cup\{29\}$。

引理 4.33. *对任意$n\equiv 3\pmod 4$，$n\geq 187$，存在一个frame-GS$(2,4,(1^{n-2}2^1),3)$。*

表 4.2: 定理 4.32中的参数

n	(t,x,y,z)	n	(t,x,y,z)	n	(t,x,y,z)	n	(t,x,y,z)
123	$(5,4,1,0)$	131	$(5,2,1,2)$	135	$(5,1,1,3)$	139	$(5,0,1,4)$
171	$(7,6,1,0)$	175	$(7,5,1,1)$	179	$(7,3,3,1)$	183	$(7,3,1,3)$

证明. 从引理2.9中取一个TD$(7,t)$，用基本构造法对前6个组的所有点加权4，对最后一个组的x,y,z个点分别加权$4,6,8$。其余点加权0。这里输入设计为frame-GS$(2,4,(4^u),3)$，$u\in\{6,7\}$（引理4.15），frame-GS$(2,4,(4^6m^1),3)$，$m\in\{6,8\}$（引理4.17）。我们得到一个frame-GS$(2,4,((4t)^6(4x+6y+8z)^1),3)$。

a. 对任意$k\geq 7$，$k\notin Q$，由引理2.9存在一个TD$(7,k)$。很容易验证可以取到合适的三元组(x,y,z)，使得$4x+6y+8z\in[18,38]_4$。

b. 对任意$k\in Q\setminus\{15,30\}$，由引理2.9存在一个TD$(7,k-1)$。很容易验证可以取到合适的三元组(x,y,z)，使得$4x+6y+8z\in[42,62]_4$。

c. 对任意$k\in\{15,30\}$，由引理2.9存在一个TD$(7,k-2)$。很容易验证可以取到合适的三元组(x,y,z)，使得$4x+6y+8z\in[66,86]_4$。

增加一个无穷点，然后在组上连同无穷点填入GS$(2,4,4t+1,3)$（定理4.28）和frame-GS$(2,4,(1^{4x+6y+8z-1}2^1),3)$（引理4.30和引理4.31），我们就得到frame-GS$(2,4,(1^{24t+4x+6y+8z-1}2^1),3)$。令$n=24t+4x+6y+8z+1$。我们就得到了frame-GS$(2,4,(1^{n-2}2^1),3)$，其中$n$可以取到如下区间：

a'. 对任意$k\geq 7$，$k\notin Q$，$n\in[24k+19,24k+39]_4$。

b'. 对任意$k\in Q\setminus\{15,30\}$，$n\in[24(k-1)+42+1,24(k-1)+62+1]_4=[24k+19,24k+39]_4$。

c'. 对任意$k\in\{15,30\}$，$n\in[24(k-2)+66+1,24(k-2)+86+1]_4=[24k+19,24k+39]_4$。

综合上述结果，我们可以得到一个frame-GS$(2,4,(1^{n-2}2^1),3)$，其中n可以取到不小于$24\times 7+19=187$ 的任何值。 □

综合引理4.30，4.31，4.32和4.33中的结果，我们得到：

定理 4.34. 对任意$n \geq 7$，$n \equiv 3 \pmod 4$，$n \notin \{7, 11, 15, 95, 103, 111, 115, 119, 143, 151, 159, 163\}$，存在一个*frame-GS*$(2, 4, (1^{n-2}2^1), 3)$。

定理 4.35. 假设下列设计都存在：

(1) 一个型为$3^{4m+1}6^1$的$\{4\}$-*GDD*，并具有如下性质：所有的区组可以分成r个部分，并且大小为6的组可以分成大小为3的子组，使得每个部分得到的码关于子组的最小距离都是5；

(2) r个超单的$OA(4, w)$；

(3) 一个$GS(2, 4, w + 1, 3)$；

(4) 一个*frame-GS*$(2, 4, (1^{2w-1}2^1), 3)$。

那么存在一个*frame-GS*$(2, 4, (1^{(4m+1)w+2w-1}2^1), 3)$。

证明. 由条件(1)和(2)，我们由构造4.13得到一个frame-GS$(2, 4, (w^{4m+1}(2w)^1), 3)$。增加一个无穷点，在大小为$w$的组上连同无穷点填入给定的GS$(2, 4, w + 1, 3)$，在大小为$2w$的组连同无穷点填入给定的frame-GS$(2, 4, (1^{2w-1})2^1, 3)$。我们就得到一个frame-GS$(2, 4, (1^{(4m+1)w+2w-1}2^1), 3)$。 □

推论 4.36. 对任意$n \in \{106, 162, 190, 210, 218, 226\}$，存在一个*frame-GS*$(2, 4, (1^{n-2}2^1), 3)$。

证明. 很容易找到型为3^56^1，3^96^1，$3^{13}6^1$，且区组集最多可以划分成15个部分的$\{4\}$-GDD。所以这里我们省略了具体构造。

对任意$w \in \{15, 19, 23, 27, 31\}$，由引理4.11存在15个超单的OA$(4, w)$，且存在GS$(2, 4, w + 1, 3)$（定理4.28），frame-GS$(2, 4, (1^{2w-1}2^1), 3)$（引理4.30）。

应用上述定理，我们可以得到需要的frame-GS$(2, 4, (1^{n-2}2^1), 3)$。具体地，当$n \in \{106, 162, 190, 218\}$时，分别取$m = 1$，$w \in \{15, 23, 27, 31\}$；当$n = 210$时，取$m = 2$，$w = 19$；当$n = 226$时，取$m = 3$，$w = 15$。 □

引理 4.37. 对任意$n \in \{250\} \cup [266, 290]_4 \cup [306, 398]_4 \cup [406, 946]_4$，存在一个*frame-GS*$(2, 4, (1^{n-1}2^1), 3)$。

表 4.3: 定理4.37中的参数

n	t	a	(x,y,z)	$4x+6y+8z$
250	9	0	$(0,1,8)$	70
290	11	0	$(4,1,6)$	70
$[266,286]_4$	9	$[4,9]$	$(0,1,8)$	70
$[306,334]_4$	11	$[4,11]$	$(0,9,2)$	70
$[338,358]_4$	12	$[7,12]$	$(1,11,0)$	70
$[362,398]_4$	13	$[4,13]$	$(0,9,4)$	86
$[406,454]_4$	16	$[4,16]$	$(13,3,0)$	70
$[458,510]_4$	17	$[4,17]$	$(1,15,1)$	102
$[514,574]_4$	19	$[4,19]$	$(0,17,2)$	118
$[578,642]_4$	21	$[5,21]$	$(0,15,6)$	138
$[646,714]_4$	24	$[4,21]$	$(0,21,3)$	150
$[718,782]_4$	28	$[5,21]$	$(15,13,0)$	138
$[786,854]_4$	31	$[4,21]$	$(18,13,0)$	150
$[858,926]_4$	33	$[4,21]$	$(11,19,3)$	182
$[930,946]_4$	36	$[15,19]$	$(33,3,0)$	150

证明. 从引理2.9取一个TD$(7,t)$，用基本构造法对前5个组的所有点，第6个组的a个点加权4。对最后一个组的x,y,z个点分别加权$4,6,8$，其中$x+y+z=t$。其余点加权0。这里输入设计为frame-GS$(2,4,(4^u),3)$，$u\in\{6,7\}$（引理4.15）和frame-GS$(2,4,(4^um^1),3)$，$u\in\{5,6\}$，$m\in\{6,8\}$（引理4.16和4.17）。我们得到了frame-GS$(2,4,((4t)^5(4a)^1(4x+6y+8z)^1),3)$。在组上填入GS$(2,4,4t,3)$，GS$(2,4,4a,3)$（定理4.28）和frame-GS$(2,4,(1^{4x+6y+8z-2}2^1),3)$（引理4.31）。我们得到frame-GS$(2,4,(1^{20t+4a+4x+6y+8z-2}2^1),3)$。令$n=20t+4a+4x+6y+8z$。我们可以取表4.3中的参数$t$，$a$和$(x,y,z)$来得到需要的$n$。 □

令$R=\{10,12,14,15,18,20,21,22,26,28,30,33,34,35,38,39,42,44,46,51,52,54,58,60,62,66,68,74\}\cup\{22,27\}$。

引理 4.38. *对任意$n\in\{238,258\}$或$n\equiv 2\pmod 4$，$n\geq 950$，存在一个frame-GS$(2,4,(1^{n-2}2^1),3)$。*

证明. 从引理2.9取一个TD$(8,t)$。用基本构造法对前6个组的所有点，第7个组的x个点加权4，对最后一个组的7个点加权10，其余点加权0。这里输入设计为frame-GS$(2,4,(4^u),3)$，$u\in\{6,7\}$（引理4.15），和frame-GS$(2,4,(4^u10^1),3)$，$u\in\{6,7\}$（引理4.17 和4.18）。我们得到了frame-GS$(2,4,((4t)^6(4x)^170^1),3)$。

a. 对$k=7$，由引理2.9存在一个TD$(8,7)$。取$x\in\{0,5\}$。

b. 对任意$k\geq 36$，$k\notin R$，由引理2.9存在一个TD$(8,k)$。取$x\in[4,9]$。

c. 对任意$k\in R\setminus\{39,52\}$，由引理2.9存在一个TD$(8,k-1)$，取$x\in[10,15]$。

d. 对任意$k\in\{39,52\}$，由引理2.9存在一个TD$(8,k-2)$。取$x\in[16,21]$。

在得到的frame-GS的组上填入GS$(2,4,4t,3)$，GS$(2,4,4x,3)$（定理4.28）和frame-GS$(2,4,(1^{68}2^1),3)$（引理4.31）就得到frame-GS$(2,4,(1^{24t+4x+68}2^1),3)$。令$n=24t+4x+70$。对任意$n\in\{238,258\}$或$n$不小于$24\times 36+16+70=950$，我们得到了需要的frame-GS$(2,4,(1^{n-2}2^1),3)$。 □

综合引理4.31，推论4.36，引理4.37和引理4.38中的结果，我们得到：

定理 4.39. *对任意$n\geq 6$，$n\equiv 2\pmod 4$，$n\notin[6,66]_4\cup\{74,78,82,90,94,98,110,114,122,126,130,142,146,154,158,174,178,186,194,222,242\}$，存在一个frame-GS$(2,4,(1^{n-1}2^1),3)$。*

4.5　结论

在本章中，我们对任意长度n，研究了最优$(n,5,4)_4$码的构造。我们对任意$n\geq 4$，除了55个值之外，确定了所有$A_4(n,5,4)$的值。特别地，我们证明了除了7个不确定的值外，GS$(2,4,n,3)$存在当且仅当$n\geq 4$，$n\equiv 0,1\pmod 4$。

定理 4.40. *对任意正整数$n\geq 4$，$A_4(n,5,4)=U(n,4)$，除了$n\in\{4,5,6,7\}$，和如下可能的例外：*

1) $n\equiv 0,1\pmod 4$，$n\in\{8,9,12,13,88,108,117\}$；

2) $n\equiv 2\pmod 4$，$n\in[10,66]_4\cup\{74,78,82,90,94,98,110,114,122,126,130,142,146,154,158,174,178,186,194,222,242\}$；

3) $n\equiv 3\pmod 4$, $n\in\{11,15,95,103,111,115,119,143,151,159,163\}$。

Chapter 5

用完全可约超单设计构造最优多元常重码

5.1 引言和主要结果

在Chee和Ling的文章[26]中，他们引入了一种新的方法来构造最优多元常重码，即通过建立组合设计理论中的各种不相交设计，包括填充、t-设计、可分组设计等与码的联系来构造最优多元常重码。利用这个方法，他们对几类$(n,d,w)_q$码，确定了$A_q(n,d,w)$的准确值。Chee等还在文[23]中推广了这个方法，并完全确定了$A_q(n,4,3)$的准确值。

基于这个思想，我们建立了完全可约超单设计与最优$(n,6,4)_q$码之间的联系。在本章中，我们将通过研究完全可约超单设计，并引入一种辅助设计：完全可约超单可分组设计来构造最优$(n,6,4)_3$码。我们对所有长度n，除了$n=17$之外，确定了$A_3(n,6,4)$的值。在此之前，这个问题只解决了$n\leq 10$的情况[115]，见表5.1。

表 5.1: 当$n\leq 10$时，$A_3(n,6,4)$的值

n	4	5	6	7	8	9	10
$A_3(n,6,4)$	1	1	3	3	5	9	15

本章中，我们所用的构造方法是基于组合设计理论中关于GDD构造的Wilson's基本构造法（WFC），和第3章中关于常重码和常重复合码构造的可分组码（GDC）的循环构造方法。因为这里的所有GDC都是重量为4，距离为6的三元GDC，因此在本章中，我们将均把三元4-GDC(6)简记为GDC。

众所周知，$A_3(n,2w,w)=\lfloor n/w\rfloor$。结合引理2.2，可以得到$A_3(n,6,4)$的一个上界。

推论 5.1. $A_3(n,6,4)\leq \left\lfloor \frac{n}{2}\left\lfloor \frac{n-1}{3}\right\rfloor\right\rfloor =: U(n,3)$。

这一章的结构如下：在第5.2节中，我们将介绍一些基本概念，并建立完全可约超单设计与最优$(n,6,4)_q$码的联系；在第5.3节中，我们将分情况构造最

优$(n,6,4)_3$码；在第5.4节中，将对本章的主要结果进行总结。

5.2 准备知识

一个设计如果没有重复的区组，就称为是*单的*（simple）。一个设计被称为是*超单的*（super-simple，SS），如果任意两个区组最多交于两个点。当$k=3$时，一个超单设计就是单的。当$\lambda=1$时，设计一定是超单的。

一个在点集X上，区组集为$\mathcal{B}$，指数为λ的设计$\mathcal{D}$，如果它的区组集$\mathcal{B}$可以写成$\mathcal{B}=\bigcup_{i=1}^{\lambda}\mathcal{B}_i$，使得对任意的$1\le i\le\lambda$，$\mathcal{B}_i$形成与$\mathcal{D}$参数相同但是指数为1的设计，则$\mathcal{D}$称为*完全可约超单*（completely reducible super-simple，CRSS）设计。这里，CRSS的定义可以用于各种设计，并用来简化符号。我们把一个点集大小为v，区组大小为k，指数为λ的完全可约超单BIBD写成(v,k,λ)-CRSS设计，把一个区组大小为k，指数为λ的完全可约超单GDD简记为(k,λ)-CRSSGDD。

引理 5.2 (Adams等[5]). *当$v\equiv 1$或$4\pmod{12}$，$v\ge 13$时，存在一个$(v,4,2)$-CRSS设计。存在型为3^5的$(4,2)$-CRSSGDD。*

令m为一个正整数，X是一个点集。令$\mathcal{H}=\{H_1,H_2,\ldots,H_m\}$是$X$的一个划分。$\mathcal{H}$的一个*横截*就是一个与每个$H_i$至多交于一个点的$X$的子集。一个H$(m,g,k,t)$设计就是一个三元组$(X,\mathcal{H},\mathcal{B})$，其中$|X|=mg$，$\mathcal{H}$把$X$划分成$m$个大小为$g$的不相交的子集，$\mathcal{B}$是$\mathcal{H}$ 的k元横截构成的集合（称为区组），使得任意t元横截都恰好包含在一个区组中。

一个H$(m,g,4,3)$设计被称为是*s-fan*的，如果它的区组集$\mathcal{B}$可以划分成不相交的子集$\mathcal{B}_1,\mathcal{B}_2,\cdots,\mathcal{B}_s$和$\mathcal{A}$，使得对任意$1\le i\le s$，$\mathcal{B}_i$都是一个H$(m,g,4,2)$的区组集，而且$\mathcal{A}=\mathcal{B}\backslash\bigcup_{i=1}^{s}\mathcal{B}_i$。

引理 5.3 (Ge [65]). *当$g\ge 4$且$g\not\equiv 2\pmod 4$时，存在一个g-fan $H(4,g,4,3)$。*

因此，我们得到了一些$(4,g)$-CRSSGDD。

引理 5.4. *当$g\ge 4$且$g\not\equiv 2\pmod 4$时，存在一个型为g^4的$(4,g)$-CRSSGDD。*

引理 5.5. *如果存在一个具有b个区组的$(n,4,q)$-CRSS设计，那么存在一个大小为b的$(n,6,4)_{q+1}$码；如果存在一个型为$g_1^{t_1}\cdots g_s^{t_s}$，具有$g$个区组的$(4,q)$-CRSSGDD，那么存在一个型为$g_1^{t_1}\cdots g_s^{t_s}$，大小为$g$的$(q+1)$元GDC。*

证明. 这里我们只需要给出第一个命题的证明。第二个命题可以类似证明。

由假设，我们有一个区组集为$\mathcal{B} = \bigcup_{i=1}^{q} \mathcal{B}_i$的$(n, 4, q)$-CRSS设计，$|\mathcal{B}| = b$。对任意的$1 \leq i, j \leq q$，$\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$，而且$\mathcal{B}_i$形成$(n, 4, 1)$-BIBD的区组集。从$q$个$(n, 4, 1)$-BIBD的区组集，我们可以得到$q$个不相交的$(n, 6, 4)_2$码$\mathcal{C}_i$，$1 \leq i \leq q$。与文[26]中的方法类似，对$\mathcal{C}_i$的每一个码字中的1用$i$替换就得到一个$(q+1)$元码$\mathcal{C}'_i$。从而$\mathcal{C}' = \bigcup_{i=1}^{q} \mathcal{C}'_i$就是一个大小为$b$，重量为4，距离为6的$(q+1)$元码。 □

结合引理5.2和5.5，我们得到如下结果：

定理 5.6. *当$v \equiv 1$或者$4 \pmod{12}$，$v \geq 13$时，存在一个有$U(v, 3)$个码字的最优的$(v, 4, 2)_3$码。*

结合引理5.4和5.5，我们得到如下结果：

定理 5.7. *当$g \geq 4$，$g \not\equiv 2 \pmod 4$时，存在一个型为g^4的g元GDC。*

定理 5.8. *当$v \equiv 0$或$3 \pmod{12}$，$v \geq 12$时，存在一个有$U(v, 3)$个码字的最优$(v, 4, 2)_3$码。*

证明. 对任意v，令$(X, \mathcal{A})$是定理5.6中的一个$(v+1, 4, 2)$-CRSS设计。去掉一个点$x \in X$得到一个$(v, 4, 2)$-填充$(Y, \mathcal{B})$，其中$Y = X \setminus \{x\}$，$\mathcal{B} = \mathcal{A} \setminus \{A \in \mathcal{A} : x \in A\}$。与引理5.5的证明类似，我们得到了一个最优$(v, 6, 4)_3$码。 □

一个*Steiner*系$S(t, k, v)$是一个$\mathrm{H}(1, v, k, t)$。$S(2, 3, v)$也称为一个*Steiner*三元系（简记为$\mathrm{STS}(v)$），$S(3, 4, v)$也称为*Steiner*四元系（简记为$\mathrm{SQS}(v)$）。一个*Steiner*系$S(t, k, v)$被称为是i-可分解的，如果它的区组集可以划分成$S(i, k, v)$，$0 \leq i \leq t$。对2-可分解SQS的研究结果很少。

引理 5.9 (Baker [8]，Teirlinck [137]). *存在2-可分解$SQS(v)$，如果$v = 4^n$或$v = 2 \cdot p^n + 2$，$p \in \{7, 31, 127\}$，n为一个正整数。*

显然，一个2-可分解$\mathrm{SQS}(v)$也是一个$(v, 4, \frac{v}{2} - 1)$-CRSS设计：如果存在一个2-可分解$\mathrm{SQS}(v)$，那么对任意$q \in [1, \frac{v}{2} - 1]$都存在一个$(v, 4, q)$-CRSS设计。由引理5.5，我们得到如下结果：

引理 5.10. *如果存在一个2-可分解$SQS(v)$，那么对任意的$q \in [1, \frac{v}{2} - 1]$，都存在一个有$\left\lfloor \frac{(q-1)v}{4} \left\lfloor \frac{v-1}{3} \right\rfloor \right\rfloor$个码字的最优的$(v, 6, 4)_{q+1}$码。*

综合引理5.9和5.10，我们得到如下结果：

定理 5.11. *当$v = 4^n$或$v = 2 \cdot p^n + 2$，$p \in \{7, 31, 127\}$，n为一个正整数，对任意$q \in [1, \frac{v}{2} - 1]$时，存在一个有$\left\lfloor \frac{(q-1)v}{4} \left\lfloor \frac{v-1}{3} \right\rfloor \right\rfloor$个码字的最优$(v, 6, 4)_{q+1}$码。*

5.3 主要证明过程

a. 一些小的GDC和最优码

在本节中，我们将直接构造一些$(4, 2)$-CRSSGDD。同时由引理5.5，我们也得到了一些GDC。

一般地，我们分别构造点集和组集相同，指数为1的两个$\{4\}$-GDD，使得任意两个区组最多交于两个点。然后把这两个$\{4\}$-GDD组合起来就得到了我们需要的$(4, 2)$-CRSSGDD。这里的构造都基于我们熟知的差方法，即：通常一个GDD的区组是由一个有限群（多是交换群$\mathbb{Z}_u$）展开。所以我们通常只列出一些基区组，而所有的区组就可以通过用加法群或其他的自同构群展开得到。在带无穷点的设计中，$x_0 \in \{x\} \times \mathbb{Z}_n$的下标是在交换群$\mathbb{Z}_u$的唯一$n$阶子群中展开。

引理 5.12. *存在一个型为4^7的$(4, 2)$-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{28}$，组集为$\{\{0, 7, 14, 21\} + i : 0 \leq i \leq 6\}$。对如下基区组在$\mathbb{Z}_{28}$上$+4 \pmod{28}$展开就得到了我们需要的设计。第一个GDD的基区组为$(0, 11, 24, 27)$，$(1, 3, 7, 9)$，$(0, 1, 12, 25)$，$(3, 18, 22, 23)$，$(2, 5, 10, 21)$，$(0, 2, 18, 20)$，$(0, 9, 19, 22)$，$(1, 2, 19, 24)$。第二个GDD的基区组是由第一个GDD的基区组乘以乘子5得到。 □

引理 5.13. *对任意$u \in \{7, 10, 13, 16, 19, 22, 28, 34, 52, 58\}$，存在型为$2^u$的$(4, 2)$-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{2u}$，组集为$\{\{0, u\} + i : 0 \leq i \leq u - 1\}$。对$u \in \{7, 13, 19\}$，用[162, 附录]中的基区组$+1 \pmod{2u}$展开就得到了我们需要的设计。对$u = 10$，用[162, 附录]中的基区组$+4 \pmod{20}$展开就得到了我们需要的设计。

对$u \in \{16, 22, 28, 34, 52, 58\}$，用[162, 附录]中的基区组+2 (mod $2u$)展开就得到了我们需要的设计。□

引理 5.14. *对任意$u \in [5, 13]$，存在一个型为6^u的$(4, 2)$-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{6u}$，组集为$\{\{0, u, 2u, \ldots, 5u\} + i : 0 \leq i \leq u - 1\}$。对$u \in \{5, 6, 8, 12\}$，用[162, 附录]中的基区组+2 (mod $6u$)展开就得到了我们需要的设计。对$u \in \{9, 11\}$，用[162, 附录]中的基区组+1 (mod $6u$)展开就得到了我们需要的设计。对$u \in \{7, 10, 13\}$，所需设计分别由型为2^7，2^{10}或2^{13}的$(4, 2)$-CRSSGDD用3膨胀得到。□

引理 5.15. *对任意$u \in \{4, 5, 6\}$，存在一个型为6^u3^1的$(4, 2)$-CRSSGDD。*

证明. 6^43^1：令点集为$\mathbb{Z}_{24} \cup (\{a\} \times \mathbb{Z}_3)$，组为$\{\{0, 4, 8, \ldots, 20\} + i : 0 \leq i \leq 3\} \cup \{\{a\} \times Z_3\}$。所需设计由如下基区组+2 (mod 24)展开得到。第一个GDD的基区组为$(1, 6, 11, a_0)$，$(2, 3, 4, a_0)$，$(0, 7, 9, 18)$，$(0, 3, 10, 21)$。第二个GDD的基区组是由第一个GDD的基区组乘以乘子5得到。

6^53^1：令点集为$\mathbb{Z}_{30} \cup (\{a, b, c\} \times \mathbb{Z}_1)$，组为$\{\{0, 5, 10, \ldots, 25\} + i : 0 \leq i \leq 4\} \cup \{\{a, b, c\} \times \mathbb{Z}_1\}$。所需设计由如下基区组+6 (mod 30)展开得到。

第一个GDD的基区组：

$$
\begin{array}{lllll}
(2, 1, 15, a_0) & (5, 12, 28, a_0) & (5, 22, 26, b_0) & (0, 13, 21, b_0) & (1, 3, 14, c_0) \\
(1, 23, 29, 12) & (1, 24, 27, 0) & (5, 21, 27, 23) & (4, 27, 28, 15) & (1, 28, 10, 7) \\
(2, 29, 25, 13) & (5, 16, 14, 2) & (2, 26, 3, 24) & (5, 6, 4, c_0) & (0, 4, 12, 26)
\end{array}
$$

第二个GDD的基区组：

$$
\begin{array}{lllll}
(3, 25, 22, a_0) & (2, 24, 23, a_0) & (0, 2, 4, b_0) & (5, 7, 9, b_0) & (0, 22, 26, c_0) \\
(5, 8, 17, 24) & (2, 21, 15, 14) & (0, 1, 18, 7) & (5, 2, 13, 1) & (0, 16, 17, 28) \\
(2, 25, 16, 8) & (3, 15, 12, 6) & (5, 22, 21, 29) & (1, 15, 17, c_0) & (1, 4, 10, 27)
\end{array}
$$

6^63^1：令点集为$\mathbb{Z}_{36} \cup (\{a\} \times \mathbb{Z}_3)$，组为$\{\{0, 6, 12, \ldots, 30\} + i : 0 \leq i \leq 5\} \cup \{\{a\} \times \mathbb{Z}_3\}$。所需设计由如下基区组+1 (mod 36)展开得到。第一个GDD的基区组为$(0, 4, 5, a_0)$，$(0, 11, 14, 27)$，$(0, 2, 10, 17)$。第二个GDD的基区组是由第一个GDD的基区组乘以乘子11得到。□

引理 5.16. *对任意$u \in \{4, 6\}$，存在一个型为6^u9^1的$(4, 2)$-CRSSGDD。*

证明. $6^4 9^1$：令点集为$\mathbb{Z}_{24} \cup (\{a,b\} \times \mathbb{Z}_4) \cup (\{c\} \times \mathbb{Z}_1)$，组为$\{\{0,4,8,\ldots,20\}+i : 0 \le i \le 3\} \cup \{(\{a,b\} \times \mathbb{Z}_4) \cup (\{c\} \times \mathbb{Z}_1)\}$。所需设计由如下基区组+3 (mod 24)展开得到。

第一个GDD的基区组：

$$(2,15,20,a_0) \quad (9,10,23,a_0) \quad (5,6,12,a_0) \quad (7,13,16,a_0) \quad (4,15,18,b_0)$$
$$(0,7,9,b_0) \quad (1,2,23,b_0) \quad (8,17,22,b_0) \quad (0,2,19,c_0)$$

第二个GDD的基区组：

$$(4,15,21,a_0) \quad (1,10,11,b_0) \quad (5,12,15,b_0) \quad (0,5,22,a_0) \quad (0,10,23,c_0)$$
$$(1,6,7,a_0) \quad (2,8,11,a_0) \quad (2,4,7,b_0) \quad (6,8,21,b_0)$$

$6^6 9^1$：令点集为$\mathbb{Z}_{36} \cup (\{a,b,c\} \times \mathbb{Z}_3)$，组为$\{\{0,6,12,\ldots,30\}+i : 0 \le i \le 5\} \cup \{\{a,b,c\} \times \mathbb{Z}_3\}$。所需设计由如下基区组+2 (mod 36)展开得到。

第一个GDD的基区组：

$$(0,1,2,a_0) \quad (3,10,35,a_0) \quad (0,7,33,b_0) \quad (2,10,23,b_0)$$
$$(4,20,31,c_0) \quad (0,22,26,31) \quad (0,15,23,c_0) \quad (0,3,17,19)$$

第二个GDD的基区组：

$$(0,3,4,a_0) \quad (1,17,20,a_0) \quad (0,1,28,b_0) \quad (3,11,20,b_0)$$
$$(1,12,23,33) \quad (3,5,34,c_0) \quad (0,13,26,c_0) \quad (0,2,16,31)$$

□

引理 5.17. *对任意$u \in \{5,6,7\}$，存在一个型为$6^u 12^1$的$(4,2)$-CRSSGDD。*

证明. $6^5 12^1$：令点集为$\mathbb{Z}_{30} \cup (\{a,b\} \times \mathbb{Z}_5) \cup (\{c\} \times \mathbb{Z}_2)$，组为$\{\{0,5,10,\ldots,25\}+i : 0 \le i \le 4\} \cup \{(\{a,b\} \times \mathbb{Z}_5) \cup (\{c\} \times \mathbb{Z}_2)\}$。所需设计由如下基区组+3 (mod 30)展开得到。

第一个GDD的基区组：

$$(6,24,25,a_0) \quad (5,11,12,a_0) \quad (8,19,22,a_0) \quad (1,3,29,a_0) \quad (0,13,17,a_0) \quad (1,22,23,c_0)$$
$$(13,19,26,b_0) \quad (3,7,25,b_0) \quad (6,12,14,b_0) \quad (2,5,23,b_0) \quad (1,15,24,b_0) \quad (2,18,21,c_0)$$

第二个GDD的基区组：

$$(12,19,23,a_0) \quad (2,13,24,a_0) \quad (3,5,21,a_0) \quad (1,7,10,a_0) \quad (11,14,15,a_0) \quad (1,8,17,c_0)$$
$$(0,17,24,b_0) \quad (3,4,6,b_0) \quad (14,20,22,b_0) \quad (1,13,27,b_0) \quad (8,25,26,b_0) \quad (4,12,21,c_0)$$

$6^6 12^1$：令点集为$\mathbb{Z}_{36} \cup (\{a,b\} \times \mathbb{Z}_3) \cup (\{c\} \times \mathbb{Z}_6)$，组为$\{\{0,6,12,\ldots,30\}+i : 0 \le i \le 5\} \cup \{(\{a,b\} \times \mathbb{Z}_3) \cup (\{c\} \times \mathbb{Z}_6)\}$。所需设计由如下基区组+2 (mod 36)展开得到。

第一个GDD的基区组：

$$(1,12,29,a_0)\quad(2,9,16,a_0)\quad(5,7,8,b_0)\quad(0,4,27,b_0)\quad(2,4,12,c_0)$$
$$(10,13,29,c_0)\quad(6,15,19,c_0)\quad(8,9,23,c_0)\quad(0,5,20,31)$$

第二个GDD的基区组：

$$(0,19,21,a_0)\quad(2,5,10,a_0)\quad(2,13,34,b_0)\quad(5,15,18,b_0)\quad(0,20,22,c_0)$$
$$(4,17,21,c_0)\quad(11,18,25,c_0)\quad(3,14,19,c_0)\quad(0,1,9,10)$$

$6^7 12^1$：令点集为$\mathbb{Z}_{42}\cup(\{a\}\times\mathbb{Z}_7)\cup(\{b,c\}\times\mathbb{Z}_2)\cup(\{d\}\times\mathbb{Z}_1)$，组为$\{\{0,7,\ldots,35\}+i : 0\le i\le 6\}\cup\{(\{a\}\times\mathbb{Z}_7)\cup(\{b,c\}\times\mathbb{Z}_2)\cup(\{d\}\times\mathbb{Z}_1)\}$。所需设计由如下基区组$+3 \pmod{42}$展开得到。

第一个GDD的基区组：

$$(10,40,1,a_0)\quad(13,39,7,a_0)\quad(11,0,23,a_0)\quad(15,6,35,a_0)\quad(5,29,16,a_0)$$
$$(17,9,33,a_0)\quad(3,20,4,a_0)\quad(0,40,15,b_0)\quad(1,20,35,b_0)\quad(4,31,26,c_0)$$
$$(0,3,41,c_0)\quad(1,21,26,d_0)\quad(0,37,6,19)\quad(2,34,38,35)\quad(0,2,4,12)$$

第二个GDD的基区组：

$$(4,1,37,a_0)\quad(6,12,24,a_0)\quad(7,9,19,a_0)\quad(14,39,34,a_0)\quad(2,8,20,a_0)$$
$$(0,31,5,a_0)\quad(11,15,38,a_0)\quad(5,6,15,b_0)\quad(4,14,31,b_0)\quad(0,19,27,c_0)$$
$$(2,5,10,c_0)\quad(0,8,4,d_0)\quad(0,11,20,22)\quad(1,20,19,18)\quad(0,29,3,16)$$

□

b. 当长度$n\equiv 2 \pmod 6$时

在本节中，我们将确定$A_3(6t+2,6,4)$的值。由引理5.5，如果存在一个型为2^{3t+1}的$(4,2)$-CRSSGDD，我们将得到一个型为2^{3t+1}的GDC，也就是一个最优$(6t+2,6,4)_3$码。

引理 5.18. *对任意$t\ge 4$，存在一个型为12^t的$(4,2)$-CRSSGDD。*

证明. 当$t\equiv 0$或$1 \pmod 4$，$t\ge 4$时，由引理2.7存在一个$(3t+1,\{4\},1)$-PBD。从这个PBD的点集去掉一个点可以得到一个型为3^t的$\{4\}$-GDD。当$t\equiv 2$或$3 \pmod 4$，$t\ge 7$时，由引理2.7存在一个$(3t+1,\{4,7^\star\},1)$-PBD。从这个PBD的点集去掉一个不在大小为7的区组中的点，可以得到一个型为3^t的$\{4,7^\star\}$-GDD。因此，对任意$t\ge 4$，$t\ne 6$，我们都有一个型为3^t的$\{4,7\}$-GDD。

把得到的设计用WFC加权4，我们就对任意$t\ge 4$，$t\ne 6$，得到一个型为12^t的$(4,2)$-CRSSGDD。这里所用的输入设计是型为4^4（引理5.4）和4^7（引理5.12）的$(4,2)$-CRSSGDD。

对$t = 6$，取一个型为4^6的$\{5\}$-GDD（见[71]），用WFC加权3得到一个型为12^6的$(4,2)$-CRSSGDD。这里输入设计是型为3^5的$(4,2)$-CRSSGDD （引理5.2）。 □

引理 5.19. *对任意$t \geq 1$，存在一个型为2^{6t+1}的$(4,2)$-CRSSGDD。*

证明. 对$t \in \{1,2,3\}$，所需设计已经在引理5.13中构造得到。对任意$t \geq 4$，从引理5.18取一个型为12^t的$(4,2)$-CRSSGDD，增加2个无穷点，并在组上连同无穷点填入型为2^7的$(4,2)$-CRSSGDD，得到型为2^{6t+1}的$(4,2)$-CRSSGDD。 □

引理 5.20. *对任意的$t \geq 1$，存在一个型为2^{6t+4}的$(4,2)$-CRSSGDD。*

证明. 对$t \in \{1,2,3,4,5,8,9\}$，所需设计已经在引理5.13中构造得到。对$t \in \{6,10\}$，分别取型为s^4，$s \in \{20,32\}$的$(4,2)$-CRSSGDD（引理5.4），再分别在组上填入型为2^{10}或2^{16}的$(4,2)$-CRSSGDD。对$t \in \{7,13\}$，对型为6^5或6^9的$(4,2)$-CRSSGDD用3膨胀，就得到了型为18^5或18^9的$(4,2)$-CRSSGDD。增加2个无穷点，并在组上连同无穷点填入型为2^{10}的$(4,2)$-CRSSGDD。对$t \in \{11,16\}$，分别取型为2^7或2^{10}的$(4,2)$-CRSSGDD，用10膨胀得到型为20^7或20^{10}的$(4,2)$-CRSSGDD，再在组上分别填入型为2^{10}的$(4,2)$-CRSSGDD就得到了所需设计。对$t = 15$，取一个型为$3^8 7^1$的$\{5\}$-GDD（通过补全型为3^8的$\{4\}$-RGDD得到，见[71]）。用WFC加权6，增加2个无穷点，分别在组上连同无穷点填入型为2^{10}或2^{22}的$(4,2)$-CRSSGDD。

对$t \in \{12,14\}$或$t \geq 17$，从引理2.4取一个$(v,\{5,6,7,8,9\},1)$-PBD。从这个PBD的点集中去掉一个点，得到型为$4^i 5^j 6^k 7^l 8^m$的$\{5,6,7,8,9\}$-GDD，其中$4i+5j+6k+7l+8m = v-1$。用WFC对这个GDD加权6并输入型为6^u，$u \in \{5,6,7,8,9\}$的$(4,2)$-CRSSGDD（引理5.14），得到型为$24^i 30^j 36^k 42^l 48^m$的$(4,2)$-CRSSGDD。增加2个无穷点，并在组上连同无穷点分别填入型为2^s，$s \in \{13, 16, 19, 22, 25\}$的$(4,2)$-CRSSGDD，我们就对任意偶数$v \in \{26,30\}$或$v \geq 36$得到了型为$2^{3(v-1)+1}$的$(4,2)$-CRSSGDD。 □

综合引理5.19和5.20中的结果，我们得到：

定理 5.21. *对任意$t \geq 2$，存在一个型为2^{3t+1}的$(4,2)$-CRSSGDD。因此，对任意$t \geq 2$，存在一个型为2^{3t+1}的GDC。即：对任意$t \geq 2$，$A_3(6t+2,6,4) = U(6t+2,3)$。*

c. 当长度$n \equiv 6,7 \pmod{12}$时

在本节中，我们将确定$A_3(12t+6,6,4)$和$A_3(12t+7,6,4)$的值。对$n \in \{6,7\}$，表5.1中已经确定了$A_3(6,6,4)$和$A_3(7,6,4)$的值。

引理 5.22. *对任意$n \in \{18,19,31,43,55\}$，$A_3(n,6,4) = U(n,3)$。*

证明. 所需码通过构造型为[2,2]的常重复合码得到。令点集为$\mathbb{Z}_n$。对$n = 18$，所需码由如下码字+2 (mod 18)得到。对$n \in \{19,31,43,55\}$，所需码由如下码字+1 (mod n)得到。

$n = 18$：$\langle 0,1,2,3\rangle$ $\langle 0,6,4,13\rangle$ $\langle 0,9,5,17\rangle$ $\langle 0,11,8,14\rangle$ $\langle 1,7,5,12\rangle$

$n = 19$：$\langle 0,3,18,4\rangle$ $\langle 0,17,10,7\rangle$ $\langle 0,5,11,13\rangle$

$n = 31$：$\langle 0,3,1,13\rangle$ $\langle 0,6,2,26\rangle$ $\langle 0,7,15,18\rangle$ $\langle 0,12,4,21\rangle$ $\langle 0,14,5,30\rangle$

$n = 43$：$\langle 0,2,26,36\rangle$ $\langle 0,10,25,38\rangle$ $\langle 0,3,8,9\rangle$ $\langle 0,1,18,22\rangle$ $\langle 0,4,11,31\rangle$ $\langle 0,13,29,32\rangle$ $\langle 0,20,12,14\rangle$

$n = 55$：$\langle 0,5,13,22\rangle$ $\langle 0,7,19,33\rangle$ $\langle 0,4,10,28\rangle$ $\langle 0,11,31,32\rangle$ $\langle 0,14,49,53\rangle$ $\langle 0,15,38,45\rangle$ $\langle 0,1,3,43\rangle$ $\langle 0,9,25,36\rangle$ $\langle 0,18,47,52\rangle$ □

引理 5.23. *对任意$u \in [4,8]$，存在一个型为$12^u 18^1$的$(4,2)$-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{12u} \cup (\{a\} \times \mathbb{Z}_6) \cup (\{b\} \times \mathbb{Z}_{12})$，组集为$\{\{0,u,2u,\ldots,11u\}+i : 0 \le i \le u-1\} \cup \{(\{a\} \times \mathbb{Z}_6) \cup (\{b\} \times \mathbb{Z}_{12})\}$。所需设计由下面基区组+1 (mod $12u$)展开得到，其中$x_0 \in \{x\} \times \mathbb{Z}_n$的下标由$\mathbb{Z}_{12u}$中唯一的$n$阶子群展开。

$12^4 18^1$：

第一个GDD的基区组：$(0,25,27,a_0)$ $(2,11,16,a_0)$ $(9,20,35,b_0)$ $(3,4,34,b_0)$ $(2,5,43,b_0)$ $(0,13,42,b_0)$

第二个GDD的基区组由上面基区组乘以乘子7得到。

$12^5 18^1$：

第一个GDD的基区组：

$$\begin{array}{cccc} (3,6,52,a_0) & (5,37,38,a_0) & (0,16,37,b_0) & (2,56,58,b_0) \\ (0,7,19,36) & (9,18,31,b_0) & (3,11,29,b_0) & \end{array}$$

第二个GDD的基区组由上面基区组乘以乘子7得到。

$12^6 18^1$：

第一个GDD的基区组：

$$\begin{array}{cccc} (2,40,69,a_0) & (0,1,65,a_0) & (2,23,55,b_0) & (8,30,33,b_0) \\ (0,4,14,49) & (5,46,61,b_0) & (4,24,63,b_0) & (0,9,11,55) \end{array}$$

第二个GDD的基区组由上面基区组乘以乘子5得到。

12^718^1：

第一个GDD的基区组：

$$(0,33,67,a_0)\quad (2,10,29,a_0)\quad (0,4,9,b_0)\quad (10,62,63,b_0)\quad (8,11,66,b_0)$$
$$(0,39,41,54)\quad (0,25,61,72)\quad (0,18,38,62)\quad (5,73,79,b_0)$$

第二个GDD的基区组由上面基区组乘以乘子5得到。

12^818^1：

第一个GDD的基区组：

$$(0,3,55,a_0)\quad (4,77,86,a_0)\quad (10,21,40,b_0)\quad (1,19,39,b_0)\quad (8,54,59,b_0)$$
$$(0,42,59,71)\quad (0,47,60,62)\quad (0,1,69,90)\quad (0,4,26,65)\quad (2,12,65,b_0)$$

第二个GDD的基区组由上面基区组乘以乘子5得到。 □

引理 5.24. *对任意$u\in[4,8]\cup\{16\}\cup[20,22]$或$u\geq 24$，存在一个型为$12^u18^1$的$(4,2)$-CRSSGDD。*

证明. 对$u\in\{4,5,6,7,8\}$，所需设计已经在引理5.23中构造。对$u\in\{21,33\}$，分别取型为12^415^1或12^715^1的$\{4\}$-GDD（见[69, 定理3.16]），用WFC加权4，增加18个无穷点，并在组上填入型为12^418^1或12^518^1的$(4,2)$-CRSSGDD，就得到了所需设计。对$u\in\{16,28,32\}$，分别取型为s^4，$s\in\{4,7,8\}$（引理5.4）的$\{4\}$-GDD，用WFC加权12，增加18个无穷点，并在组上连同无穷点填入型为12^s18^1的$(4,2)$-CRSSGDD。对$u\in\{22,26\}$，分别取型为6^49^1或6^59^1的$\{4\}$-GDD（见[77, 定理1.6]），用WFC加权8，增加18个无穷点，并在组上连同无穷点填入型为12^418^1或12^618^1的$(4,2)$-CRSSGDD。对$u=31$，取型为4^67^1的$\{4\}$-GDD（见[69, 引理3.17]），用WFC加权12，增加18个无穷点并在组上连同无穷点填入型为12^418^1或12^718^1的$(4,2)$-CRSSGDD。对$u=27$，取型为15^421^1的$\{4\}$-GDD（见[69, 定理4.1]），用WFC加权4，增加18个无穷点，并在组上连同无穷点填入型为12^518^1或12^718^1的$(4,2)$-CRSSGDD。

对$u\in\{20,24,25,29,30\}$或$u\geq 34$，从引理2.4取一个$(u+1,\{5,6,7,8,9\},1)$-PBD。从这个PBD的点集去掉一个点得到一个型为$4^i5^j6^k7^l8^m$ 的$\{5,6,7,8,9\}$-GDD，其中$4i+5j+6k+7l+8m=u$。用WFC加权12，输入设计是型为12^t，$t\in\{5,6,7,8,9\}$的$(4,2)$-CRSSGDD（引理5.18），得到型为$48^i60^j72^k84^l96^m$的$(4,2)$-CRSSGDD。增加18个无穷点，并在组上连同无穷点分别填入型为12^s18^1，

$s \in \{4,5,6,7,8\}$的$(4,2)$-CRSSGDD（引理5.23），我们就得到了型为12^u18^1，$u \in \{20,24,25,29,30\}$或$u \geq 34$的$(4,2)$-CRSSGDD。 □

引理 5.25. 当$r \in \{6,7\}$时，对任意$t \in [2,9] \cup \{17\} \cup [21,23]$或$t \geq 25$，$A_3(12t+r,6,4) = U(12t+r,3)$。

证明. 对任意$t \in \{2,3,4\}$，取一个型为6^{2t+1}的GDC（引理5.14）。所需的长度为$12t+6$的码可以通过在GDC的所有组中填入最优$(6,6,4)_3$码得到。所需的长度为$12t+7$的码在引理5.22中构造得到。

由引理5.24，对任意$u \in [4,8] \cup \{16\} \cup [20,22]$或$u \geq 24$，我们都有型为$12^u18^1$的GDC。如果在这个GDC的每个组上填入长度为12或18的最优码，对任意$t \in [5,9] \cup \{17\} \cup [21,23]$或$t \geq 25$，我们就得到了最优$(12t+6,6,4)_3$码。如果增加一个无穷点，并在这个GDC的组上连同这个无穷点填入长度为13或19的最优码，我们就得到了相应的最优$(12t+7,6,4)_3$码。 □

引理 5.26. 当$r \in \{6,7\}$时，对任意$t \in [10,16] \cup [18,20] \cup \{24\}$，$A_3(12t+r,6,4) = U(12t+r,3)$。

证明. 首先，我们构造型为36^um^1，其中$(u,m) \in \{(5,42),(6,18),(6,30),(6,78)\}$的$(4,2)$-CRSSGDD。取一个TD$(6,7)$，去掉一个区组中的5个点得到了一个型为$6^57^1$的$\{5,6\}$-GDD，用WFC加权6，就得到了型为$36^542^1$的$(4,2)$-CRSSGDD。取一个TD$(7,7)$，去掉一个区组的6个点得到型为$6^67^1$的$\{6,7\}$-GDD。用WFC把大小为6的组的所有点加权6，最后一个组的x,y,z个点分别加权$0,6,12$。这里输入设计是型为6^5，6^6和6^7的$(4,2)$-CRSSGDD，和型为6^512^1和6^612^1的$(4,2)$-CRSSGDD。令$(x,y,z) = (0,1,6)$，我们就得到型为36^678^1的$(4,2)$-CRSSGDD；令$(x,y,z) = (2,5,0)$，得到型为36^630^1 的$(4,2)$-CRSSGDD；令$(x,y,z) = (4,3,0)$，就得到型为的36^618^1的$(4,2)$-CRSSGDD。

然后，我们构造型为24^um^1，其中$(u,m) \in \{(4,30),(5,18),(5,30),(6,18),(6,30),(7,18),(7,30)\}$的$(4,2)$-CRSSGDD。取一个型为$6^ua^1$的$(4,2)$-CRSSGDD，去掉组大小为$a$中的点，再用WFC加权4。这里，输入设计是型为$4^4$的$\{4\}$-MGDD，和型为$4^3$的可分解$\{3\}$-MGDD。我们就得到了两个具有CRSS性质的型为$(24,6^4)^u$的$\{3,4\}$-DGDD，且所有大小为3的区组形成$3a$个平行类。增加$3a$个无穷点补全平行类，并填入型为6^uw^1的$(4,2)$-CRSSGDD，就得到了型为$24^u(3a+w)^1$的$(4,2)$-CRSSGDD。

由于我们有型为$6^4 9^1$和$6^4 3^1$的$(4,2)$-CRSSGDD，令$(a,w)=(9,3)$，就得到型为$24^4 30^1$的$(4,2)$-CRSSGDD。由于我们有型为$6^u 6^1$，$u \in \{5,6,7\}$，和型为$6^u 12^1$，$u \in \{5,6,7\}$的$(4,2)$-CRSSGDD。令$(a,w)=(6,0)$，就得到型为$24^u 18^1$，$u \in \{5,6,7\}$的$(4,2)$-CRSSGDD；令$(a,w)=(6,12)$，就得到型为$24^u 30^1$，$u \in \{5,6,7\}$的$(4,2)$-CRSSGDD。

由引理5.5，我们得到型为$36^u m^1$，$(u,m) \in \{(5,42),(6,18),(6,30),(6,78)\}$和$24^u m^1$，$(u,m) \in \{(4,30),(5,18),(5,30),(6,18),(6,30),(7,18),(7,30)\}$的GDC。在这些GDC的组上填入相应的最优码，我们就得到了最优$(12t+6,6,4)_3$码，其中$t \in [10,16] \cup [18,21] \cup \{24\}$。同样，如果增加一个无穷点，并在所有GDC的组上连同无穷点填入相应的最优码，我们就得到了最优$(12t+7,6,4)_3$码。 □

综合上述结果，我们得到：

定理 5.27. *对任意$t \geq 0$，$A_3(12t+6,6,4) = U(12t+6,3)$；对任意$t \geq 1$，$A_3(12t+7,6,4) = U(12t+7,3)$。*

d. 当长度$n \equiv 9,10 \pmod{12}$时

在本节中，我们将确定$A_3(12t+9,6,4)$和$A_3(12t+10,6,4)$的值。对$n \in \{9,10\}$，$A_3(9,6,4)$和$A_3(10,6,4)$的值已经在表5.1中确定。

引理 5.28. *对任意$n \in \{21,22,33,34\}$，$A_3(n,6,4) = U(n,3)$。*

证明. 对$n=21$，所需的码通过构造最优$(21,6,[2,2])_3$码得到。令点集为$\mathbb{Z}_{21}$，所需的码由码字$\langle 0,1,3,11\rangle$，$\langle 0,8,6,15\rangle$，$\langle 0,9,4,5\rangle$ $+1 \pmod{21}$展开得到。

对$n \in \{22,34\}$，令点集为$\mathbb{Z}_n$，所需的码通过由如下码字$+2 \pmod{n}$展开得到。

$(22,6,4)_3$码：$\langle 9_2,5_2,18_2,15_1\rangle$ $\langle 1_2,16_1,21_2,15_1\rangle$ $\langle 21_2,0_2,2_1,6_2\rangle$ $\langle 21_2,4_2,7_1,11_1\rangle$ $\langle 18_1,12_1,5_1,7_1\rangle$ $\langle 0_1,10_1,1_1,18_2\rangle$ $\langle 1_2,0_2,20_1,12_2\rangle$

$(34,6,4)_3$码：$\langle 1_2,4_2,3_2,7_2\rangle$ $\langle 0_2,6_2,30_1,10_1\rangle$ $\langle 28_2,3_2,11_2,21_2\rangle$ $\langle 27_1,0_1,22_1,16_1\rangle$ $\langle 30_1,31_1,21_1,22_1\rangle$ $\langle 26_2,15_2,3_2,24_2\rangle$ $\langle 20_2,28_2,1_2,6_2\rangle$ $\langle 27_1,8_1,10_1,5_1\rangle$ $\langle 2_2,21_2,20_2,7_2\rangle$ $\langle 3_1,31_1,16_1,29_1\rangle$ $\langle 9_1,25_1,5_1,2_1\rangle$

对$n=33$，所需的码通过在型为$6^4 9^1$的GDC的组上填入长度为6或9的最优码得到。 □

引理 5.29. *对任意$u \in [4,8]$，存在一个型为$12^u 9^1$的$(4,2)$-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{12u} \cup (\{a,b,c\} \times \mathbb{Z}_3)$，组集为$\{\{0,u,2u,\ldots,11u\}+i : 0 \le i \le u-1\} \cup \{\{a,b,c\} \times \mathbb{Z}_3\}$。所需设计由下面基区组+2 (mod $12u$)展开得到。

$12^4 9^1$：

第一个GDD的基区组：

$(0,7,14,a_0)$　$(3,17,22,a_0)$　$(0,37,39,b_0)$　$(2,11,28,b_0)$　$(3,13,26,c_0)$
$(5,30,40,c_0)$　$(0,1,2,19)$　$(0,3,30,45)$　$(0,6,11,33)$

第二个GDD的基区组是由如上基区组乘以乘子19得到。

$12^5 9^1$：

第一个GDD的基区组：

$(1,3,52,a_0)$　$(5,18,32,a_0)$　$(0,56,57,b_0)$　$(5,13,46,b_0)$　$(1,2,23,c_0)$　$(0,13,32,49)$
$(0,51,58,c_0)$　$(0,3,7,24)$　$(1,7,30,38)$　$(1,17,29,43)$　$(0,12,38,54)$

第二个GDD的基区组是由如上基区组乘以乘子7得到。

$12^6 9^1$：

第一个GDD的基区组：

$(0,14,43,a_0)$　$(3,5,10,a_0)$　$(5,16,32,b_0)$　$(1,21,54,b_0)$　$(0,4,9,c_0)$
$(5,26,37,c_0)$　$(0,33,41,55)$　$(0,2,34,71)$　$(0,1,17,26)$　$(0,27,50,53)$
$(1,38,48,69)$　$(0,13,23,57)$　$(0,7,20,64)$

第二个GDD的基区组是由如上基区组乘以乘子5得到。

$12^7 9^1$：

第一个GDD的基区组：

$(4,36,83,a_0)$　$(1,14,75,a_0)$　$(3,18,43,b_0)$　$(4,5,38,b_0)$　$(4,37,57,c_0)$
$(5,72,80,c_0)$　$(1,20,33,63)$　$(0,46,48,58)$　$(1,26,30,48)$　$(1,61,77,79)$
$(1,4,10,49)$　$(1,44,73,74)$　$(1,28,47,51)$　$(1,18,58,82)$　$(0,5,16,31)$

第二个GDD的基区组是由如上基区组乘以乘子11得到。

$12^8 9^1$：

第一个GDD的基区组：

$(2,4,47,a_0)$　$(3,42,79,a_0)$　$(5,24,63,b_0)$　$(2,40,61,b_0)$　$(0,3,95,c_0)$　$(0,4,69,91)$
$(2,49,64,c_0)$　$(0,55,67,73)$　$(1,48,62,63)$　$(0,6,66,76)$　$(1,11,18,71)$　$(0,41,44,71)$
$(1,72,84,95)$　$(1,12,29,43)$　$(1,22,68,90)$　$(0,19,54,63)$　$(0,5,18,51)$

第二个GDD的基区组是由如上基区组乘以乘子19得到。　□

引理 5.30. *对任意$u \in [4,8] \cup \{16\} \cup [20,22]$或$u \ge 24$，存在一个型为$12^u 9^1$的$(4,2)$-CRSSGDD。*

证明. 证明与引理5.24的证明类似。这里，我们需要增加9个无穷点，然后填入型为12^u9^1，$u \in \{4,5,6,7,8\}$的$(4,2)$-CRSSGDD（引理5.29）。 □

引理 5.31. 当$r \in \{9,10\}$时，对任意$t \in [4,8] \cup \{16\} \cup [20,22]$或$t \geq 24$，$A_3(12t+r,6,4) = U(12t+r,3)$。

证明. 由引理5.30，我们有型为12^t9^1，$t \in [4,8] \cup \{16\} \cup [20,22]$或$u \geq 24$的GDC。在组上填入长度为12或9的最优码，就得到了最优$(12t+9,6,4)_3$码。如果增加一个无穷点，在组上连同无穷点填入长度为13或10的最优码，就得到了最优$(12t+10,6,4)_3$码。 □

引理 5.32. 当$r \in \{9,10\}$时，对任意$t \in [9,15] \cup [17,19] \cup \{3,23\}$，$A_3(12t+r,6,4) = U(12t+r,3)$。

证明. 首先，我们构造型为36^um^1，$(u,m) \in \{(5,33),(6,21),(6,69)\}$的$(4,2)$-CRSSGDD。取一个TD$(6,7)$，去掉一个区组中的5个点得到型为$6^57^1$的$\{5,6\}$-GDD。用WFC对大小为6的组的所有点加权6，大小为7的组中的4个点加权6，3个点加权3。这里，输入设计是型为6^5，6^6，6^43^1和6^53^1的$(4,2)$-CRSSGDD。因此，我们得到了型为36^533^1的$(4,2)$-CRSSGDD。从一个TD$(7,7)$出发，去掉一个区组中的6个点得到型为6^67^1的$\{6,7\}$-GDD。用WFC对大小为6的组的所有点加权6，对最后一个组的x,y,z个点分别加权$3,6,12$。令$(x,y,z) = (7,0,0)$，就得到型为36^621^1的$(4,2)$-CRSSGDD；令$(x,y,z) = (1,1,5)$，就得到型为36^669^1的$(4,2)$-CRSSGDD。

然后，我们构造型为24^um^1，$(u,m) \in \{(5,9),(5,21),(6,21),(6,33)\}$的$(4,2)$-CRSSGDD。构造与引理5.26中构造型为$24^um^1$，$(u,m) \in \{(4,30),(5,18),(5,30),(6,18),(6,30),(7,18),(7,30)\}$的$(4,2)$-CRSSGDD的构造类似。我们有型为$6^53^1$，$6^56^1$，$6^66^1$和$6^69^1$的$(4,2)$-CRSSGDD。令$u = 5$，$(a,w) = (3,0)$，就得到型为$24^59^1$的$(4,2)$-CRSSGDD；令$u = 5$，$(a,w) = (6,3)$，就有型为$24^521^1$的$(4,2)$-CRSSGDD；令$u = 6$，$(a,w) = (6,3)$，就得到型为$24^621^1$的$(4,2)$-CRSSGDD；令$u = 6$，$(a,w) = (9,6)$，就得到型为$24^633^1$的$(4,2)$-CRSSGDD。

最后，我们构造型为9^u，$u \in \{5,13,17,21,25\}$的$(4,2)$-CRSSGDD。对一个型为3^5的$(4,2)$-CRSSGDD用3膨胀，得到型为9^5的$(4,2)$-CRSSGDD。分别取型为3^4或4^4的$\{4\}$-GDD，或一个TD$(5,4)$，用WFC加权9，增加9个无穷点，填入型为9^5的$(4,2)$-CRSSGDD就分别得到了型为9^{13}，9^{17}或9^{21}的$(4,2)$-CRSSGDD。

取一个TD$(5,5)$，用WFC加权9，填入型为9^5的$(4,2)$-CRSSGDD就得到了型为9^{25}的$(4,2)$-CRSSGDD。

由引理5.5，我们得到了型为$36^u m^1$，$(u,m) \in \{(5,33),(6,21),(6,69)\}$，型为$24^u m^1$，$(u,m) \in \{(5,9),(5,21),(6,21),(6,33)\}$，和型为$9^u$，$u \in \{5,13,17,21,25\}$的GDC。如果在这些GDC的组上填入适当长度的最优码，我们就得到了最优$(12t+9,6,4)_3$码，其中$t \in [9,15] \cup [17,19] \cup \{3,23\}$。如果增加一个无穷点，并在所有组上连同无穷点填入适当长度的最优码，我们就得到了相应的最优$(12t+10,6,4)_3$码。 □

综合上述结果，我们得到：

定理 5.33. 对任意$t \geq 0$，$A_3(12t+9,6,4) = U(12t+9,3)$；对任意$t \geq 0$，$A_3(12t+10,6,4) = U(12t+10,3)$。

e. 当长度$n \equiv 5 \pmod 6$时

在本节中，我们将确定$A_3(6t+5,6,4)$的值。在这个类，我们找到的长度最小的最优码是23，但是对$n \in \{11,17\}$，我们有如下下界。

引理 5.34. $A_3(11,6,4) \geq U(11,3)-1$；$A_3(17,6,4) \geq U(17,3)-2$。

证明. 对$n=11$，我们直接构造15个码字的$(11,6,[2,2])_3$码：

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

对$n=17$，所需的码通过构造两个超单填充得到，每一个超单填充可以得到一个$(17,6,4)_2$码。与引理5.5的证明类似，我们可以得到一个$(17,6,4)_3$码。

第一个填充的区组：

$(7,4,10,1)$　$(13,12,2,5)$　$(10,14,6,13)$　$(8,4,11,14)$　$(10,9,8,2)$　$(7,2,14,15)$　$(2,6,0,4)$
$(8,16,1,6)$　$(9,14,1,12)$　$(0,10,12,11)$　$(15,11,9,6)$　$(13,3,9,4)$　$(5,3,15,10)$　$(0,5,7,9)$
$(7,6,3,12)$　$(0,14,3,16)$　$(4,16,15,12)$　$(0,13,8,15)$　$(1,11,2,3)$　$(7,11,13,16)$

第二个填充的区组：

$(9,7,13,1)$　$(1,3,6,15)$　$(15,12,10,2)$　$(3,8,16,2)$　$(11,3,10,9)$　$(14,16,6,12)$　$(1,5,2,0)$
$(4,6,5,10)$　$(2,11,6,7)$　$(10,16,13,0)$　$(0,12,3,4)$　$(5,15,16,9)$　$(11,0,15,14)$　$(6,9,0,8)$
$(14,3,7,5)$　$(2,9,4,14)$　$(11,13,8,12)$　$(4,7,8,15)$　$(10,14,1,8)$　$(4,1,11,16)$

□

引理 5.35. *存在一个型为*$2^9 5^1$*的*$(4,2)$*-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{18} \cup (\{a\} \times \mathbb{Z}_3) \cup (\{b,c\} \times \mathbb{Z}_1)$，组集为$\{\{0,9\}+i : 0 \le i \le 8\} \cup \{(\{a\} \times \mathbb{Z}_3) \cup (\{b,c\} \times \mathbb{Z}_1)\}$。所需设计是由如下基区组+6 (mod 18)展开得到。

第一个GDD的基区组：

$(1,4,12,a_0)$ $(3,5,7,b_0)$ $(0,13,14,17)$ $(0,3,6,a_0)$ $(5,9,17,a_0)$ $(0,5,8,16)$ $(10,11,16,a_0)$
$(2,7,13,a_0)$ $(0,2,4,b_0)$ $(8,14,15,a_0)$ $(3,4,8,c_0)$ $(0,1,11,c_0)$ $(4,7,9,15)$

第二个GDD的基区组：

$(1,2,8,a_0)$ $(0,12,14,a_0)$ $(4,7,10,a_0)$ $(3,5,15,a_0)$ $(6,9,16,a_0)$ $(2,3,4,17)$ $(11,13,17,a_0)$
$(0,4,8,11)$ $(0,5,13,b_0)$ $(3,8,16,b_0)$ $(0,16,17,c_0)$ $(1,3,14,c_0)$ $(0,1,7,15)$

□

引理 5.36. *对任意*$u \in \{12,15,18,21,24,36\}$*，存在型为*$2^u 5^1$*的*$(4,2)$*-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{2u} \cup (\{a,b,c,d,e\} \times \mathbb{Z}_1)$，组集为$\{\{0,u\}+i : 0 \le i \le u-1\} \cup \{\{a,b,c,d,e\} \times \mathbb{Z}_1\}$。对$u \in \{12,18,24,36\}$，所需设计是由如下基区组+3 (mod $2u$)展开得到。对$u \in \{15,21\}$，所需设计由如下基区组+6 (mod $2u$)展开得到。

$2^{12}5^1$：

第一个GDD的基区组：

$(2,18,22,a_0)$ $(0,1,2,b_0)$ $(2,9,16,c_0)$ $(2,7,21,d_0)$
$(0,16,23,e_0)$ $(0,13,19,22)$ $(2,8,10,23)$ $(0,3,14,18)$

第二个GDD的基区组：

$(1,9,11,a_0)$ $(2,3,10,b_0)$ $(1,5,15,c_0)$ $(0,1,8,d_0)$
$(1,2,21,e_0)$ $(1,7,20,22)$ $(2,5,9,20)$ $(0,3,9,22)$

$2^{18}5^1$：

第一个GDD的基区组：

$(2,7,33,a_0)$ $(0,7,29,b_0)$ $(2,24,25,c_0)$ $(1,2,12,d_0)$ $(0,22,32,e_0)$ $(0,6,8,23)$
$(1,4,8,20)$ $(0,11,12,27)$ $(0,4,13,34)$ $(1,13,18,21)$ $(2,8,10,35)$

第二个GDD的基区组：

$(2,12,34,a_0)$ $(1,12,32,b_0)$ $(2,3,13,c_0)$ $(0,11,31,d_0)$ $(2,19,21,e_0)$ $(2,26,28,29)$
$(1,4,21,33)$ $(0,1,13,28)$ $(0,3,5,9)$ $(1,8,23,31)$ $(2,9,24,32)$

$2^{24}5^1$：

第一个GDD的基区组：

$(0,1,8,a_0)$　$(0,4,29,b_0)$　$(0,11,40,c_0)$　$(2,13,30,d_0)$　$(2,6,16,e_0)$　$(2,20,23,36)$
$(0,16,38,47)$　$(0,6,18,39)$　$(0,3,5,37)$　$(0,7,19,46)$　$(0,17,22,23)$　$(1,16,21,46)$
$(2,17,24,37)$　$(2,4,10,14)$

第二个GDD的基区组：

$(0,13,32,a_0)$　$(1,30,32,b_0)$　$(1,17,18,c_0)$　$(0,25,26,d_0)$　$(0,1,38,e_0)$　$(2,5,17,44)$
$(1,28,35,43)$　$(0,3,18,23)$　$(2,15,22,25)$　$(2,4,36,40)$　$(1,3,14,44)$　$(2,6,28,46)$
$(0,28,37,42)$　$(0,9,17,36)$

$2^{36}5^1$：

第一个GDD的基区组：

$(1,32,57,a_0)$　$(0,17,46,b_0)$　$(2,12,52,c_0)$　$(0,11,13,d_0)$　$(0,23,37,e_0)$　$(0,14,22,51)$
$(0,12,15,20)$　$(2,3,9,36)$　$(2,17,22,45)$　$(2,15,41,71)$　$(1,20,31,42)$　$(0,32,63,67)$
$(0,34,55,68)$　$(0,1,2,25)$　$(2,8,53,62)$　$(0,10,30,54)$　$(0,19,58,64)$　$(2,26,58,70)$
$(1,8,55,70)$　$(1,3,10,56)$

第二个GDD的基区组：

$(0,1,50,a_0)$　$(2,36,46,b_0)$　$(0,46,65,c_0)$　$(1,6,59,d_0)$　$(0,2,28,e_0)$　$(2,8,11,59)$
$(1,53,58,71)$　$(1,13,24,64)$　$(0,17,21,64)$　$(2,12,15,60)$　$(1,15,21,46)$　$(1,23,39,62)$
$(2,14,54,70)$　$(2,31,32,64)$　$(0,4,7,57)$　$(0,11,42,54)$　$(2,3,29,66)$　$(1,32,49,67)$
$(0,5,33,70)$　$(1,35,43,60)$

$2^{15}5^1$：

第一个GDD的基区组：

$(21,17,8,a_0)$　$(28,6,25,a_0)$　$(0,14,5,b_0)$　$(21,19,16,b_0)$　$(5,1,8,c_0)$　$(5,12,15,18)$
$(0,21,28,c_0)$　$(21,12,22,d_0)$　$(7,20,23,d_0)$　$(0,26,25,e_0)$　$(21,5,10,e_0)$　$(14,3,8,15)$
$(0,12,20,16)$　$(0,1,29,11)$　$(14,22,2,16)$　$(0,7,13,2)$　$(7,3,25,16)$　$(5,22,4,11)$
$(21,1,15,23)$

第二个GDD的基区组：

$(16,12,25,b_0)$　$(27,29,26,b_0)$　$(0,8,5,e_0)$　$(27,13,22,e_0)$　$(5,7,26,c_0)$　$(5,24,15,6)$
$(0,27,16,c_0)$　$(19,20,11,a_0)$　$(27,24,4,a_0)$　$(0,2,25,d_0)$　$(27,5,10,d_0)$　$(8,21,26,15)$
$(0,7,23,17)$　$(8,4,14,22)$　$(0,19,1,14)$　$(0,24,20,22)$　$(19,21,25,22)$　$(5,4,28,17)$
$(27,7,15,11)$

$2^{21}5^1$：

第一个GDD的基区组：

$(0,13,17,a_0)$　$(2,3,22,a_0)$　$(0,38,40,b_0)$　$(5,15,25,b_0)$　$(0,2,16,c_0)$　$(4,21,34,37)$
$(3,5,7,c_0)$　$(0,25,27,d_0)$　$(2,28,41,d_0)$　$(2,21,24,e_0)$　$(4,11,19,e_0)$　$(2,12,17,26)$
$(1,6,25,36)$　$(0,26,34,35)$　$(1,7,21,38)$　$(1,17,31,34)$　$(0,1,8,11)$　$(1,2,9,14)$
$(0,3,9,29)$　$(0,15,23,24)$　$(4,8,14,31)$　$(5,9,20,33)$　$(3,4,10,15)$　$(4,23,35,41)$
$(0,4,22,36)$

第二个GDD的基区组：

$(0,17,19,b_0)$ $(22,33,32,b_0)$ $(0,40,20,c_0)$ $(13,39,23,c_0)$ $(0,22,8,a_0)$ $(2,21,38,29)$
$(33,13,35,a_0)$ $(0,23,3,d_0)$ $(22,14,31,d_0)$ $(22,21,12,e_0)$ $(2,37,41,e_0)$ $(22,6,19,34)$
$(11,24,23,18)$ $(0,34,38,7)$ $(11,35,21,40)$ $(11,19,5,38)$ $(0,11,4,37)$ $(11,22,15,28)$
$(0,33,15,25)$ $(0,39,1,12)$ $(2,4,28,5)$ $(13,15,10,27)$ $(33,2,26,39)$ $(2,1,7,31)$
$(0,2,32,18)$

□

引理 5.37. *对任意$u \in \{30,33,39,42,51\}$，存在一个型为2^u5^1的$(4,2)$-CRSSGDD。*

证明. 这里所用方法与文[68]中方法类似。令点集为$\mathbb{Z}_{2u} \cup \{\infty_1,\infty_2,\ldots,\infty_5\}$，组集为$\{\{0,u\}+i : 0 \le i \le u-1\} \cup \{\infty_1,\infty_2,\ldots,\infty_5\}$。令$2u=3x$。设计所需区组由两部分组成。第一部分是由如下基区组$+3 \pmod{2u}$展开得到。

第一个GDD的第一部分基区组：

当$x \equiv 1 \pmod 3$**时**

$$\begin{array}{rrrr} 0 & x & x+1 & \infty_1 \\ 2x+1 & 2x+2 & 2x & \infty_2 \\ x+2 & 4 & x+4 & \infty_3 \\ 3 & 1 & 2x+3 & \infty_4 \\ 2x+4 & x+3 & 2 & \infty_5 \end{array}$$

当$x \equiv 2 \pmod 3$**时**

$$\begin{array}{rrrr} 0 & 2x & 2x+1 & \infty_1 \\ x+1 & x+2 & x & \infty_2 \\ 2x+2 & 4 & 2x+4 & \infty_3 \\ 3 & 1 & x+3 & \infty_4 \\ x+4 & 2x+3 & 2 & \infty_5 \end{array}$$

第二个GDD的第一部分基区组：

当$x \equiv 1 \pmod 3$**时**

$$\begin{array}{cccc} x+2 & x & 2x & \infty_1 \\ 3 & 2x+2 & x+4 & \infty_2 \\ 2x+4 & 4 & 2x+3 & \infty_3 \\ 0 & 1 & 2 & \infty_4 \\ 2x+1 & x+3 & x+1 & \infty_5 \end{array}$$

当$x \equiv 2 \pmod 3$**时**

$$\begin{array}{cccc} 2x+2 & 2x & x & \infty_1 \\ 3 & x+2 & 2x+4 & \infty_2 \\ x+4 & 4 & x+3 & \infty_3 \\ 0 & 1 & 2 & \infty_4 \\ x+1 & 2x+3 & 2x+1 & \infty_5 \end{array}$$

对$u \in \{30, 42\}$，所需设计的第二部分区组是由如下基区组$+1 \pmod{2u}$展开得到。

$2^{30}5^1$：

第一个GDD的第二部分基区组：$(0, 29, 35, 52)$ $(0, 15, 39, 49)$ $(0, 5, 18, 32)$ $(0, 4, 48, 57)$

第二个GDD的第二部分基区组：$(0, 8, 11, 36)$ $(0, 5, 17, 26)$ $(0, 4, 18, 33)$ $(0, 6, 16, 53)$

$2^{42}5^1$：

第一个GDD的第二部分基区组：$(0, 12, 22, 81)$ $(0, 31, 38, 70)$ $(0, 60, 65, 78)$ $(0, 9, 49, 57)$ $(0, 30, 41, 64)$ $(0, 4, 21, 37)$

第二个GDD的第二部分基区组：$(0, 5, 23, 54)$ $(0, 14, 47, 59)$ $(0, 41, 50, 63)$ $(0, 17, 57, 81)$ $(0, 65, 73, 80)$ $(0, 36, 68, 74)$

对$u \in \{33, 39, 51\}$，第二部分是由如下基区组$+2 \pmod{2u}$展开得到。

$2^{33}5^1$：

第一个GDD的第二部分基区组：

$(0, 24, 49, 63)$　$(1, 7, 41, 54)$　$(1, 8, 13, 38)$　$(0, 31, 35, 40)$　$(1, 20, 37, 52)$
$(1, 40, 43, 51)$　$(0, 8, 14, 18)$　$(0, 7, 45, 55)$　$(0, 9, 38, 54)$

第二个GDD的第二部分基区组：

$(0,26,50,62)$ $(1,11,15,36)$ $(0,5,8,55)$ $(0,9,37,49)$ $(0,3,18,56)$
$(0,6,17,35)$ $(0,7,14,39)$ $(0,15,21,57)$ $(0,19,27,32)$

$2^{39}5^1$：

第一个GDD的第二部分基区组：

$(1,47,60,70)$ $(1,5,19,43)$ $(1,12,57,73)$ $(1,13,16,21)$ $(0,8,29,38)$ $(0,13,20,34)$
$(0,6,23,33)$ $(0,32,43,73)$ $(1,28,32,44)$ $(1,30,48,72)$ $(0,3,22,37)$

第二个GDD的第二部分基区组：

$(1,5,50,59)$ $(0,5,13,49)$ $(0,40,58,74)$ $(0,3,67,70)$ $(1,33,38,52)$ $(0,17,35,48)$
$(1,17,58,73)$ $(0,31,61,71)$ $(0,51,63,72)$ $(0,24,36,43)$ $(0,10,32,55)$

$2^{51}5^1$：

第一个GDD的第二部分基区组：

$(1,5,49,77)$ $(0,43,66,93)$ $(0,17,64,78)$ $(0,3,19,58)$ $(1,13,18,95)$ $(1,43,65,89)$
$(0,45,86,90)$ $(0,21,31,84)$ $(0,52,59,92)$ $(0,33,60,73)$ $(0,46,76,99)$ $(0,5,71,82)$
$(0,54,65,83)$ $(1,66,88,94)$ $(1,8,16,97)$

第二个GDD的第二部分基区组：

$(1,4,67,88)$ $(0,27,38,90)$ $(1,6,39,59)$ $(0,23,76,80)$ $(1,7,25,84)$ $(0,13,30,58)$
$(0,47,55,95)$ $(1,72,77,81)$ $(1,31,44,47)$ $(0,7,17,36)$ $(1,32,42,53)$ $(0,37,65,79)$
$(0,14,54,96)$ $(0,46,75,87)$ $(0,69,78,94)$

□

引理 5.38. *存在一个型为$2^{27}5^1$的$(4,2)$-CRSSGDD。*

证明. 令点集为$\{\mathbb{Z}_3 \times \mathbb{Z}_{18}\} \cup (\{a,b,c,d,e\} \times \mathbb{Z}_1)$，组集为$\{\{(i,2j),(i,2j+1)\} : 0 \le i \le 2, 0 \le j \le 8\} \cup \{\{a,b,c,d,e\} \times \mathbb{Z}_1\}$。如下带无穷点的基区组$(-,+1 \pmod{18})$展开，其他的基区组$(+1 \pmod 3, +2 \pmod{18})$展开，就得到我们需要的设计。

第一个GDD的基区组：

$((0,0),(1,0),(2,1),a_0)$ $((0,1),(1,2),(2,0),b_0)$ $((0,2),(1,4),(2,4),c_0)$
$((0,3),(1,1),(2,3),d_0)$ $((0,4),(1,3),(2,2),e_0)$ $((0,1),(0,3),(0,13),(1,8))$
$((0,0),(0,9),(0,10),(1,15))$ $((0,1),(0,16),(1,10),(2,6))$ $((0,1),(1,4),(2,11),(2,15))$
$((0,1),(1,11),(1,16),(2,7))$ $((0,0),(0,5),(0,12),(0,16))$ $((0,0),(0,15),(1,8),(2,12))$

第二个GDD的基区组：

$((0,0),(1,1),(2,2),d_0)$	$((0,2),(1,0),(2,0),a_0)$	$((0,4),(1,4),(2,3),c_0)$
$((0,1),(1,3),(2,1),e_0)$	$((0,3),(1,2),(2,4),b_0)$	$((0,1),(0,16),(1,8),(1,12))$
$((0,1),(0,5),(0,14),(2,9))$	$((0,0),(0,11),(0,13),(2,5))$	$((0,0),(0,6),(0,16),(1,13))$
$((0,0),(1,4),(2,9),(2,12))$	$((0,0),(1,12),(2,3),(2,15))$	$((0,0),(0,7),(0,17),(1,11))$

□

引理 5.39. *对任意$t \geq 3$，存在型为$2^{3t}5^1$的$(4,2)$-CRSSGDD。*

证明. 对$t \in [3,14] \cup \{17\}$，所需设计在引理 5.35–5.38中构造得到。对$t \in \{15,18,21,27,33\}$，取型为6^u，$u \in \{5,6,7,9,11\}$的$(4,2)$-CRSSGDD并用3膨胀。增加5个无穷点，在组上连同无穷点填入型为2^95^1的$(4,2)$-CRSSGDD得到所需设计。对$t = 16$，取型为8^4的$(4,2)$-CRSSGDD并用3膨胀，增加5个无穷点，在组上连同无穷点填入型为$2^{12}5^1$的$(4,2)$-CRSSGDD得到所需设计。对$t \in \{28,32\}$，取型为6^u，$u \in \{7,8\}$的$\{4\}$-GDD，用WFC加权4，增加5个无穷点，在组上连同无穷点填入型为$2^{12}5^1$的$(4,2)$-CRSSGDD。对$t \in \{22,26\}$，取型为6^u9^1，$u \in \{4,5\}$ 的$\{4\}$-GDD（见[77, 定理1.6]），用WFC加权4，增加5个无穷点，在组上连同无穷点填入型为$2^{12}5^1$或$2^{18}5^1$的$(4,2)$-CRSSGDD得到所需设计。

对$t = 31$，取型为3^87^1的$\{5\}$-GDD，用WFC加权6，增加5个无穷点，在组上连同无穷点填入型为2^95^1或$2^{21}5^1$的$(4,2)$-CRSSGDD得到所需设计。对$t = 23$，取一个TD$(5,5)$，用WFC对前四个组的所有点，和最后一个组的一个点加权6，其余点加权3得到型为30^418^1的$(4,2)$-CRSSGDD。增加5个无穷点，在组上连同无穷点填入型为$2^{15}5^1$或2^95^1的$(4,2)$-CRSSGDD得到所需设计。对$t = 19$，取一个TD$(5,4)$，用WFC对前四个组的所有点，及最后一个组的两个点加权6，其余点加权3，得到型为24^418^1的$(4,2)$-CRSSGDD。增加5个无穷点，在组上连同无穷点填入型为$2^{12}5^1$或2^95^1的$(4,2)$-CRSSGDD得到所需设计。

对$t \in \{20,24,25,29,30\}$或$t \geq 34$，从引理2.4取一个$(t+1,\{5,6,7,8,9\},1)$-PBD。去掉一个点得到型为$4^i5^j6^k7^l8^m$的$\{5,6,7,8,9\}$-GDD，其中$4i+5j+6k+7l+8m = t$。用WFC加权6，输入型为6^u，$u \in \{5,6,7,8,9\}$（引理5.14）的$(4,2)$-CRSSGDD得到型为$24^i30^j36^k42^l48^m$的$(4,2)$-CRSSGDD。增加5个无穷点，在组上连同无穷点填入型为$2^{3s}5^1$，$s \in \{4,5,6,7,8\}$的$(4,2)$-CRSSGDD。我们就得到了型为$2^{3t}5^1$，$t \in \{20,24,25,29,30\}$或$t \geq 34$的$(4,2)$-CRSSGDD。 □

表 5.2: 引理5.40中所需置换

n	置换
23	(0,17,15,11,12,1,20,18,5,19,4,9,8,14,3,21,6,7,10,16,22,2,13)
29	(0,28,12)(1,2,16,3,8,7,21,27,13,4,11,14,15,24,6)(5,23,20,10,17,26,9)(18)(19)(22,25)
35	(0,33,18,24,11,14,30,8,1,31,2,20,13,21,4,27,5,29,3,32,12,17,9,23,15,6,25,22,10,19,28,26,34,7)(16)
41	(0,32,14,39,26,16,30,23,29,34,11,40,5,13,2,25,18,3,28,27,37)(1,33,4,36,19,22,6,8,31,12,17,35,7, 38,10,24,9,21,15)(20)
47	(0,25,20,26,38,43,8,11,4,3,28,46,5,44,40,27,30,45,23,1,32,6,18,2,35,21,24,14,31,22,39,37,16,36,9, 7)(10,29,33,13,15,42)(12)(17,19)(34,41)
53	(0,8,26,18,2,20,36)(1,31,38,32,46,43,15,44,34,24,23,13,30,12,45,22,28,11,7,29,40,50,19,14,6,27, 39,47,48,41,37,49,25)(3,42,17,16)(4,51)(5,9,21,10,52,33)(35)
59	(0,46,41,5,38)(1,6,18,10,21,17,27,45,58,42,22,23,51,52)(2,44,12,30,49,15,29,19,54)(3,31,8,13,16, 56,53,33,37,36,11,55,26,25,14,32,40,34,24,4,7)(9,57,28,20)(35,39)(43,50,48,47)
65	(0,46,13,55,32,19,59,23,54,53,33,60,50,25,51,47,20,5,42,11,57,1)(2,35,8,18,56,22,10,64,27,62)(3, 48,58,17,34,49,41,7,31,12,43,40,24,9)(4,61,16,15,26,14,30,45,38,29,6,44,36,39,52)(21)(28,63)(37)
77	(0,46,60,72,55,52,36,63,33,62,9,75,64,47,39,53,67,11,31,35,34,45,24,48,2,30,25,19,56,50,61,68,28, 16,65,1,22,17,4,27,51,69,32,5,10,71,42,58,41,12,7,44,37,57,21)(3,8,70,26,23,54,20,73,18,15)(6,13, 14,59,43,74,66,76)(29,38,49)(40)
89	(0,46,44,49,58,10,70,68,43,16,54,39,62,67,41,34,38,84,88,6,81,26,69,40,86,66,74,47,12,82,55,2,27, 78,11,13,71,80,76,7,48,51,24)(1,22,56,83,42,77,53,60,29,19,65,50,37,35,25,17,30,23,73,9,72,33,79, 5,85,64,52,21,4,63,20,15,32,59,36,45,28,61,87,18,3,8,75)(14,31,57)

引理 5.40. *对任意$n = 6t + 5$，$t \in [3, 10] \cup \{12, 14\}$，$A_3(n, 6, 4) = U(n, 3)$。*

证明. 对任意$n = 6t + 5$，从引理5.35–5.38取一个型为$2^{3t}5^1$的$(4, 2)$-CRSSGDD。为了简便，我们把大小为5的组中的点记为$6t$，$6t + 1$，$6t + 2$，$6t + 3$，$6t + 4$。即：当$t = 3$时，我们分别把a_0，b_0，c_0，a_1，a_2用$6t$，$6t + 1$，$6t + 2$，$6t + 3$，$6t + 4$替换；当$t \in [4, 9] \cup \{12\}$时，我们分别把a_0，b_0，c_0，d_0，e_0用$6t$，$6t + 1$，$6t + 2$，$6t + 3$，$6t + 4$替换；当$t \in \{10, 14\}$时，我们分别把∞_1，∞_2，∞_3，∞_4，∞_5用$6t$，$6t + 1$，$6t + 2$，$6t + 3$，$6t + 4$替换。这里，对$t = 9$，我们先需要用映射$(a, b) \mapsto 18 \cdot a + b$作用在第一个GDD的点集上。在大小为5的组上填入一个新的区组$\{6t, 6t + 1, 6t + 2, 6t + 3\}$，从而得到一个在点集$\{0, 1, 2, \ldots, 6t + 4\}$上的指数为1的最优填充。用表5.2中的置换作用在点集上，就得到了第二个最优填充，并且这两个最优填充满足CRSS性质。由引理5.5的证明，我们就得到了相应的最优$(6t + 5, 6, 4)_3$码。 □

引理 5.41. *对任意$u \in \{24, 30, 42\}$，存在一个型为2^u23^1的$(4, 2)$-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{2u} \cup \{\infty_1, \infty_2, \ldots, \infty_5\} \cup M$，组集为$\{\{0, u\} + i : 0 \leq i \leq u-1\} \cup \{\{\infty_1, \infty_2, \ldots, \infty_5\} \cup M\}$。令$2u = 3x$。所需设计的基区组是由两部分组成。第一部分是由引理5.37中的第一部分基区组$+3 \pmod{2u}$展开得到。第二部分是由如下基区组$+1$或$+2 \pmod{2u}$展开得到。

$2^{24}23^1$：$+2 \pmod{48}$；M=$(\{a\} \times \mathbb{Z}_{12}) \cup (\{b\} \times \mathbb{Z}_6)$

第一个GDD的第二部分基区组：

$(0, 41, 3, a_0)$　$(7, 18, 13, a_0)$　$(9, 4, 29, a_0)$　$(14, 6, 36, a_0)$　$(15, 2, 8, a_0)$　$(11, 23, 44, a_0)$
$(22, 43, 34, a_0)$　$(5, 35, 27, b_0)$　$(4, 14, 1, b_0)$　$(8, 12, 31, b_0)$　$(1, 16, 45, a_0)$　$(6, 34, 45, b_0)$

第二个GDD的第二部分基区组：

$(15, 40, 22, a_0)$　$(20, 17, 8, a_0)$　$(6, 44, 2, b_0)$　$(11, 41, 22, b_0)$　$(21, 14, 34, a_0)$　$(18, 43, 47, a_0)$
$(0, 11, 26, a_0)$　$(12, 4, 7, a_0)$　$(1, 29, 37, a_0)$　$(7, 45, 40, b_0)$　$(3, 9, 30, a_0)$　$(0, 13, 39, b_0)$

$2^{30}23^1$：$+1 \pmod{60}$；M=$(\{a\} \times \mathbb{Z}_{15}) \cup (\{b\} \times \mathbb{Z}_3)$

第一个GDD的第二部分基区组：

$(7, 35, 23, a_0)$　$(3, 45, 58, a_0)$　$(1, 5, 12, b_0)$　$(1, 4, 40, a_0)$
$(9, 26, 59, a_0)$　$(2, 27, 36, a_0)$　$(0, 6, 14, 29)$

第二个GDD的第二部分基区组：

$(1, 11, 45, b_0)$　$(5, 19, 48, a_0)$　$(8, 55, 47, a_0)$　$(0, 11, 7, a_0)$
$(9, 42, 14, a_0)$　$(1, 13, 36, a_0)$　$(0, 3, 9, 45)$

$2^{42}23^1$：$+1 \pmod{84}$；M=$(\{a, b, c\} \times \mathbb{Z}_6)$

第一个GDD的第二部分基区组：

$(1, 45, 48, a_0)$　$(2, 10, 23, a_0)$　$(0, 5, 14, b_0)$　$(1, 46, 81, b_0)$　$(0, 10, 33, c_0)$
$(1, 17, 44, c_0)$　$(0, 6, 73, 25)$　$(0, 24, 31, 46)$　$(0, 12, 30, 64)$

第二个GDD的第二部分基区组：

$(0, 3, 7, a_0)$　$(2, 11, 16, a_0)$　$(0, 8, 19, b_0)$　$(3, 41, 16, b_0)$　$(0, 15, 31, c_0)$
$(5, 40, 50, c_0)$　$(0, 6, 54, 33)$　$(0, 12, 34, 52)$　$(0, 17, 37, 60)$

□

引理 5.42. 对任意$t \geq 3$，$t \notin \{16, 20, 22, 29, 32, 40\}$，$A_3(6t+5, 6, 4) = U(6t+5)$。

证明. 对$t \in [3, 10] \cup \{12, 14\}$，所需的$(6t+5, 6, 4)_3$码在引理5.40中构造得到。对其余的$t$，我们构造型为$2^{3s}23^1$，$s \geq 8$，$s \notin \{9, 11, 13, 17, 19, 26, 29, 37\}$的$(4, 2)$-CRSSGDD。

对$s \in \{8, 10, 14\}$，所需设计在引理5.41中构造得到。对$s \in \{12, 15, 18, 21, 24, 27, 30, 33, 36\}$，取型为$6^u$，$5 \leq u \leq 13$的$(4, 2)$-CRSSGDD，并用3膨胀。在组上填入型为$2^9 5^1$的$(4, 2)$-CRSSGDD就得到了型为$2^{9(u-1)}23^1$的$(4, 2)$-CRSSGDD。对$s = 16$，取一个TD$(5, 4)$，用WFC对前4个组的所有点，最后一个组的3个点加权6，其余点加权3。增加2个无穷点并在组上连同无穷点填入型为2^{13}的$(4, 2)$-CRSSGDD就得到所需设计。对$s = 28$，取型为$6^4 3^1$的$\{4\}$-GDD，用WFC加权7，增加2个无穷点并填入型为2^{22}的$(4, 2)$-CRSSGDD就得到所需设计。对$s = 32$，取一个TD$(4, 4)$，用WFC 加权12，增加23个无穷点，并连同无穷点填入型为$2^{24}23^1$的$(4, 2)$-CRSSGDD就得到所需设计。

对$s \in \{20, 22, 23, 25\}$，取一个TD$(6, 5)$，用WFC对前4个组的点，第5个组的x个点，第6个组的2个点加权6，第6个组的其余点加权3。其余点加权0。这里的输入设计是型为6^5，6^6，$6^4 3^1$和$6^5 3^1$的$(4, 2)$-CRSSGDD。增加2个无穷点，并填入型为2^7，2^{10}或2^{16}的$(4, 2)$-CRSSGDD就得到所需设计。令$x = 5$，就得到型为$2^{75}23^1$的$(4, 2)$-CRSSGDD；令$x = 3$，就得到型为$2^{69}23^1$的$(4, 2)$-CRSSGDD；令$x = 2$，就得到型为$2^{66}23^1$的$(4, 2)$-CRSSGDD；令$x = 0$，就得到型为$2^{60}23^1$的$(4, 2)$-CRSSGDD。

对$s \in \{31, 34\}$，取一个TD$(6, 7)$，用WFC对前四个组的所有点，第5个组的x个点加权6，最后一个组的点加权3，其余点加权0。这里的输入设计是型为$6^4 3^1$和$6^5 3^1$的$(4, 2)$-CRSSGDD。增加2个无穷点，在组上连同无穷点填入型为2^{22}或2^{3x+1}的$(4, 2)$-CRSSGDD，就得到所需设计。令$x = 6$，就得到型为$2^{102}23^1$的$(4, 2)$-CRSSGDD；令$x = 3$，就得到型为$2^{93}23^1$的$(4, 2)$-CRSSGDD。

取一个TD$(12, 11)$，用WFC对前5个组的所有点，最后一个组的3个点，剩余的第i个组的x_i个点，$1 \leq i \leq 6$，加权6。其余点加权0。取$x_i = 0$或$3 \leq x_i \leq 11$。增加5个无穷点，在组上连同无穷点填入型为$2^{3u}5^1$，$u \in [3, 11]$的$(4, 2)$-CRSSGDD，就得到型为$2^{5\cdot 33+3\sum x_i}23^1 \equiv 2^{3s}23^1$的$(4, 2)$-CRSSGDD，其中$s = 5\cdot 11 + \sum x_i \in \{55\} \cup [58, 121]$。类似地，如果取TD$(9, 8)$，我们将得到$s \in \{40\} \cup [43, 64]$；如果取TD$(8, 7)$，我们将得到$s \in \{35\} \cup [38, 49]$。

对$s \geq 83$，从引理2.9取一个TD$(7, n)$，用WFC对前5个组的所有点，第6个组的x个点，最后一个组的3个点加权6。其余点都加权0。我们得到了型为$(6n)^5(6x)^1 18^1$，$x = 0$或$3 \leq x \leq n$的$(4, 2)$-CRSSGDD。增加5个无穷点，在前6个组连同无穷点填入型为$2^{3n}5^1$或$2^{3x}5^1$的$(4, 2)$-CRSSGDD，就得到型

为$2^{3(5n+x)}23^1$的$(4,2)$-CRSSGDD，其中$s=5n+x$可以取到不小于83的任何正整数。

由引理5.5，我们就得到了型为$2^{3s}23^1$，$s\geq 8$，$s\notin\{9,11,13,17,19,26,29,37\}$的GDC。在大小为23的组上填入最优$(23,6,4)_3$码就得到了所需的码。　□

引理 5.43. *对任意$t\in\{16,20,22,29,32,40\}$，$A_3(6t+5,6,4)=U(6t+5,3)$。*

证明. 首先，我们构造型为$2^{3s}29^1$，$s\in\{12,16,18,25,28,36\}$的$(4,2)$-CRSSGDD。对$s\in\{12,18\}$，分别取型为$6^49^1$或$6^69^1$的$(4,2)$-CRSSGDD，用3膨胀，得到型为$18^427^1$或$18^627^1$的$(4,2)$-CRSSGDD。增加2个无穷点，在大小为18的组上连同无穷点填入型为2^{10}的$(4,2)$-CRSSGDD得到所需设计。对$s=16$，取一个TD$(5,4)$，用WFC加权6得到型为24^5的$(4,2)$-CRSSGDD。增加5个无穷点，在前4个大小为24的组上连同无穷点填入型为$2^{12}5^1$的$(4,2)$-CRSSGDD得到所需设计。

对$s=25$，取一个TD$(6,5)$，用WFC对前5个组的点，最后一个组的4个点加权6。其余点加权0。得到型为30^524^1的$(4,2)$-CRSSGDD。增加5个无穷点，在大小为30的组连同无穷点填入型为$2^{15}5^1$的$(4,2)$-CRSSGDD得到所需设计。对$s=28$，取型为6^8的$\{4\}$-GDD，用WFC加权4得到型为24^8的$(4,2)$-CRSSGDD。增加5个无穷点，在前7个组连同无穷点填入型为$2^{12}5^1$的$(4,2)$-CRSSGDD得到所需设计。对$s=36$，取一个TD$(7,7)$，去掉一个点得到型为6^67^1的$\{6,7\}$-GDD。用WFC对前6个组的点，最后一个组的4个点加权6，其余点加权0，得到型为36^624^1的$(4,2)$-CRSSGDD。增加5个无穷点，在大小为36的组上连同无穷点填入型为$2^{18}5^1$的$(4,2)$-CRSSGDD得到所需设计。

由引理5.5，我们得到型为$2^{3s}29^1$，$s\in\{12,16,18,25,28,36\}$的GDC。在这些GDC的大小为29的组上填入最优$(29,6,4)_3$码就得到了所需的码。　□

综合上述结果，我们得到：

定理 5.44. *对任意$t\geq 3$，$A_3(6t+5,6,4)=U(6t+5,3)$；$A_3(11,6,4)\geq U(11,3)-1$；$A_3(17,6,4)\geq U(17,3)-2$。*

5.4　结论

在本章中，我们几乎完全确定了最优$(n,6,4)_3$码的码字个数。我们把结果总结如下：

定理 5.45. 对任意整数$n \geq 4$，

$$A_3(n,6,4) = \begin{cases} 1, & \text{当} n \leq 5\text{时} \\ 3, & \text{当} n = 7\text{时} \\ 5, & \text{当} n = 8\text{时} \\ \left\lfloor \frac{n}{2} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor, & \text{当} n \geq 6, \ n \notin \{7,8,11,17\}\text{时} \end{cases}$$

$A_3(11,6,4) \in [15,16]$，$A_3(17,6,4) \in [40,42]$。

注：文[159]中一个审稿人用计算机搜索确定了$A_3(11,6,4) = 15$。

Chapter 6

组大小为四的完全可约超单设计和相关超单填充

6.1 引言和主要结果

完全可约超单（CRSS）设计与q元常重码（CWC）密切相关。一个$(v,4,q)$-CRSS设计就是一个最优$(v,6,4)_{q+1}$码。CRSS可分组设计（CRSSGDD）可以用来构造q元可分组码（GDC），而可分组码在q元CWC的构造中起了重要作用。在第5章中，我们用上述CRSS设计和CWC的联系几乎完全确定了最优$(v,6,4)_3$码的码字个数。然而，虽然对CWC已经有很多人研究过，目前对CRSS设计的结果却不多，如[5]。

在本章中，我们将继续研究区组大小为4的CRSS设计的存在性。首先，我们完全确定了$(v,4,3)$-CRSS设计的存在性。因此，我们也得到了一些新的最优$(v,6,4)_4$码。其次，我们给出了一个用斜Room frame构造$(4,4)$-CRSSGDD的方法，并证明了一个型为g^u的$(4,2)$-CRSSGDD存在的必要条件，除了几组值$(g,u)\in\{(2,4),(3,4),(6,4)\}$外，也是充分的。

超单设计是由Gronau等于1992年提出的[83]。超单设计不但其存在性本身是组合设计理论中一个有趣的研究问题，而且在实际中也有各种重要的应用。例如这种设计可以用来构造完美哈希函数[130]和覆盖设计[13]，一些新的设计[12]，和叠加码[100]等。

目前，关于超单设计的大多数工作都是考虑区组大小为4，指数$\lambda\in\{2,3,4,5,6,9\}$（见文[5, 21, 29–31, 81, 83, 99]），或者区组大小为5，指数$\lambda\in\{2,4,5\}$（见文[1, 2, 34, 35, 82]）的超单BIBD的存在性。然而，对超单填充的存在性，却几乎没有任何结果。然而，从文[159]中可以看出这种设计却与CWC有着密切联系。所以，在本章中，我们将研究最优超单填充的存在性，并且证明对任意$v\geq 4$，除了确定的值$v\in\{4,5,6,9\}$外，最优超单$(v,4,2)$-填充都是存在的。

这一章的结构如下：在第6.2节中，我们将介绍一些基本概念和结果；在第6.3节中，我们将构造$(v,4,3)$-CRSS设计，并得到一类最优$(v,6,4)_3$码；在

第6.4节中，我们将给出一个用斜Room frame构造$(4,4)$-CRSSGDD的方法，并在第6.5节中，证明型为g^u的$(4,2)$-CRSSGDD的存在性；在第6.6节中，我们将解决最优超单$(v,4,2)$-填充的存在性。

6.2 准备知识和基本构造方法

与文[5]中证明类似，我们有如下CRSSGDD存在的必要条件。

引理 6.1. *一个型为g^u的$(4,\lambda)$-CRSSGDD存在的必要条件是：*

(i) $u \geq 4$，

(ii) $(u-1)g \equiv 0 \pmod 3$，

(iii) $u(u-1)g^2 \equiv 0 \pmod{12}$，

(iv) $ug \geq 2\lambda + 2g$，*若*$g \neq 1$。

第四个条件是为了保证所有可能的三元组数大于出现在设计的区组中的三元组数。特别的，当$g = 1$时，我们就得到了$(v,4,\lambda)$-CRSS设计存在的必要条件是$v \equiv 1$或$4 \pmod{12}$，$v \geq 2\lambda + 2$或$v = 1$。

对GDD和PBD的循环构造，通常用的是“加权”构造和Wilson's基本构造法（见[147]），就是通常从一个“主”GDD和一些小的输入设计来得到新的GDD。我们对CRSSGDD的构造也将采用这样的方法。我们从一个CRSSGDD出发，用TD作为输入设计，或者从一个GDD出发，把一些CRSSGDD作为输入设计。具体来说，我们将用到如下两个构造，即：膨胀法和GDD的Wilson's基本构造法（WFC）（见文[41]）。

构造 6.2. （膨胀法） *假设存在一个型为$\{h_1, h_2, \ldots, h_n\}$的$(K,\lambda)$-CRSSGDD，且对任意$k \in K$，存在一个$TD(k,m)$。那么存在一个型为$\{mh_1, mh_2, \ldots, mh_n\}$的$(K,\lambda)$-CRSSGDD。*

构造 6.3. （WFC） *令$(X,\mathcal{G},\mathcal{B})$是一个GDD，令$w : X \to Z^+ \cup \{0\}$是$X$上的加权函数。假设对任意$B \in \mathcal{B}$，都存在一个型为$\{w(x) : x \in B\}$的$(K,\lambda)$-CRSSGDD。那么存在一个型为$\{\sum_{x\in G} w(x) : G \in \mathcal{G}\}$的$(K,\lambda)$-CRSSGDD。*

在GDD和PBD的构造中，“补洞”的方法起着重要作用。

构造 6.4. (补洞)

(i) 假设存在一个型为$\{s_i : 1 \le i \le n\}$的(K,λ)-*CRSSGDD*。令$a \ge 0$为一个整数。如果，对任意$1 \le i \le n-1$，都存在一个型为$\{s_{ij} : 1 \le j \le k_i\} \cup \{a\}$的$(K,\lambda)$-*CRSSGDD*，其中$s_i = \sum_{1\le j\le k_i} s_{ij}$。那么存在一个型为$\{s_{ij} : 1 \le j \le k_i, 1 \le i \le n-1\} \cup \{a+s_n\}$的$(K,\lambda)$-*CRSSGDD*。

(ii) 假设存在一个型为$\{s_i : 1 \le i \le n\}$的(K,λ)-*CRSSGDD*。进一步假设存在一个型为$\{t_j : 1 \le j \le t\}$的(K,λ)-*CRSSGDD*，其中$s_n = \sum_{1\le j\le t} t_j$。那么存在一个型为$\{s_i : 1 \le i \le n-1\} \cup \{t_j : 1 \le j \le t\}$的$(K,\lambda)$-*CRSSGDD*。

一个洞为H的（$|H| = w$）的(v,k,λ)-填充，记为$(v,w;k,\lambda)$-填充，是一个三元组$(X,H,\mathcal{B})$，其中X是一个大小为v的点集，H为它的一个大小为w的子集，称为洞，区组集$\mathcal{B}$是X中一些k元子集的集合，使得不在洞里的任意相异点对最多出现在λ个区组中，且没有区组包含洞中的点对。

一个洞大小为w的(v,k,λ)-最大不完全填充设计（maximum incomplete packing design，MIPD），记为$(v,w;k,\lambda)$-MIPD，就是一个三元组$(X,Y,\mathcal{A})$，其中X是一个v元集合（称为点），$Y \subseteq X$是一个w元集合（称为洞），$\mathcal{A}$是X中的一些k元子集的集合（称为区组），且满足如下条件：

1. 对X中的任意相异点对x、y，如果x和y至少有一个不出现在Y中，那么这个点对最多出现在$\mathcal{A}$的λ个区组中；
2. Y中的点对不出现在任何区组中；
3. $\lambda(v-1) \equiv \lambda(w-1) \equiv d \pmod{k-1}$，其中$d$是满足$0 \le d \le k-2$的一个整数；
4. $(X\times X)\backslash(Y\times Y)$中不出现在$\mathcal{A}$的任何区组中的点对恰好有$d(v-w)/2$个。

MIPD的概念是由Yin和Assaf在文[155]中提出的，他们还给出了一些循环构造方法。

构造 6.5 (Yin，Assaf [155]). 假设存在一个型为$\{t_1,t_2,\ldots,t_n\}$的(k,λ)-*GDD*，且对任意$1 \le i \le n-1$，存在一个$(t_i+w,w;k,\lambda)$-*MIPD*。那么存在一个$(t+w,t_n+w;k,\lambda)$-*MIPD*，其中$t = \sum_{1\le i\le n} t_i$。

构造 6.6 (Yin，Assaf [155]). 假设存在一个$(v,w;k,\lambda)$-*MIPD*。如果$w \leq k-1$，或者存在一个最优(w,k,λ)-填充，那么存在一个(v,k,λ)-填充。

我们把一个超单(v,k,λ)-填充的填充数记为$D'_\lambda(v,k,2)$，显然$D'_\lambda(v,k,2) \leq D_\lambda(v,k,2)$，其中$D_\lambda(v,k,2)$为一个$(v,k,\lambda)$-填充的填充数。

对一个$(v,4,2)$-填充，有如下结果：

引理 6.7 (Assaf [7]，Billington等[11]). 对任意$v \neq 9$，$D_2(v,4,2) = U_2(v,4,2)$；$D_2(9,4) = U_2(9,4,2)\ -1$。

6.3 $(v,4,3)$-CRSS设计的存在性

在本节中，我们将完全确定$(v,4,3)$-CRSS设计的存在性。同时我们也得到了一类新的$(v,6,4)_4$码。

首先，我们将用与文[159]中相同的方法直接构造一些小的设计。当找一个指数为λ的CRSS设计时，我们将分别构造点集和组集相同但是指数为1的设计，使得任意两个区组最多交于两个点，然后再把它们合并起来构成一个指数为λ的CRSS设计。下文中，我们经常用乘子乘以第一个设计的基区组得到第二个或第三个设计的基区组。

引理 6.8. 分别存在型为4^7和12^6的$(4,3)$-*CRSSGDD*。

证明. 对型为4^7的$(4,3)$-CRSSGDD，令点集为$\mathbb{Z}_{28}$，组集为$\{\{0,7,14,21\}+i : 0 \leq i \leq 6\}$。所需设计由如下基区组在$\mathbb{Z}_{28}$中+4 (mod 28)展开得到。第一个GDD的基区组：$\{2,5,10,21\}$，$\{0,2,18,20\}$，$\{0,11,24,27\}$，$\{3,18,22,23\}$，$\{1,3,7,9\}$，$\{0,9,19,22\}$，$\{0,1,12,25\}$，$\{1,2,19,24\}$。第二个GDD的基区组由第一个GDD的基区组乘以乘子5得到。第三个GDD的基区组由第一个GDD的基区组乘以乘子17得到。

对型为12^6的$(4,3)$-CRSSGDD，令点集为$\mathbb{Z}_{72}$，组集为$\{\{0,6,\ldots,66\}+i : 0 \leq i \leq 5\}$。所需设计由如下基区组在$\mathbb{Z}_{72}$中+1 (mod 72)展开得到。第一个GDD的基区组：$\{0,39,55,64\}$，$\{0,15,29,52\}$，$\{0,28,62,69\}$，$\{0,22,26,27\}$，$\{0,2,13,53\}$。第二个GDD的基区组由第一个GDD的基区组乘以乘子11得到。第三个GDD的基区组由第一个GDD的基区组乘以乘子13得到。 □

引理 6.9. 对任意$t \geq 4$，存在一个型为12^t的$(4,3)$-*CRSSGDD*。

证明. 当$t \equiv 0$或1 (mod 4)，$t \geq 4$时，由引理2.7，存在一个$(3t+1, \{4\}, 1)$-PBD。从这个PBD的点集去掉一个点，得到一个型为3^t的$\{4\}$-GDD。当$t \equiv 2$或3 (mod 4)，$t \geq 7$时，由引理2.7，存在一个$(3t+1, \{4, 7^\star\}, 1)$-PBD。从这个PBD的点集去掉一个不在大小为7的区组中的点，得到型为3^t的$\{4, 7^\star\}$-GDD。因此，对任意$t \geq 4$，$t \neq 6$，我们都有型为3^t的$\{4, 7\}$-GDD。

对这个GDD用WFC加权4得到型为12^t的$(4, 3)$-CRSSGDD，其中$t \geq 4$，$t \neq 6$。这里的输入设计是型为4^4和4^7的$(4, 3)$-CRSSGDD（引理5.4和6.8）。对$t = 6$，所需设计由引理6.8直接构造得到。 □

引理 6.10. *对任意$v \in \{25, 28, 37, 40\}$，存在一个$(v, 4, 3)$-CRSS设计。*

证明. 对$v = 25$，令点集为$GF(25)$。令本元多项式为$f(x) = x^2 + x + 2$。第一个BIBD的区组是在由基区组$\{0, 1, x^8, x^{16}\}$，$\{0, x^2, x^{10}, x^{18}\}$在$GF(25)$中的加法群展开得到。第二个BIBD的基区组由第一个BIBD的基区组乘以乘子x展开得到。第三个BIBD的基区组由第一个BIBD的基区组乘以乘子x^4展开得到。

对$v = 28$，令点集为$\mathbb{Z}_{28}$。所需设计由如下基区组在$\mathbb{Z}_{28}$中+4 (mod 28)展开得到。第一个BIBD的基区组：$\{2, 3, 11, 14\}$，$\{3, 13, 25, 27\}$，$\{1, 11, 24, 26\}$，$\{0, 3, 9, 10\}$，$\{2, 7, 8, 9\}$，$\{0, 6, 14, 16\}$，$\{1, 9, 14, 18\}$，$\{3, 8, 12, 19\}$，$\{1, 5, 8, 16\}$。第二个BIBD的基区组由第一个BIBD的基区组乘以乘子5展开得到。第三个BIBD的基区组由第一个BIBD的基区组乘以乘子17展开得到。

对$v = 37$，令点集为$\mathbb{Z}_{37}$。所需设计由如下基区组在$\mathbb{Z}_{37}$中+1 (mod 37)展开得到。第一个BIBD的基区组：$\{0, 1, 3, 24\}$，$\{0, 4, 9, 15\}$，$\{0, 7, 17, 25\}$。第二个BIBD的基区组由第一个BIBD的基区组乘以乘子6展开得到。第三个BIBD的基区组由第一个BIBD的基区组乘以乘子31展开得到。

对$v = 40$，令点集为$\mathbb{Z}_{39} \cup \{\infty\}$。所需设计由如下基区组+3 (mod 39)得到，其中，∞在自同构作用下保持不动。

第一个BIBD的基区组：

$$\begin{array}{ccccc} \{1, 5, 24, 34\} & \{1, 14, 18, 31\} & \{1, 4, 20, 25\} & \{1, 9, 28, 33\} & \{0, 1, 3, 12\} \\ \{0, 4, 29, \infty\} & \{0, 11, 33, 38\} & \{2, 9, 23, 34\} & \{0, 2, 18, 26\} & \{2, 4, 5, 35\} \end{array}$$

第二个BIBD的基区组：

$$\begin{array}{ccccc} \{0, 7, 8, 11\} & \{0, 34, 2, \infty\} & \{1, 21, 7, 20\} & \{2, 27, 32, 12\} & \{1, 37, 10, 35\} \\ \{0, 22, 4, 33\} & \{2, 10, 9, 26\} & \{1, 27, 25, 9\} & \{1, 11, 23, 29\} & \{0, 27, 23, 36\} \end{array}$$

第三个BIBD的基区组由第一个BIBD的基区组乘以乘子5展开得到。 □

定理 6.11. 对任意$v \equiv 1, 4 \pmod{12}$，$v \geq 13$，存在一个$(v, 4, 3)$-*CRSS*设计。

证明. 对$v \in \{13, 16\}$，所需设计在文[5]中给出。对$v \in \{25, 28, 37, 40\}$，所需设计在引理6.10中构造得到。

对任意$v \geq 49$，从引理6.9取一个型为12^t的$(4, 3)$-CRSSGDD。如果增加一个点，并在组上连同无穷点填入$(13, 4, 3)$-CRSS设计，我们就对任意$t \geq 4$得到了$(12t + 1, 4, 3)$-CRSS设计。如果增加4个无穷点，并在一个组上连同无穷点填入$(16, 4, 3)$-CRSS设计，其它组上连同无穷点填入型为$1^{12}4^1$的$(4, 3)$-CRSSGDD（见文[5]），我们就对任意$t \geq 4$得到了$(12t + 4, 4, 3)$-CRSS设计。 □

由引理5.5，我们得到了一类新的最优$(v, 6, 4)_4$码，即：

推论 6.12. 对任意$v \equiv 1, 4 \pmod{12}$，$v \geq 13$，$A_4(v, 6, 4) = \frac{v(v-1)}{4}$。

6.4 用斜Room frame构造$(4, 4)$-CRSSGDD

在本节中，我们将给出一个用斜Room frame构造$(4, 4)$-CRSSGDD的方法。

令$\{S_1, \ldots, S_n\}$是集合S的划分，一个$\{S_1, \ldots, S_n\}$-*Room frame*就是一个用S中的元素标记的$|S| \times |S|$阵列F，满足：

1. F中的每个单元或者为空，或者包含S中的一个无序点对，

2. 对任意$1 \leq i \leq n$，子阵列$S_i \times S_i$是空的，（这些子阵列称为洞），

3. 任意$x \notin S_i$恰好包含在第s行（列），$s \in S_i$恰好一次，

4. F中的点对是$\{s, t\}$，其中$(s, t) \in (S \times S) \setminus \bigcup_{i=1}^{n}(S_i \times S_i)$。

一个$\{S_1, \ldots, S_n\}$-Room frame F的型是一个多重集$\{|S_1|, \ldots, |S_n|\}$。如果对$1 \leq j \leq k$，有u_j个S_i的大小为t_j，我们说F的型为$t_1^{u_1} \ldots t_k^{u_k}$。一个Room frame是斜的如果单元$(i, j)$非空，那么单元$(j, i)$一定是空的。型为$1^n$的Room frame也称为*Room*方。

斜Room frame对构造区组大小为4的BIBD和GDD，解决弱3-着色BIBD的存在性问题都起到了重要作用（见文[119]和[120]）。

从一个型为t^u的斜Room frame F，我们可以得到一个型为$(6t)^u$的$\{4\}$-GDD（见文[119]）。其中，这个$\{4\}$-GDD的点集为$\{S_i \times \mathbb{Z}_6 : 1 \le i \le n\}$，区组集$\mathcal{B}$包含所有的区组$\{(a,j),(b,j),(c,1+j),(r,4+j)\}$，其中$j \in \mathbb{Z}_6$，$\{a,b\}$是在$F$的第$c$列第$r$行的元素。

引理 6.13 (Chen，Zhu[36]，Zhang，Ge[163]). *一个型为t^u的斜Room frame存在的必要条件，即：$u \ge 4$，$t(u-1)$是偶数，除了确定的值$(t,u) \in \{(1,5),(2,4)\}$和如下不确定的值以外，也是充分的：*

(i) $u = 4$，$t \equiv 2 \pmod 4$，

(ii) $u = 5$，$t \in \{17,19,23,29,31\}$。

构造 6.14. *若存在一个型为t^u的斜Room frame，则存在一个型为$(6t)^u$的$(4,4)$-CRSSGDD。*

证明. 令F是给定的型为t^u的斜Room frame。我们构造四个型为$(6t)^u$的$(4,1)$-GDD，其中点集为$\{\{(i+k,j) : 0 \le i \le t-1, j \in \mathbb{Z}_6\} : k = 0,t,\ldots,t(u-1)\}$，四个不同的设计分别包含区组$\{(x,j),(y,j),(c,1+j),(r,4+j)\}$，$\{(x,j),(y,j),(c,4+j),(r,1+j)\}$，$\{(x,j),(y,j),(c,2+j),(r,5+j)\}$，$\{(x,j),(y,j),(c,5+j),(r,2+j)\}$其中$j \in \mathbb{Z}_6$，$\{x,y\} \in F$，$\{x,y\}$是$F$的第$c$列第$r$行的元素。很容易验证这样就得到了四个型为$(6t)^u$的$\{4\}$-GDD，并且任意两个区组最多交于两个点。　□

结合引理6.13和构造6.14，我们有如下结果：

定理 6.15. *若$u \ge 4$，$t(u-1)$是偶数，除了$(t,u) \in \{(1,5),(2,4)\}$和如下的$(t,u)$外，存在一个型为$(6t)^u$的$(4,4)$-CRSSGDD：*

(i) $u = 4$，$t \equiv 2 \pmod 4$，

(ii) $u = 5$，$t \in \{17,19,23,29,31\}$。

令$t = 1$，我们就得到了如下结果：

推论 6.16. *若u是奇数，且$u \ge 7$，则存在一个型为6^u的$(4,4)$-CRSSGDD。*

6.5 型为g^u的$(4,2)$-CRSSGDD的存在性

在本节中，我们将证明型为g^u的$(4,2)$-CRSSGDD存在的必要条件，除了确定的值$(g,u)\in\{(2,4),(3,4),(6,4)\}$以外也是充分的。

我们在表6.1中分类列出引理6.1中型为g^u的$(4,2)$-CRSSGDD存在的必要条件。

表 6.1: 型为g^u的$(4,2)$-CRSSGDD存在的必要条件

g	u
$g\equiv 0 \pmod{12}$	$u\geq 4$，$u\in\mathbb{N}$
$g\equiv 1,5,7,11 \pmod{12}$	$u\geq 4$，$u\equiv 1,4 \pmod{12}$，$(g,u)\neq(1,4)$
$g\equiv 2,10 \pmod{12}$	$u\geq 4$，$u\equiv 1 \pmod 3$
$g\equiv 3,9 \pmod{12}$	$u\geq 4$，$u\equiv 0,1 \pmod 4$
$g\equiv 4,8 \pmod{12}$	$u\geq 4$，$u\equiv 1 \pmod 3$
$g\equiv 6 \pmod{12}$	$u\geq 4$，$u\in\mathbb{N}$

由膨胀法和引理5.2，引理6.9中的已知结果，我们只需要考虑当$g\in\{2,3,4,6\}$时型为g^u的$(4,2)$-CRSSGDD的存在性。

a. 型为6^u的$(4,2)$-CRSSGDD

引理 6.17. *对任意$u\in\{14,18\}$，存在一个型为6^u的$(4,2)$-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{6u}$，组集为$\{\{0,u,2u,\ldots,5u\}+i:0\leq i\leq u-1\}$。所需设计由如下基区组在$\mathbb{Z}_{6u}$中$+2 \pmod{6u}$展开得到。

$u=14$：

第一个GDD的基区组：

$\{1,10,11,18\}$ $\{1,21,32,69\}$ $\{0,9,12,27\}$ $\{0,18,38,59\}$ $\{0,22,45,47\}$ $\{0,2,7,51\}$
$\{0,26,55,61\}$ $\{0,48,79,80\}$ $\{0,6,50,74\}$ $\{1,14,53,77\}$ $\{0,13,17,43\}$ $\{0,3,54,65\}$
$\{0,19,57,69\}$

第二个GDD的基区组由第一个GDD的基区组乘以乘子25得到。

$u=18$：

第一个GDD的基区组：

$\{1,2,64,75\}$ $\{1,22,48,51\}$ $\{1,5,33,100\}$ $\{1,18,32,38\}$ $\{0,15,22,38\}$ $\{0,23,75,105\}$
$\{1,3,23,52\}$ $\{0,24,51,63\}$ $\{0,28,60,93\}$ $\{0,34,69,83\}$ $\{0,37,53,64\}$ $\{0,42,98,100\}$
$\{0,7,55,96\}$ $\{1,41,47,85\}$ $\{0,21,31,40\}$ $\{0,1,43,104\}$ $\{0,17,25,30\}$

第二个GDD的基区组由第一个GDD的基区组乘以乘子5得到。 □

定理 6.18. *对任意$u \geq 5$，存在一个型为6^u的$(4,2)$-CRSSGDD。*

证明. 对$u \in [5,13]$，所需设计在文[159, 引理3.3]中已给出。对$u \in \{14,18\}$，所需设计由引理6.17得到。对$u \in \{15,17,19,23,27,29,33\}$，所需设计由推论6.16得到。

对$u \in \{16,22,28,34\}$，所需设计由对型为2^u，$u \in \{16,22,28,34\}$的$(4,2)$-CRSSGDD用3膨胀得到。对$u \in \{20,24,32\}$，分别取型为30^4（定理6.30），36^4或48^4（引理5.4）的$(4,2)$-CRSSGDD，并在组上分别填入型为6^5，6^6或6^8的$(4,2)$-CRSSGDD，就得到了所需设计。对任意$u \in \{21,25,26,30,31\}$或$u \geq 35$，从引理2.4取一个$(u,\{5,6,7,8,9\},1)$-PBD。用WFC加权6并填入型为6^s，$s \in \{5,6,7,8,9\}$ 的$(4,2)$-CRSSGDD就得到了所需设计。 □

b. 型为4^u的$(4,2)$-CRSSGDD

引理 6.19. *存在一个型为4^{10}的$(4,2)$-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{40}$，组集为$\{\{0,10,20,30\}+i : 0 \leq i \leq 9\}$。第一个GDD是由基区组$\{0,1,4,13\}$，$\{0,2,7,24\}$，$\{0,6,14,25\}$在$\mathbb{Z}_{40}$中$+1 \pmod{40}$展开得到。第二个GDD的基区组由第一个GDD的基区组乘以乘子7得到。 □

定理 6.20. *对所有$u \equiv 1 \pmod 3$，$u \geq 4$，存在型为4^u的$(4,2)$-CRSSGDD。*

证明. 对$u \in \{4,7,10\}$，所需设计由引理5.4，6.8和6.19得到。对任意$u \geq 13$，在引理6.9中取型为12^t，$t \geq 4$的$(4,2)$-CRSSGDD，增加一个无穷点，并在组上连同无穷点填入型为4^4的$(4,2)$-CRSSGDD就得到了型为4^{3t+1}，$t \geq 4$的$(4,2)$-CRSSGDD。 □

c. 型为3^u的$(4,2)$-CRSSGDD

引理 6.21. *对任意$u \in \{9,13\}$，存在一个型为3^u的$(4,2)$-CRSSGDD。*

证明. 对$u=9$，令点集为$\mathbb{Z}_{27}$，组集为$\{\{0,9,18\}+i : 0 \leq i \leq 8\}$。所需设计由如下基区组在$\mathbb{Z}_{27}$中$+9 \pmod{27}$展开得到。

第一个GDD的基区组：

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

第二个GDD的基区组由第一个GDD的基区组乘以乘子10得到。

对$u=13$，令点集为$\mathbb{Z}_{39}$，组集为$\{\{0,13,26\}+i:0\le i\le 12\}$。所需设计由如下基区组在$\mathbb{Z}_{39}$中+1 (mod 39)展开得到。第一个GDD的基区组$\{0,1,6,31\}$，$\{0,2,12,23\}$，$\{0,3,7,22\}$。第二个GDD的基区组由第一个GDD的基区组乘以乘子14得到。□

引理 6.22. *对所有$u\equiv 1 \pmod 4$，$u\ge 5$，存在型为3^u的$(4,2)$-CRSSGDD。*

证明. 对$u=5$，所需设计在文[5]中给出。对$u\in\{9,13\}$，所需设计在引理6.21中构造得到。对任意$u\ge 17$，从引理6.9中取型为12^t，$t\ge 4$的$(4,2)$-CRSSGDD，增加3个点，并在组上连同无穷点填入型为3^5的$(4,2)$-CRSSGDD，就得到了型为3^{4t+1}，$t\ge 4$的$(4,2)$-CRSSGDD。□

引理 6.23. *对任意$u\in\{8,12,16,24,28\}$，存在一个型为3^u的$(4,2)$-CRSSGDD。*

证明. 对任意给定的u，令点集为$\mathbb{Z}_{3(u-1)}\cup(\{a\}\times\mathbb{Z}_3)$，组集为$\{\{0,u-1,2u-2\}+i:0\le i\le u-2\}\cup\{\{a\}\times\mathbb{Z}_3\}$。所需设计由[160, 表 2]中的基区组在$\mathbb{Z}_{3(u-1)}$中+1 (mod $3(u-1)$)展开得到。其中，元素$x_0\in\{x\}\times\mathbb{Z}_n$的下标是在$\mathbb{Z}_{3(u-1)}$的唯一的$n$阶子群展开。□

引理 6.24. *不存在型为3^4的$(4,2)$-CRSSGDD。*

证明. 假设存在这样的设计。令组为$\{\{0,4,8\},\{1,5,9\},\{2,6,10\},\{3,7,11\}\}$，$\mathcal{B}_1$为第一个GDD的9个区组构成的集合，$\mathcal{B}_2$为第二个GDD的9个区组构成的集合。记第一个GDD中包含x的区组形成三元组集$F_x=\{\{a,b,c\}|\{a,b,c,x\}\in\mathcal{B}_1\}$，第二个GDD中包含$x$的区组形成三元组集$S_x=\{\{a,b,c\}|\{a,b,c,x\}\in\mathcal{B}_2\}$。不失一般性，我们假设$F_0=\{\{1,2,3\},\{5,6,7\},\{9,10,11\}\}$。因为任意两个区组最多交于两个点，$S_0$一定是$\{\{1,6,11\},\{2,7,9\},\{3,5,10\}\}$或者$\{\{1,7,10\},\{2,5,11\},\{3,6,9\}\}$。任何一种情况中，都容易看出没有办法去构造$S_1$的剩余区组。□

引理 6.25. *对所有$u\equiv 0 \pmod 4$，$u\ge 8$，存在型为3^u的$(4,2)$-CRSSGDD。*

证明. 对$u\in\{8,12,16,24,28\}$，所需设计在引理6.23中给出。对$u\in\{20,32,36\}$，对型为s^4，$s\in\{5,8,9\}$（引理5.4）的$(4,2)$-CRSSGDD用3膨胀，并在组上填入型为3^s的$(4,2)$-CRSSGDD得到所需设计。

对任意$u \equiv 0 \pmod 8$，$u \geq 40$，从引理2.8取型为6^t，$t \geq 5$的$\{4\}$-GDD。把这个GDD用WFC加权4得到型为24^t的$(4,2)$-CRSSGDD，再在组上填入型为3^8的$(4,2)$-CRSSGDD就得到了型为3^{8t}，$t \geq 5$的$(4,2)$-CRSSGDD。对任意$u \equiv 4 \pmod 8$，$u \geq 44$，取型为6^t9^1，$t \geq 4$的$\{4\}$-GDD（见[77, 定理1.6]）。把这个GDD用WFC加权4，得到型为24^t36^1的$(4,2)$-CRSSGDD，再在大小为24的组上填入型为3^8的$(4,2)$-CRSSGDD，在大小为36的组上填入型为3^{12}的$(4,2)$-CRSSGDD，就得到了型为3^{8t+12}，$t \geq 4$的$(4,2)$-CRSSGDD。 □

d. 型为g^4，$g \equiv 2 \pmod 4$的$(4,2)$-CRSSGDD

一个组大小为n，区组大小为k，指数为λ，洞大小为$h_1,\ldots,h_s$的不完全横截设计，记为$\mathrm{ITD}_\lambda(k,n;h_1,\ldots,h_s)$（或$\mathrm{TD}_\lambda(k,n)-\sum_{1\leq i\leq s}\mathrm{TD}_\lambda(k,h_i)$），是一个四元组$(X,\mathcal{G},\mathcal{H},\mathcal{B})$，其中

1. X是kn个元素的集合；
2. $\mathcal{G}$把X划分k个部分（组），每个大小为n；
3. $\mathcal{H}=\{H_1,\ldots,H_s\}$是$X$的一些不相交的子集，称为洞，且对任意$1\leq i\leq s$和任意$G\in\mathcal{G}$，$|G\cap H_i|=h_i$；
4. $\mathcal{B}$是X中的一些k元子集的集合（区组），使得不在同一个组和同一个洞里的任意点对都恰好出现在λ个区组中；
5. 包含在同一个组或者同一个洞里的任意点对都不包含在任何区组中。

当$\lambda=1$时，我们可以将下标省略。

如下构造是Wilson关于MOLS的构造法的基本形式（见[40]）。很容易验证如果输入设计具有CRSS性质，那么由构造6.26得到的设计也具有CRSS性质。

构造 6.26. 假设存在一个$\mathrm{TD}_\mu(k+l,t)$ $(X,\mathcal{G},\mathcal{B})$，且对任意$B\in\mathcal{B}$，都存在一个$\mathrm{TD}_\lambda(k,m+\sum_{1\leq i\leq l}w_i^B)-\sum_{1\leq i\leq l}\mathrm{TD}_\lambda(k,w_i^B)$。那么存在一个$\mathrm{TD}_{\lambda\mu}(k,mt+\sum_{1\leq i\leq l}\sum_{1\leq j\leq t}w_{ij})-\sum_{1\leq i\leq l}\mathrm{TD}_{\lambda\mu}(k,\sum_{1\leq j\leq t}w_{ij})$。

首先，我们直接构造一些小的设计。我们将用不同的方法来构造MOLS（见[41]），然后用MOLS和TD之间的联系来构造TD（或ITD）。当我们有了第

一个TD （或ITD），第二个可以用适当的置换作用在第一个的点集上得到。对一个矩阵M，令$M(i,j)$表示M的第i行第j列的值。

引理 6.27. *对任意$g \in \{10,18,22,26\}$，存在一个型为g^4的$(4,2)$-CRSSGDD。*

证明. 对$g=10$，取[109, 注 35.19]中的两个MOLS(10)如下：

0	4	7	6	2	1	9	8	3	5
2	1	5	0	8	9	4	3	6	7
3	5	2	8	7	6	0	1	9	4
1	6	9	3	5	7	8	2	4	0
7	8	1	2	4	3	5	9	0	6
8	7	4	9	6	5	1	0	2	3
5	9	0	1	3	8	6	4	7	2
9	2	6	5	0	4	3	7	1	8
6	0	3	4	9	2	7	5	8	1
4	3	8	7	1	0	2	6	5	9

0	8	6	1	7	9	2	5	4	3
3	1	4	6	9	0	5	2	7	8
1	7	2	4	0	8	9	3	5	6
2	9	8	3	6	4	7	1	0	5
9	0	5	8	4	7	1	6	3	2
6	2	1	7	3	5	4	8	9	0
8	3	7	0	5	2	6	9	1	4
4	5	0	9	2	3	8	7	6	1
5	4	9	2	1	6	3	0	8	7
7	6	3	5	8	1	0	4	2	9

我们用L_1和L_2来分别表示上述两个MOLS(10)，并分别用置换$p_1 = (0\ 1\ 2\ 6)(3\ 9\ 8\ 4)(5\ 7)$和$p_2 = (0\ 1\ 7\ 8\ 5\ 6\ 2\ 4\ 3\ 9)$作用在点集上得到了两个新的MOLS(10)，$L_3$和$L_4$。我们用这两个MOLS(10)来构造两个具有超单性质的TD$(4,10)$，其中：点集为$\{\{(0,i),(1,i),\ldots,(9,i)\} : 0 \le i \le 3\}$，区组集分别为$\{\{(i,0),(j,1),(L_1(i,j),2),(L_2(i,j),3)\} : 0 \le i,j \le 9\}$和$\{\{(i,0),(j,1),(L_3(i,j),2),(L_4(i,j),3)\} : 0 \le i,j \le 9\}$。

对$g=18$，取[3, 定理 3.48]中的矩阵如下：

$$\left(\begin{array}{cc|cccccccccc} 0 & 0 & 10 & 1 & 8 & 5 & 7 & 0 & 4 & 6 & 13 \\ 7 & 1 & 2 & 3 & 11 & 9 & 12 & - & - & - & - \\ \hline 1 & 7 & 12 & 0 & 6 & 2 & 3 & 8 & 9 & 10 & 5 \\ 8 & 4 & 11 & - & - & - & - & 13 & 7 & 4 & 1 \end{array}\right)$$

对每一列$(a,b,c,d)^T$，除了第一列以外，分别用列$(a,b,c,d)^T$和$(b,a,d,c)^T$替换得到两列，并增加列$(0,0,0,0)^T$得到一个新的矩阵M。把M中每行的符号“–”分别用“$\infty_0,\infty_1,\infty_2,\infty_3$”替换。再把$M$的列$(+1 \pmod{14},-)$展开就得到了一个ITD$(4,18;4)$，其中组集为$\{\{(0,i),(1,i),\ldots,(13,i),(\infty_0,i),\ldots,(\infty_3,i)\} : 0 \le i \le 3\}$，洞为$\{\{(\infty_0,i),(\infty_1,i),(\infty_2,i),(\infty_3,i)\} : 0 \le i \le 3\}$，基区组为$\{\{(M(0,j),0),(M(1,j),1),(M(2,j),2),(M(3,j),3)\} : 0 \le j \le 21\}$。在同样的组集和洞下构造第二个ITD$(4,18;4)$，基区组为$\{\{(M(0,j)+1,0),(M(1,j)+1,1),(M(2,j)+2,2),(M(3,j)+2,3)\} : 0 \le j \le 21\}$，其中若$M(i,j) \in \mathbb{Z}_{14}$，

$M(i,j)+a = M(i,j)+a \pmod{14}$（$i \in \{2,3\}$）；否则若$M(i,j) = \infty_k$，$k \in \mathbb{Z}_4$，$M(i,j) + a = \infty_{k+a}$（$i \in \{2,3\}$）。最后，对得到的两个ITD分别填入两个具有超单性质的TD$(4,4)$（见引理5.4）就得到了一个型为18^4的超单$(4,2)$-CRSSGDD。

对$g = 22$，取[4, 推论 3.9]中的矩阵如下：

$$\begin{pmatrix} - & 0 & 0 & 0 & 0 & - & 0 & 0 & 0 & 0 & 0 \\ 0 & - & 2 & 3 & 4 & 1 & - & 5 & 6 & 7 & 8 \\ 2 & 2 & - & 6 & 8 & 9 & 7 & - & 12 & 14 & 13 \\ 5 & 6 & 9 & - & 10 & 16 & 2 & 13 & - & 3 & 5 \\ 13 & 12 & 13 & 11 & - & 13 & 9 & 15 & 3 & - & 10 \end{pmatrix}$$

把每一列$(a,b,c,d,e)^T$分别用列$(a,b,c,d,e)^T$和$(-a,-b,-c,-d,-e)^T$在$\mathbb{Z}_{17}$替换得到两列，这样得到一个新的矩阵M。把M的每一行的符号“$-$”分别用“$\infty_0,\infty_1,\infty_2,\infty_3$”替换。再把如下矩阵$B$与矩阵$M$合并，就得了一个新的有27列的矩阵$M'$。

$$B = \begin{pmatrix} \infty_4 & 0 & 1 & 1 & 0 \\ 0 & \infty_4 & 0 & 1 & 1 \\ 1 & 0 & \infty_4 & 0 & 1 \\ 1 & 1 & 0 & \infty_4 & 0 \\ 0 & 1 & 1 & 0 & \infty_4 \end{pmatrix}$$

取M'的前四行，把M'的每一列$(+1 \pmod{17}, -)$展开得到一个ITD$(4, 22; 5)$，其中组集为$\{\{(0,i),(1,i),\ldots,(16,i),(\infty_0,i),(\infty_1,i),(\infty_2,i),\ldots,(\infty_4,i)\} : 0 \le i \le 3\}$，洞为$\{\{(\infty_0,i),(\infty_1,i),(\infty_2,i),(\infty_3,i),(\infty_4,i)\} : 0 \le i \le 3\}$，基区组为$\{\{(M'(0,j),0),(M'(1,j),1),(M'(2,j),2),(M'(3,j),3)\} : 0 \le j \le 26\}$。在同样的组集和洞上构造第二个ITD$(4, 22; 5)$，基区组为$\{\{(M'(0,j),0),(M'(1,j),1),(M'(2,j)+1,2),(M'(3,j)+3,3)\} : 0 \le j \le 26\}$，其中若$M'(i,j) \in \mathbb{Z}_{17}$，$M'(i,j)+a = M'(i,j)+a \pmod{17}$（$i \in \{2,3\}$）；否则若$M(i,j) = \infty_k$，$k \in \mathbb{Z}_5$，$M'(i,j) + a = \infty_{k+a}$（$i \in \{2,3\}$）。最后在得到的两个ITD中分别填入两个具有超单性质的TD$(4,5)$（见5.4）就得到了型为22^4的$(4,2)$-CRSSGDD。

对$g = 26$，取[3, 定理 3.53]中的矩阵如下：

$$\begin{pmatrix} - & - & - & - & - \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 6 & 7 & 8 & 14 \\ 3 & 11 & 20 & 18 & 10 \\ 6 & 10 & 14 & 1 & 5 \\ 4 & 19 & 5 & 12 & 2 \end{pmatrix}$$

把每一列用把此列做列循环得到的六列替换，并增加列$(0,0,0,0,0,0)^T$得到一个新的矩阵M。把M的每行中的符号"$-$"分别用"$\infty_0,\infty_1,\infty_2,\infty_3,\infty_4$"替换。取前四行，把$M$的每列$(+1 \pmod{21},-)$展开得到一个ITD$(4,26;5)$，其中组集为$\{\{(0,i),(1,i),\ldots,(20,i),(\infty_0,i),(\infty_1,i),(\infty_2,i),(\infty_3,i),(\infty_4,i)\}:0\le i\le 3\}$，洞为$\{\{(\infty_0,i),(\infty_1,i),(\infty_2,i),(\infty_3,i),(\infty_4,i)\}:0\le i\le 3\}$，基区组为$\{\{(M(0,j),0),(M(1,j),1),(M(2,j),2),(M(3,j),3)\}:0\le j\le 30\}$。在同样的组集和洞上构造第二个ITD$(4,26;5)$，基区组为$\{\{(M(0,j),0),(M(1,j),1),(M(2,j)+1,2),(M(3,j)+8,3)\}:0\le j\le 30\}$，其中若$M(i,j)\in\mathbb{Z}_{21}$，$M(i,j)+a=M(i,j)+a \pmod{21}$（$i\in\{2,3\}$）；否则若$M(i,j)=\infty_k$，$k\in\mathbb{Z}_5$，$M(i,j)+a=\infty_{k+a}$（$i\in\{2,3\}$）。最后在得到的两个ITD中分别填入具有超单性质的两个TD$(4,5)$（引理5.4）就得到了型为26^4的$(4,2)$-CRSSGDD。 □

引理 6.28. *分别存在一个*CRSSITD$_2(4,6;2)$*和一个*CRSSITD$_2(4,14;4)$。

证明. 对CRSSITD$_2(4,6;2)$，令点集为$\{0,1,\ldots,23\}$，组集为$\{\{0,4,\ldots,20\}+i:0\le i\le 3\}$，洞为$\{16,17,\ldots,23\}$。所需的区组如下：

第一个ITD的区组：

$\{0,11,22,5\}$ $\{10,9,19,12\}$ $\{17,7,2,12\}$ $\{1,2,11,16\}$ $\{16,9,6,3\}$ $\{23,0,9,2\}$
$\{19,8,13,2\}$ $\{13,22,12,3\}$ $\{6,17,0,15\}$ $\{16,14,5,7\}$ $\{7,22,4,9\}$ $\{8,7,6,21\}$
$\{13,7,18,0\}$ $\{13,23,14,4\}$ $\{1,15,22,8\}$ $\{8,23,5,10\}$ $\{5,2,3,20\}$ $\{13,6,11,20\}$
$\{14,17,8,3\}$ $\{12,5,18,15\}$ $\{9,11,8,18\}$ $\{1,23,12,6\}$ $\{5,19,6,4\}$ $\{10,16,13,15\}$
$\{0,14,1,19\}$ $\{15,9,20,14\}$ $\{20,1,7,10\}$ $\{21,0,3,10\}$ $\{1,4,3,18\}$ $\{11,14,12,21\}$
$\{2,4,15,21\}$ $\{4,10,11,17\}$

第二个ITD的区组：

$\{19,9,8,6\}$ $\{12,1,7,22\}$ $\{4,17,14,15\}$ $\{6,3,21,4\}$ $\{10,19,13,0\}$ $\{10,16,1,3\}$
$\{17,3,0,2\}$ $\{6,1,15,20\}$ $\{11,6,17,12\}$ $\{3,8,5,22\}$ $\{14,3,13,20\}$ $\{12,9,3,18\}$
$\{2,19,1,4\}$ $\{0,9,15,22\}$ $\{4,11,13,22\}$ $\{5,23,0,6\}$ $\{9,14,11,16\}$ $\{1,14,8,23\}$
$\{23,4,10,9\}$ $\{15,5,16,2\}$ $\{10,20,5,11\}$ $\{9,2,7,20\}$ $\{23,2,13,12\}$ $\{13,7,16,6\}$
$\{11,2,21,8\}$ $\{8,7,17,10\}$ $\{19,14,5,12\}$ $\{4,5,7,18\}$ $\{8,13,15,18\}$ $\{21,12,10,15\}$
$\{11,18,0,1\}$ $\{7,21,14,0\}$

对CRSSITD$_2(4,14;4)$，令点集为$\{0,1,\ldots,55\}$，组集为$\{\{0,4,\ldots,52\}+i:0\le i\le 3\}$，洞为$\{40,41,\ldots,55\}$。所需区组由如下基区组通过自同构群$G=\langle(0\ 4\ \ldots\ 36)(1\ 5\ \ldots\ 37)(2\ 6\ \ldots\ 38)(3\ 7\ \ldots\ 39)(40)(41)(42)(43)(44)(45)(46)(47)(48)(49)(50)(51)(52)(53)(54)(55)\rangle$展开得到。

第一个ITD的基区组：

$\{1,34,47,12\}$ $\{2,41,4,31\}$ $\{2,19,13,48\}$ $\{1,50,15,24\}$ $\{1,35,28,46\}$ $\{1,2,3,0\}$
$\{1,32,22,55\}$ $\{2,5,24,23\}$ $\{0,45,14,11\}$ $\{2,29,40,15\}$ $\{2,35,49,16\}$ $\{1,39,42,4\}$
$\{1,16,51,10\}$ $\{1,36,43,6\}$ $\{2,17,27,52\}$ $\{2,11,36,53\}$ $\{1,18,23,44\}$ $\{1,8,54,31\}$

第二个ITD的基区组：

$\{0,15,29,54\}$ $\{47,8,29,18\}$ $\{28,50,37,7\}$ $\{37,55,36,30\}$ $\{31,1,6,40\}$ $\{52,7,5,2\}$
$\{38,7,45,20\}$ $\{0,11,13,22\}$ $\{36,19,49,2\}$ $\{31,13,28,46\}$ $\{27,48,6,5\}$ $\{39,41,8,38\}$
$\{29,43,32,6\}$ $\{29,2,44,35\}$ $\{29,3,42,36\}$ $\{29,14,51,12\}$ $\{0,5,26,39\}$ $\{27,30,53,32\}$

□

引理 6.29. *存在一个型为*$4^6 10^1$*的*$(4,2)$*-CRSSGDD。*

证明. 令点集为$\mathbb{Z}_{24} \cup (\{a\} \times \mathbb{Z}_8) \cup (\{b\} \times \mathbb{Z}_2)$，组集为$\{\{0,6,12,18\}+i : 0 \le i \le 5\} \cup \{(\{a\} \times \mathbb{Z}_8) \cup (\{b\} \times \mathbb{Z}_2)\}$。所需设计由如下基区组在$\mathbb{Z}_{24}$中$+3 \pmod{24}$展开得到，其中元素$x_0 \in \{x\} \times \mathbb{Z}_n$的下标在$\mathbb{Z}_{24}$中的唯一$n$阶子群展开。

第一个GDD的基区组：

$\{1,6,3,a_0\}$ $\{2,9,23,a_0\}$ $\{10,20,11,a_0\}$ $\{4,8,21,a_0\}$ $\{7,14,18,a_0\}$
$\{0,23,15,b_0\}$ $\{0,5,16,a_0\}$ $\{22,12,13,a_0\}$ $\{1,4,20,b_0\}$ $\{15,17,19,a_0\}$

第二个GDD的基区组：

$\{3,2,13,a_0\}$ $\{4,21,13,b_0\}$ $\{8,23,16,a_0\}$ $\{4,5,15,a_0\}$ $\{11,9,0,a_0\}$
$\{12,17,7,a_0\}$ $\{21,19,18,a_0\}$ $\{1,20,22,a_0\}$ $\{6,10,14,a_0\}$ $\{0,17,20,b_0\}$

□

定理 6.30. *对任意*$g \equiv 2 \pmod 4$，$g \ge 10$，*存在一个型为*g^4*的*$(4,2)$*-CRSSGDD。*

证明. 对$g \in \{10,18,22,26\}$，所需设计在引理6.27中构造得到。对$g=14$，取引理6.28中的$\mathrm{CRSSITD}_2(4,14;4)$，在洞中填入一个型为$4^4$的$(4,2)$-CRSSGDD（引理5.4）就得所需设计。对$g=34$，对型为$4^6 10^1$的$(4,2)$-CRSSGDD用4膨胀，用型为$4^4$的$\{4\}$-MGDD做为输入设计，就得到了一个型为$(16,4^4)^6(40,10^4)^1$的$(4,2)$-CRSSDGDD。在洞中分别填入$\mathrm{CRSSTD}_2(4,4)$和$\mathrm{CRSSTD}_2(4,10)$就得到了所需设计。

对$g=30$或$g \ge 38$，应用构造6.26，令$\mu=l=1$，$k=m=4$，$\lambda=2$，$w_{ij} \in \{0,2\}$就得到了一个$\mathrm{CRSSITD}_2(4,50;14)$，并对任意$t \ge 5$，$t \notin \{6,10\}$得

到了CRSSITD$_2(4, 4t + 10; 10)$。这里，输入设计为CRSSTD$_2(4, 4)$（引理5.4）和CRSSITD$_2(4, 6; 2)$（引理6.28）。再填入CRSSTD$_2(4, 14)$和CRSSTD$_2(4, 10)$得到所需设计。 □

结合引理2.8，5.4，6.24和定理6.30，我们得到如下结果。

定理 6.31. 一个型为g^4的$(4, 2)$-*CRSSGDD*存在当且仅当$g \geq 4$，$g \neq 6$。

e. 型为g^u的$(4, 2)$-CRSSGDD的主要结果

定理 6.32. 型为g^u的$(4, 2)$-*CRSSGDD*存在的必要条件，除了确定的值$(g, u) \in \{(2, 4), (3, 4), (6, 4)\}$以外，也是充分的。

证明. 对$u = 4$，此设计的存在性由定理6.31给出，因此这里我们只考虑$u \geq 5$的情况。

（i）当$g \equiv 0 \pmod 6$时

对$g \in \{6, 12\}$，$u \geq 5$，所需设计由引理6.18和6.9得到。对$g = 36$，$u \geq 5$，对型为12^u，$u \geq 5$的$(4, 2)$-CRSSGDD用3膨胀得到所需设计。对任意$g > 12$，$g \neq 36$，对型为6^u的$(4, 2)$-CRSSGDD用$g/6$膨胀就得到了型为g^u，$u \geq 5$的$(4, 2)$-CRSSGDD。

（ii）当$g \equiv 1, 5, 7, 11 \pmod{12}$时

对$g = 1$，$u \equiv 1, 4 \pmod{12}$，$u \geq 13$，所需设计由引理5.2得到。对$g \geq 5$，$u \equiv 1, 4 \pmod{12}$，$u \geq 13$，对$(u, 4, 2)$-CRSS设计用g膨胀得到所需的型为g^u的$(4, 2)$-CRSSGDD。

（iii）当$g \equiv 2, 10 \pmod{12}$时

对$g = 2$，$u \equiv 1 \pmod 3$，$u \geq 7$，所需设计由引理5.19和5.20得到。对$g \geq 10$，$u \equiv 1 \pmod 3$，$u \geq 7$，对型为2^u的$(4, 2)$-CRSSGDD用$g/2$膨胀得到型为g^u的$(4, 2)$-CRSSGDD。

（iv）当$g \equiv 3, 9 \pmod{12}$时

对$g = 3$，$u \equiv 0, 1 \pmod 4$，$u \geq 5$，所需设计由引理6.22和6.25得到。对$g \geq 9$，$u \equiv 0, 1 \pmod 4$，$u \geq 5$，对型为3^u的$(4, 2)$-CRSSGDD用$g/3$膨胀得到型为g^u的$(4, 2)$-CRSSGDD。

（v）当$g \equiv 4, 8 \pmod{12}$时

对$g = 4$，$u \equiv 1 \pmod 3$，$u \geq 7$，所需设计由引理6.20得到。对$g = 8$，$u \equiv 1 \pmod 3$，$u \geq 7$，对型为2^u的$(4,2)$-CRSSGDD用4膨胀得到所需设计。对$g \geq 16$，$u \equiv 1 \pmod 3$，$u \geq 7$，对型为4^u的$(4,2)$-CRSSGDD用$g/4$膨胀得到型为g^u的$(4,2)$-CRSSGDD。 □

6.6　最优超单$(v,4,2)$-填充的存在性

在本节中，我们将研究超单$(v,4,2)$-填充的存在性。首先，我们给出了一个最优$(v,6,4)_3$码和最优超单$(v,4,2)$-填充的联系。然后，我们证明了对任意$v \geq 4$，除了确定的值$v \in \{4,5,6,9\}$外，最优超单$(v,4,2)$-填充都是存在的。

a. 当$v \equiv 1,2 \pmod 3$时

在文[159]中，作者确定了最优$(v,6,4)_3$码的存在性，即：如果$v \geq 4$，$v \notin \{4,5,7,8,11,17\}$，$A_3(v,6,4) = \left\lfloor \frac{v}{2} \left\lfloor \frac{v-1}{3} \right\rfloor \right\rfloor$。可以证明当$v \equiv 1,2 \pmod 3$时，具有$\left\lfloor \frac{v}{2} \left\lfloor \frac{v-1}{3} \right\rfloor \right\rfloor$个码字的最优$(v,6,4)_3$码就是一个最优超单$(v,4,2)$-填充。然而，反之却不成立。

引理 6.33. *当$v \equiv 1,2 \pmod 3$时，如果存在一个具有$\left\lfloor \frac{v}{2} \left\lfloor \frac{v-1}{3} \right\rfloor \right\rfloor$个码字的最优$(v,6,4)_3$码，那么存在一个最优超单$(v,4,2)$-填充。*

证明. 令X为一个大小为v的点集，$\mathcal{D}$为最优$(v,6,4)_3$码的所有码字的支撑集构成的集合。那么$\mathcal{D}$形成一个区组大小为4的设计。

首先，我们指出X中的任意点对在$\mathcal{D}$中最多出现在两个区组中。如果一个点对出现在两个区组中，那么在这两个码字中这两个位置上的元素为$\langle 1,1\rangle$，$\langle 2,2\rangle$或$\langle 1,2\rangle$，$\langle 2,1\rangle$。因此，$\mathcal{D}$是一个$(v,4,2)$-填充。其次，我们指出$\mathcal{D}$具有超单性质。如果有两个区组交于多于两个点，那么这两个码字的最小距离最多是5，这就与距离条件矛盾。所以$\mathcal{D}$是超单的。最后，很容易检验当$v \equiv 1,2 \pmod 3$时，一个最优$(v,6,4)_3$码的码字个数，即$\left\lfloor \frac{v}{2} \left\lfloor \frac{v-1}{3} \right\rfloor \right\rfloor$，恰好达到了最优超单$(v,4,2)$-填充的区组个数。因此，我们就证明了由码得到的超单$(v,4,2)$-填充也是最优的。 □

引理 6.34. *对任意$v \in \{7,8,11,17\}$，存在一个最优超单$(v,4,2)$-填充。*

证明. 对$v = 7$，所需设计就是超单$(7, 4, 2)$-BIBD（见文[83]）。对$v \in \{8, 11\}$，所需设计在点集$\{0, 1, \ldots, v-1\}$上构造，区组如下：

$v = 8$：$\{2,1,6,5\}$ $\{1,2,4,7\}$ $\{3,6,0,7\}$ $\{5,7,4,0\}$ $\{7,5,1,3\}$ $\{0,6,4,1\}$ $\{0,3,5,2\}$ $\{4,6,2,3\}$

$v = 11$：

$\{0,1,2,3\}$ $\{0,4,5,6\}$ $\{0,7,8,9\}$ $\{1,4,0,10\}$ $\{1,5,8,7\}$ $\{2,1,6,9\}$ $\{2,5,10,0\}$ $\{3,2,4,7\}$
$\{3,5,9,1\}$ $\{3,6,8,0\}$ $\{4,9,2,8\}$ $\{6,7,3,10\}$ $\{7,6,4,1\}$ $\{8,5,4,3\}$ $\{8,10,6,2\}$ $\{9,10,7,5\}$

对$v = 17$，所需设计在点集$\mathbb{Z}_{15} \cup \{\infty_0, \infty_1\}$上构造。所需区组由如下基区组在$\mathbb{Z}_{15}$中$+5 \pmod{15}$展开得到，$\infty_0$和$\infty_1$在自同构作用下保持不动。

$\{0,2,4,6\}$ $\{0,1,2,3\}$ $\{0,9,12,\infty_1\}$ $\{0,3,6,11\}$ $\{12,5,\infty_0,3\}$ $\{5,3,4,\infty_1\}$ $\{13,7,\infty_1,6\}$
$\{0,1,4,5\}$ $\{3,7,9,14\}$ $\{5,12,2,13\}$ $\{3,9,1,13\}$ $\{13,14,\infty_0,5\}$ $\{1,4,7,11\}$ $\{\infty_0,11,9,2\}$

□

对任意$v \equiv 1, 2 \pmod 3$，$v \geq 7$，$v \notin \{7, 8, 11, 17\}$，我们由引理6.33得到了最优超单$(v, 4, 2)$-填充。对$v \in \{4, 5\}$，显然所需设计是平凡的，只有一个区组。因此，我们得到了：

引理 6.35. 对任意$v \equiv 1, 2 \pmod 3$，$v \geq 7$，$D_2'(v, 4, 2) = U_2(v, 4, 2)$；对任意$v \in \{4, 5\}$，$D_2'(v, 4, 2) = U_2(v, 4, 2) - 1$。

b. 当$v \equiv 0 \pmod 3$时

引理 6.36. 对任意$v \in \{6, 9\}$，$D_2'(v, 4, 2) = U_2(v, 4, 2) - 1$。

证明. 对$v = 6$，显然：在一个最优超单$(6, 4, 2)$-填充中，任意一个点最多包含在两个区组中。所以此设计最多有$\frac{2\times 6}{4} = 3$个区组。我们在点集$\{0, 1, 2, 3, 4, 5\}$上构造所需设计的3个区组$\{0, 1, 2, 3\}$，$\{2, 3, 4, 5\}$，$\{0, 1, 4, 5\}$。

对$v = 9$，由引理6.7，$D_2(9, 4, 2) = U_2(9, 4, 2) - 1$。因此，对一个超单$(9, 4, 2)$-填充，$D_2'(9, 4, 2) \leq U_2(9, 4, 2) - 1$。我们在点集$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$上构造所需的10个区组如下：

$\{0,1,2,3\}$ $\{0,4,5,6\}$ $\{1,0,7,8\}$ $\{2,1,5,4\}$ $\{2,6,7,0\}$
$\{3,5,7,1\}$ $\{5,8,3,0\}$ $\{6,8,4,1\}$ $\{8,6,5,2\}$ $\{3,4,2,8\}$

□

引理 6.37. 对任意$v \in \{12, 24, 36\}$，存在一个最优超单$(v, 4, 2)$-填充。

证明. 所需设计在$\mathbb{Z}_v$上构造，并由如下基区组在$\mathbb{Z}_v$中$+4 \pmod v$展开得到。

$v = 12$：$\{0,1,2,3\}$ $\{0,4,10,9\}$ $\{0,7,11,8\}$ $\{3,9,6,2\}$ $\{3,5,1,11\}$ $\{6,10,3,8\}$ $\{2,5,9,8\}$

$v = 24$：

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

$v = 36$：

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

□

引理 6.38. *对任意$v \in \{15,27,39\}$，存在一个最优超单$(v,4,2)$-填充。*

证明. 所需设计在$\mathbb{Z}_{v-3} \cup (\{a\} \times \mathbb{Z}_3)$上构造，其中$\{\{a\} \times \mathbb{Z}_3\}$为一个洞。所需设计由如下基区组在$\mathbb{Z}_{v-3}$中$+4 \pmod{v-3}$展开得到，其中$x_0 \in \{x\} \times \mathbb{Z}_n$元素的下标是在$\mathbb{Z}_{v-3}$中的唯一的$n$阶子群中展开。

$v = 15$：

$\{9,3,7,0\}$　$\{0,4,9,a_0\}$　$\{2,7,a_1,5\}$　$\{a_1,4,3,11\}$　$\{a_2,6,1,5\}$　$\{0,a_1,10,8\}$
$\{0,1,3,2\}$　$\{5,2,4,10\}$　$\{2,6,a_0,3\}$　$\{3,a_2,10,4\}$　$\{3,9,5,a_1\}$

$v = 27$：

$\{2,23,4,10\}$　$\{9,2,16,5\}$　$\{23,13,8,a_1\}$　$\{11,9,7,19\}$　$\{20,14,10,a_0\}$　$\{10,19,a_1,20\}$
$\{0,16,23,2\}$　$\{21,5,8,9\}$　$\{14,21,13,2\}$　$\{14,3,18,9\}$　$\{5,23,a_0,20\}$　$\{12,a_0,15,17\}$
$\{0,8,20,17\}$　$\{10,2,8,3\}$　$\{a_2,5,19,14\}$　$\{19,8,12,23\}$　$\{17,a_1,18,23\}$　$\{a_0,13,12,10\}$
$\{3,19,2,13\}$

$v = 39$：

$\{2,5,25,7\}$　$\{10,11,19,1\}$　$\{6,31,28,27\}$　$\{30,8,0,10\}$　$\{22,24,29,5\}$　$\{8,30,22,20\}$
$\{1,0,30,29\}$　$\{28,3,12,25\}$　$\{19,29,17,7\}$　$\{0,34,6,18\}$　$\{1,11,18,31\}$　$\{16,12,a_1,19\}$
$\{a_2,9,17,6\}$　$\{17,a_2,0,26\}$　$\{6,35,10,a_2\}$　$\{1,33,2,a_2\}$　$\{13,29,35,0\}$　$\{2,19,35,34\}$
$\{3,6,17,30\}$　$\{16,7,11,a_0\}$　$\{0,19,21,25\}$　$\{a_0,26,5,0\}$　$\{21,19,6,24\}$　$\{a_1,12,35,27\}$
$\{29,4,20,8\}$　$\{3,24,32,33\}$　$\{3,15,34,28\}$

□

注意到引理6.38中构造的最优超单$(v,4,2)$-填充，$v \in \{15,27,39\}$也是超单$(v,3;4,2)$-MIPD。

引理 6.39. *对任意$v \equiv 0,3 \pmod{12}$，$v \geq 12$，存在最优超单$(v,4,2)$-填充。*

证明. 对$12 \leq v \leq 39$，所需设计在引理6.37和6.38中构造得到。对任意$v \geq 48$，从引理6.9中取一个型为12^t，$t \geq 4$的$(4,2)$-CRSSGDD。由构造6.5和6.6，如果我们在组上填入最优超单$(12,4,2)$-填充，我们就对任意$t \geq 4$得到了最优超单$(12t,4,2)$-填充。如果增加3个点，并在组上连同无穷点填入超单$(15,3;4,2)$-MIPD，我们就对任意$t \geq 4$得到了最优超单$(12t+3,4,2)$-填充。 □

引理 6.40. 对任意$v \in \{18,21,30\}$，存在一个最优超单$(v,4,2)$-填充。

证明. 对$v=18$，所需设计在$\{0,1,\ldots,17\}$上直接构造，区组如下：

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

对$v=21$，所需设计在$\mathbb{Z}_{20}\cup\{\infty\}$上构造。所需区组由如下基区组在$\mathbb{Z}_{20}$中$+5 \pmod{20}$展开得到，其中$\infty$在自同构的作用下保持不动。

$\{0,2,5,7\}$ $\{4,3,14,5\}$ $\{1,17,9,13\}$ $\{11,16,0,19\}$ $\{10,0,11,4\}$ $\{3,18,7,17\}$
$\{6,3,\infty,9\}$ $\{6,18,16,7\}$ $\{4,7,10,19\}$ $\{5,18,12,\infty\}$ $\{0,12,13,6\}$ $\{18,10,15,13\}$
$\{3,13,6,4\}$ $\{17,4,19,2\}$ $\{13,11,5,9\}$ $\{11,16,7,15\}$ $\{1,7,14,\infty\}$

对$v=30$，所需设计在$\mathbb{Z}_{30}$上构造。所需区组由如下基区组在$\mathbb{Z}_{30}$中$+15 \pmod{30}$展开得到。

$\{19,8,0,11\}$ $\{19,20,0,21\}$ $\{15,12,0,11\}$ $\{23,6,19,24\}$ $\{17,26,12,9\}$ $\{16,29,23,28\}$
$\{20,1,24,5\}$ $\{16,24,1,27\}$ $\{21,22,27,6\}$ $\{20,11,4,13\}$ $\{21,5,29,13\}$ $\{18,20,15,21\}$
$\{17,8,11,6\}$ $\{22,10,8,12\}$ $\{16,13,0,17\}$ $\{21,3,26,10\}$ $\{22,21,29,7\}$ $\{14,24,26,11\}$
$\{18,8,2,13\}$ $\{21,5,27,14\}$ $\{21,15,9,24\}$ $\{18,17,29,0\}$ $\{16,12,0,18\}$ $\{16,15,17,18\}$
$\{23,9,3,13\}$ $\{18,27,6,26\}$ $\{18,5,25,28\}$ $\{24,28,12,2\}$ $\{22,26,17,28\}$ $\{20,18,23,22\}$
$\{22,4,24,8\}$ $\{17,1,23,20\}$ $\{23,11,5,29\}$ $\{10,21,18,4\}$ $\{19,17,22,14\}$ $\{20,22,26,16\}$
$\{20,8,3,25\}$ $\{22,11,28,3\}$ $\{17,10,27,5\}$ $\{19,29,27,8\}$ $\{22,15,13,25\}$ $\{25,12,13,27\}$
$\{18,12,7,1\}$ $\{25,14,16,7\}$ $\{20,27,2,29\}$ $\{24,19,3,12\}$ $\{14,16,13,10\}$ $\{21,13,28,19\}$
$\{17,10,6,2\}$ $\{18,19,22,1\}$ $\{17,7,19,15\}$ $\{21,0,14,28\}$ $\{20,15,11,10\}$ $\{22,12,23,15\}$
$\{18,14,3,9\}$ $\{24,7,10,26\}$ $\{22,13,5,24\}$ $\{23,0,25,10\}$ $\{10,14,29,24\}$ $\{21,24,25,16\}$
$\{16,8,23,6\}$ $\{21,1,11,17\}$ $\{20,17,7,24\}$ $\{26,19,1,13\}$ $\{16,15,29,19\}$ $\{14,27,11,23\}$
$\{2,9,10,19\}$ $\{15,8,9,28\}$ $\{18,14,2,19\}$ $\{19,4,20,27\}$ $\{19,10,16,11\}$

□

引理 6.41. *对任意$v \in \{54, 57\}$，存在一个最优超单$(v, 4, 2)$-填充。*

证明. 我们用文[7]中的方法去构造所需$(v, 4, 2)$-填充。首先，我们在点集$\mathbb{Z}_{56}$上构造一个型为2^{28}的$\{4\}$-GDD，其中组集为$\{\{0, 28\} + i : 0 \le i \le 27\}$，区组集$\mathcal{D}_1$由如下基区组$+2 \pmod{56}$展开得到。

$$\begin{array}{lllll} \{0,3,33,52\} & \{0,35,43,55\} & \{0,8,19,22\} & \{0,9,15,20\} & \{1,15,19,44\} \\ \{0,2,12,18\} & \{0,26,47,49\} & \{0,1,17,32\} & \{0,5,29,39\} & \end{array}$$

对$v = 54$，我们在$\mathbb{Z}_{52}$上构造一个$(52, 4, 1)$-BIBD，其中区组集由如下基区组$+4 \pmod{52}$展开得到。记其区组集为$\mathcal{D}_2$。

$$\begin{array}{llllll} \{7,29,50,30\} & \{0,12,16,6\} & \{0,50,41,24\} & \{7,13,10,38\} & \{7,11,1,24\} & \{14,49,25,39\} \\ \{0,15,43,44\} & \{21,8,26,40\} & \{21,28,6,13\} & \{7,28,39,47\} & \{7,4,18,26\} & \{21,12,33,17\} \\ \{0,49,47,10\} & \{7,14,32,33\} & \{14,15,50,2\} & \{7,21,43,41\} & \{0,7,25,2\} & \end{array}$$

我们能看到在$\mathcal{D}_1$中有一个区组$\{15, 30, 54, 55\}$，它是由$\{0, 1, 17, 32\}$展开得到的。在$\mathcal{D}_1$中分别用点$52, 53, 15, 30$替代$15, 30, 52, 53$就得到了一个新的区组集$\mathcal{D}_1'$，其中$\{52, 53, 54, 55\}$是一个区组。去掉这个区组，并在剩余的区组$\mathcal{D}_1'$中用52代替55，用53代替54就得到了一个区组集$\mathcal{D}_1''$。用置换(0 48 31 6 21 7 28 27 12 5 44 45 13 23 11 34 32 15)(1 8)(2)(3 43 20 4 30)(9)(10)(14)(16)(17)(18)(19)(22)(24)(25)(26)(29)(33)(35)(36)(37)(38)(39)(40)(41)(42)(46 50)(47)(49)(51)(52)(53)作用在$\mathcal{D}_2$的每个点上就得到了$\mathcal{D}_2'$。最后，把$\mathcal{D}_1''$和$\mathcal{D}_2'$合并就得到了需要的设计。

对$v = 57$，我们在点集$\{0, 1, \ldots, 57\}$上构造一个型$1^{51}7^1$的$\{4\}$-GDD，其中组集为$\{\{\{i\} : 0 \le i \le 50\} \cup \{51, 52, \ldots, 57\}\}$。用自同构群$G = \langle(0\ 3\ \cdots\ 48)(1\ 4\ \cdots\ 49)(2\ 5\ \cdots\ 50)(51)(52)(53)(54)(55)(56)(57)\rangle$对如下基区组展开得到区组集$\mathcal{D}_3$。

$$\begin{array}{llllll} \{1,4,34,46\} & \{2,3,23,26\} & \{1,20,26,35\} & \{0,6,10,18\} & \{0,26,36,38\} & \{0,21,34,48\} \\ \{0,8,19,57\} & \{2,22,35,37\} & \{2,16,21,54\} & \{2,7,42,51\} & \{1,30,44,56\} & \{0,25,47,55\} \\ \{0,9,40,44\} & \{2,36,43,53\} & \{2,46,48,52\} & \{0,1,28,29\} & & \end{array}$$

对$\mathcal{D}_1$中的每个点x，如果$x < 28$，那么用映射$x \mapsto 2x$，否则，用映射$x \mapsto 2(x - 28) + 1$就得到了$\mathcal{D}_1'''$。在$\mathcal{D}_3$中，用56代替57，并增加区组$\{51, 52, 53, 56\}$，$\{51, 54, 55, 56\}$，$\{52, 53, 54, 55\}$得到$\mathcal{D}_3'$。用置换(0 10 29)(1 11)(2 31 48 12)(3)(4 26 22 27 50 35 14 37 51 44 47 33 6)(5 21)(7 8)(13)(23)(28)(9 43)(15 49 20 19 18 17 16)(24 25)(30 36)(32)(34)(38)(39)(40)(41)(42)(45)(46)(52)(53)(54)(55)(56)作用在$\mathcal{D}_3'$中的每个点上就得到了$\mathcal{D}_3''$。最后，把$\mathcal{D}_1'''$和$\mathcal{D}_3''$ 合并就得到了所需设计。

□

引理 6.42. 对任意$(v,w)\in\{(33,7),(42,10),(45,13)\}$，分别存在区组个数为166，268，300的超单$(v,w;4,2)$-填充。

证明. 在点集$\{0,1,\ldots,32\}$上构造具有166个区组的超单$(33,7;4,2)$-填充，其中洞为$\{26,27,\ldots,32\}$。所需设计由如下基区组通过自同构群$G=\langle(0\ 13)(1\ 14)(2\ 15)\cdots(12\ 25)(26\ 27)(28\ 29)(30\ 31)(32)\rangle$展开得到。

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

在点集$\{0,1,\ldots,41\}$上构造具有268个区组的超单$(42,10;4,2)$-填充，其中洞为$\{32,33,\ldots,41\}$，并且区组集由如下基区组通过自同构群$G=\langle(0\ 8\ \cdots\ 24)(1\ 9\ \cdots\ 25)\cdots(7\ 15\ \cdots\ 31)(32\ 33\ 34\ 35)(36\ 37\ 38\ 39)(40\ 41)\rangle$展开得到。

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

在点集$\{0,1,\ldots,44\}$上构造具有300个区组的超单$(45,13;4,2)$-填充，其中洞为$\{32,33,34,\ldots,44\}$。所需区组集由如下基区组由自同构群$G=\langle(0\ 8\ 16\ 24)(1\ 9\ 17\ 25)\cdots(7\ 15\ 23\ 31)(32\ 33\ 34\ 35)(36\ 37\ 38\ 39)(40\ 41\ 42\ 43)(44)\rangle$展开得

到。

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

□

在文[159, 引理 5.3, 引理 5.5]中，作者有如下$(4,2)$-CRSSGDD的结果。

引理 6.43 (Zhang，Ge[159]). *对任意$u \in [4,8] \cup \{16\} \cup [20,22]$或$u \geq 24$，存在一个型为$12^u 18^1$的$(4,2)$-CRSSGDD。对任意$(u,m) \in \{(4,30),(5,18),(5,30),(6,18),(6,30),(7,18),(7,30)\}$，存在一个型为$24^u m^1$的$(4,2)$-CRSSGDD。对任意$(u,m) \in \{(5,42),(6,18),(6,30),(6,78)\}$，存在一个型为$36^u m^1$的$(4,2)$-CRSSGDD。*

引理 6.44. *对任意$v \equiv 6,9 \pmod{12}$，$v \geq 18$，存在一个最优超单$(v,4,2)$-填充。*

证明. 对$v \in \{18,21,30,54,57\}$，所需设计在引理6.40和6.41中构造得到。对$v \in \{33,42,45\}$，从引理6.42取超单$(v,w;4,2)$-填充，其中$(v,w) \in \{(33,7),(42,10),(45,13)\}$，然后在组上分别填入最优超单$(w,4,2)$-填充，$w \in \{7,10,13\}$（引理6.35）得到所需设计。

由构造6.5和6.6，如果在引理6.43中的CRSSGDD的组上填入适当的最优超单$(v,4,2)$-填充，$v \in \{12,18,24,30,36,42,78\}$（引理6.39），我们就对任意$t \geq 4$得到了需要的最优超单$(12t+18,4,2)$-填充；如果对这些CRSSGDD增加3个点，并在组上连同无穷点填入恰当的超单$(v,3;4,2)$-MIPD，$v \in \{15,27,39\}$（引理6.38）和最优超单$(v,4,2)$-填充，$v \in \{21,33,45,81\}$，我们就对任意$t \geq 4$得到了最优超单$(12t+21,4,2)$-填充。 □

结合引理6.35，6.36，6.39和6.44，我们得到了如下结果。

定理 6.45. 对任意$v \geq 4$，$v \notin \{4,5,6,9\}$，$D'_3(v,4,2) = U(v,4,2)$；对$v \in \{4,5,6,9\}$，$D'_3(v,4,2) = U(v,4,2) - 1$。

Chapter 7

用Hanani三元填充构造线性大小最优多元常重码

7.1 引言及主要结果

目前，对$A_q(n,d,w)$的研究工作多是给定d和w，研究某个确定的q，通常是$q \leq 4$。对任意正整数n和$q \geq 2$，$A_q(n,d,w)$都确定的情况只有当$(d,w) = (3,2)$ 和$(4,3)$时[23, 26]。

最近，Chee等在文[24]中对任意$q \geq 2$，给出了重量为w，距离为$d = 2w - 1$时，最优q元常重码的码字个数的渐近结果。这种参数下的码也称为是线性大小的，因为$A_q(n, 2w-1, w) = O(n)$ [24]。事实上，他们运用了一种三角差集的推广，并得到如下结果：

定理 7.1 (Chee等[24]). 若$w|(q-1)n$，对任意$n \geq 2w(w(q-1)-1)^2+1$，$A_q(n,2w-1,w) = (q-1)n/w$。若$w|n$，对任意$n \geq w((w-1)(q-2)+1)$，$A_q(n,2w-1,w) = (q-1)n/w$。

对线性大小的最优q元常重码，还有如下已知结果：

(1) 当$w = 2$时，对任意正整数n和$q \geq 2$，$A_q(n,3,2) = \min\left\{\left\lfloor \frac{(q-1)n}{2} \right\rfloor, \binom{n}{2}\right\}$ [26]。

(2) 当$q = 3$时，对任意w，$A_3(n, 2w-1, w) = \max\{M | n \geq \lceil Mw/2 \rceil + \max\{\lfloor Mw/2 \rfloor - \binom{M}{2}, 0\}\}$ [115]。

然而，当$w \geq 3$且$q \geq 4$时，对$A_q(n, 2w-1, w)$除了定理7.1中的渐近结果外没有任何已知结果了。

在本章中，我们将对任意正整数n和$q \geq 2$确定$A_q(n,5,3)$的准确值。我们的方法是基于Hanani三元填充的构造。我们将在下一节中给出它的定义及它与最优码的联系。

由引理2.2中的Johnson界，我们可以很容易得到如下线性大小的常重码的界：

推论 7.2. $A_q(n, 2w-1, w) \leq \left\lfloor \frac{n(q-1)}{w} \right\rfloor$。

特别的，当$(d, w) = (5, 3)$时，我们得到$A_q(n, 5, 3) \leq \left\lfloor \frac{(q-1)n}{3} \right\rfloor$。

这一章的结构如下：在第7.2节中，我们将给出填充设计和Hanani三元填充设计与最优码的联系；在第7.3节中，我们构造强Hanani三元填充得到几乎所有长度的最优码；第7.4节中，我们将对剩余的值逐个解决；在第7.5节中，我们将解决Hanani三元填充的存在性，并在第7.6节中，总结本章结果。

7.2 设计与码的联系

a. 最优填充与最优码的联系

Chee等在文[24]中建立了一个$(n, 2w-1, w)_q$码$\mathcal{C}$的如下充要条件：

(C1) 对任意不同的$\mathsf{u}, \mathsf{v} \in \mathcal{C}$，$|\mathrm{supp}(\mathsf{u}) \cap \mathrm{supp}(\mathsf{v})| \leq 1$。

(C2) 对任意不同的$\mathsf{u}, \mathsf{v} \in \mathcal{C}$，如果$x \in \mathrm{supp}(\mathsf{u}) \cap \mathrm{supp}(\mathsf{v})$，那么$\mathsf{u}_x \neq \mathsf{v}_x$。

因此，我们可以很容易得到下面结果。

引理 7.3. 令$\mathcal{C} \subset \mathbb{Z}_q^X$是一个$(n, 2w-1, w)_q$码，$\mathcal{B} = \{\mathrm{supp}(\mathsf{u}) : \mathsf{u} \in \mathcal{C}\}$。那么$(X, \mathcal{B})$是一个$(n, w, 1)$-填充。

由引理7.3，$A_q(n, 2w-1, w)$不超过填充数$D(n, w, 2)$。事实上我们可以证明当q充分大时，$A_q(n, 2w-1, w) = D(n, w, 2)$。

对一个集合系统$(X, \mathcal{B})$，令$P \subset B$。对一个正整数i，令$\mathcal{C}(P, i) := \{\mathsf{u}^B : B \in P\}$是一个码，其中码字$\mathsf{u}^B$如下定义：

$$\mathsf{u}_x^B = \begin{cases} i, & \text{若} x \in B, \\ 0, & \text{若} x \notin B。 \end{cases}$$

引理 7.4. 对任意$q \geq \left\lfloor \frac{n-1}{w-1} \right\rfloor + 1$，$A_q(n, 2w-1, w) = D(n, w, 2)$。

证明. 令$(X, \mathcal{B})$是一个最优$(n, w, 1)$-填充，那么每个点最多出现在$\left\lfloor \frac{n-1}{w-1} \right\rfloor$个区组中。构造码$\mathcal{C}(\mathcal{B}, 1)$，其中每个坐标最多有$\left\lfloor \frac{n-1}{w-1} \right\rfloor$个1。我们把$\mathcal{C}(\mathcal{B}, 1)$的这些1分别用1, 2, 3, $\cdots$替换，使得每个坐标的非零元素都不同。那么我们就得到了一个有$D(n, w, 2)$个码字的$(n, 2w-1, w)_{\left\lfloor \frac{n-1}{w-1} \right\rfloor + 1}$码。对任意$q \geq \left\lfloor \frac{n-1}{w-1} \right\rfloor + 1$，它当然也是一个$(n, 2w-1, w)_q$码。由引理7.3可知，我们构造的码是最优的。 □

因为当$w \in \{3,4\}$时，最优$(n,w,1)$-填充的填充数已经完全被确定，所以由引理7.4，我们能得到很多最优码。

推论 7.5. 对任意$q \geq \lfloor \frac{n-1}{2} \rfloor + 1$，$A_q(n,5,3) = D(n,3,2)$。

b. Hanani三元填充的定义

一个*Hanani*三元填充（Hanani triple packing，HTP）就是一个最优$(n,3,1)$-填充，它的区组集可以划分成一些PPC的集合，且除了最多一个以外，其余都是最大的，并记为HTP(n)。Hanani三元填充是组合设计里一些已知结构，如Hanani三元系[140]，Kirkman三元系[41]的推广。给定一个$(n,k,1)$-填充$(X,\mathcal{B})$和一个PPC $P \subset \mathcal{B}$，我们用$\overline{P}$来表示P空缺的点，即：$\overline{P} = X \setminus \{x : x \in B, B \in P\}$。

对任意n，令$h = \lfloor \frac{n-1}{2} \rfloor$，$b = \lfloor n/3 \rfloor$，$t = \lfloor n/6 \rfloor$，$c \equiv n \pmod 3$，且$0 \leq c \leq 2$。那么$n = 3b + c$，且：

$$A_q(n,5,3) \leq \left\lfloor \frac{(q-1)(3b+c)}{3} \right\rfloor = (q-1)b + \left\lfloor \frac{(q-1)c}{3} \right\rfloor 。$$

我们在表7.1列出一个HTP(n)所需区组个数。我们将主要用HTP(n)来构造当$q \leq h+1$时的最优$(n,5,3)_q$码。事实上，我们需要一个更强的定义。

表 7.1: 一个HTP(n)所需的区组个数

n	$D(n,3,2) = b \cdot h + \star$
$6t$	$6t^2 - 2t = 2t(3t-1) + 0$
$6t+1$	$6t^2 + t = 2t \cdot 3t + t$
$6t+2$	$6t^2 + 2t = 2t \cdot 3t + 2t$
$6t+3$	$6t^2 + 5t + 1 = (2t+1)(3t+1) + 0$
$6t+4$	$6t^2 + 6t + 1 = (2t+1)(3t+1) + t$
$6t+5$	$6t^2 + 9t + 2 = (2t+1)(3t+2) + 2t$

定义 7.6. 当$n \not\equiv 0 \pmod 3$时，假设一个*HTP*(n)有*MPPC* $\mathcal{P}_i$，$i \in [h]$，一个*PPC* $\mathcal{P}_{h+1}$。假设$\overline{\mathcal{P}_i} = \{a_{i,j} : j = 1, \ldots, c\}$，$i \in [h]$。当$c = 2$时，$\overline{\mathcal{P}_i}$中的点是有序的。

在这种情况下，一个*HTP*(n)被称为是强的如果所有的*PPC*满足如下条件，对任意$s \in [t]$：

(i) 对任意$j=1,\ldots,c$，$\{a_{3s-2,j},a_{3s-1,j},a_{3s,j}\}$是最后一个*PPC*的区组；

(ii) 若$c=2$，前$3s-1$个*MPPC*和区组$\{a_{3s-2,1},a_{3s-2,2},a_{3s-1,1}\}$形成一个$(n,3,1)$-填充，即：$\{a_{3s-2,1},a_{3s-2,2},a_{3s-1,1}\}$中的任何点对不出现在$\bigcup_{i=1}^{3s-1}\mathcal{P}_i$的任何区组中。

当$n\equiv 0 \pmod 3$时，一个$HTP(n)$也是强的。

例 7.7. 一个强$HTP(8)$：

令$X=\mathbb{Z}_6\cup\{\infty_0,\infty_1\}$。下面列出了*MPPC* $\mathcal{P}_i$，相应的有序集合$\overline{\mathcal{P}_i}$，$i\in[3]$，和一个*PPC* $\mathcal{P}_4$。

$$\begin{aligned}
&\mathcal{P}_1=\{\{1,5,\infty_0\},\{2,4,\infty_1\}\}, \quad \overline{\mathcal{P}_1}=\{0,3\};\\
&\mathcal{P}_2=\{\{2,3,\infty_0\},\{0,5,\infty_1\}\}, \quad \overline{\mathcal{P}_2}=\{1,4\};\\
&\mathcal{P}_3=\{\{0,4,\infty_0\},\{1,3,\infty_1\}\}, \quad \overline{\mathcal{P}_3}=\{2,5\};\\
&\mathcal{P}_4=\{\{0,1,2\},\{3,4,5\}\}。
\end{aligned}$$

例 7.8. 一个强$HTP(10)$：

令$X=\mathbb{Z}_6\cup\{\infty_0,\infty_1,\infty_2,\infty_3\}$。下面列出了*MPPC* $\mathcal{P}_i$，$\overline{\mathcal{P}_i}$，$i\in[4]$，和一个*PPC* $\mathcal{P}_5$。

$$\begin{aligned}
&\mathcal{P}_1=\{\{\infty_2,0,1\},\{\infty_3,2,3\},\{\infty_0,4,5\}\}, \quad \overline{\mathcal{P}_1}=\{\infty_1\};\\
&\mathcal{P}_2=\{\{\infty_1,2,4\},\{\infty_3,0,5\},\{\infty_0,1,3\}\}, \quad \overline{\mathcal{P}_2}=\{\infty_2\};\\
&\mathcal{P}_3=\{\{\infty_1,1,5\},\{\infty_2,3,4\},\{\infty_0,0,2\}\}, \quad \overline{\mathcal{P}_3}=\{\infty_3\};\\
&\mathcal{P}_4=\{\{\infty_1,0,3\},\{\infty_2,2,5\},\{\infty_3,1,4\}\}, \quad \overline{\mathcal{P}_4}=\{\infty_0\};\\
&\mathcal{P}_5=\{\{\infty_1,\infty_2,\infty_3\}\}。
\end{aligned}$$

例 7.9. 一个强$HTP(17)$：

令$X=\mathbb{Z}_{12}\cup\{\infty_0,\infty_1,\infty_2,\infty_3,\infty_4\}$。下面列出了*MPPC* $\mathcal{P}_i$，相应的有序集合$\overline{\mathcal{P}_i}$，$i\in[8]$。最后一个*PPC* $\mathcal{P}_9=\{\{0,4,8\}+i:i=0,1,2,3\}$。

$$\begin{aligned}
&\mathcal{P}_1=\{\{2,8,\infty_0\}\{6,5,\infty_1\}\{4,3,\infty_2\}\{9,11,\infty_3\}\{10,7,\infty_4\}\}, \quad \overline{\mathcal{P}_1}=\{0,1\};\\
&\mathcal{P}_2=\{\{9,3,\infty_0\}\{1,7,\infty_1\}\{0,10,\infty_2\}\{6,8,\infty_3\}\{11,2,\infty_4\}\}, \quad \overline{\mathcal{P}_2}=\{4,5\};\\
&\mathcal{P}_3=\{\{7,6,\infty_0\}\{3,10,\infty_1\}\{11,5,\infty_2\}\{0,2,\infty_3\}\{1,4,\infty_4\}\}, \quad \overline{\mathcal{P}_3}=\{8,9\};\\
&\mathcal{P}_4=\{\{11,10,\infty_0\}\{8,9,\infty_1\}\{1,6,\infty_2\}\{7,4,\infty_3\}\{0,5,\infty_4\}\}, \quad \overline{\mathcal{P}_4}=\{2,3\};\\
&\mathcal{P}_5=\{\{5,4,\infty_0\}\{0,11,\infty_1\}\{2,9,\infty_2\}\{1,10,\infty_3\}\{3,8,\infty_4\}\}, \quad \overline{\mathcal{P}_5}=\{6,7\};\\
&\mathcal{P}_6=\{\{1,0,\infty_0\}\{2,4,\infty_1\}\{8,7,\infty_2\}\{3,5,\infty_3\}\{6,9,\infty_4\}\}, \quad \overline{\mathcal{P}_6}=\{10,11\};\\
&\mathcal{P}_7=\{\{0,9,7\}\{11,4,6\}\{2,3,1\}\{8,5,10\}\{\infty_0,\infty_1,\infty_2\}\}, \quad \overline{\mathcal{P}_7}=\{\infty_3,\infty_4\};\\
&\mathcal{P}_8=\{\{0,6,3\}\{4,10,9\}\{1,8,11\}\{2,5,7\}\{\infty_0,\infty_3,\infty_4\}\}, \quad \overline{\mathcal{P}_8}=\{\infty_1,\infty_2\}。
\end{aligned}$$

c. Hanani三元填充与最优码的联系

如下引理给出一个对任意$q\geq 2$，构造最优$(n,5,3)_q$码的方法。

引理 7.10. *如果存在一个强$HTP(n)$，那么对任意$q \geq 2$，$A_q(n,5,3) = \min\left\{\lfloor (q-1)n/3 \rfloor, D(n,3,2)\right\}$。*

证明. 首先，我们证明$q \leq \lfloor \frac{n-1}{2} \rfloor + 1$的情况。

当$n \equiv 0 \pmod 3$时，一个强HTP(n)恰好有h个MPPC $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_h$。对任意$q \in [2, h+1]$，令$\mathcal{C}_q = \bigcup_{i=1}^{q-1} \mathcal{C}(\mathcal{P}_i, i)$。很容易验证$\mathcal{C}_q$就是最优$(n,5,3)_q$码。

当$n \equiv 1 \pmod 3$，一个强HTP(n)有h个MPPC $\mathcal{P}_i$，$i \in [h]$，和一个有t个区组的PPC $\mathcal{P}_{h+1}$。令$\{x_i\} = \overline{\mathcal{P}_i}$，$i \in [h]$。对任意$s \in [h]$，若$s$被3整除，定义一个支撑集为$\{x_{s-2}, x_{s-1}, x_s\}$的码字$\mathsf{u}^s$，其中对任意$i \in [s-2, s]$，$\mathsf{u}^s_{x_i} = i$。令$\mathcal{C}_2 = \mathcal{C}(\mathcal{P}_1, 1)$。对任意$q \in [3, h+1]$，定义

$$\mathcal{C}_q = \begin{cases} \mathcal{C}_{q-1} \cup \mathcal{C}(\mathcal{P}_{q-1}, q-1), & \text{若} q \not\equiv 1 \pmod 3, \\ \mathcal{C}_{q-1} \cup \mathcal{C}(\mathcal{P}_{q-1}, q-1) \cup \{\mathsf{u}^{q-1}\}, & \text{否则。} \end{cases}$$

由强Hanani三元填充的第一个性质，每个$\mathcal{C}_q$都是一个最优$(n,5,3)_q$码。

当$n \equiv 2 \pmod 3$，一个强HTP(n)有$h+1$个MPPC $\mathcal{P}_i$，$i \in [h+1]$，其中如果$n \equiv 2 \pmod 6$，$\mathcal{P}_{h+1}$是最大的，如果$n \equiv 5 \pmod 6$，$\mathcal{P}_{h+1}$是非最大的。假设$\{a_{i,1}, a_{i,2}\}$是$\overline{\mathcal{P}_i}$，$i \in [h]$中的有序点对。对任意$s \in [h]$，定义一个码字u^s，其中它的支撑集为

$$\mathrm{supp}(\mathsf{u}^s) = \begin{cases} \{a_{s,1}, a_{s,2}, a_{s+1,1}\}, & \text{若} s \equiv 1 \pmod 3, \\ \{a_{s-1,1}, a_{s,1}, a_{s+1,1}\}, & \text{若} s \equiv 2 \pmod 3, \\ \{a_{s-2,2}, a_{s-1,2}, a_{s,2}\}, & \text{若} s \equiv 0 \pmod 3。 \end{cases}$$

而且$\mathsf{u}^s_{a_{i,j}} = i$，$i \in [s-2, s+1]$。令$\mathcal{C}_2 = \mathcal{C}(\mathcal{P}_1, 1)$。对任意$q \in [3, h+1]$，除了$n \equiv 5 \pmod 6$，$q = h+1$，定义

$$\mathcal{C}_q = \begin{cases} \mathcal{C}_{q-1} \cup \mathcal{C}(\mathcal{P}_{q-1}, q-1) \cup \{\mathsf{u}^{q-2}\}, & \text{若} q \equiv 0 \pmod 3, \\ \mathcal{C}_{q-1} \cup \mathcal{C}(\mathcal{P}_{q-1}, q-1) \cup \{\mathsf{u}^{q-2}, \mathsf{u}^{q-1}\} \setminus \{\mathsf{u}^{q-3}\}, & \text{若} q \equiv 1 \pmod 3, \\ \mathcal{C}_{q-1} \cup \mathcal{C}(\mathcal{P}_{q-1}, q-1), & \text{若} q \equiv 2 \pmod 3。 \end{cases}$$

对$n \equiv 5 \pmod 6$，$q = h+1$，定义$\mathcal{C}_q = \mathcal{C}_{q-1} \cup \mathcal{C}(\mathcal{P}_{q-1}, q-1)$。那么$\mathcal{C}_q$就是最优$(n,5,3)_q$码。

由定义，一个强HTP(n)也是一个最优$(n,3,1)$-填充，并且所有区组在构造中都用到。所以由引理7.3，对任意$q > \lfloor \frac{n-1}{2} \rfloor + 1$，都不能有更多的码字。　□

在本节结束之前，我们将利用例7.7–7.9给出引理7.10的例子。

例 7.11. 对$n=8$，取：

- $\mathcal{C}_2=\mathcal{C}(\mathcal{P}_1,1)=\{01000110,00101001\}$；
- $\mathcal{C}_3=\mathcal{C}_2\cup\mathcal{C}(\mathcal{P}_2,2)\cup\{\mathsf{u}^1\}$，其中$\mathsf{u}^1$是一个$\mathsf{u}^1_0=1$，$\mathsf{u}^1_3=1$，$\mathsf{u}^1_1=2$，对任意其余$x\in X$，$\mathsf{u}^1_x=0$的码字，即$\mathcal{C}_3=\mathcal{C}_2\cup\{00220020,20000202,12010000\}$；
- $\mathcal{C}_4=(\mathcal{C}_3\backslash\{\mathsf{u}^1\})\cup\mathcal{C}(\mathcal{P}_3,3)\cup\{\mathsf{u}^2,\mathsf{u}^3\}$，其中$\mathcal{C}(\mathcal{P}_3,3)=\{30003030,03030003\}$，$\mathsf{u}^2=12300000$，$\mathsf{u}^3=00012300$。

很容易验证，对任意$q\in[2,4]$，$\mathcal{C}_q$都是所需最优$(8,5,3)_q$码。

在下面两个例子中，我们将省略$\mathcal{C}(\mathcal{P}_i,i)$中的码字。

例 7.12. 对$n=10$，取$\mathcal{C}_2=\mathcal{C}(\mathcal{P}_1,1)$；$\mathcal{C}_3=\mathcal{C}_2\cup\mathcal{C}(\mathcal{P}_2,2)$；$\mathcal{C}_4=\mathcal{C}_3\cup\mathcal{C}(\mathcal{P}_3,3)\cup\{\mathsf{u}^3\}$，其中$\mathsf{u}^3=0000000123$；$\mathcal{C}_5=\mathcal{C}_4\cup\mathcal{C}(\mathcal{P}_4,4)$。很容易验证，对任意$q\in[2,5]$，$\mathcal{C}_q$就是所需最优$(10,5,3)_q$码。

例 7.13. 对$n=17$，取$\mathcal{C}_2=\mathcal{C}(\mathcal{P}_1,1)$；$\mathcal{C}_3=\mathcal{C}_2\cup\mathcal{C}(\mathcal{P}_2,2)\cup\{\mathsf{u}^1\}$，其中$\mathsf{u}^1=11002000000000000$；$\mathcal{C}_4=(\mathcal{C}_3\backslash\{\mathsf{u}^1\})\cup\mathcal{C}(\mathcal{P}_3,3)\cup\{\mathsf{u}^2,\mathsf{u}^3\}$，其中$\mathsf{u}^2=10002000300000000$，$\mathsf{u}^3=01000200030000000$；$\mathcal{C}_5=\mathcal{C}_4\cup\mathcal{C}(\mathcal{P}_4,4)$；$\mathcal{C}_6=\mathcal{C}_5\cup\mathcal{C}(\mathcal{P}_5,5)\cup\{\mathsf{u}^4\}$，其中$\mathsf{u}^4=00440050000000000$；$\mathcal{C}_7=(\mathcal{C}_6\setminus\{\mathsf{u}^4\})\cup\mathcal{C}(\mathcal{P}_6,6)\cup\{\mathsf{u}^5,\mathsf{u}^6\}$，其中$\mathsf{u}^5=00400050006000000$，$\mathsf{u}^6=00040005000600000$；$\mathcal{C}_8=\mathcal{C}_7\cup\mathcal{C}(\mathcal{P}_7,7)$；$\mathcal{C}_9=\mathcal{C}_8\cup\mathcal{C}(\mathcal{P}_8,8)$。很容易验证，对任意$q\in[2,9]$，$\mathcal{C}_q$就是所需最优$(17,5,3)_q$码。

7.3 强Hanani三元填充的存在性

在本节中，我们将建立强Hanani三元填充的存在性。显然，当$n\le5$时，强HTP(n)的存在性是平凡的。

一个*k-frame*就是一个$\{k\}$-GDD $(X,\mathcal{G},\mathcal{B})$，使得$\mathcal{B}$可以分成一些PPC的集合，且每个PPC的补是GDD的某个组。

引理 7.14 ([41]). 下面3-*frame*都存在：

(1) 型为h^u，$u\ge4$，$h\equiv0\pmod2$，$h(u-1)\equiv0\pmod3$，

(2) 型为12^um^1，$u\ge4$，$m\in\{6,18\}$。

a. 当$n \equiv 0 \pmod 3$**时**

显然，当$n = 6t + 3$，$t \geq 0$时，一个KTS$(6t + 3)$就是一个HTP$(6t + 3)$；当$n = 6t$，$t \geq 3$时，一个型为2^{3t}的$\{3\}$-RGDD就是一个HTP$(6t)$，并且都是强的。由引理2.12，我们得到下面结果。

推论 7.15. *令*$n \equiv 0 \pmod 3$*。那么存在一个*$HTP(n)$*当且仅当*$n \notin \{6, 12\}$*。*

b. 当$n \equiv 1 \pmod 6$**时**

令$v = 6t + 1$，一个阶数为v的Hanani三元填充也是一个型为1^{6t+1}的$\{3\}$-GDD，且区组可以划分成$3t$个MPPC，和一个具有t的区组的PPC。这样的设计也称为一个*Hanani三元系*。

引理 7.16 (Vanstone等[140])**.** *一个阶数为*n*的Hanani三元系存在当且仅当*$n \equiv 1 \pmod 6$，$n \notin \{7, 13\}$*。*

下面推论说明一个Hanani三元系就是一个强Hanani三元填充。

推论 7.17. *令*$n \equiv 1 \pmod 6$*。一个强*$HTP(n)$*存在当且仅当*$n \notin \{7, 13\}$*。*

证明. 令$(X, \mathcal{B})$是一个阶数为$6t + 1$的Hanani三元系，$\mathcal{B}$可以划分成$3t$个MPPC $\mathcal{P}_i$，$i \in [3t]$，和一个有t个区组的PPC $\mathcal{P}_{3t+1}$。如果x是$\mathcal{P}_{3t+1}$中的点，那么x一定被恰好一个$\mathcal{P}_i$，$i \in [3t]$空缺，因为X中的每个点都恰好出现在$3t$个区组中。因此，我们可以重新排列$\mathcal{P}_i$，$i \in [3t]$，使得对任意$s \in [t]$，$\overline{\mathcal{P}_{3s-2}} \cup \overline{\mathcal{P}_{3s-1}} \cup \overline{\mathcal{P}_{3s}}$是$\mathcal{P}_{3t+1}$中的一个区组。 □

c. 当$n \equiv 2 \pmod 6$**时**

显然，一个型为2^{2t+1}的3-frame就是一个HTP$(6t+2)$。为了得到强HTP$(6t+2)$，我们需要下面结果。

引理 7.18. *存在强*$HTP(20)$*。*

证明. 令$X = \mathbb{Z}_{18} \cup \{\infty_0, \infty_1\}$，我们在$X$上构造一个强HTP(20)。我们在下面列出了MPPC $\mathcal{P}_1, \mathcal{P}_4, \mathcal{P}_7$，和相应的空缺的点。对任意$i \in \{2, 3, 5, 6, 8, 9\}$，

MPPC $\mathcal{P}_i$，可以通过对$\mathcal{P}_{i-1}$在$\mathbb{Z}_{18}$中加6得到，$\overline{\mathcal{P}_i}$也是用同样的方法得到。最后一个PPC是$\mathcal{P}_{10} = \{\{0,6,12\} + i : i = 0,1,\ldots,5\}$。

$\mathcal{P}_1 = \{\{14,7,\infty_0\},\{10,15,\infty_1\},\{5,16,8\},\{1,3,11\},\{2,12,4\},\{13,6,17\}\}$，　$\overline{\mathcal{P}_1} = \{0,9\}$；
$\mathcal{P}_4 = \{\{16,9,\infty_0\},\{17,1,\infty_1\},\{14,13,10\},\{0,4,5\},\{7,3,6\},\{8,12,15\}\}$，　$\overline{\mathcal{P}_4} = \{2,11\}$；
$\mathcal{P}_7 = \{\{6,5,\infty_0\},\{12,14,\infty_1\},\{8,9,11\},\{4,17,3\},\{0,16,13\},\{7,2,15\}\}$，　$\overline{\mathcal{P}_7} = \{1,10\}$。

□

引理 7.19. *对任意$t \neq 2$，存在一个强$HTP(6t+2)$。*

证明. 对$t \in \{1,3\}$，由例7.7和引理7.18，存在强HTP$(6t+2)$。

对任意$t \geq 4$，从引理7.14取一个型为6^t的3-frame $(X,\mathcal{G},\mathcal{B})$，其中$X = \mathbb{Z}_6 \times [t]$，$\mathcal{G} = \{\mathbb{Z}_6 \times \{i\} : i \in [t]\}$，$\mathcal{B}$可以划分成PPC $\mathcal{P}_i$，$i \in [3t]$。假设$\mathcal{P}_{3i-2}$，$\mathcal{P}_{3i-1}$，$\mathcal{P}_{3i}$是空缺组$\mathbb{Z}_6 \times \{i\}$，$i \in [t]$的PPC。增加两个无穷点$\{\infty_0,\infty_1\}$。对任意$i \in [t]$，在$(\mathbb{Z}_6 \times \{i\}) \cup \{\infty_0,\infty_1\}$上构造一个强HTP(8)，其中MPPC为$\mathcal{P}_1^i$，$\mathcal{P}_2^i$，$\mathcal{P}_3^i$，$\mathcal{P}_4^i$，使得$\overline{\mathcal{P}_4^i} = \{\infty_0,\infty_1\}$。令$\mathcal{P}'_{j+3(i-1)} = \mathcal{P}_{j+3(i-1)} \cup \mathcal{P}_j^i$，$i \in [t]$，$j \in [3]$。进一步，令$\mathcal{P}'_{3t+1} = \cup_{i=1}^t \mathcal{P}_4^i$。那么$(X \cup \{\infty_0,\infty_1\}, \cup_{i=1}^{3t+1} \mathcal{P}'_i)$就是所需设计。 □

d. 当$n \equiv 4 \pmod 6$时

引理 7.20. *对任意$t \in [2,7]$，存在一个强$HTP(6t+4)$。*

证明. 对任意$t \in [2,7]$，我们在$\mathbb{Z}_{6t} \cup \{\infty_0,\infty_1,\infty_2,\infty_3\}$上构造一个强HTP$(6t+4)$。其中，对任意$t$，我们在下面列出MPPC $\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3$。对任意$i \in [3]$，$s \in [t-1]$，MPPC $\mathcal{P}_{i+3s}$是由$\mathcal{P}_i$在$\mathbb{Z}_{6t}$中加$6s$得到。$\mathcal{P}_{3t+1} = \{\{0,2t,4t\} + i : i = 0,1,\ldots,2t-1\} \cup \{\{\infty_1,\infty_2,\infty_3\}\}$。每个MPPC包含一个点，且$\overline{\mathcal{P}_{3i-2}} \cup \overline{\mathcal{P}_{3i-1}} \cup \overline{\mathcal{P}_{3i}}$，$i \in [t]$形成最后一个PPC $\mathcal{P}_{3t+2}$的t个区组。

$t = 2$：
$\mathcal{P}_1 = \{9,2,\infty_0\}\{3,10,\infty_1\}\{7,8,\infty_2\}\{4,5,\infty_3\}\{6,11,1\}$；
$\mathcal{P}_2 = \{10,7,\infty_0\}\{1,0,\infty_1\}\{11,4,\infty_2\}\{8,6,\infty_3\}\{2,3,5\}$；
$\mathcal{P}_3 = \{0,11,\infty_0\}\{5,8,\infty_1\}\{9,6,\infty_2\}\{3,1,\infty_3\}\{2,4,7\}$。

$t = 3$：
$\mathcal{P}_1 = \{5,13,\infty_0\}\{2,7,\infty_1\}\{3,16,\infty_2\}\{14,4,\infty_3\}\{8,6,1\}\{9,10,17\}\{15,11,12\}$；
$\mathcal{P}_2 = \{14,15,\infty_0\}\{6,3,\infty_1\}\{5,8,\infty_2\}\{12,17,\infty_3\}\{2,1,9\}\{4,0,7\}\{13,16,11\}$；
$\mathcal{P}_3 = \{10,12,\infty_0\}\{17,16,\infty_1\}\{6,7,\infty_2\}\{13,9,\infty_3\}\{1,3,5\}\{15,2,4\}\{11,8,0\}$。

$t = 4$：

$\mathcal{P}_1 = \{16,7,\infty_0\}\{18,21,\infty_1\}\{6,8,\infty_2\}\{4,3,\infty_3\}\{9,13,23\}\{2,20,22\}\{12,17,19\}\{15,1,14\}$
$\{10,5,11\}$；
$\mathcal{P}_2 = \{9,18,\infty_0\}\{5,16,\infty_1\}\{4,11,\infty_2\}\{1,12,\infty_3\}\{7,2,6\}\{13,20,17\}\{0,19,10\}\{15,22,8\}$
$\{23,14,3\}$；
$\mathcal{P}_3 = \{14,5,\infty_0\}\{19,20,\infty_1\}\{17,0,6\}\{1,3,\infty_2\}\{8,11,\infty_3\}\{9,15,4\}\{10,7,13\}\{21,12,2\}$
$\{22,18,16\}$。

$t=5$：
$\mathcal{P}_1 = \{20,28,\infty_0\}\{17,3,\infty_1\}\{25,8,\infty_2\}\{19,24,\infty_3\}\{11,12,29\}\{10,16,15\}\{22,6,18\}\{0,1,13\}$
$\{26,9,27\}\{7,5,14\}\{21,23,4\}$；
$\mathcal{P}_2 = \{23,1,\infty_0\}\{20,22,\infty_1\}\{6,17,\infty_2\}\{4,15,\infty_3\}\{25,26,18\}\{21,0,27\}\{7,11,10\}\{9,2,13\}$
$\{14,8,12\}\{16,19,28\}\{3,29,24\}$；
$\mathcal{P}_3 = \{21,18,\infty_0\}\{13,24,\infty_1\}\{22,15,\infty_2\}\{29,2,\infty_3\}\{1,9,7\}\{0,28,6\}\{26,5,12\}\{4,20,8\}$
$\{19,14,3\}\{16,11,25\}\{17,10,23\}$。

$t=6$：
$\mathcal{P}_1 = \{27,7,\infty_0\}\{35,18,\infty_1\}\{26,10,\infty_2\}\{14,17,\infty_3\}\{13,23,15\}\{20,9,29\}\{34,4,11\}\{16,6,5\}$
$\{32,31,2\}\{8,12,21\}\{1,24,30\}\{33,22,3\}\{28,25,19\}$；
$\mathcal{P}_2 = \{17,26,\infty_0\}\{14,1,\infty_1\}\{27,28,\infty_3\}\{3,25,\infty_2\}\{0,8,19\}\{35,20,34\}\{12,10,2\}\{5,11,7\}$
$\{33,18,23\}\{16,30,31\}\{32,29,15\}\{24,13,21\}\{22,6,9\}$；
$\mathcal{P}_3 = \{4,12,\infty_0\}\{22,15,\infty_1\}\{6,17,\infty_2\}\{31,0,\infty_3\}\{21,23,30\}\{19,34,2\}\{29,10,13\}\{20,5,18\}$
$\{7,3,35\}\{28,26,33\}\{24,8,9\}\{1,32,27\}\{16,25,11\}$。

$t=7$：
$\mathcal{P}_1 = \{29,40,\infty_0\}\{36,38,\infty_1\}\{25,22,\infty_2\}\{19,12,\infty_3\}\{27,24,30\}\{34,1,10\}\{39,7,17\}\{16,32,13\}$
$\{11,4,6\}\{2,31,14\}\{33,9,26\}\{20,28,21\}\{5,35,8\}\{15,23,41\}\{0,37,18\}$；
$\mathcal{P}_2 = \{33,14,\infty_0\}\{39,41,\infty_1\}\{27,32,\infty_2\}\{3,16,\infty_3\}\{37,38,12\}\{26,15,31\}\{5,36,10\}\{25,21,19\}$
$\{28,13,11\}\{40,8,30\}\{1,9,0\}\{24,17,4\}\{20,22,2\}\{7,23,29\}\{35,18,6\}$；
$\mathcal{P}_3 = \{7,18,\infty_0\}\{10,25,\infty_1\}\{36,17,\infty_2\}\{8,11,\infty_3\}\{23,31,19\}\{34,15,40\}\{13,2,37\}\{14,5,6\}$
$\{27,39,12\}\{38,0,32\}\{4,9,3\}\{22,41,26\}\{20,33,29\}\{1,21,30\}\{28,16,24\}$。

□

引理 7.21. *对任意正整数t，存在一个强$HTP(6t+4)$。*

证明. 对$t \le 7$，所需强HTP$(6t+4)$由例7.8和引理7.20构造得到。对$t \ge 8$，我们分两部分构造：

当$t = 2s$，$s \ge 4$时，从引理7.14取一个型为12^s的3-frame $(X, \mathcal{G}, \mathcal{B})$，其中$X = \mathbb{Z}_{12} \times [s]$，$\mathcal{G} = \{\mathbb{Z}_{12} \times \{i\} : i \in [s]\}$，$\mathcal{B}$可以划分成PPC $\mathcal{P}_i$，$i \in [6s]$。假设对任意$i \in [s]$，$\mathcal{P}_j$，$j \in [6i-5, 6i]$是空缺组$\mathbb{Z}_{12} \times \{i\}$ 的6个PPC。令$Y = \{\infty_0, \infty_1, \infty_2, \infty_3\}$。对任意$i \in [s]$，在$(\mathbb{Z}_{12} \times \{i\}) \cup Y$上构造一个强HTP(16)，其中7个MPPC为$\mathcal{P}_j^i$，$j \in [7]$，一个PPC为$\mathcal{P}_8^i$，使得$\{\infty_1, \infty_2, \infty_3\}$是$\mathcal{P}_7^i$中的区组，且$\overline{\mathcal{P}_7^i} = \{\infty_0\}$。令$\mathcal{P}'_{j+6(i-1)} = \mathcal{P}_{j+6(i-1)} \cup \mathcal{P}_j^i$，$i \in [s]$，$j \in [6]$。最后，令$\mathcal{P}'_{6s+1} = \cup_{i=1}^{s} \mathcal{P}_7^i$，$P'_{6s+2} = \cup_{i=1}^{s} \mathcal{P}_8^i$。那么，$(X \cup Y, \cup_{i=1}^{6s+2} \mathcal{P}'_i)$就是所需设计。

当$t=2s+1$，$s\geq 4$时，从引理7.14取一个型为12^s6^1的3-frame $(X,\mathcal{G},\mathcal{B})$，其中$X=(\mathbb{Z}_{12}\times[s])\cup(\mathbb{Z}_6\times\{s+1\})$，$\mathcal{G}=\{\mathbb{Z}_{12}\times\{i\}:i\in[s]\}\cup\{\mathbb{Z}_6\times\{s+1\}\}$，$\mathcal{B}$可以划分成有$4s-2$个区组的PPC $\mathcal{P}_i$，$i\in[6s]$，和有$4s$个区组的PPC $\mathcal{P}_i$，$i\in[6s+1,6s+3]$。假设对任意$i\in[s]$，$\mathcal{P}_j$，$j\in[6i-5,6i]$是空缺组$\mathbb{Z}_{12}\times\{i\}$的PPC $\mathcal{P}_j$，$j\in[6s+1,6s+3]$是空缺组$\mathbb{Z}_6\times\{s+1\}$的PPC。令$Y=\{\infty_0,\infty_1,\infty_2,\infty_3\}$。对任意$i\in[s]$，在$(\mathbb{Z}_{12}\times\{i\})\cup Y$上构造一个强HTP(16)，其中7个MPPC为$\mathcal{P}_j^i$，$j\in[7]$，一个PPC为$\mathcal{P}_8^i$，使得$\{\infty_1,\infty_2,\infty_3\}$是$\mathcal{P}_7^i$中的一个区组，且$\overline{\mathcal{P}_7^i}=\{\infty_0\}$。最后，在$(\mathbb{Z}_6\times\{s+1\})\cup Y$上构造一个强HTP(10)，其中4个MPPC为$\mathcal{P}_j^{s+1}$，$j\in[4]$，一个PPC为$\mathcal{P}_5^{s+1}=\{\infty_1,\infty_2,\infty_3\}$。令$\mathcal{P}'_{j+6(i-1)}=\mathcal{P}_{j+6(i-1)}\cup\mathcal{P}_j^i$，$i\in[s]$，$j\in[6]$；$\mathcal{P}'_{6s+j}=\mathcal{P}_{6s+j}\cup\mathcal{P}_j^{s+1}$，$j\in[3]$；$\mathcal{P}'_{6s+4}=(\cup_{i=1}^s(\mathcal{P}_7^i\setminus\{\{\infty_1,\infty_2,\infty_3\}\}))\cup\mathcal{P}_4^{s+1}$，$\mathcal{P}'_{6s+5}=(\cup_{i=1}^s\mathcal{P}_8^i)\cup\mathcal{P}_5^{s+1}$。那么$(X\cup Y,\cup_{i=1}^{6s+5}\mathcal{P}'_i)$就是所需设计。 □

e. 当$n\equiv 5\pmod 6$时

引理 7.22. *存在一个强HTP(23)。*

证明. 令$X=\mathbb{Z}_{18}\cup\{\infty_0,\infty_1,\infty_2,\infty_3,\infty_4\}$。我们在下面列出了MPPC $\mathcal{P}_i$，$i\in\{1,4,7\}$和相应的集合$\overline{\mathcal{P}_i}$。对$i\in\{2,3,5,6,8,9\}$，MPPC $\mathcal{P}_i$可以由$\mathcal{P}_{i-1}$在$\mathbb{Z}_{18}$中加6得到，$\overline{\mathcal{P}_i}$可以用相同的方法得到。令$\mathcal{P}_{10}=\{\{14,10,13\}+6i,\{17,9,6\}+6i:i=0,1,2\}\cup\{\{\infty_0,\infty_1,\infty_2\}\}$，$\mathcal{P}_{11}=\{\{8,10,0\}+6i,\{1,3,5\}+6i:i=0,1,2\}\cup\{\{\infty_0,\infty_3,\infty_4\}\}$。最后令$\mathcal{P}_{12}=\{\{0,6,12\}+i:i=0,1,\ldots,5\}$。

$\mathcal{P}_1=\{\{0,1,\infty_0\},\{16,8,\infty_1\},\{4,5,\infty_2\},\{11,13,\infty_3\},\{7,12,\infty_4\},\{14,17,3\},\{15,2,6\}\}$，
$\overline{\mathcal{P}_1}=\{9,10\}$；
$\mathcal{P}_4=\{\{14,11,\infty_0\},\{7,3,\infty_1\},\{9,12,\infty_2\},\{6,8,\infty_3\},\{10,15,\infty_4\},\{4,17,0\},\{5,13,16\}\}$，
$\overline{\mathcal{P}_4}=\{1,2\}$；
$\mathcal{P}_7=\{\{3,4,\infty_0\},\{0,5,\infty_1\},\{8,13,\infty_2\},\{16,9,\infty_3\},\{11,2,\infty_4\},\{12,10,1\},\{7,14,15\}\}$，
$\overline{\mathcal{P}_7}=\{6,17\}$。

□

引理 7.23. *对任意正整数t，$t\notin\{1,4,5,6,7,9\}$，存在一个强HTP$(6t+5)$。*

证明. 对$t\in\{2,3\}$，所需设计在例7.9和引理7.22中构造得到。对$t\geq 8$，$t\neq 9$，我们分两种情况构造：

对$t=2s$，$s\geq 4$，从引理7.14取一个型为12^s的3-frame $(X,\mathcal{G},\mathcal{B})$，其中$X=\mathbb{Z}_{12}\times[s]$，$\mathcal{G}=\{\mathbb{Z}_{12}\times\{i\}:i\in[s]\}$，$\mathcal{B}$可以划分成PPC $\mathcal{P}_i$，$i\in[6s]$。假设$\mathcal{P}_j$，$j\in[6i-5,6i]$是空缺组$\mathbb{Z}_{12}\times\{i\}$，$i\in[s]$的6个PPC。令$Y=\{\infty_0,\infty_1,\infty_2,\infty_3,\infty_4\}$。

对任意$i \in [s]$，在$(\mathbb{Z}_{12} \times \{i\}) \cup Y$上构造一个强HTP(17)，其中8个MPPC为$\mathcal{P}_j^i$，$j \in [8]$，最后一个PPC为$\mathcal{P}_9^i$，使得$\{\infty_0, \infty_1, \infty_2\} \in \mathcal{P}_7^i$，$\overline{\mathcal{P}_7^i} = \{\infty_3, \infty_4\}$，$\{\infty_0, \infty_3, \infty_4\} \in \mathcal{P}_8^i$，$\overline{\mathcal{P}_8^i} = \{\infty_1, \infty_2\}$。令$\mathcal{P}'_{j+6(i-1)} = \mathcal{P}_{j+6(i-1)} \cup \mathcal{P}_j^i$，$i \in [s]$，$j \in [6]$，$\mathcal{P}'_{6s+1} = \cup_{i=1}^s \mathcal{P}_7^i$，$\mathcal{P}'_{6s+2} = \cup_{i=1}^s \mathcal{P}_8^i$，$\mathcal{P}'_{6s+3} = \cup_{i=1}^s \mathcal{P}_9^i$。那么$(X \cup Y, \cup_{i=1}^{6s+3} \mathcal{P}'_i)$就是所需设计。

对$t = 2(s+1)+1$，$s \geq 4$，从引理7.14取一个型为$12^s 18^1$的3-frame $(X, \mathcal{G}, \mathcal{B})$，其中$X = (\mathbb{Z}_{12} \times [s]) \cup (\mathbb{Z}_{18} \times \{s+1\})$，$\mathcal{G} = \{\mathbb{Z}_{12} \times \{i\} : i \in [s]\} \cup \{\mathbb{Z}_{18} \times \{s+1\}\}$，$\mathcal{B}$可以划分成有$4s+2$个区组的PPC $\mathcal{P}_i$，$i \in [6s]$，和有$4s$个区组的PPC $\mathcal{P}_i$，$i \in [6s+1, 6s+9]$。假设对任意$i \in [s]$，$\mathcal{P}_j$，$j \in [6i-5, 6i]$是空缺组$\mathbb{Z}_{12} \times \{i\}$ 的PPC $\mathcal{P}_j$，$j \in [6s+1, 6s+9]$是空缺组$\mathbb{Z}_{18} \times \{s+1\}$的PPC。令$Y = \{\infty_0, \infty_1, \infty_2, \infty_3, \infty_4\}$。对任意$i \in [s]$，在$(\mathbb{Z}_{12} \times \{i\}) \cup Y$上构造一个强HTP(17)，其中8个MPPC为$\mathcal{P}_j^i$，$j \in [8]$，最后一个PPC为$\mathcal{P}_9^i$，使得$\{\infty_0, \infty_1, \infty_2\} \in \mathcal{P}_7^i$，$\overline{\mathcal{P}_7^i} = \{\infty_3, \infty_4\}$，$\{\infty_0, \infty_3, \infty_4\} \in \mathcal{P}_8^i$，$\overline{\mathcal{P}_8^i} = \{\infty_1, \infty_2\}$。最后在$(\mathbb{Z}_{18} \times \{s+1\}) \cup Y$上构造一个强HTP(23)，其中11个MPPC为$\mathcal{P}_j^{s+1}$，$j \in [11]$，最后一个PPC为$\mathcal{P}_{12}^{s+1}$使得$\{\infty_0, \infty_1, \infty_2\} \in \mathcal{P}_{10}^{s+1}$，$\overline{\mathcal{P}_{10}^{s+1}} = \{\infty_3, \infty_4\}$，$\{\infty_0, \infty_3, \infty_4\} \in \mathcal{P}_{11}^{s+1}$，$\overline{\mathcal{P}_{11}^{s+1}} = \{\infty_1, \infty_2\}$。令$\mathcal{P}'_{j+6(i-1)} = \mathcal{P}_{j+6(i-1)} \cup \mathcal{P}_j^i$，$i \in [s]$，$j \in [6]$；$\mathcal{P}'_{6s+j} = \mathcal{P}_{6s+j} \cup \mathcal{P}_j^{s+1}$，$j \in [9]$；$\mathcal{P}'_{6s+j} = (\cup_{i=1}^s \mathcal{P}_{j-3}^i) \cup \mathcal{P}_j^{s+1}$，$j \in \{10, 11\}$；$\mathcal{P}'_{6s+12} = \cup_{i=0}^s \mathcal{P}_9^i \cup \mathcal{P}_{12}^{s+1}$。那么$(X \cup Y, \cup_{i=1}^{6s+12} \mathcal{P}'_i)$就是所需设计。 □

我们用计算机搜索确定不存在一个HTP(11)。结合推论7.15，引理7.17，引理7.19，引理7.21和引理7.23，我们得到了强Hanani三元填充的存在结果。

定理 7.24. *对任意正整数n，除了确定的值$n \in \{6, 7, 11, 12, 13\}$，和不确定的值$n \in \{14, 29, 35, 41, 47, 59\}$外，都存在一个强$HTP(n)$。*

7.4　$A_q(n, 5, 3)$的确定

对定理7.24中的结果应用引理7.10，我们就得到了对任意$n \notin \{6, 7, 11, 12, 13, 14, 29, 35, 41, 47, 59\}$，$q \geq 2$，$A_q(n, 5, 3) = \left\lfloor \frac{(q-1)n}{3} \right\rfloor$。在这节中，我们将确定剩余的$n$。由推论7.5，我们将只确定当$2 \leq q \leq \lfloor \frac{n-1}{2} \rfloor$时，$A_q(n, 5, 3)$的值。

引理 7.25. *对$n \in \{6, 12\}$，$2 \leq q \leq \lfloor \frac{n-1}{2} \rfloor$，$A_q(n, 5, 3) = \frac{(q-1)n}{3}$。*

证明. 对$n=6$，显然$A_2(6,5,3)=2$。对$n=12$，取一个$\mathbb{Z}_{12}$上的$(12,3,1)$-填充，其中所有区组可以划分成如下四个PC $\mathcal{P}_i$，$i\in[4]$如下：

$$\begin{aligned}
&\mathcal{P}_1=\{\{0,8,7\}+6i,\{9,10,11\}+6i:i=0,1\};\\
&\mathcal{P}_2=\{\{0,1,9\}+6i,\{4,8,11\}+6i:i=0,1\};\\
&\mathcal{P}_3=\{\{5,7,9\}+6i,\{6,8,10\}+6i:i=0,1\};\\
&\mathcal{P}_4=\{\{1,5,8\}+6i,\{0,3,10\}+6i:i=0,1\}。
\end{aligned}$$

对任意$q\in[2,5]$，$\mathcal{C}_q=\cup_{i=1}^{q-1}\mathcal{C}(\mathcal{P}_i,i)$是一个最优$(12,5,3)_q$码。因此对任意$q\in[2,5]$，$A_q(12,5,3)=4(q-1)$。 □

引理 7.26. 对$n\in\{7,13\}$，$2\le q\le\lfloor\frac{n-1}{2}\rfloor$，$A_q(n,5,3)=\lfloor\frac{(q-1)n}{3}\rfloor$。

证明. 对$n=7$，显然$A_2(7,5,3)=2$。我们可以构造一个最优$(7,5,3)_3$码，$\mathcal{C}_3=\{1110000,2000110,0020021,0200202\}$，所以$A_3(7,5,3)=4$。

对$n=13$，在$\mathbb{Z}_{13}$上构造一个$(13,3,1)$-填充，其中所有区组可以划分成5个MPPC $\mathcal{P}_i$，$i\in[5]$和一个PPC $\mathcal{P}_6=\{\{0,1,2\}\}$。注意到$\mathcal{P}_i$，$i\in[3]$ 空缺的点分别为$0,1,2$。

$$\begin{aligned}
&\mathcal{P}_1=\{\{5,8,9\},\{1,3,6\},\{2,4,7\},\{12,11,10\}\};\\
&\mathcal{P}_2=\{\{0,3,7\},\{4,12,8\},\{11,6,5\},\{2,9,10\}\};\\
&\mathcal{P}_3=\{\{3,9,12\},\{1,5,7\},\{8,10,6\},\{11,4,0\}\};\\
&\mathcal{P}_4=\{\{12,6,7\},\{2,8,3\},\{10,0,5\},\{9,1,11\}\};\\
&\mathcal{P}_5=\{\{9,0,6\},\{11,7,8\},\{5,2,12\},\{1,4,10\}\}。
\end{aligned}$$

这里，对任意$q\in\{2,3\}$，令$\mathcal{C}_q=\cup_{i=1}^{q-1}\mathcal{C}(\mathcal{P}_i,i)$。对任意$q\in\{4,5,6\}$，令$\mathcal{C}_q=\cup_{i=1}^{q-1}\mathcal{C}(\mathcal{P}_i,i)\cup\{\mathsf{u}\}$，其中$\mathsf{u}=1230000000000$。很容易验证对任意$q\in[2,6]$，$\mathcal{C}_q$就是最优$(13,5,3)_q$码。 □

引理 7.27. 对任意$2\le q\le 5$，$A_q(11,5,3)=\lfloor(q-1)11/3\rfloor$。

证明. 在$\mathbb{Z}_{11}$上构造一个$(11,3,1)$-填充，其中所有区组可以划分成如下4个MPPC。

$$\begin{aligned}
&\mathcal{P}_1=\{\{1,8,0\},\{3,6,9\},\{5,7,10\}\};\\
&\mathcal{P}_2=\{\{1,6,7\},\{3,8,10\},\{4,9,0\}\};\\
&\mathcal{P}_3=\{\{1,4,5\},\{2,6,8\},\{3,7,0\}\};\\
&\mathcal{P}_4=\{\{1,2,3\},\{4,7,8\},\{5,6,0\}\}。
\end{aligned}$$

令$\mathsf{u}^1=00101200000$，$\mathsf{u}^2=00201000003$，$\mathsf{u}^3=00100200030$。定义$\mathcal{C}_2=\mathcal{C}(\mathcal{P}_1,1)$，$\mathcal{C}_3=\cup_{i=1}^{2}\mathcal{C}(\mathcal{P}_i,i)\cup\{\mathsf{u}^1\}$；对$q\in\{4,5\}$，$\mathcal{C}_q=\cup_{i=1}^{q-1}\mathcal{C}(\mathcal{P}_i,i)\cup\{\mathsf{u}^2,\mathsf{u}^3\}$。那么对任意$q\in[2,5]$，$\mathcal{C}_q$就是最优$(11,5,3)_q$码。 □

引理 7.28. 对任意$2 \le q \le 6$，$A_q(14,5,3) = \lfloor (q-1)14/3 \rfloor$。

证明. 在$\mathbb{Z}_{14}$上构造一个$(14,3,1)$-填充，其中所有区组可以划分成如下5个MPPC和一个PPC $\mathcal{P}_6 = \{\{0,4,8\},\{6,10,2\}\}$。

$$\begin{aligned}
\mathcal{P}_1 &= \{\{4,11,12\},\{10,5,13\},\{2,9,7\},\{3,8,1\}\};\\
\mathcal{P}_2 &= \{\{0,9,12\},\{1,2,13\},\{5,3,6\},\{11,7,8\}\};\\
\mathcal{P}_3 &= \{\{1,6,12\},\{0,7,13\},\{4,5,9\},\{3,11,10\}\};\\
\mathcal{P}_4 &= \{\{10,8,12\},\{3,4,13\},\{6,11,9\},\{0,5,2\}\};\\
\mathcal{P}_5 &= \{\{2,3,12\},\{8,9,13\},\{0,1,10\},\{4,6,7\}\}。
\end{aligned}$$

很容易验证构造的$(14,3,1)$-填充，满足强Hanani三元填充的两个性质。所以对任意$q \in [2,6]$，我们得到了最优$(14,5,3)_q$码。 □

引理 7.29. 对任意$n \equiv 5 \pmod 6$，$n \ge 17$，$A_q(n,5,3) = \lfloor (q-1)n/3 \rfloor$，其中$q = \lfloor (n-1)/2 \rfloor$。

证明. 令$n = 6t+5$，其中$t \ge 2$。从文[41]中取一个型为$3^{2t}5^1$的$\{3\}$-GDD $(X,\mathcal{G},\mathcal{B})$，其中$X = \mathbb{Z}_{3t} \cup \{\infty_0,\ldots,\infty_4\}$，$\{\infty_0,\ldots,\infty_4\}$是最后一个组。那么$\mathcal{B} \cup \{\{\infty_0,\infty_1,\infty_2\}\}$就是一个区组个数为$6t^2+7t+1 = \lfloor (q-1)n/3 \rfloor$的$(n,3,1)$-填充。那么最优码可以用与引理7.4中相同的方法构造，因为每个点最多出现在$3t+1$个区组中。 □

引理 7.30. 对任意$n \in \{29,35,47\}$，$2 \le q \le \lfloor (n-1)/2 \rfloor$，$A_q(n,5,3) = \lfloor (q-1)n/3 \rfloor$。

证明. 令$n = 6t+5$，$t \in \{4,5,7\}$。我们在$X = \mathbb{Z}_{6t} \cup \{\infty_0,\ldots,\infty_4\}$上构造一个$(n,3,1)$-填充，其中所有区组可以划分成$3t$个MPPC $\mathcal{P}_i$，$i \in [3t]$，和一个PPC $\mathcal{P}_{3t+1} = \{\{0,2t,4t\}+i : i = 0,1,\ldots,2t-1\}$。

对任意n，我们在下面列出第一个MPPC $\mathcal{P}_1$。对任意$i \in [t-1]$，$\mathcal{P}_{3i+1}$可以由$\mathcal{P}_1$在$\mathbb{Z}_{6t}$中加$2i$得到，$\mathcal{P}_{i+1}$可以由$\mathcal{P}_i$ 在$\mathbb{Z}_{6t}$中加$2t$得到。$\overline{\mathcal{P}_i}$也由同样的方法得到。

29 : $\{2,4,7\}\{3,5,6\}\{8,17,\infty_0\}\{9,15,19\}\{10,16,20\}\{11,22,\infty_1\}\{12,23,\infty_2\}\{13,18,\infty_3\}$
$\{14,21,\infty_4\}$

35 : $\{2,4,7\}\{8,12,19\}\{9,20,\infty_0\}\{10,23,27\}\{11,26,\infty_1\}\{3,5,6\}\{13,18,\infty_2\}\{14,22,28\}$
$\{15,21,29\}\{16,25,\infty_3\}\{17,24,\infty_4\}$

47 : $\{2,4,7\}\{8,12,18\}\{9,13,19\}\{10,17,32\}\{24,39,\infty_0\}\{11,27,36\}\{14,33,\infty_2\}\{15,26,34\}$
$\{16,28,37\}\{20,31,38\}\{3,5,6\}\{21,29,41\}\{22,35,\infty_3\}\{23,40,\infty_4\}\{25,30,\infty_1\}$

很容易验证构造的$(n,3,1)$-填充，$n\in\{29,35,41\}$满足强Hanani三元填充的两个性质。因此，我们可以用引理7.10中的方法来对任意$q\in[2,3t+1]$，构造最优$(n,5,3)_q$码$\mathcal{C}_q$。当$q=3t+2$，最优码由引理7.29得到。 □

引理 7.31. 对任意$2\le q\le 20$，$A_q(41,5,3)=\lfloor(q-1)41/3\rfloor$。

证明. 令$X=\mathbb{Z}_{36}\cup\{\infty_0,\ldots,\infty_4\}$。我们在$X$上构造一个$(41,3,1)$-填充，其中区组可以划分成18个MPPC $\mathcal{P}_i$，$i\in[18]$，和一个PPC $\mathcal{P}_{19}=\{\{0,12,24\}+i:i=0,1,\ldots,11\}$。我们在下面列出MPPC $\mathcal{P}_1$，$\mathcal{P}_{10}$，其中它们分别空缺$\{0,1\}$和$\{2,3\}$。

$$\begin{aligned}\mathcal{P}_1=\ & \{\{\infty_0,2,4\},\{\infty_1,3,5\},\{\infty_2,6,9\},\{\infty_3,7,8\},\{\infty_4,10,15\},\{11,14,18\},\{12,16,19\},\\ & \{13,17,20\},\{21,26,35\},\{22,29,30\},\{23,28,33\},\{24,32,34\},\{25,27,31\}\};\\ \mathcal{P}_{10}=\ & \{\{\infty_0,1,11\},\{\infty_1,0,14\},\{\infty_2,12,35\},\{\infty_3,17,34\},\{\infty_4,4,21\},\{5,18,28\},\\ & \{6,19,27\},\{7,16,25\},\{8,23,29\},\{9,20,31\},\{10,24,30\},\{13,22,33\},\{15,26,32\}\}。\end{aligned}$$

对任意$i\in\{1,2\}$，$j\in\{1,10\}$，$\mathcal{P}_{3i+j}$是由$\mathcal{P}_j$在$\mathbb{Z}_{36}$中加$4i$得到。对任意$i\in\{0,1,\ldots,5\}$，$j\in\{2,3\}$，$\mathcal{P}_{3i+j}$是由$\mathcal{P}_{3i+j-1}$在$\mathbb{Z}_{36}$中加12得到。对任意$i\in[18]\setminus\{1,10\}$，$\overline{\mathcal{P}_i}$是由$\overline{\mathcal{P}_1}$或$\overline{\mathcal{P}_{10}}$的顺序决定。

很容易验证这个$(41,3,1)$-填充满足强Hanani三元填充的两个性质，因此我们可以用引理7.30中类似的方法对任意$q\in[2,19]$，构造最优q元码。当$q=20$时，最优码由引理7.29得到。 □

引理 7.32. 对任意$2\le q\le 29$，$A_q(59,5,3)=\lfloor(q-1)59/3\rfloor$。

证明. 从引理7.14取一个型为12^46^1的3-frame $(X,\mathcal{G},\mathcal{B})$，其中$X=(\mathbb{Z}_{12}\times[4])\cup(\mathbb{Z}_6\times\{5\})$，$\mathcal{G}=\{\mathbb{Z}_{12}\times\{i\}:i\in[4]\}\cup\{\mathbb{Z}_6\times\{5\}\}$，$\mathcal{B}$可以划分成有14个区组的PPC $\mathcal{P}_i$，$i\in[24]$，和有16个区组的PPC $\mathcal{P}_i$，$i\in[25,27]$。假设对任意$i\in[4]$，$\mathcal{P}_j$，$j\in[6i-5,6i]$是空缺组$\mathbb{Z}_{12}\times\{i\}$的PPC，$\mathcal{P}_j$，$j\in[25,27]$是空缺组$\mathbb{Z}_6\times\{5\}$的PPC。令$Y=\{\infty_0,\infty_1,\infty_2,\infty_3,\infty_4\}$。对任意$i\in[4]$，在$(\mathbb{Z}_{12}\times\{i\})\cup Y$上构造一个强HTP(17)，其中8个MPPC为$\mathcal{P}_j^i$，$j\in[8]$，一个PPC为$\mathcal{P}_9^i$，且$\{\infty_0,\infty_1,\infty_2\}\in\mathcal{P}_7^i$，$\overline{\mathcal{P}_7^i}=\{\infty_3,\infty_4\}$，$\{\infty_0,\infty_3,\infty_4\}\in\mathcal{P}_8^i$，$\overline{\mathcal{P}_8^i}=\{\infty_1,\infty_2\}$。

令$\mathcal{P}'_{j+6(i-1)}=\mathcal{P}_{j+6(i-1)}\cup\mathcal{P}_j^i$，$i\in[4]$，$j\in[6]$。$\mathcal{P}'_{25}=\cup_{i=1}^s\mathcal{P}_9^i$。那么$(X\cup Y,\cup_{i=1}^{25}\mathcal{P}'_i)$就是一个满足强Hanani三元填充性质的$(59,3,1)$-填充。因此，对任意$q\in[2,25]$，我们可以得到最优$q$元码$\mathcal{C}_q$。

现在我们在$(\mathbb{Z}_6 \times \{5\}) \cup Y$上构造长度为11的最优$k$元码，记为$D_k$，$k \in [2,4]$。对$D_k$的每个非零元加24就得了$D_{k+24}$，其中非零元取值为$[25,27]$。对$q \in [26,28]$，$\mathcal{C}_q = \mathcal{C}_{25} \cup (\cup_{i=25}^{q-1} \mathcal{C}(\mathcal{P}_i, i)) \cup D_q$就是一个最优$(41,5,3)_q$码。对$q=29$，最优码由引理7.29 得到。 □

7.5　Hanani三元填充的存在性

很容易证明当$n \equiv 0,1 \pmod 3$时，一个HTP(n)也是一个强HTP(n)。因此，为了结果的完整性，我们将证明HTP(n)的存在性。

引理 7.33. *存在一个HTP*(29)。

证明. 令$X = \mathbb{Z}_{24} \cup \{\infty_0, \ldots, \infty_4\}$。我们在$X$上构造一个HTP$(29)$，其中区组可以划分成12个MPPC $\mathcal{P}_i$，$i \in [12]$和3个PPC $\mathcal{P}_i$，$i \in [13,15]$。我们在下面列出$\mathcal{P}_i$，$i \in [4]$和$\mathcal{P}_{15}$。$\mathcal{P}_i$，$i \in [5,12]$可以由$\mathcal{P}_{i-4}$在$\mathbb{Z}_{24}$上加8得到。$\mathcal{P}_{13} = \{B+8 : B \in \mathcal{P}_{15}\} \cup \{\{\infty_0, \infty_1, \infty_2\}\}$，$\mathcal{P}_{14} = \{B+16 : B \in \mathcal{P}_{15}\} \cup \{\{\infty_0, \infty_3, \infty_4\}\}$。

$\mathcal{P}_1 = \{\infty_0,2,3\}\{\infty_1,4,5\}\{\infty_2,6,7\}\{\infty_3,8,9\}\{\infty_4,10,12\}\{11,13,14\}\{15,16,19\}\{17,20,22\}\{18,21,23\}$;
$\mathcal{P}_2 = \{\infty_0,0,4\}\{\infty_1,1,7\}\{\infty_2,5,8\}\{\infty_3,6,10\}\{\infty_4,9,11\}\{12,15,20\}\{13,17,21\}\{14,19,23\}\{16,18,22\}$;
$\mathcal{P}_3 = \{\infty_0,1,13\}\{\infty_1,10,22\}\{\infty_2,11,18\}\{\infty_3,12,23\}\{\infty_4,15,21\}\{0,7,19\}\{2,9,16\}\{3,14,20\}\{6,8,17\}$;
$\mathcal{P}_4 = \{\infty_0,15,22\}\{\infty_1,3,16\}\{\infty_2,1,20\}\{\infty_3,5,19\}\{\infty_4,0,14\}\{2,11,12\}\{4,10,21\}\{8,13,23\}\{9,17,18\}$;
$\mathcal{P}_{15} = \{\{0,8,20\}\{1,11,19\}\{2,15,18\}\{3,12,21\}\{4,14,17\}\{5,10,16\}\{6,13,22\}\{7,9,23\}$。

□

引理 7.34. *存在一个HTP*(41)。

证明. 令$X = \mathbb{Z}_{36} \cup \{\infty_0, \ldots, \infty_4\}$。我们在$X$上构造一个HTP$(41)$，其中区组可以划分成20个MPPC $\mathcal{P}_i$，$i \in [20]$和一个PPC $\mathcal{P}_{21}$。我们在下面列出了$\mathcal{P}_i$，$i \in [2]$。$\mathcal{P}_i$，$i \in [3,18]$可以由$\mathcal{P}_{i-2}$在$\mathbb{Z}_{36}$中加4得到。令$D = \{\{0,15,28\},\{1,14,29\},\{6,20,34\},\{7,21,35\}\}$。$\mathcal{P}_{21} = \{B+12i : B \in D, i=0,1,2\}$，$\mathcal{P}_{19} = \{B+4 : B \in \mathcal{P}_{21}\} \cup \{\{\infty_0, \infty_1, \infty_2\}\}$，$\mathcal{P}_{20} = \{B+8 : B \in \mathcal{P}_{21}\} \cup \{\{\infty_0, \infty_3, \infty_4\}\}$。

$\mathcal{P}_1 = \{\{\infty_0,2,3\},\{\infty_1,4,5\},\{\infty_2,6,8\},\{\infty_3,7,9\},\{\infty_4,10,13\},\{11,12,14\},\{15,19,24\},$
$\{16,20,23\},\{17,27,33\},\{18,29,31\},\{21,25,32\},\{22,28,34\},\{26,30,35\}\}$;
$\mathcal{P}_2 = \{\{\infty_0,1,16\},\{\infty_1,7,18\},\{0,5,24\},\{6,23,35\},\{\infty_2,13,31\},\{\infty_3,4,22\},\{\infty_4,15,32\},$
$\{8,19,34\},\{9,14,33\},\{10,17,26\},\{11,21,27\}\{12,25,28\},\{20,29,30\}\}$。

□

引理 7.35. *对任意*$n \in \{35,47,59\}$，*存在一个HTP*(n)。

证明. 令$n = 6t + 5$，$t \in \{5, 7\}$，$X = \mathbb{Z}_{6t} \cup \{\infty_0, \ldots, \infty_4\}$。我们在$X$上构造HTP$(n)$，其中区组可以划分成$3t + 2$个MPPC $\mathcal{P}_i$，$i \in [3t + 2]$ 和一个PPC $\mathcal{P}_{3t+3}$。对任意n，我们在下面列出$\mathcal{P}_1$。对任意$i \in [2, 3t]$，$\mathcal{P}_i$可以由$\mathcal{P}_1$在$\mathbb{Z}_{3t}$中加$2(i-1)$得到。令$D = \{\{0, 1, 2\}, \{3, 5, 10\}\}$。$\mathcal{P}_{3t+3} = \{B + 6i : B \in D, i = 0, 1, \ldots, t-1\}$，$\mathcal{P}_{3t+1} = \{B + 2 : B \in \mathcal{P}_{3t+3}\} \cup \{\{\infty_0, \infty_1, \infty_2\}\}$，$\mathcal{P}_{3t+2} = \{B + 4 : B \in \mathcal{P}_{3t+3}\} \cup \{\{\infty_0, \infty_3, \infty_4\}\}$。

35 : $\{\infty_0, 2, 5\}\{\infty_1, 3, 6\}\{\infty_2, 4, 13\}\{\infty_3, 7, 20\}\{\infty_4, 16, 21\}\{8, 18, 24\}\{9, 15, 25\}\{10, 17, 29\}$
$\{11, 19, 28\}\{12, 23, 27\}\{14, 22, 26\}$

47 : $\{\infty_0, 2, 5\}\{\infty_1, 3, 6\}\{\infty_2, 4, 9\}\{\infty_3, 7, 16\}\{\infty_4, 8, 17\}\{10, 21, 34\}\{11, 27, 38\}\{12, 24, 37\}$
$\{13, 28, 32\}\{14, 31, 35\}\{15, 23, 33\}\{18, 26, 40\}\{19, 25, 39\}\{20, 30, 36\}\{22, 29, 41\}$

59 : $\{\infty_0, 9, 32\}\{\infty_1, 8, 37\}\{\infty_2, 35, 16\}\{\infty_3, 36, 19\}\{42, 2, 6\}\{\infty_4, 31, 40\}\{44, 53, 50\}\{38, 30, 51\}$
$\{29, 21, 33\}\{17, 3, 46\}\{52, 25, 20\}\{12, 28, 45\}\{24, 14, 48\}\{43, 49, 27\}\{0, 15, 26\}\{41, 18, 5\}$
$\{22, 10, 7\}\{4, 39, 11\}\{23, 13, 47\}$

□

结合强Hanani三元填充的结果，我们得到如下结果：

定理 7.36. *对任意正整数n，除了确定的值$n \in \{6, 7, 11, 12, 13\}$外，都存在一个$HTP(n)$。*

7.6 结论

在本章中，我们通过研究Hanani三元填充的构造，对任意正整数n和$q \geq 2$确定了最优$(n, 5, 3)_q$码的码字个数。在此之前，$A_q(n, 5, 3)$只有当$q \in \{2, 3\}$，和一般的q在$w|(q-1)n$且n充分大时才被确定。

定理 7.37. $A_q(n, 5, 3) = \min\left\{\lfloor\frac{(q-1)n}{3}\rfloor, D(n, 3, 2)\right\}$，*其中*

$$D(n, 3, 2) = \begin{cases} \lfloor\frac{n}{3}\lfloor\frac{n-1}{2}\rfloor\rfloor - 1, & \text{若} n \equiv 5 \pmod 6, \\ \lfloor\frac{n}{3}\lfloor\frac{n-1}{2}\rfloor\rfloor, & \text{否则。} \end{cases} \tag{7.1}$$

Hanani三元填充是Hanani三元系的一个推广。我们还完全确定了Hanani三元填充的存在性。

Chapter 8

用可分组码构造最优常重复合码

8.1 引言和主要结果

常重复合码（constant-composition code，CCC）是常重码的一种特殊情况，它在编码理论中发挥重要作用。常重复合码中的置换码在无记忆信道中零误差的判定反馈能力的确定[138]，多重访问通信[54]，球形码调制[55]，DNA码[27, 101, 110]，电力线通信[37, 43]，跳频[38]，频率排列阵列[94]和有限带宽的信道编码[46]等方面都有重要应用。

上世纪九十年代末，对常重复合码就有了系统的研究[14, 17, 133]。现在，人们为了确定常重复合码的最大可能的码字个数引入了各种各样的方法，如计算机搜索方法[16]，填充设计[38, 49, 50, 93, 144, 153, 154, 157]，竞赛设计[158]，多项式和非线性函数[38, 47, 48, 51, 52]，PBD闭包方法[25, 28]和一些其他的方法[105, 106, 134, 149]等。

重量为3的常重复合码的码字个数由Chee，Ge和Ling在文[25]中完全确定。Gao和Ge在文[61]中完全确定了重量为4，距离为5的最优三元常重复合码的码字个数。Zhu和Ge在文[164]中确定了重量为4，距离为5或6的最优四元常重复合码的码字个数。文[24, 25]中还确定了一些特殊参数的最优常重复合码的码字个数。

引理 8.1 (Chee等[25]).

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

因引理2.3，我们得到：

推论 8.2. $A_3(n,6,[2,2]) \le \left\lfloor \frac{n}{2} A_3(n-1,6,[2,1]) \right\rfloor = \left\lfloor \frac{n}{2} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor := U(n,6,[2,2])$。

在本章中，我们将构造重量为4，距离为6，型为[2,2]的最优三元常重复合码，即$(n,6,[2,2])_3$码的码字个数。我们将对任意长度$n \not\equiv 5 \pmod 6$，$n \notin \{13,14,16,22,76,88,94,124,142,166,184\}$，确定$A_3(n,6,[2,2])_3$的值。对$n \equiv 5 \pmod 6$，我们也得到好的下界。所用的方法是第3章中给出的对GDC的循环构造方法。因为在本章中，我们考虑的都是[2,2]-GDC(6)。所以在下文中，我们将[2,2]-GDC(6)都简记为GDC。

这一章的结构如下：在第8.2节中，我们将介绍一个用斜Room frame构造GDC的方法；在第8.3节中，我们将分情况构造最优$(n,6,[2,2])_3$码；在第8.4节中，将对本章的主要结果进行总结。

8.2 一个斜Room frame构造法

引理 8.3. *如果存在一个型为t^u的斜Room frame，那么存在一个型为$(6t)^u$，大小为$6t^2u(u-1)$的GDC。*

证明. 令F为一个给定的型为t^u的斜Room frame。我们在组集$\{\{(i+k,j): 0 \le i \le t-1, j \in \mathbb{Z}_6\} : k = 0,t,\ldots,t(u-1)\}$上构造一个型为$(6t)^u$的GDC，它包含所有的码字$\langle (x,j),(y,j),(c,1+j),(r,4+j)\rangle$，$\langle (c,4+j),(r,1+j),(x,j),(y,j)\rangle$，其中$j \in \mathbb{Z}_6$，$\{x,y\}$是在F的第$c$列第$r$行的元素。 □

综合引理6.13和引理8.3，我们得到：

定理 8.4. *令$u \ge 4$，$t(u-1) \equiv 0 \pmod 2$，除了$(t,u) \in \{(1,5),(2,4)\}$，和如下可能的$(t,u)$外，存在型为$(6t)^u$，大小为$6t^2u(u-1)$的GDC：*

(i) $u = 4$，$t \equiv 2 \pmod 4$，

(ii) $u = 5$，$t \in \{17,19,23,29,31\}$。

8.3 主要证明过程

a. 一些小的GDC

引理 8.5. *存在一个型为2^{10}，大小为60的GDC。*

证明. 令$X = \mathbb{Z}_{20}$，$\mathcal{G} = \{\{i, i+10\} : 0 \le i \le 9\}$。那么$(X, \mathcal{G}, \mathcal{C})$是一个型为$2^{10}$的GDC，如果$\mathcal{C}$是由码字$\langle 0,5,3,7\rangle$，$\langle 0,4,1,13\rangle$，$\langle 0,8,14,19\rangle$在$\mathbb{Z}_{20}$中$+1 \pmod{20}$展开得到。 □

引理 8.6. *对任意$5 \le t \le 11$，存在一个型为6^t，大小为$6t(t-1)$的GDC。*

证明. 对$t \in \{5, 8\}$，令$X_t = \mathbb{Z}_{6t}$，$\mathcal{G}_t = \{\{i, i+t, i+2t, i+3t, i+4t, i+5t\} : 0 \le i \le t-1\}$。那么$(X_t, \mathcal{G}_t, \mathcal{C}_t)$是一个型为$6^t$，大小为$6t(t-1)$的GDC，如果$\mathcal{C}_t$由如下码字$+1 \pmod{6t}$展开得到。其中$\mathcal{C}_5$为$\langle 0,24,1,13\rangle$，$\langle 0,3,17,26\rangle$，$\langle 0,9,8,11\rangle$，$\langle 0,12,4,28\rangle$；$\mathcal{C}_8$为$\langle 0,18,13,3\rangle$，$\langle 0,6,5,7\rangle$，$\langle 0,46,27,9\rangle$，$\langle 0,4,19,39\rangle$，$\langle 0,10,22,36\rangle$，$\langle 0,14,31,37\rangle$，$\langle 0,28,21,25\rangle$。

对$t = 6$，令$X_6 = \mathbb{Z}_{12} \times \mathbb{Z}_3$，$\mathcal{G}_6 = \{\{(i,0),(i+6,0),(i,1),(i+6,1),(i,2),(i+6,2)\} : 0 \le i \le 5\}$。那么$(X_6, \mathcal{G}_6, \mathcal{C}_6)$是一个型为$6^6$，大小为180的GDC，如果$\mathcal{C}_6$由如下码字在$\mathbb{Z}_{12} \times \mathbb{Z}_3$中$(+1 \pmod{12}, -)$展开得到。

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

对$t \in \{7, 9, 11\}$，所需GDC由定理8.4得到。对$t = 10$，所需GDC由对型为2^{10}的GDC用3膨胀得到。 □

令$P = [9,19] \cup [21,23] \cup [26,28] \cup [31,33]$。

引理 8.7. *对任意的$t \ge 9$，$t \notin P$，存在一个型为$24^i 30^j 36^k 42^l 48^m$的GDC，其中i，j，k，l，m是非负整数且$4i + 5j + 6k + 7l + 8m = t$。*

证明. 对任意$t \ge 9$，$t \notin P$，从引理2.4取一个$(t+1, \{5,6,7,8,9\}, 1)$-PBD。从这个PBD的点集去掉一个点得到一个型为$4^i 5^j 6^k 7^l 8^m$的$\{5,6,7,8,9\}$-GDD，其中$4i + 5j + 6k + 7l + 8m = t$。对这个GDD用基本构造法加权6，并输入型为$6^u$，$u \in \{5,6,7,8,9\}$的GDC（引理8.6），得到型为$24^i 30^j 36^k 42^l 48^m$的GDC。 □

引理 8.8. *如下GDC均存在：*

i) 型为18^u，大小为$54u(u-1)$，$u \in \{4,5,6,7,9,11\}$；

ii) 型为24^u，大小为$96u(u-1)$，$u \in \{4,7,8\}$；

iii) 型为24^u36^1，大小为$96u(u+2)$，$u \in \{4,5\}$；

iv) 型为18^842^1，大小为2520；

v) 型为30^418^1，大小为1260；

vi) 型为24^418^1，大小为864。

证明. i)一个型为18^4的GDC由引理8.32直接构造得到。对任意$t \in \{5,6,7,9,11\}$，从引理8.6取一个型为6^t的GDC，并用3膨胀得到型为18^t的GDC。ii)所需GDC由定理8.4得到。iii)取型为6^u9^1，$u \in \{4,5\}$的$\{4\}$-GDD（见[77, 定理1.6]）。用基本构造法加权4得到需要的GDC。这里输入的是型为4^4的GDC（引理8.32）。iv)取一个型为3^87^1的$\{5\}$-GDD（见[71]）。用基本构造法加权6得到型为18^842^1的GDC。这里，输入的是型为6^5的GDC（引理8.6）。v)取一个TD$(5,5)$，用基本构造法对前四个组的所有点，和最后一个组的1个点加权6，其余点加权3，得到型为30^418^1的GDC。这里输入的是型为6^5和6^43^1的GDC（引理8.6和8.33）。vi)取一个TD$(5,4)$，用基本构造法对前四个组的所有点，最后一个组的2个点加权6，其余点加权3得到型为24^418^1的GDC。这里输入型为6^5和6^43^1的GDC（引理8.6和8.33）。 □

b. 当长度$n \equiv 0,1 \pmod 6$时

引理 8.9. $A_3(7,6,[2,2]) = 3$，$A_3(13,6,[2,2]) \geq 21$。

证明. 对$n=7$，由文[159]中$(7,6,4)_3$码的结果可知$A_3(7,6,[2,2]) \leq 3$。很容易构造$\{0,1,2,3,4,5,6\}$上的3个码字$\langle 0,1,2,3\rangle$，$\langle 0,4,5,6\rangle$，$\langle 2,5,1,4\rangle$。

对$n=13$，令点集为$\{0,1,2,\ldots,12\}$。所需的21个码字如下：

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

□

引理 8.10. 对任意$t \in [3,11] \cup \{13,14,17\}$，$A_3(6t+1,6,[2,2]) = U(6t+1,6,[2,2])$。

表 8.1: 引理8.10中最优$(6t+1,6,[2,2])_3$码的基码

t	码字
3	$\langle 0,1,4,16\rangle$ $\langle 0,7,9,17\rangle$ $\langle 0,8,13,14\rangle$
4	$\langle (0,3),(2,0),(3,0),(4,3)\rangle$ $\langle (0,2),(2,3),(2,1),(0,4)\rangle$ $\langle (0,2),(1,0),(1,4),(0,3)\rangle$ $\langle (0,0),(1,1),(2,0),(4,1)\rangle$
5	$\langle 0,3,11,23\rangle$ $\langle 0,7,2,5\rangle$ $\langle 0,6,15,22\rangle$ $\langle 0,14,4,10\rangle$ $\langle 0,12,13,30\rangle$
6	$\langle 0,23,27,35\rangle$ $\langle 0,8,11,17\rangle$ $\langle 0,5,25,1\rangle$ $\langle 0,6,22,36\rangle$ $\langle 0,18,2,7\rangle$ $\langle 0,13,10,28\rangle$
7	$\langle 0,35,26,23\rangle$ $\langle 0,16,33,37\rangle$ $\langle 0,29,22,38\rangle$ $\langle 0,3,10,18\rangle$ $\langle 0,30,11,12\rangle$ $\langle 0,1,6,20\rangle$ $\langle 0,4,2,32\rangle$
8	$\langle 0,36,40,45\rangle$ $\langle 0,28,14,47\rangle$ $\langle 0,42,10,32\rangle$ $\langle 0,33,25,18\rangle$ $\langle 0,44,15,26\rangle$ $\langle 0,11,48,12\rangle$ $\langle 0,22,3,46\rangle$ $\langle 0,43,23,2\rangle$
9	$\langle 0,8,1,21\rangle$ $\langle 0,43,19,42\rangle$ $\langle 0,32,34,39\rangle$ $\langle 0,20,30,45\rangle$ $\langle 0,28,9,26\rangle$ $\langle 0,17,41,14\rangle$ $\langle 0,5,16,49\rangle$ $\langle 0,22,4,51\rangle$ $\langle 0,15,6,18\rangle$
10	$\langle 0,27,36,41\rangle$ $\langle 0,11,21,39\rangle$ $\langle 0,3,22,26\rangle$ $\langle 0,1,47,53\rangle$ $\langle 0,5,35,37\rangle$ $\langle 0,17,24,25\rangle$ $\langle 0,4,33,16\rangle$ $\langle 0,6,51,54\rangle$ $\langle 0,18,38,49\rangle$ $\langle 0,2,15,42\rangle$
11	$\langle 0,20,33,44\rangle$ $\langle 0,1,32,41\rangle$ $\langle 0,10,49,53\rangle$ $\langle 0,30,48,51\rangle$ $\langle 0,3,28,65\rangle$ $\langle 0,7,26,36\rangle$ $\langle 0,8,23,35\rangle$ $\langle 0,9,54,61\rangle$ $\langle 0,4,42,50\rangle$ $\langle 0,12,14,34\rangle$ $\langle 0,11,16,17\rangle$
13	$\langle 0,11,54,56\rangle$ $\langle 0,5,49,60\rangle$ $\langle 0,18,35,64\rangle$ $\langle 0,63,66,76\rangle$ $\langle 0,29,65,71\rangle$ $\langle 0,10,24,33\rangle$ $\langle 0,7,15,19\rangle$ $\langle 0,1,22,40\rangle$ $\langle 0,9,57,62\rangle$ $\langle 0,4,34,41\rangle$ $\langle 0,2,27,28\rangle$ $\langle 0,6,38,58\rangle$ $\langle 0,20,51,67\rangle$
14	$\langle 0,9,41,53\rangle$ $\langle 0,1,50,83\rangle$ $\langle 0,45,47,63\rangle$ $\langle 0,46,61,70\rangle$ $\langle 0,4,25,59\rangle$ $\langle 0,17,27,28\rangle$ $\langle 0,8,56,75\rangle$ $\langle 0,16,74,80\rangle$ $\langle 0,19,22,62\rangle$ $\langle 0,6,29,36\rangle$ $\langle 0,7,38,42\rangle$ $\langle 0,12,26,72\rangle$ $\langle 0,34,54,71\rangle$ $\langle 0,52,57,65\rangle$
17	$\langle 0,20,62,63\rangle$ $\langle 0,10,58,88\rangle$ $\langle 0,3,59,95\rangle$ $\langle 0,17,24,50\rangle$ $\langle 0,1,76,97\rangle$ $\langle 0,12,46,66\rangle$ $\langle 0,36,64,81\rangle$ $\langle 0,74,85,99\rangle$ $\langle 0,5,40,49\rangle$ $\langle 0,19,87,90\rangle$ $\langle 0,9,47,70\rangle$ $\langle 0,21,53,72\rangle$ $\langle 0,14,69,79\rangle$ $\langle 0,2,6,18\rangle$ $\langle 0,23,31,60\rangle$ $\langle 0,26,39,41\rangle$ $\langle 0,30,52,57\rangle$

证明. 令$X_4=\mathbb{Z}_5\times\mathbb{Z}_5$。那么$(X_4,\mathcal{C}_4)$是所需的最优$(25,6,[2,2])_3$码，如果$\mathcal{C}_4$是由表8.1中的码字在$\mathbb{Z}_5\times\mathbb{Z}_5$上$(+1\pmod 5,+1\pmod 5)$展开得到。

对$t\neq 4$，令$X_t=\mathbb{Z}_{6t+1}$。那么$(X_t,\mathcal{C}_t)$是所需的最优$(6t+1,6,[2,2])_3$码，如果$\mathcal{C}_t$由表8.1中的码字在$\mathbb{Z}_{6t+1}$上$+1\pmod{6t+1}$展开得到。 □

引理 8.11. 对任意$t\geq 12$，$t\notin\{13,14,17\}$，$A_3(6t+1,6,[2,2])=U(6t+1,6,[2,2])$。

证明. 对任意$t\geq 9$，$t\notin P$，从引理8.8取一个型为$24^i30^j36^k42^l48^m$的GDC。增加一个无穷点，并在组上连同无穷点填入相应的最优码得到需要的码。对

任意$t \in \{12, 15, 16, 18, 19, 21, 22, 23, 26, 27, 28, 31, 32, 33\}$，取引理8.8中的GDC。增加一个无穷点，并在组上连同无穷点填入相应的最优码得到需要的码。 □

定理 8.12. 对任意$t \geq 3$，$A_3(6t+1, 6, [2, 2]) = U(6t+1, 6, [2, 2])$；$A_3(7, 6, [2, 2]) = 3$；$A_3(13, 6, [2, 2]) \geq 21$。

c. 当长度$n \equiv 0 \pmod 6$时

定理 8.13. 对任意$t \geq 1$，$A_3(6t, 6, [2, 2]) = U(6t, 6, [2, 2])$。

证明. 对$t \in \{1, 2\}$，令$X_t = \mathbb{Z}_{6t}$。那么所需的码$\mathcal{C}_t$是由如下码字在集合$\mathbb{Z}_{6t}$上$+2 \pmod{6t}$展开得到。其中$\mathcal{C}_1$为$\langle 0, 1, 2, 3\rangle$，$\mathcal{C}_2$为$\langle 0, 2, 8, 5\rangle$，$\langle 0, 9, 7, 11\rangle$，$\langle 1, 5, 0, 10\rangle$。对任意$t \geq 3$，从定理8.12中的最优$(6t + 1, 6, [2, 2])_3$码去掉一个坐标和在这个坐标上为不为零的所有码字得到需要的码。 □

d. 当长度$n \equiv 2 \pmod 6$时

引理 8.14. $A_3(8, 6, [2, 2]) = 5$，$A_3(14, 6, [2, 2]) \geq 27$。

证明. 对$n = 8$，由文[159]中$(8, 6, 4)_3$码的结果得到$A_3(8, 6, [2, 2]) \leq 5$。我们在集合$\{0, 1, 2, 3, 4, 5, 6, 7\}$上构造所需的码字如下：$\langle 0, 1, 2, 3\rangle$，$\langle 0, 4, 5, 6\rangle$，$\langle 1, 5, 4, 7\rangle$，$\langle 2, 3, 6, 7\rangle$，$\langle 6, 7, 0, 1\rangle$。

对$n = 14$，令点集为$\{0, 1, 2, \ldots, 13\}$，所需的码字如下：

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

□

很容易可以看出如果存在一个型为2^{3t+1}，大小为$2t(3t+1)$的GDC，那么存在一个最优$(6t + 2, 6, [2, 2])_3$码。所以我们将通过构造型为2^{3t+1}的GDC构造最优码。

引理 8.15. 对任意$3 \leq t \leq 11$，$t \in \{14, 17\}$，存在一个型为2^{3t+1}，大小为$2t(3t+1)$的GDC。

表 8.2: 引理8.15中型为2^{3t+1}的GDC的基码

t	码字
4	$\langle 0,4,3,11\rangle$ $\langle 0,5,6,15\rangle$ $\langle 0,9,2,23\rangle$ $\langle 0,8,20,24\rangle$
5	$\langle 0,28,9,29\rangle$ $\langle 1,7,2,12\rangle$ $\langle 0,15,24,7\rangle$ $\langle 0,10,30,12\rangle$ $\langle 0,18,23,21\rangle$ $\langle 1,14,22,9\rangle$ $\langle 1,15,11,5\rangle$ $\langle 1,3,0,26\rangle$ $\langle 0,26,25,11\rangle$ $\langle 1,21,4,8\rangle$
6	$\langle 0,7,20,5\rangle$ $\langle 0,21,11,27\rangle$ $\langle 0,23,14,35\rangle$ $\langle 0,30,24,25\rangle$ $\langle 0,22,18,26\rangle$ $\langle 0,1,3,10\rangle$
7	$\langle 0,5,21,33\rangle$ $\langle 0,32,34,42\rangle$ $\langle 0,14,23,29\rangle$ $\langle 0,6,7,25\rangle$ $\langle 0,36,40,35\rangle$ $\langle 0,20,17,3\rangle$ $\langle 0,18,11,31\rangle$
8	$\langle 0,40,29,34\rangle$ $\langle 0,30,2,11\rangle$ $\langle 0,37,3,33\rangle$ $\langle 0,45,12,27\rangle$ $\langle 0,35,21,8\rangle$ $\langle 0,49,18,42\rangle$ $\langle 0,24,28,38\rangle$ $\langle 0,9,7,6\rangle$
9	$\langle 0,39,33,45\rangle$ $\langle 0,12,48,53\rangle$ $\langle 0,22,35,9\rangle$ $\langle 0,5,3,37\rangle$ $\langle 0,29,31,47\rangle$ $\langle 0,4,25,42\rangle$ $\langle 0,16,23,24\rangle$ $\langle 0,26,19,46\rangle$ $\langle 0,1,11,15\rangle$
10	$\langle 0,9,38,57\rangle$ $\langle 0,22,30,33\rangle$ $\langle 0,15,39,5\rangle$ $\langle 0,20,12,21\rangle$ $\langle 0,58,23,45\rangle$ $\langle 0,3,2,17\rangle$ $\langle 0,19,51,55\rangle$ $\langle 0,6,13,50\rangle$ $\langle 0,28,46,26\rangle$ $\langle 0,25,35,41\rangle$
11	$\langle 0,55,33,19\rangle$ $\langle 0,37,65,49\rangle$ $\langle 0,52,8,63\rangle$ $\langle 0,67,60,2\rangle$ $\langle 0,10,4,35\rangle$ $\langle 0,59,66,48\rangle$ $\langle 0,50,22,21\rangle$ $\langle 0,23,38,64\rangle$ $\langle 0,26,5,56\rangle$ $\langle 0,14,20,43\rangle$ $\langle 0,17,44,53\rangle$
14	$\langle 0,1,20,31\rangle$ $\langle 0,7,47,68\rangle$ $\langle 0,11,15,78\rangle$ $\langle 0,14,71,80\rangle$ $\langle 0,23,82,83\rangle$ $\langle 0,5,29,41\rangle$ $\langle 0,2,46,56\rangle$ $\langle 0,9,35,42\rangle$ $\langle 0,12,18,70\rangle$ $\langle 0,17,25,39\rangle$ $\langle 0,34,37,50\rangle$ $\langle 0,13,62,64\rangle$ $\langle 0,10,38,55\rangle$ $\langle 0,21,48,53\rangle$
17	$\langle 0,1,81,86\rangle$ $\langle 0,4,37,58\rangle$ $\langle 0,8,65,74\rangle$ $\langle 0,12,59,76\rangle$ $\langle 0,22,71,72\rangle$ $\langle 0,51,78,90\rangle$ $\langle 0,2,40,62\rangle$ $\langle 0,5,11,46\rangle$ $\langle 0,9,32,88\rangle$ $\langle 0,17,30,61\rangle$ $\langle 0,31,45,98\rangle$ $\langle 0,69,89,93\rangle$ $\langle 0,7,75,77\rangle$ $\langle 0,48,84,91\rangle$ $\langle 0,21,55,63\rangle$ $\langle 0,3,19,29\rangle$ $\langle 0,10,25,28\rangle$

证明. 对$t=3$，所需的码在引理8.5中构造。对任意$4\le t\le 11$或$t\in\{14,17\}$，令$X_t=\mathbb{Z}_{6t+2}$，$\mathcal{G}_t=\{\{i,i+3t+1\}:0\le i\le 3t\}$。那么，$(X_t,\mathcal{G}_t,\mathcal{C}_t)$就是型为$2^{3t+1}$，大小为$2t(3t+1)$的GDC，如果$\mathcal{C}_5$是由表8.2中的码字在$\mathbb{Z}_{32}$中$+2 \pmod{32}$展开得到，当$t\neq 5$时，$\mathcal{C}_t$由表8.2中码字在$\mathbb{Z}_{6t+2}$中$+1 \pmod{6t+2}$展开得到。 □

引理 8.16. *对任意$t\ge 12$，$t\notin\{14,17\}$，存在一个型为2^{3t+1}，大小为$2t(3t+1)$的GDC。*

证明. 对任意$t\ge 9$，$t\notin P$，从引理8.8取一个型为$24^i30^j36^k42^l48^m$的GDC。增加一个无穷点，在组上连同无穷点填入型为2^u，$u\in\{13,16,19,22,25\}$的GDC得到所需GDC。对任意$t\in\{12,15,16,18,19,21,22,23,26,27,28,31,32,33\}$，取引理8.8中的GDC，增加一个无穷点，在组上连同无穷点填入型为2^u，$u\in\{10,13,19\}$的GDC得到所需GDC。对$t=13$，取一个TD$(4,5)$，用基本构造法

加权4得到型为20^4的GDC，再在组上填入型为2^{10}的GDC，就得到了所需GDC。□

定理 8.17. 对任意$t \geq 3$，$A_3(6t+2, 6, [2,2]) = U(6t+2, 6, [2,2])$；$A_3(8, 6, [2,2]) = 5$；$A_3(14, 6, [2,2]) \geq 27$。

e. 当长度$n \equiv 5 \pmod 6$时

引理 8.18. $A_3(5, 6, [2,2]) = 1$，$A_3(11, 6, [2,2]) = 15$，$A_3(17, 6, [2,2]) \geq 40$。

证明. 第一个等式很显然。由文[159]中的最优$(11, 6, 4)_3$码的结果，我们得到$A_3(11, 6, [2,2]) \leq A_3(11, 6, 4) = 15$。一个最优$(11, 6, [2,2])_3$在文[159]中构造得到。

对$n = 40$，令点集为$\mathbb{Z}_{16} \cup \{\infty\}$。所需的40个码字由码字$\langle 0, 3, 9, 5\rangle$，$\langle 0, 11, 12, 10\rangle$，$\langle 1, 6, \infty, 12\rangle$，$\langle 1, 5, 8, 14\rangle$，$\langle 1, 2, 15, 9\rangle$，$\langle 0, \infty, 13, 15\rangle$，$\langle 3, 13, 7, 12\rangle$，$\langle 3, 10, 15, 6\rangle$，$\langle 2, 4, 5, 6\rangle$，$\langle 0, 6, 7, 4\rangle$在$\mathbb{Z}_{16}$中$+4 \pmod{16}$展开得到。□

引理 8.19. 对任意$3 \leq t \leq 8$，存在一个型为$2^{3t}5^1$，大小为$2t(3t+4)$的*GDC*。

证明. 令$X_t = \mathbb{Z}_{6t+5}$，$\mathcal{G}_t = \{\{i, i+3t\} : 0 \leq i \leq 3t-1\} \cup \{\{6t, 6t+1, 6t+2, 6t+3, 6t+4\}\}$。那么$(X_t, \mathcal{G}_t, \mathcal{C}_t)$是一个型为$2^{3t}5^1$的GDC，如果$\mathcal{C}_3$是由表8.3中的码字由自同构群$G = \langle (0\ 3\ 6\ \cdots\ 15)(1\ 4\ 7\ \cdots\ 16)(2\ 5\ 8\ \cdots\ 17)(18\ 19\ 20)\ (21\ 22)\rangle$展开得到；当$t > 3$，$\mathcal{C}_t$是由表8.3中的码字由自同构群$G = \langle (0\ 3\ 6\ \cdots\ 6t-3)(1\ 4\ 7\ \cdots\ 6t-2)(2\ 5\ 8\ \cdots\ 6t-1)(6t)(6t+1)(6t+2)(6t+3)(6t+4)\rangle$展开得到。□

引理 8.20. 对任意$t \geq 12$，$t \notin \{13, 14, 17\}$，存在一个型为$2^{3t}5^1$，大小为$2t(3t+4)$的*GDC*。

证明. 对任意$t \geq 9$，$t \notin P$，从引理8.7中取一个型为$24^i30^j36^k42^l48^m$的GDC，其中$4i+5j+6k+7l+8m = t$。增加一个无穷点，在组上连同无穷点填入型为$2^{3s}5^1$，$s \in \{4, 5, 6, 7, 8\}$的GDC，得到需要的GDC。对任意$t \in \{12, 15, 16, 18, 19, 21, 22, 23, 26, 27, 28, 31, 32, 33\}$，取引理8.8 中的GDC。增加一个无穷点，在组上连同无穷点填入型为$2^{3s}5^1$，$s \in \{3, 4, 5, 6, 7\}$的GDC得到所需GDC。□

表 8.3: 引理8.19中型为$2^{3t}5^1$的GDC的基码

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

引理 8.21. 对任意$t \geq 3$，$t \notin \{9,10,11,14\}$，$A_3(6t+5,6,[2,2]) \geq U(6t+5,3)-1$；对$t=14$，$A_3(6t+5,6,[2,2]) \geq U(6t+5,3)-2$。

证明. 对任意$t \notin \{9,10,11,13,14,17\}$，从引理8.19和8.20取型为$2^{3t}5^1$，$t \geq 3$，$t \notin \{9,10,11,13,14,17\}$的GDC。在大小为5的组上填入只有一个码字的最优$(5,5,[2,2])_3$得到需要的码。对任意$t \in \{13,14,17\}$，从引理8.35分别取型为$18^46^1$，$18^412^1$或$24^46^1$的GDC。增加5个无穷点，在大小为18或24的组上连同无穷点填入型为2^95^1或$2^{12}5^1$的GDC，并在最后一个组上连同无穷点填入引理8.18中长度为11或17的码就得到了所需的码。 □

定理 8.22. 对任意$t \geq 3$，$t \notin \{9,10,11,14\}$，$A_3(6t+5,6,[2,2]) \geq U(6t+5,6,[2,2])-1$；$A_3(5,6,[2,2])=1$；$A_3(11,6,[2,2])=15$；对$t \in \{2,14\}$，$A_3(6t+5,6,[2,2]) \geq U(6t+5,6,[2,2])-2$。

表 8.4: 引理8.23中的最优$(6t+4,6,[2,2])_3$码的基码

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

f. 当长度$n\equiv 4 \pmod 6$时

引理 8.23. 对任意$t=1$或$4\le t\le 9$，$A_3(6t+4,6,[2,2])=U(6t+4,6,[2,2])$。

证明. 令$X_t=\mathbb{Z}_{6t+4}$。那么$(X_t,\mathcal{C}_t)$是所需的最优$(6t+4,6,[2,2])_3$，如果$\mathcal{C}_t$是由表8.4中的码字在$\mathbb{Z}_{6t+4}$中$+2 \pmod{6t+4}$展开得到。 □

引理 8.24. 对任意$t\ge 142$，$A_3(6t+4,6,[2,2])=U(6t+4,6,[2,2])$。

证明. 从引理2.9取一个TD$(8,k)$。用基本构造法对前6个组的所有点，第7个组的x个点加权6，第7个组的3个点加权3，其余点加权0。这里，输入设计为型为6^s，$s\in\{6,7\}$的GDC（引理8.6），和型为6^s3^1，$s\in\{6,7\}$的GDC（引理8.33）。我们得到了型为$(6k)^6(6x)^19^1$的GDC，其中$x=0$ 或$3\le x\le k$。增加一个无穷点，在大小为$6k$或$6x$的组上连同无穷点填入长度为$6k+1$或$6x+1$的最优码（定理8.12），在大小为9的组连同无穷点填入最优$(10,6,[2,2])_3$码。我们就得到了长度为$n=36k+6x+10=6(6k+x+1)+4$的最优码。取$k\ge 23$，我们得到了长度为$n=6t+4$的最优码，其中$t=6k+x+1$可以取任何$t\ge 142$的正整数。 □

引理 8.25. 对任意$t = 43$，或$46 \le t \le 141$，$t \ne 51$，$A_3(6t+4, 6, [2,2]) = U(6t+4, 6, [2,2])$。

证明. 从引理2.9中取一个TD(m,k)，$k \in \{7,8,9,13\}$，$8 \le m \le 12$，$m \le k+1$。用基本构造法对前6个组的所有点加权6，最后一个组的3个点加权3，对剩余的$m-7$个组的x_i个点，$1 \le i \le m-7$加权6。其余点加权0。其中$x_i = 0$或者$3 \le x_i \le k$。这里输入码为型为6^s，$6 \le s \le 11$的GDC（引理8.6）和型为6^s3^1，$6 \le s \le 11$的GDC（引理8.33）。我们就得到了型为$(6k)^6 x_1^1 x_2^1 \dots x_{m-7}^1 9^1$的GDC。增加一个点，在前$m-1$个组上连同无穷点填入长度为$6k+1$或$6x_i+1$的最优码（定理8.12），在长度为9的组连同无穷点填入最优$(10, 6, [2,2])_3$码，就得到了长度为$n = 36k + 6\sum_{i=1}^{m-7} x_i + 10 = 6(6k + \sum_{i=1}^{m-7} x_i + 1) + 4$的最优码。

令$t = 6k + \sum_{i=1}^{m-7} x_i + 1$。取$k = 7$，$m = 8$，我们有$t \in \{43\} \cup [46, 50]$；取$k = 8$，$m = 9$，我们有$t \in [52, 65]$；取$k = 9$，$m = 10$，我们有$t \in [66, 82]$；取$k = 13$，$m = 12$，我们有$t \in [83, 141]$。 □

引理 8.26. 对任意$t \in \{24\} \cup [32, 34] \cup [36, 44]$，$A_3(6t+4, 6, [2,2]) = U(6t+4, 6, [2,2])$。

证明. 从引理2.9取一个TD$(5,k)$，$k \in \{5,7,8,9\}$。用基本构造法对前4个组的所有点，最后一个组的x个点加权6，对最后一个组的y个点加权3，其中$x+y=k$。这里，输入的是型为6^5的GDC（引理8.6）和型为$6^4 3^1$的GDC（引理8.33）。我们得到了型为$(6k)^4(6x+3y)^1$的GDC。增加一个无穷点，在前四个组上连同无穷点填入长度为$6k+1$的最优码（定理8.12），在大小为$6x+3y$的组上连同无穷点填入最优$(6x+3y+1, 6, [2,2])_3$码（引理8.23），就得到了长度为$n = 24k + 6x + 3y + 1 = 6(4k + x + \frac{y-1}{2}) + 4$的最优码。令$t = 4k + x + \frac{y-1}{2}$。对任意$t$，参数$(k, x, y)$和需要填入的码长$s = 6x + 3y + 1$在表8.5 中给出。 □

表 8.5: 引理8.26中所需参数

t	(k,x,y)	s	t	(k,x,y)	s	t	(k,x,y)	s
24	(5, 4, 1)	28	32	(7, 2, 5)	28	33	(7, 4, 3)	34
34	(7, 6, 1)	40	36	(8, 1, 7)	28	37	(8, 3, 5)	34
38	(8, 5, 3)	40	39	(8, 7, 1)	46	40	(9, 0, 9)	28
41	(9, 2, 7)	34	42	(9, 4, 5)	40	43	(9, 6, 3)	46
44	(9, 8, 1)	52						

引理 8.27. 对任意$t \in \{10, 11, 13, 16, 17, 18, 19, 21, 22, 25, 26, 28, 31, 45, 51\}$，$A_3(6t + 4, 6, [2, 2]) = U(6t + 4, 6, [2, 2])$。

证明. 对$t = 11$，从引理8.32取型为10^7的GDC，在组上填入最优$(10, 6, [2, 2])_3$码得到所需的码。对$t = 17$，从引理8.35取一个型为$24^4 9^1$的GDC，增加一个无穷点，在组上连同无穷点填入最优$(25, 6, [2, 2])_3$码或最优$(10, 6, [2, 2])_3$码得到所需的码。对任意$t \in \{10, 13, 16, 18, 19, 21, 22, 25, 26, 28, 31, 45, 51\}$，我们把得到$t$所需的参数列在表8.6中。我们把一个型为$g^u m^1$的GDC用$w$膨胀，增加$a$个点，然后在组上连同无穷点填入长度为$s \in S$的码得到所需的码。 □

表 8.6: 引理8.27中所需参数

t	n	$g^u m^1 \times w$	来源	a	S
10	64	$3^7 \times 3$	引理8.32	1	10
13	82	$6^4 3^1 \times 3$	引理8.33	1	19, 10
16	100	$3^{11} \times 3$	引理8.32	1	10
18	112	$4^4 \times 7$	引理8.32	0	28
19	118	$3^{13} \times 3$	引理8.32	1	10
21	130	$2^{13} \times 5$	引理8.15	0	10
22	136	$6^7 3^1 \times 3$	引理8.33	1	19, 10
25	154	$6^7 9^1 \times 3$	引理8.34	1	19, 28
26	160	$4^4 \times 10$	引理8.32	0	40
28	172	$6^8 9^1 \times 3$	引理8.34	1	19, 28
31	190	$3^7 \times 9$	引理8.32	1	28
45	274	$3^7 \times 13$	引理8.32	1	40
51	310	$1^{31} \times 10$	引理8.10	0	10

引理 8.28. 对$t \in \{29, 35\}$，$A_3(6t + 4, 6, [2, 2]) = U(6t + 4, 6, [2, 2])$。

证明. 对$t = 29$，取一个型为6^7的GDC（引理8.6），并用4膨胀。这里的输入设计是型为4^4的$\{4\}$-MGDD。我们就得到了一个GDC，且支撑集形成指数为2的型为$(24, 6^4)^7$的DGDD。增加9个无穷点，填入型为$6^7 9^1$的GDC得到了型为$24^7 9^1$的GDC。增加一个无穷点，在组上连同无穷点填入长度为25或10的最优码得到需要的码。对$t = 35$，取型为6^7的GDC，并去掉最后一个组的所有点和包含这个点的码字，并用5膨胀。这里输入的是型为5^4的$\{4\}$-MGDD和型为5^3的可分解$\{3\}$-MGDD。得到的GDC的支撑集构成一个$\{3, 4\}$-DGDD，并且所有的三元组形成24个平行类。增加24个点，补全平行类。再增加9个无穷点，

并填入型为$6^6 9^1$的GDC就得到了型为$30^6 33^1$的GDC。再增加一个无穷点，并在组上连同无穷点填入长度为31或34的最优码就得到了所需的最优码。　□

综合上述引理，我们得到：

定理 8.29. 对任意$t \geq 1$，$t \notin \{2,3,12,14,15,20,23,27,30\}$，$A_3(6t+4,6,[2,2]) = U(6t+4,6,[2,2])$。

g. 当长度$n \equiv 3 \pmod 6$时

定理 8.30. 对任意$t \geq 1$，$A_3(6t+3,6,[2,2]) = U(6t+3,3)$。

证明. 对任意$t \geq 1$，$t \notin \{2,3,12,14,15,20,23,27,30\}$，从定理8.29中的最优$(6t+4,6,[2,2])_3$码去掉一个坐标和在这个坐标不为零的码字得到相应的码。对$t=3$，显然引理8.32中的型为3^7的GDC就是所需的码。对$t \in \{12,15,27,30\}$，分别取型为18^4（引理8.32），18^5，18^9（定理8.4）或18^{10}（对一个型为1^{10}的GDC，引理8.23，用18膨胀得到）的GDC。增加3个无穷点，在组上连同无穷点填入型为3^7的GDC，就分别得到了型为3^{25}，3^{31}，3^{55}或3^{61}的GDC。很容易验证它们就是所需的码。对$t=23$，从引理2.9取一个TD$(5,5)$。用基本构造法对前4个组的所有点，最后一个组的2个点加权6，最后一个组的3个点加权3，就得到了型为$30^4 21^1$的GDC。在组上填入长度为21或30的最优码就得到了所需的码。

对$t \in \{2,14,20\}$，令$X_t = \mathbb{Z}_{6t+3}$。那么$(X_t, \mathcal{C}_t)$就是最优$(6t+3,6,[2,2])_3$码，如果$\mathcal{C}_t$是由下面码字在$\mathbb{Z}_{6t+3}$中$+1 \pmod{6t+3}$展开得到。

$t=2$：$\langle 0,3,4,14\rangle$ $\langle 0,5,7,13\rangle$

$t=14$：

$\langle 0,1,68,8\rangle$　$\langle 0,24,47,61\rangle$　$\langle 0,41,16,36\rangle$　$\langle 0,73,57,40\rangle$　$\langle 0,14,49,5\rangle$
$\langle 0,29,40,38\rangle$　$\langle 0,58,68,27\rangle$　$\langle 0,20,54,84\rangle$　$\langle 0,60,62,9\rangle$　$\langle 0,57,51,63\rangle$
$\langle 0,22,25,53\rangle$　$\langle 0,43,33,32\rangle$　$\langle 0,60,6,45\rangle$　$\langle 0,28,71,60\rangle$

$t=20$：

$\langle 0,16,46,63\rangle$　$\langle 0,92,85,7\rangle$　$\langle 0,34,122,9\rangle$　$\langle 0,10,43,74\rangle$　$\langle 0,5,109,82\rangle$
$\langle 0,6,21,79\rangle$　$\langle 0,24,22,94\rangle$　$\langle 0,23,37,55\rangle$　$\langle 0,13,42,62\rangle$　$\langle 0,17,2,8\rangle$
$\langle 0,56,81,68\rangle$　$\langle 0,20,95,39\rangle$　$\langle 0,45,93,97\rangle$　$\langle 0,4,57,80\rangle$　$\langle 0,18,54,59\rangle$
$\langle 0,11,102,3\rangle$　$\langle 0,72,35,69\rangle$　$\langle 0,58,1,84\rangle$　$\langle 0,27,71,87\rangle$　$\langle 0,83,50,61\rangle$

□

8.4 结论

在本章中，我们研究了最优$(n,6,[2,2])_3$码的码字个数。我们把结果总结如下：

定理 8.31. *对任意整数*$n \geq 4$，

$$A_3(n,6,[2,2]) = \begin{cases} 1, & \text{当} n \leq 5\text{时} \\ 3, & \text{当} n = 7\text{时} \\ 5, & \text{当} n = 8\text{时} \\ 15, & \text{当} n = 11\text{时} \\ \left\lfloor \frac{n}{2} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor, & \text{当} n \geq 6, n \not\equiv 5 \pmod 6, n \notin \{7,8,16,22, \\ & \qquad 76,88,94,124,142,166,184\}\text{时} \end{cases}$$

$A_3(13,6,4) \in [21,26]$，$A_3(14,6,4) \in [27,28]$。

当$n \equiv 5 \pmod 6$时，对任意$t \geq 3$，$t \notin \{9,10,11,14\}$，

$$A_3(6t+5,6,[2,2]) \in [2(3t+1)(t+1)-1, 2(3t+1)(t+1)],$$

对$t \in \{2,14\}$，

$$A_3(6t+5,6,[2,2]) \in [2(3t+1)(t+1)-2, 2(3t+1)(t+1)]。$$

8.5 附录

引理 8.32. *分别存在型为*3^7，3^{11}，3^{13}，4^4，10^7*和*18^4*的*GDC。

证明. 对任意型为g^u的GDC，令$X = \mathbb{Z}_{gu}$，$\mathcal{G} = \{\{i, i+u, i+2u, \ldots, i+(g-1)u\} : 0 \leq i \leq u-1\}$。那么，$(X,\mathcal{G},\mathcal{C})$就是所需的GDC，如果$\mathcal{C}$是由下面码字在$\mathbb{Z}_{gu}$中展开得到。

3^7：$+1 \pmod{21}$ $\langle 7,3,18,13\rangle$ $\langle 4,3,12,16\rangle$ $\langle 0,5,2,3\rangle$

3^{11}：$+1 \pmod{33}$ $\langle 13,27,15,25\rangle$ $\langle 25,15,0,7\rangle$ $\langle 2,15,18,32\rangle$ $\langle 10,5,1,14\rangle$ $\langle 0,7,1,6\rangle$

3^{13}：$+1 \pmod{39}$ $\langle 20,2,25,10\rangle$ $\langle 21,6,23,17\rangle$ $\langle 6,12,5,26\rangle$ $\langle 30,3,28,19\rangle$ $\langle 21,24,31,4\rangle$ $\langle 0,9,1,4\rangle$

4^4：$+8 \pmod{16}$

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

10^7：+1 (mod 70)

$\langle 0,17,27,58\rangle$ $\langle 0,61,24,46\rangle$ $\langle 0,25,6,68\rangle$ $\langle 0,3,2,40\rangle$ $\langle 0,32,16,52\rangle$
$\langle 0,34,47,64\rangle$ $\langle 0,11,26,29\rangle$ $\langle 0,62,57,66\rangle$ $\langle 0,48,1,60\rangle$ $\langle 0,31,50,5\rangle$

18^4：+2 (mod 72)

$\langle 1,3,8,22\rangle$ $\langle 0,34,1,15\rangle$ $\langle 0,26,11,13\rangle$ $\langle 1,35,32,58\rangle$ $\langle 1,7,16,54\rangle$ $\langle 1,15,50,56\rangle$
$\langle 0,2,21,71\rangle$ $\langle 0,7,18,25\rangle$ $\langle 0,30,23,61\rangle$ $\langle 1,11,62,40\rangle$ $\langle 1,31,34,44\rangle$ $\langle 0,14,43,17\rangle$
$\langle 0,9,54,63\rangle$ $\langle 0,10,5,47\rangle$ $\langle 0,22,49,55\rangle$ $\langle 1,27,26,28\rangle$ $\langle 0,6,51,41\rangle$ $\langle 1,23,60,18\rangle$

□

引理 8.33. 对任意$4 \le t \le 11$，$t \ne 5$，存在一个型为6^t3^1，大小为$3t^2$的*GDC*。

证明. 令$X_t = \mathbb{Z}_{6t+3}$，$\mathcal{G}_t = \{\{i, i+t, i+2t, \ldots, i+5t\} : 0 \le i \le t-1\} \cup \{\{6t, 6t+1, 6t+2\}\}$。那么，$(X_t, \mathcal{G}_t, \mathcal{C}_t)$是一个型为$6^t3^1$的GDC，如果$\mathcal{C}_4$是由下面码字在$\mathbb{Z}_{27}$中由自同构群$G = \langle(0\ 2\ 4\ \cdots\ 22)(1\ 3\ 5\ \cdots\ 23)(24\ 25\ 26)\rangle$展开得到，而$6 \le t \le 11$时，$\mathcal{C}_t$是由下面码字在$\mathbb{Z}_{6t+3}$中由自同构群$G = \langle(0\ 1\ 2\ \cdots\ 6t-1)(6t\ 6t+1\ 6t+2)\rangle$展开得到。

$t = 4$：$\langle 1,25,8,6\rangle$ $\langle 1,3,18,0\rangle$ $\langle 0,10,24,23\rangle$ $\langle 1,7,10,20\rangle$ $\langle 0,22,7,1\rangle$ $\langle 0,6,21,11\rangle$ $\langle 1,11,12,26\rangle$ $\langle 8,24,3,1\rangle$

$t = 6$：$\langle 0,34,27,5\rangle$ $\langle 0,28,3,13\rangle$ $\langle 0,10,19,35\rangle$ $\langle 0,20,17,15\rangle$ $\langle 0,37,32,4\rangle$ $\langle 0,14,1,38\rangle$

$t = 7$：$\langle 0,8,12,38\rangle$ $\langle 0,26,25,44\rangle$ $\langle 0,43,20,22\rangle$ $\langle 0,6,23,33\rangle$ $\langle 0,40,1,9\rangle$ $\langle 0,10,15,39\rangle$ $\langle 0,18,31,37\rangle$

$t = 8$：

$\langle 0,10,12,46\rangle$ $\langle 0,4,21,31\rangle$ $\langle 0,26,41,45\rangle$ $\langle 0,28,5,23\rangle$
$\langle 0,48,11,37\rangle$ $\langle 0,42,1,29\rangle$ $\langle 0,14,13,49\rangle$ $\langle 0,18,3,9\rangle$

$t = 9$：

$\langle 0,52,5,21\rangle$ $\langle 0,54,49,53\rangle$ $\langle 0,38,3,51\rangle$ $\langle 0,34,12,22\rangle$ $\langle 0,4,28,30\rangle$
$\langle 0,6,17,37\rangle$ $\langle 0,14,1,47\rangle$ $\langle 0,44,15,29\rangle$ $\langle 0,8,43,55\rangle$

$t = 10$：

$\langle 0,12,36,37\rangle$ $\langle 0,54,45,57\rangle$ $\langle 0,8,29,35\rangle$ $\langle 0,4,9,17\rangle$ $\langle 0,34,23,61\rangle$
$\langle 0,22,53,55\rangle$ $\langle 0,28,7,11\rangle$ $\langle 0,58,16,42\rangle$ $\langle 0,62,19,41\rangle$ $\langle 0,1,15,47\rangle$

$t = 11$：

$\langle 0,10,1,13\rangle$ $\langle 0,67,7,17\rangle$ $\langle 0,12,30,38\rangle$ $\langle 0,64,25,46\rangle$ $\langle 0,4,23,39\rangle$ $\langle 0,34,5,65\rangle$
$\langle 0,16,36,40\rangle$ $\langle 0,21,49,63\rangle$ $\langle 0,6,15,47\rangle$ $\langle 0,8,59,61\rangle$ $\langle 0,14,43,68\rangle$

□

引理 8.34. 对任意$t \in \{6,7,8\}$，存在一个型为6^t9^1，大小为$6t(t+2)$的*GDC*。

证明. 令$X_t = \mathbb{Z}_{6t+9}$，$\mathcal{G}_t = \{\{i, i+t, i+2t, \ldots, i+5t\} : 0 \le i \le t-1\} \cup \{\{6t, 6t+1, 6t+2, \ldots, 6t+8\}\}$。那么，$(X_t, \mathcal{G}_t, \mathcal{C}_t)$是型为$6^t9^1$的GDC，如果$\mathcal{C}_t$是由下面码字在$\mathbb{Z}_{6t+9}$中由自同构群$G = \langle(0\ 1\ 2\ \cdots\ 6t-1)(6t\ 6t+1\ 6t+2\ 6t+3\ 6t+4\ 6t+5)(6t+6\ 6t+7\ 6t+8)\rangle$展开得到。

$t=6$：

$\langle 0,22,13,29\rangle$ $\langle 0,34,21,38\rangle$ $\langle 0,16,19,37\rangle$ $\langle 0,36,5,15\rangle$

$\langle 0,43,17,31\rangle$ $\langle 0,41,33,25\rangle$ $\langle 0,8,4,44\rangle$ $\langle 0,10,9,11\rangle$

$t=7$：

$\langle 0,36,34,10\rangle$ $\langle 0,45,8,39\rangle$ $\langle 0,23,25,49\rangle$ $\langle 0,44,3,22\rangle$ $\langle 0,29,33,42\rangle$

$\langle 0,48,38,1\rangle$ $\langle 0,24,41,12\rangle$ $\langle 0,11,20,26\rangle$ $\langle 0,5,46,32\rangle$

$t=8$：

$\langle 0,10,3,15\rangle$ $\langle 0,14,54,37\rangle$ $\langle 0,49,27,29\rangle$ $\langle 0,36,31,1\rangle$ $\langle 0,46,42,4\rangle$

$\langle 0,22,51,33\rangle$ $\langle 0,56,47,19\rangle$ $\langle 0,18,9,35\rangle$ $\langle 0,48,7,21\rangle$ $\langle 0,20,52,45\rangle$

□

引理 8.35. 分别存在型为$18^4 6^1$，$18^4 12^1$，$24^4 6^1$和$24^4 9^1$的GDC。

证明. 对任意型为$g^u m^1$的GDC，令$X=\mathbb{Z}_{gu+m}$，$\mathcal{G}=\{\{0,u,2u,\ldots,(g-1)u\}+i:0\le i\le u-1\}\cup\{\{gu,gu+1,gu+2,\ldots,gu+m-1\}\}$。那么$(X,\mathcal{G},\mathcal{C})$是需要的GDC，如果$\mathcal{C}$是由下面码字在$\mathbb{Z}_{gu+m}$中由自同构群$G$展开得到。

$18^4 6^1$：$G=\langle(0\ 1\ 2\ \cdots\ 71)(72\ 73\ 74\ 75\ 76\ 77)\rangle$。

$\langle 0,30,1,7\rangle$ $\langle 0,50,53,76\rangle$ $\langle 0,54,21,59\rangle$ $\langle 0,72,29,51\rangle$ $\langle 0,26,9,19\rangle$ $\langle 0,10,25,67\rangle$

$\langle 0,2,13,71\rangle$ $\langle 0,66,17,35\rangle$ $\langle 0,58,31,33\rangle$ $\langle 0,77,37,63\rangle$ $\langle 0,34,61,73\rangle$

$18^4 12^1$：$G=\langle(0\ 1\ 2\ \cdots\ 71)(72\ 73\ 74\ 75\ 76\ 77)\ (78\ 79\ 80\ 81\ 82\ 83)\rangle$。

$\langle 0,46,7,72\rangle$ $\langle 0,77,57,71\rangle$ $\langle 0,34,63,79\rangle$ $\langle 0,22,49,78\rangle$ $\langle 0,6,19,41\rangle$ $\langle 0,76,15,25\rangle$

$\langle 0,14,1,31\rangle$ $\langle 0,18,23,61\rangle$ $\langle 0,42,39,45\rangle$ $\langle 0,82,21,67\rangle$ $\langle 0,83,9,11\rangle$ $\langle 0,10,47,65\rangle$

$\langle 0,70,51,73\rangle$

$24^4 6^1$：$G=\langle(0\ 1\ 2\ \cdots\ 95)(96\ 97\ 98\ 99\ 100\ 101)\rangle$。

$\langle 0,86,25,75\rangle$ $\langle 0,62,5,19\rangle$ $\langle 0,42,23,29\rangle$ $\langle 0,82,81,97\rangle$ $\langle 0,46,41,79\rangle$ $\langle 0,6,7,61\rangle$

$\langle 0,38,11,89\rangle$ $\langle 0,26,3,98\rangle$ $\langle 0,18,27,49\rangle$ $\langle 0,74,37,71\rangle$ $\langle 0,30,21,47\rangle$ $\langle 0,2,15,45\rangle$

$\langle 0,101,63,65\rangle$ $\langle 0,100,57,67\rangle$

$24^4 9^1$：$G=\langle(0\ 1\ 2\ \cdots\ 95)(96\ 97\ 98)(99\ 100\ 101)\ (103\ 104\ 102)\rangle$。

$\langle 0,82,15,73\rangle$ $\langle 0,38,3,49\rangle$ $\langle 0,46,47,98\rangle$ $\langle 0,102,35,37\rangle$ $\langle 0,99,53,79\rangle$ $\langle 0,54,41,59\rangle$

$\langle 0,18,45,31\rangle$ $\langle 0,6,39,69\rangle$ $\langle 0,30,51,9\rangle$ $\langle 0,22,17,104\rangle$ $\langle 0,2,57,67\rangle$ $\langle 0,34,23,101\rangle$

$\langle 0,96,43,77\rangle$ $\langle 0,10,81,7\rangle$ $\langle 0,26,19,25\rangle$

□

Chapter 9

用可分组覆盖构造最优多元常重覆盖码

9.1 引言和主要结果

令X是一个有限集。$|X| = n$。称$\mathbb{Z}_q^X$中的元素为一个字。$\mathbb{Z}_q$上的(n, w, t, d)常重覆盖码是$\mathbb{Z}_q^X$中一个重量为w的子集，使得每个重量为t的字$\mathsf{u} \in \mathbb{Z}_q^X$与至少一个码字的距离为$d$。记这个码的最小可能的码字个数为$K_q(n, w, t, d)$，达到这个码字个数的码称为是最优的。

研究覆盖码的一个出发点是由于它在数据压缩算法中的应用，见[39, 80]。考虑一个编码器，它包含了一些常重覆盖码，每个码的重量都不同。任意一个输入向量x被编码器压缩成一个点对(i, j)，其中i表示根据x的重量选择的码，j表示选择的码中与x最接近的码字。除了这些应用外，$K_q(n, w, t, d)$的确定本身也是组合理论中的一个基本问题，在过去的六十年中有很多数学家研究。在组合设计理论中，有很多类似的组合结构[41]，例如Turán设计，彩票方案和覆盖设计等。当$w - t \geq 0$时，一个$\mathbb{Z}_q$上的$(n, w, t, w - t)$常重覆盖码等价于一些可分组覆盖设计。当$q = 2$ 时，有很多文章研究$K_q(n, w, t, d)$的上界和下界，如[20, 57]。然而，完全确定的只有几类特殊的值，例如：$K_2(n, 2, t, t-2)$ [139]，$K_2(n, 3, 2, 1)$ [58]，$K_2(n, 4, 3, 1)$ [88]，$K_2(n, w, 2, w - 2)$ [90] 等。当$q \geq 3$时，文[89]中也有一些结果。

在本节中，我们将对$q = 3$，4或$q = 2^m + 1$，$m \geq 2$，除了$(q, n) = (3, 5)$外，完全确定$K_q(n, 4, 3, 1)$的值。问题的解决依赖于用组合工具构造一个等价的组合问题，即可分组覆盖，和一种相关的辅助设计H-frame，它对构造可分组3-设计起着与烛台型设计在构造3平衡设计时类似的作用。

这一章的结构如下：在第9.2节中，我们将介绍一些基本概念和基本构造方法；在第9.3节中，我们将构造最优三元常重覆盖码；在第9.4节中，我们将构造最优四元常重覆盖码；在第9.5节中，我们将对任意$q = 2^m + 1$（$m \geq 2$），构造最优q元常重覆盖码；在第9.6节中，将对本章的主要结果进行总结。

9.2 准备知识和构造方法

令v和t为正整数，K是一个正整数集。一个阶数为v，区组大小为K的可分组t覆盖（group divisible covering，GDC），记为GDC(t,K,v)，是一个三元组$(X,\mathcal{G},\mathcal{B})$，其中：

1. X是一个v个元素的集合（称为点）；
2. $\mathcal{G}=\{G_1,G_2,\dots\}$是$X$的一个划分（称为组）；
3. $\mathcal{B}$是$\mathcal{G}$的一组横截（称为区组）的集合，使得任意区组大小为K中的元素，其中每一个横截是X的一个子集且与每个组至多交于一个点；
4. $\mathcal{G}$中的任意t个元素的横截至少包含在一个区组中。

一个t-GDC的剩余是$\mathcal{G}$的t元横截T构成的多重集，其中重数为$|\{B\in\mathcal{B}:T\subset B\}|-1$。GDC$(t,K,v)$的型定义为$\{|G||G\in\mathcal{G}\}$。如果一个GDC有$n_i$个大小为$g_i$的组，$1\le i\le r$，那么我们用指数符号$g_1^{n_1}g_2^{n_2}\cdots g_r^{n_r}$来表示组的型。一个$t$-GDC被称是一致的如果所有的组大小都相同。当$K=\{k\}$时，我们把$K$简记为$k$。

一个t-GDC被称为可分组t-设计（t-GDD），记为GDD(t,k,v)，如果$\mathcal{G}$中的任意t元横截T都恰好包含在一个区组中。Mills在文[113]中用H$(n,g,4,3)$设计来表示型为g^n的GDD$(3,4,ng)$。一个型为1^n的GDD(t,K,n)也称为一个阶数为n，组大小为K的t平衡设计，记为S(t,K,n)。当$t=3$，$K=\{4\}$时，也称为*Steiner*四元系，记为SQS(n)。Hanani在文[84]中指出：一个SQS(n)存在当且仅当$n\equiv 2,4\pmod 6$。

定理 9.1 (Mills [113]，Ji [96]). 对任意$n>3$，$n\neq 5$，一个型为g^n的$GDD(3,4,gn)$存在当且仅当ng是偶数且$g(n-1)(n-2)$可以被3整除。对$n=5$，当g是偶数，$g\neq 2$且$g\neq 10,26\pmod{48}$时，存在一个型为g^5的$GDD(3,4,5g)$。

令$C(n,g,k,t)$表示任意型为g^n的GDC(t,k,ng)的最小可能的区组个数。一个型为g^n的GDC(t,k,ng) $(X,\mathcal{G},\mathcal{B})$是最优的（OGDC）如果$|\mathcal{B}|=C(n,g,k,t)$。显然，如果存在一个型为$g^n$的GDC$(t,k,ng)$，那么它就是最优的。

令$L(n,g,k,t)=\lceil\frac{gn}{k}\lceil\frac{g(n-1)}{k-1}\cdots\lceil\frac{g(n-t+1)}{k-t+1}\rceil\cdots\rceil\rceil$。Schönheim在文[121]中指出对任意$n\ge k\ge t\ge 1$，$C(n,g,k,t)\ge L(n,g,k,t)$。

对$t=3$，$k=4$，$g=1$，Mills在文[111]中指出对任意$n \not\equiv 7 \pmod{12}$，$C(n,1,4,3)=L(n,1,4,3)$。Kalbfleisch等[98]，Swift[136]指出$C(7,1,4,3)=L(7,1,4,3)+1=12$。Mills [112]证明了$C(499,1,4,3)=L(499,1,4,3)$。Hartman等在文[88]中指出对任意$n \geq 52423$，$C(n,1,4,3)=L(n,1,4,3)$。最近Ji [95]改进了他们的结果得到对任意$n$，除了$n=7$，和可能的不确定的值$n=12k+7$，$k \in \{1,2,3,4,5,7,8,9,10,11,12,16,21,23,25,29\}$外，$C(n,1,4,3)=L(n,1,4,3)$。

引理 9.2. *一个型为g^n的$OGDC(t,k,ng)$的存在性等价于一个$\mathbb{Z}_{g+1}$上的最优$(n,k,t,k-t)$常重覆盖码，即：$C(n,g,k,t)=K_{g+1}(n,k,t,k-t)$。*

证明. 假设我们有一个型为g^n的OGDC(t,k,ng)，$(I_n \times I_g, \{\{i\} \times I_g : i \in I_n\}, \mathcal{B})$，其中$I_s=\{1,2,\ldots,s\}$。对任意区组$\{(a_1,b_1),(a_2,b_2),\ldots,(a_k,b_k)\} \in \mathcal{B}$，通过对任意$1 \leq j \leq k$，在第$b_j$位置放$a_j$，其余位置放0，我们得到一个长度为$n$的码字。很容易看出所有的码字形成一个$\mathbb{Z}_{g+1}$上的最优$(n,k,t,k-t)$常重覆盖码。

反之，假设我们有一个$\mathbb{Z}_{g+1}$上的最优$(n,k,t,k-t)$常重覆盖码$\mathcal{C}$。对每一个码字$\mathsf{u} \in \mathcal{C}$，如果$\mathsf{u}$的非零位置为$a_1,a_2,\ldots,a_k$，相应位置的元素是$b_a,b_2,\ldots,b_k$，那么我们可以得到一个区组$\{(a_1,b_1),(a_2,b_2),\ldots,(a_k,b_k)\}$。很容易验证所有的区组形成一个$I_n \times I_g$上，组集为$\{\{i\} \times I_g : i \in I_n\}$上的OGDC$(t,k,ng)$。 □

现在，我们给出H-frame的定义，它是文[88]中的一个推广。一个$H(t,K,v)$ *frame*是一个具有如下性质的有序四元组$(X,\mathcal{G},\mathcal{B},\mathcal{F})$：

1. X是一个v个点的集合；
2. $\mathcal{G}=\{G_1,G_2,\ldots\}$把$X$划分成组；
3. $\mathcal{F}$是$\mathcal{G}$的一族子集$\{F_i\}$，称为洞。每个$F_i \in \mathcal{F}$，$F_i=\{G_{i_1},G_{i_2},\ldots,G_{i_s}\}$，且如果$F_i$和$F_j$是洞，那么$F_i \cap F_j$也是洞。洞中组的个数称为它的大小。
4. $\mathcal{B}$是$\mathcal{G}$的一些横截的集合（称为区组），每个区组大小属于集合K，使得$\mathcal{G}$的任意t元横截，如果不是某个洞$F_i \in \mathcal{F}$的t元横截，恰好包含在一个区组中，没有区组包含洞中的t元横截。

如果$\mathcal{G}$中所有组的大小均为g，那么$(X,\mathcal{G},\mathcal{B},\mathcal{F})$就是一个$H(v/g,g,K,t)$ *frame*，简记为HF$(v/g,g,K,t)$，这与文[88]中定义相同。如果一个HF$(q,g,K,3)$

有n_i个大小为m_i+s个洞，$i=1,2,\ldots,r$，且交于一个公共的大小为s的洞，那么我们把这个设计记为K-HF$_g(m_1^{n_1}m_2^{n_2}\cdots m_r^{n_r}:s)$。当$g=1$时，一个$K$-HF$_1(m_1^{n_1}m_2^{n_2}\cdots m_r^{n_r}:s)$也称为一个**烛台型设计**，记为$K$-CS$(m_1^{n_1}m_2^{n_2}\cdots m_r^{n_r}:s)$ $(X,S,\Gamma,\mathcal{B})$，其中S是一个公共的洞，称为**干**，$\Gamma=\{F\setminus S:F\in\mathcal{F}\}$是一个组的集合。当$K=\{4\}$，也称为**烛台型四元系**（CQS）。如果一个HF$(q,g,K,3)$只有一个大小为s的洞，那么我们称它为一个**不完全可分组设计**，记为IGDD$((q:s),g,K,3)$。

如果一个H$(3,K,v)$ frame，$(X,\mathcal{G},\mathcal{B},\mathcal{F})$具有性质：$\mathcal{G}$中所有的组除了$G_1$的大小为$g-1$外，大小均为$g$，而且$\mathcal{F}$有$n_i$个大小为$m_i+s$的洞，$i=1,2,\ldots,r$，它们交于一个公共的大小为$s$的洞，$G_1$属于这个公共的洞，那么我们称这个H$(3,K,v)$为*modified $H(3,K,v)$ frame*，记为K-MHF$_g(m_1^{n_1}m_2^{n_2}\cdots m_r^{n_r}:s)$。

引理 9.3 (Mills [111]). *对任意$n\geq 0$，存在一个$CQS(6^n:0)$。*

引理 9.4. *对任意$n\geq 3$，存在一个$\{4,6\}$-$CS(2^n:2)$。*

证明. 对任意$n\equiv 0,1\pmod 3$，$n\geq 3$，可以从SQS$(2n+2)$得到一个CQS$(2^n:2)$。对任意$n\equiv 2\pmod 3$，$n\geq 5$，可以从CQS$(6^{(n+1)/3}:0)$取不同组的两个点构成干得到一个$\{4,6\}$-CS$(2^n:2)$。 □

引理 9.5. *假设$(X,S,\Gamma,\mathcal{A})$是一个K-$CS(m^n:s)$，$\infty\in S$。令$K_1=\{|A|:\infty\in A\in\mathcal{A}\}$，$K_2=\{|A|:\infty\notin A\in\mathcal{A}\}$。如果对任意$k_1\in K_1$，存在一个4-$HF_g(t^{k_1-1}:a)$（或4-$MHF_g(t^{k_1-1}:a)$），对任意$k_2\in K_2$，存在一个型为$(gt)^{k_2}$的$GDD(3,4,gtk_2)$，那么分别存在一个4-$HF_g((tm)^n:t(s-1)+a)$和（或4-$MHF_g((tm)^n:t(s-1)+a)$）。*

证明. 假设给定的K-CS$(m^n:s)$的组集为$\Gamma=\{G_1,\ldots,G_n\}$。我们首先给出4-HF$_g((tm)^n:t(s-1)+a)$的构造。定义$G'_{x,j}=x\times\{j\}\times\mathbb{Z}_g$。令$X'=((X\setminus\{\infty\})\times\mathbb{Z}_t\times\mathbb{Z}_g)\cup(\{\infty\}\times\mathbb{Z}_a\times\mathbb{Z}_g)$，$\mathcal{G}'=\{G'_{x,j}:x\in X\setminus\{\infty\},j\in\mathbb{Z}_t\}\cup\{G'_{\infty,j}:j\in\mathbb{Z}_a\}$，$\mathcal{F}=\{F_i:0\leq i\leq n\}$，其中$F_0=\{G'_{x,j}:x\in S\setminus\{\infty\},j\in\mathbb{Z}_t\}\cup\{G'_{\infty,j}:j\in\mathbb{Z}_a\}$是大小为$t(s-1)+a$的公共的洞，且$F_i=\{G'_{x,j}:x\in G_i,j\in\mathbb{Z}_t\}\cup F_0$，$1\leq i\leq n$。

对任意$B\in\mathcal{A}$，$\infty\in B$，构造一个4-HF$_g(t^{|B|-1}:a)$，其中点集为$((B\setminus\{\infty\})\times\mathbb{Z}_t\times\mathbb{Z}_g)\cup(\{\infty\}\times\mathbb{Z}_a\times\mathbb{Z}_g)$，组集为$\{G'_{x,j}:x\in B\setminus\{\infty\},j\in\mathbb{Z}_t\}\cup\{G'_{\infty,j}:$

$j \in \mathbb{Z}_a\}$，洞为$F_x = \{G'_{x,j} : j \in \mathbb{Z}_t\} \cup F_\infty$，$x \in B \setminus \{\infty\}$，交于一个大小为$a$公共的洞$F_\infty = \{G'_{\infty,j} : j \in \mathbb{Z}_a\}$。记区组集为$\mathcal{A}_B$。

对任意$B \in \mathcal{A}$，$\infty \notin B$，构造一个型为$(gt)^{k_2}$的GDD$(3, 4, gtk_2)$，其中点集为$B \times \mathbb{Z}_t \times \mathbb{Z}_g$，组集为$\{x \times \mathbb{Z}_t \times \mathbb{Z}_g : x \in B\}$。记区组集为$\mathcal{C}_B$。

令$\mathcal{A}' = (\cup_{B\in\mathcal{A},\infty\in B}\mathcal{A}_B) \cup (\cup_{B\in\mathcal{A},\infty\notin B}\mathcal{C}_B)$。容易验证$\mathcal{A}'$是$X'$上组集为$\mathcal{G}'$，洞为$\mathcal{F}$的4-HF$_g((tm)^n : t(s-1)+a)$的区组集。

构造4-MHF$_g((tm)^n : t(s-1)+a)$的证明与上面类似。记$\mathbb{Z}_a^* = \mathbb{Z}_a \setminus \{0\}$。令$X'' = ((X \setminus \{\infty\}) \times \mathbb{Z}_t \times \mathbb{Z}_g) \cup (\{\infty\} \times ((\mathbb{Z}_a \times \mathbb{Z}_g) \setminus \{(0,0)\}))$，$\mathcal{G}'' = \{G'_{x,j} : x \in X \setminus \{\infty\}, j \in \mathbb{Z}_t\} \cup \{G'_{\infty,j} : j \in \mathbb{Z}_a^*\} \cup \{G'_{\infty,0} \setminus \{(\infty,0,0)\}\}$，$\mathcal{F}' = \{F'_i : 0 \le i \le n\}$，其中$F'_0 = \{G'_{x,j} : x \in S \setminus \{\infty\}, j \in \mathbb{Z}_t\} \cup \{G'_{\infty,j} : j \in \mathbb{Z}_a^*\} \cup \{G'_{\infty,0} \setminus \{(\infty,0,0)\}\}$是一个大小为$t(s-1)+a$的公共的洞，而且$F'_i = \{G'_{x,j} : x \in G_i, j \in \mathbb{Z}_t\} \cup F'_0$，$1 \le i \le n$。很容易通过构造4-HF$_g((tm)^n : t(s-1)+a)$类似的方法构造$X''$上组集为$\mathcal{G}''$，洞集为$\mathcal{F}'$的4-MHF$_g((tm)^n : t(s-1)+a)$。 □

9.3　最优三元常重覆盖码

在本节中，我们将确定$K_3(n, 4, 3, 1)$，即$C(n, 2, 4, 3)$的值。由定理9.1，如果$n \equiv 1, 2 \pmod 3$，$n \ne 5$，存在型为2^n的GDD$(3, 4, 2n)$，就是对任意这样的n，$C(n, 2, 4, 3) = L(n, 2, 4, 3)$。我们将给出$C(5, 2, 4, 3)$的下界和上界。

引理 9.6. $L(5, 2, 4, 3) + 2 \le C(5, 2, 4, 3) \le 24$。

证明. 可以很容易构造出来具有24个区组的型为2^5的GDC$(3, 4, 10)$。令$X = \mathbb{Z}_8$，$\mathcal{G} = \{\{i, i+4\} : i = 0, 1, 2, 3\}\}$。那么分别存在点集为$X$，组集为$\mathcal{G}$上的型为$2^4$的GDD$(3, 4, 8)$和GDD$(2, 3, 8)$，记其区组集分别为$\mathcal{B}$和$\mathcal{T}$，它们均有8个区组。令$X' = X \cup \{\infty_1, \infty_2\}$，$\mathcal{G}' = \mathcal{G} \cup \{\{\infty_1, \infty_2\}\}$。对任意$i = 1, 2$，令$\mathcal{C}_i = \{T \cup \{\infty_i\} : T \in \mathcal{T}\}$。显然，$\mathcal{B} \cup \mathcal{C}_1 \cup \mathcal{C}_2$是一个点集$X'$，组集$\mathcal{G}'$上的有24个区组的型为$2^5$的GDC$(3, 4, 10)$。因此，$C(5, 2, 4, 3) \le 24$。

对下界，我们只需要证明具有21个区组的型为2^5的GDC$(3, 4, 10)$不存在。假设$(X', \mathcal{G}', \mathcal{A})$是一个型为$2^5$的GDC$(3, 4, 10)$，其中$|\mathcal{A}| = 21$，剩余为$E$。那么$|E| = 4$，$E$包含12个元素，其中至少三个是不同的。假设$E$包含5个或更多的点。那么$E$包含至少15个的元素，因为对剩余中的每个点，剩余中包含这个点的三元组数都被3整除。假设E恰好包含3个不同的点，设为a, b, c，那么

它们在E中出现的次数只能是$3,3,6$。但是这样不可能形成$\{a,b,c\}$ 上的四元组。所以E一定包含四个不同的点，设为a，b，c，d，且每一个包含在E的三个三元组中。所以E应该是由$\{a,b,c\}$，$\{a,b,d\}$，$\{a,c,d\}$，$\{b,c,d\}$组成的。而且$\{a,b,c,d\}\notin\mathcal{A}$。因为否则，我们能从区组集中去掉$\{a,b,c,d\}$得到一个型为$2^5$的GDD$(3,4,10)$。这与它的存在性矛盾。因此，$\{a,b,c\}$，$\{a,b,d\}$，$\{a,c,d\}$，$\{b,c,d\}$一定包含$\mathcal{A}$ 的八个区组中。因为$\{\{a,b,c\},\{a,b,d\},\{a,c,d\},\{b,c,d\}\}$中的任意两个三元组交于两个公共的点，且$\{a,b,c\}$，$\{a,b,d\}$，$\{a,c,d\}$，$\{b,c,d\}$是剩余中仅有的四个三元组，$\mathcal{A}$中的八个区组的最后一个点应该是两两不同的。因此，我们就有了X'中的至少12个点，这就与$|X'|=10$相矛盾。 □

当$n\equiv 0\pmod 3$时，$L(n,2,4,3)=n(n^2-3n+3)/3$。我们称一个型为2^n的GDD$(3,\{4,6\},2n)$是*好的*如果它恰好有$n/3$个大小为6的区组。

引理 9.7. *若存在型为2^n好的$GDD(3,\{4,6\},2n)$，则$C(n,2,4,3)=L(n,2,4,3)$。*

证明. 型为2^n的好的GDD$(3,\{4,6\},2n)$中大小为4的区组数为$n(n^2-3n-3)/3$。把任意大小为6的区组用型为1^6的OGDC$(3,4,6)$替换。因为$C(6,1,4,3)=6$，我们就得到了所需结果。 □

注意到文[142]中对所有$n\equiv 0\pmod 3$构造了型为2^n的GDD$(3,\{4,6\},2n)$，但不是所有都是好的。

引理 9.8 (Wang，Ji [142])**.** *对任意$n\in\{6,9,15\}$，存在一个型为2^n的好的$GDD(3,\{4,6\},2n)$。*

引理 9.9. *对任意$n\equiv 0\pmod 6$，存在一个型为2^n的好的$GDD(3,\{4,6\},2n)$。*

证明. 对任意$n=6k$，$k\geq 1$，从引理9.3取一个CQS$(6^k:0)$。对每个点加权2，并在每个区组上构造一个型为2^4的GDD$(3,4,8)$，就得到了一个4-HF$_2(6^k:0)$。在4-HF$_2(6^k:0)$的洞上填入型为2^6的好的GDD$(3,\{4,6\},12)$得到了所需的型为2^{6k}的好的GDD$(3,\{4,6\},12k)$。 □

引理 9.10. *存在有两个大小为6的区组的$IGDD((9:3),2,\{4,6\},3)$。*

证明. 令点集为$\mathbb{Z}_{18}$，组集为$\{\{i,i+9\}:i=0,1,\ldots,8\}$，洞为$\{\{i,i+9\}:i=6,7,8\}$。两个大小为6的区组是$\{0,1,2,3,4,5\}$ 和$\{9,10,11,12,13,14\}$。剩余

的52×3个大小为4的区组由如下52个基区组由自同构$\langle(0\ 1\ 2)(3\ 4\ 5)(6\ 7\ 8)(9\ 10\ 11)(12\ 13\ 14)(15\ 16\ 17)\rangle$展开得到。

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

□

引理 9.11. *存在一个*4-$HF_2(3^5:0)$。

证明. 令点集为$\mathbb{Z}_{30}$，组集为$\{G_i=\{i,i+15\}:i=0,1,\ldots,4\}$，五个洞为$F_i=\{G_i,G_{i+5},G_{i+10}\}$，$i=0,1,\ldots,4$。所需设计由如下基区组在$\mathbb{Z}_{30}$上+1 (mod 30)展开得到。

$\{0,6,13,27\}$	$\{0,8,11,29\}$	$\{0,3,12,17\}$	$\{0,4,10,23\}$	$\{0,1,4,7\}$	$\{0,21,28,29\}$
$\{0,19,24,28\}$	$\{0,2,7,16\}$	$\{0,1,20,26\}$	$\{0,7,14,26\}$	$\{0,18,23,26\}$	$\{0,2,12,24\}$
$\{0,4,26,29\}$	$\{0,6,7,12\}$	$\{0,13,17,29\}$	$\{0,11,12,19\}$	$\{0,16,18,22\}$	$\{0,2,10,18\}$
$\{0,3,20,23\}$	$\{0,1,3,28\}$	$\{0,5,7,13\}$	$\{0,5,17,26\}$	$\{0,2,4,13\}$	$\{0,2,9,22\}$
$\{0,13,19,22\}$	$\{0,9,10,19\}$	$\{0,5,6,22\}$	$\{0,10,14,24\}$	$\{0,5,16,19\}$	$\{0,1,11,13\}$

□

下面结果基于Hartman在[86, 第4节]中对CQS$((6n)^3:2s)$的构造，主要的辅助设计是一类称为*A-pairing*（记为$A(n,2s)$）的设计。

定理 9.12. *对任意*$3n\geq s\geq 0$，*存在一个*4-$HF_2((3n)^3:s)$。

证明. 对任意$3n\geq s\geq 0$，$(n,s)\neq(1,1)$，Hartman在[86, 第4节]中构造了一类CQS$((6n)^3:2s)$，其中点集$X=\{a_i:a\in\mathbb{Z}_{6n},i\in\mathbb{Z}_3\}\cup\{\infty_1,\infty_2,\ldots,\infty_{2s}\}$，组集$\{\{a_i:a\in\mathbb{Z}_{6n}\}:i\in\mathbb{Z}_3\}$，干为$\{\infty_1,\infty_2,\ldots,\infty_{2s}\}$。令区组集为$\mathcal{B}$，其中有一类区组：

$$\phi=\{\{a_i,b_i,c_{i+1},d_{i+1}\}:\{a,b\}\in F_i^{(k)},\{c,d\}\in F_{i+1}^{(k)},\\ 1\leq k\leq 6n-1-2r-2h,i\in\mathbb{Z}_3\},$$

这里，$F_i^{(1)}|F_i^{(2)}|\ldots|F_i^{(6n-1-2r-2h)}$是由$A(n,2s)$定义的图$\mathbb{Z}_{6n}\times\{i\}$的一因子分解。由[86, 第5节]中$A(n,2s)$的具体构造，我们知道$6n-1-2r-2h\geq 1$。

所需的4-HF$_2((3n)^3:s)$将在点集X上构造，其中组集$\mathcal{G}=\{\{a_i,b_i\}:\{a,b\}\in F_i^{(1)},i\in\mathbb{Z}_3\}\cup\{\{\infty_i,\infty_{i+s}\}:1\le i\le s\}$，三个洞$\mathcal{F}_{i+1}=\{\{a_i,b_i\}:\{a,b\}\in F_i^{(1)}\}\cup\mathcal{F}_0$，$i\in\mathbb{Z}_3$，交于一个公共的洞$\mathcal{F}_0=\{\{\infty_i,\infty_{i+s}\}:1\le i\le s\}$。

令

$$\phi_1=\{\{a_i,b_i,c_{i+1},d_{i+1}\}:\{a,b\}\in F_i^{(1)},\{c,d\}\in F_{i+1}^{(1)},i\in\mathbb{Z}_3\}.$$

注意到$\phi_1\subset\phi$，而且ϕ_1中的每个区组交于$\mathcal{G}$中两个不同洞的组。很容易验证$\mathcal{B}\setminus\phi_1$就是所需4-HF$_2((3n)^3:s)$的区组集。

对$(n,s)=(1,1)$，一个4-HF$_2(3^3:1)$可以由引理9.5，并用文[84]中的CQS$(3^3:1)$和一个型为2^4的GDD$(3,4,8)$得到。 □

引理 9.13. *对所有$n\equiv3\pmod 6$，$n\ge9$，存在型为2^n好的$GDD(3,\{4,6\},2n)$。*

证明. 对$n\in\{9,15\}$，所需设计由引理9.8得到。对任意$n=6m+3$，$m\ge3$，由引理9.4存在一个$\{4,6\}$-CS$(2^m:2)$。应用引理9.5，取$g=2$，$t=3$，$a=0$就得到了4-HF$_2(6^m:3)$。这里输入设计为4-HF$_2(3^{k-1}:0)$和型为6^k的GDD$(3,4,6k)$，$k\in\{4,6\}$（定理9.1，9.12和引理9.11）。对4-HF$_2(6^m:3)$的前$m-1$个洞，填入IGDD$((9:3),2,\{4,6\},3)$（引理9.10）。在最后一个洞填入一个型为2^9的好的GDD$(3,\{4,6\},18)$。我们就得到了一个型为2^n的好的GDD$(3,\{4,6\},2n)$。 □

综合引理9.6，9.7，9.9和9.13，我们得到：

定理 9.14. *对任意$n\ge4$，$n\ne5$，$C(n,2,4,3)=L(n,2,4,3)$。*

9.4 最优四元常重覆盖码

在本节中，我们将确定$K_4(n,4,3,1)$，即$C(n,3,4,3)$的值。由定理9.1，对任意$n\equiv0\pmod 2$，存在型为3^n的GDD$(3,4,3n)$，即$C(n,3,4,3)=L(n,3,4,3)$。当$n\equiv1\pmod 2$时，$L(n,3,4,3)=3n(n-1)(3n-5)/8$。型为$3^n$的GDC$(3,4,3n)$被称为是好的，如果它的剩余形成一个型为$3^n$的GDD$(2,3,3n)$。容易验证一个型为$3^n$的好的GDC$(3,4,3n)$的区组个数恰好为$L(n,3,4,3)$。我们得到：

引理 9.15. *若存在型为3^n好的$GDC(3,4,3n)$，则$C(n,3,4,3)=L(n,3,4,3)$。*

引理 9.16. 对任意$n \in \{5,7,9,11\}$，存在一个型为3^n的好的$GDC(3,4,3n)$。

证明. 对任意$n \in \{5,7,9,11\}$，一个型为3^n的好的GDC$(3,4,3n)$是在点集$\mathbb{Z}_{3n}$，组集$\{\{i,i+n,i+2n\} : i = 0,1,\ldots,n-1\}$上构造，所需区组由如下基区组在$\mathbb{Z}_{3n}$上展开得到。

$n=5$：$\{0,1,2,4\}$ $\{0,1,4,13\}$ $\{0,1,7,9\}$ $\{0,1,8,12\}$ $\{0,2,8,11\}$

$n=7$：

$\{0,11,15,17\}$ $\{0,12,18,20\}$ $\{0,8,9,11\}$ $\{0,1,6,11\}$ $\{0,16,17,20\}$ $\{0,1,12,16\}$
$\{0,2,8,18\}$ $\{0,3,5,8\}$ $\{0,9,12,15\}$ $\{0,8,19,20\}$ $\{0,4,8,16\}$ $\{0,2,4,13\}$

$n=9$：

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

$n=11$：

$\{0,1,10,14\}$ $\{0,17,18,21\}$ $\{0,21,23,29\}$ $\{0,25,29,32\}$ $\{0,9,19,25\}$ $\{0,4,10,19\}$
$\{0,9,14,26\}$ $\{0,1,13,17\}$ $\{0,8,16,23\}$ $\{0,2,6,19\}$ $\{0,17,20,30\}$ $\{0,1,6,20\}$
$\{0,1,15,16\}$ $\{0,21,28,31\}$ $\{0,2,5,14\}$ $\{0,4,6,9\}$ $\{0,3,8,24\}$ $\{0,20,26,27\}$
$\{0,8,10,29\}$ $\{0,13,21,26\}$ $\{0,7,9,24\}$ $\{0,5,6,8\}$ $\{0,4,12,13\}$ $\{0,7,14,30\}$
$\{0,14,17,23\}$ $\{0,2,10,28\}$ $\{0,1,5,31\}$ $\{0,13,15,28\}$ $\{0,2,16,31\}$ $\{0,23,28,32\}$
$\{0,9,15,21\}$ $\{0,8,18,28\}$ $\{0,6,13,25\}$ $\{0,15,27,30\}$ $\{0,1,8,32\}$

□

为了给出循环构造，我们需要定义一种不完全的好的可分组覆盖。令X是一个大小为$3n$的点集，$\mathcal{G}$是X的一个分成n个大小为3的组的划分。假设$\mathcal{H} \subset \mathcal{G}$是一个大小为$m$的洞，也就是$m$个组的集合。$\mathcal{B}$是一族横截四元组（区组）使得没有区组包含洞中的三元组，每个不在洞中的横截三元组包含在至少一个区组中，并且剩余形成一个型为$3^{n-m}(3m)^1$的GDD$(2,3,3n)$。那么$(X,\mathcal{G},\mathcal{H},\mathcal{B})$就称为一个型为$(3^n:3^m)$的不完全的好的GDC$(3,4,3n)$。

引理 9.17. 假设存在一个4-$MHF_3(m^n:s)$。如果存在一个型为$(3^{m+s}:3^s)$的不完全的好的$GDC(3,4,3(m+s))$，那么分别存在型为$(3^{mn+s}:3^s)$和$(3^{mn+s}:3^{m+s})$的不完全的好的$GDC(3,4,3(mn+s))$。进一步，如果存在一个型为3^{m+s}的好的$GDC(3,4,3(m+s))$，那么存在一个型为3^{mn+s}的好的$GDC(3,4,3(mn+s))$。

证明. 令$(X,\mathcal{G},\mathcal{B},\mathcal{F})$是给定的4-MHF$_3(m^n:s)$，其中$G_1=\{\alpha,\beta\}$是一个洞$F_0$中的大小为2的特殊组。令$G_1'=G_1\cup\{\infty\}$，$\infty\notin X$。令$X'=X\cup\{\infty\}$，$\mathcal{G}'=$

$\mathcal{G}\cup\{G_1'\}\setminus\{G_1\}$，$\mathcal{F}'=\{\mathcal{F}\cup\{\mathcal{G}_\infty'\}\setminus\{\mathcal{G}_\infty\}:\mathcal{F}\in\mathcal{F}\}$。令$T_\alpha=\{B\setminus\{\alpha\}:\alpha\in B\in\mathcal{B}\}$。那么$T_\alpha$形成型为$(3m)^n$的GDD$(2,3,3mn)$，其中点集为$X\setminus(\cup_{G\in F_0}G)$，组集为$\{\cup_{G\in(F\setminus F_0)}G:F\in\mathcal{F},F\neq F_0\}$。令$B_\infty=\{T\cup\{\infty\}:T\in T_\alpha\}$，$\mathcal{B}'=\mathcal{B}\cup B_\infty$。对任意大小为$m+s$的洞$F'\in\mathcal{F}'$，构造一个型为$(3^{m+s}:3^s)$，洞为$F_0'=F_0\cup\{G_1'\}\setminus\{G_1\}$的不完全的GDC$(3,4,3(m+s))$。记区组集为$\mathcal{A}_{F'}$，剩余形成长组为$\cup_{G\in F_0'}G$的型为$3^m(3s)^1$的GDD$(2,3,3(m+s))$。令$\mathcal{C}=\mathcal{B}'\cup(\cup_{F'\in\mathcal{F}',F'\neq F_0'}\mathcal{A}_{F'})$。很容易验证$\mathcal{C}$的剩余形成长组为$\cup_{G\in F_0'}G$的型为$3^{mn}(3s)^1$的GDD$(2,3,3(mn+s))$。因此，$\mathcal{C}$是$X'$上组集为$\mathcal{G}'$，洞为$F_0'$，型为$(3^{mn+s}:3^s)$的好的GDC$(3,4,3(mn+s))$。如果我们保留最后一个洞，或者填入一个型为$3^{m+s}$的GDC$(3,4,3(m+s))$，我们就分别得到了一个型为$(3^{mn+s}:3^{m+s})$不完全的好的GDC$(3,4,3(mn+s))$或一个型为$3^{mn+s}$的好的GDC$(3,4,3(mn+s))$。□

引理 9.18. *存在一个型为$(3^7:3^3)$的不完全的好的$GDC(3,4,21)$。*

证明. 令点集为$\mathbb{Z}_{21}$，组集为$\{\{i,i+7,i+14\}:i=0,1,\ldots,6\}$，洞为$\{\{i,i+7,i+14\}:i=4,5,6\}$。所需设计由如下基区组由自同构群$\langle(0\ 7\ 14)(1\ 2\ 3\ 8\ 9\ 10\ 15\ 16\ 17)(4\ 5\ 6\ 11\ 12\ 13\ 18\ 19\ 20)\rangle$展开得到。

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

□

引理 9.19. *存在一个型为$(3^9:3^3)$的不完全的好的$GDC(3,4,27)$。*

证明. 令点集为$\mathbb{Z}_{27}$，组集为$\{\{i,i+9,i+18\}:i=0,1,\ldots,8\}$，洞为$\{\{i,i+9,i+18\}:i=6,7,8\}$。所需设计由如下基区组由自同构群$\langle(0\ 1\ 2\ 9\ 10\ 11\ 18\ 19\ 20)(3\ 4\ 5\ 12\ 13\ 14\ 21\ 22\ 23)(6\ 7\ 8)(15\ 16\ 17)(24\ 25\ 26)\rangle$展开得到。

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

□

引理 9.20. *存在一个*4-$MHF_3(2^3:1)$。

证明. 令点集为$\mathbb{Z}_{20}$，组集为$\{G_i=\{i,i+6,i+12\}:i=0,1,\ldots,5\}$，三个洞$\{G_i,G_{i+3}\}\cup S$，$i=0,1,2$交于一个公共的洞$S=\{\{18,19\}\}$。所需设计由如下基区组由自同构群$\langle(0\ 6\ 12)(1\ 7\ 13)(2\ 8\ 14)(3\ 9\ 15)(4\ 10\ 16)(5\ 11\ 17)(18)(19)\rangle$展开得到。

$\{3,5,6,8\}$	$\{0,10,11,18\}$	$\{2,10,13,17\}$	$\{0,2,9,10\}$	$\{4,8,12,13\}$	$\{2,3,4,18\}$
$\{0,8,16,18\}$	$\{0,3,4,7\}$	$\{2,3,10,19\}$	$\{0,14,16,19\}$	$\{9,10,11,19\}$	$\{1,3,8,18\}$
$\{6,9,11,16\}$	$\{0,7,9,11\}$	$\{1,9,17,18\}$	$\{4,9,17,19\}$	$\{6,11,13,19\}$	$\{0,13,14,18\}$
$\{0,7,15,16\}$	$\{0,1,4,15\}$	$\{5,8,10,13\}$	$\{0,5,13,16\}$	$\{1,5,9,19\}$	$\{0,2,7,18\}$
$\{0,2,4,5\}$	$\{2,9,16,18\}$	$\{7,10,14,15\}$	$\{1,11,15,18\}$	$\{4,5,6,9\}$	$\{0,2,13,19\}$
$\{5,10,12,14\}$	$\{0,4,11,13\}$	$\{6,7,17,19\}$	$\{0,4,17,18\}$	$\{1,2,4,12\}$	$\{12,13,17,18\}$

$\{1,2,5,10\}$	$\{4,7,9,12\}$	$\{1,8,10,15\}$	$\{2,3,5,7\}$	$\{2,5,9,12\}$	$\{2,3,6,11\}$
$\{3,8,12,16\}$	$\{12,13,14,15\}$	$\{5,9,14,16\}$	$\{1,8,11,12\}$	$\{2,5,15,16\}$	$\{3,10,12,13\}$
$\{0,10,17,19\}$	$\{3,7,8,19\}$	$\{0,9,13,17\}$	$\{0,1,8,17\}$	$\{2,7,9,19\}$	$\{10,15,17,18\}$
$\{5,8,12,15\}$	$\{0,4,8,19\}$	$\{10,11,13,14\}$	$\{1,2,9,11\}$	$\{11,13,15,16\}$	$\{1,4,5,14\}$
$\{2,3,12,17\}$	$\{0,3,8,13\}$	$\{4,5,13,15\}$			

□

引理 9.21. *存在一个*4-$MHF_3(2^5:1)$。

证明. 令点集为$\mathbb{Z}_{32}$，组集为$\{G_i=\{i,i+10,i+20\}:i=0,1,\ldots,9\}$，五个洞$\{G_i,G_{i+5}\}\cup S$，$i=0,1,2,3,4$交于一个公共的洞$S=\{\{30,31\}\}$。所需设计由如下基区组由自同构群$\langle(0\ 1\ 2\ 3\ 4\ 5\ 6\ \cdots 21\ 22\ 23\ 24\ 25\ 26\ 27\ 28\ 29)(30\ 31)\rangle$展开得到。

$\{12,17,26,28\}$	$\{15,24,27,31\}$	$\{10,18,22,24\}$	$\{2,6,17,19\}$	$\{6,12,19,31\}$	$\{2,9,15,21\}$
$\{7,19,22,25\}$	$\{1,9,23,27\}$	$\{2,7,19,24\}$	$\{6,7,23,24\}$	$\{3,6,7,22\}$	$\{0,6,14,21\}$
$\{0,4,18,31\}$	$\{2,3,5,10\}$	$\{18,25,26,29\}$	$\{2,11,18,20\}$	$\{6,14,23,31\}$	$\{0,1,7,12\}$
$\{1,18,22,27\}$	$\{2,3,4,31\}$	$\{3,18,24,25\}$	$\{6,11,14,27\}$	$\{7,8,26,29\}$	$\{13,15,19,22\}$
$\{19,22,24,26\}$	$\{4,23,25,28\}$	$\{12,15,26,30\}$	$\{2,6,13,30\}$	$\{18,19,23,24\}$	$\{12,14,15,29\}$
$\{7,12,19,26\}$	$\{2,13,19,21\}$	$\{11,13,19,31\}$			

□

引理 9.22. *对所有*$n\equiv 3\pmod 4$，$n\geq 7$，*存在型为*3^n*的好的*$GDC(3,4,3n)$。

证明. 对$n\in\{7,11\}$，所需设计在引理9.16中构造得到。对$n=4m+3$，$m\geq 3$，从引理9.4取一个$\{4,6\}$-CS$(2^m:2)$。应用引理9.5，这里用4-MHF$_3(2^{k-1}:1)$和型为6^k的GDD$(3,4,6k)$，$k\in\{4,6\}$作为输入设计，我们就得到了4-MHF$_3(4^m:3)$。然后用引理9.17用$m-1$个不完全的型为$(3^7:3^3)$的好的GDC$(3,4,21)$和一个型为3^7的好的GDC$(3,4,21)$作为输入设计就得到了所需结果。这里的输入设计来源于引理9.18，9.20和9.21。 □

如下的4-MHF$_3((2n)^3 : s)$也是基于Hartman在文[86, 第4节]对CQS$((6n)^3 : 2s)$的构造。首先，我们介绍一些概念。对$x \in \mathbb{Z}_n$，令$|x|$为x，若$0 \le x \le n/2$，为$n-x$，若$n/2 < x < n$。对图$\mathbb{Z}_n$的任意边集E，我们用LE来表示E中的边的长度的集合，即：$LE = \{|x-y| : \{x,y\} \in E\}$。对$n \ge 2$，$L \subseteq \{1,2,\ldots,\lfloor n/2 \rfloor\}$，令G$(n,L)$是点集$\mathbb{Z}_n$上，边集为$E$的正则图，使得$\{x,y\} \in E$当且仅当$|x-y| \in L$。

定理 9.23. *对任意正整数n和奇数s，$6n \ge 3s-1$，存在一个4-$MHF_3((2n)^3 : s)$。*

证明. 对$(n,s) = (1,1)$，所需设计由引理9.20得到。对任意正整数n和奇数s，$6n \ge 3s-1$，$(n,s) \ne (1,1)$，我们在$\mathbb{Z}_{6n}$上构造与文[86]中的A-pairing类似的辅助设计$(D, H, R_0, R_1, R_2)_{(n,s)}$。这里，长度为$2n$的边不出现。

1. 当$n = 2$，$s = 1$时，令$D = \{4, 10\}$，$H = \{\{1,-1\}\{2,7\}\}$，$R_0 = \{\{3,6\}\}$，$R_1 = \{\{5,8\}\}$，$R_2 = \{\{0,9\}\}$。

2. 当$n \ge 3$，$s = 1$时，令$D = \{2n, 4n-1\}$，$H = \{\{1,-1\},\{2,-2\}\}$，$R_0 = \{\{0,2n-1\}\} \cup \{\{k, 2n-k+1\} : k = 3,4,\ldots,n\}$，$R_1 = \{\{2n+k, 4n-k-1\} : k = 1,2,\ldots,n-1\}$，$R_2 = \{\{4n+k, 6n-3-k\} : k = 0,1,\ldots,n-2\}$。

3. 当$s \ge 3$，$6n \ge 3s-1$时，$(D, H, R_0, R_1, R_2)_{(n,s)}$由$(D', H', R_0', R_1', R_2')_{(n,s-2)}$循环构造得到。令$r_i$是$R_i'$中的元素。那么$D = D' \cup (\cup_{i=0}^{i=2} r_i)$，$H = H'$，$R_i = R_i' \setminus \{r_i\}$，$i = 0,1,2$。

对如上的任意点对(n,s)，很容易验证图$G(6n, LH \cup LR_i \cup \{2n\})$的补图存在一因子分解$F_i^{(1)}|F_i^{(2)}|\ldots|F_i^{(4n+s-6)}$，$i = 0,1,2$。现在所需的4-MHF$_3((2n)^3 : s)$如下构造：令$X = \{a_i : a \in \mathbb{Z}_{6n}, i \in \mathbb{Z}_3\} \cup \{\infty_1, \infty_2, \ldots, \infty_{3s-1}\}$，$G_{i,j} = \{j_i, (j+2n)_i, (j+4n)_i\}$，$i = 0,1,2$，$j = 0,\ldots,2n-1$，$G_{\infty,j} = \{\infty_j, \infty_{j+s}, \infty_{j+2s}\}$，$j = 1,2,\ldots,s-1$，$G_{\infty,s} = \{\infty_s, \infty_{2s}\}$。这里有三个洞$F_i = \{G_{i,j} : j = 0,\ldots,2n-1\} \cup S$，$i = 0,1,2$交于一个公共的洞$S = \{G_{\infty,j} : j = 1,2,\ldots,s\}$。令区组集

为$\mathcal{B}$，它包含如下五个区组集：

$$\begin{aligned}
\delta = \{&\{\infty_j, (a+d)_0, (b-d)_1, (c+d)_2\}:\ a+b+c \equiv 0 \pmod{6n},\\
&D\text{是}d\text{的第}j\text{个元素}, 1 \le j \le 3s-1\},\\
\rho = \{&\{(a+q)_i, (a+t)_i, b_{i+1}, c_{i+2}\} : a+b+c \equiv 0 \pmod{6n},\\
&\{q,t\} \in R_i, i \in \mathbb{Z}_3\},\\
\phi = \{&\{a_i, b_i, c_{i+1}, d_{i+1}\} : \{a,b\} \in F_i^{(k)}, \{c,d\} \in F_{i+1}^{(k)},\\
&1 \le k \le 4n+s-6, i \in \mathbb{Z}_3\},\\
\chi_1 = \{&\{a_{i+1}, (a+3\epsilon)_{i+2}, (x-2a-3\epsilon)_i, (y-2a-3\epsilon)_i\} :\\
&a \in \mathbb{Z}_{6n}, i \in \mathbb{Z}_3, \epsilon \in \mathbb{Z}_{2n}, \{x,y\} \in H\},\\
\chi_2 = \{&\{a_i, (a+|x-y|)_i, (a+3\epsilon)_{i+1}, (a+3\epsilon+|x-y|)_{i+1}\} :\\
&a \in \mathbb{Z}_{6n}, i \in \mathbb{Z}_3, \epsilon \in \mathbb{Z}_{2n}, \{x,y\} \in H\}。
\end{aligned}$$

剩下的证明与文[86]中的证明类似，我们将略去。 □

引理 9.24. *对任意$n \equiv 5 \pmod 8$，存在一个型为3^n的好的$GDC(3,4,3n)$。*

证明. 对$n=5$，所需设计由引理9.16得到。对任意$n \equiv 5, 13 \pmod{24}$，$n \ge 13$，从SQS$((n+3)/4)$得到CQS$(1^{(n-1)/4}:1)$。用引理9.5，用4-MHF$_3(4^3:1)$和一个型为12^4的GDD$(3,4,48)$作为输入设计，我们就得到了一个4-MHF$_3(4^{(n-1)/4}:1)$。然后用引理9.17，并将型为3^5的好的GDC$(3,4,15)$作为输入设计。这里的输入设计4-MHF$_3(4^3:1)$来自定理9.23。

对$n=21$，从定理9.23取一个4-MHF$_3(6^3:3)$。应用引理9.17，并把不完全的型为$(3^9:3^3)$的好的GDC$(3,4,27)$（引理9.19）和型为3^9的好的GDC$(3,4,27)$（引理9.16）作为输入设计，就得到了型为3^{21}的好的GDC$(3,4,63)$和型为$(3^{21}:3^9)$的不完全的好的GDC$(3,4,63)$。

对$n=45$，从定理9.23取一个4-MHF$_3(12^3:9)$。应用引理9.17，并把型为3^{21}的好的GDC$(3,4,63)$，和型为$(3^{21}:3^9)$的不完全的好的GDC$(3,4,63)$作为输入设计，就得到了型为3^{45}的好的GDC$(3,4,135)$和型为$(3^{45}:3^{21})$的不完全的好的GDC$(3,4,135)$。

对$n=69$，从定理9.23取一个4-MHF$_3(8^3:1)$。用引理9.17，并把型为3^9的好的GDC$(3,4,27)$和型为$(3^9:3^3)$的不完全的好的GDC$(3,4,27)$作为输入设

计就得到了型为$(3^{25}:3^3)$的不完全的好的GDC$(3,4,75)$和一个型为3^{25}的好的GDC$(3,4,75)$。然后从定理9.23取一个4-MHF$_3(22^3:3)$，并应用引理9.17，把型为$(3^{25}:3^3)$的不完全的好的GDC$(3,4,75)$，和型为3^{25}的好的GDC$(3,4,75)$作为输入设计就得到了型为3^{69}的好的GDC$(3,4,207)$。

对任意$n=24k+21$，$k\geq 3$，我们先说明存在CQS$(6^k:6)$。事实上，假设$(X,\mathcal{G},\mathcal{B})$是一个型为$6^{k+1}$的GDD$(3,4,6(k+1))$，其中$\mathcal{G}=\{G_i:i=1,2,\ldots,k+1\}$。对任意$i=1,2,\ldots,k$，点集为$G_i$的完全图存在一因子分解$F_i^{(1)}|F_i^{(2)}|\cdots|F_i^{(5)}$。对任意点对$\{i,j\}\subset\{1,2,\ldots,k\}$，令$\mathcal{A}_{i,j}=\{\{a,b,c,d\}:\{a,b\}\in F_i^{(l)},\{c,d\}\in F_j^{(l)},l=1,2,\ldots,5\}$。那么$\mathcal{B}\cup(\cup_{\{i,j\}\subset\{1,2,\ldots,k\}}\mathcal{A}_{i,j})$就是$X$上，组集为$\mathcal{G}\setminus\{G_{k+1}\}$，干为$G_{k+1}$的CQS$(6^k:6)$的区组集。这里取一个CQS$(6^k:6)$，应用引理9.5，并把4-MHF$_3(4^3:1)$和一个型为$12^4$的GDD$(3,4,48)$作为输入设计就得到了4-MHF$_3(24^k:21)$。然后应用引理9.17，把型为$3^{45}$的好的GDC$(3,4,135)$和型为$(3^{45}:3^{21})$的好的GDC$(3,4,135)$作为输入设计就得到了所需设计。 □

定理 9.25. *对任意正整数n和奇数s，$6n\geq 3s-1$，存在一个4-$MHF_3((2n)^4:s)$。*

证明. 对任意正整数n和奇数s，$6n\geq 3s-1$，Granville和Hartman在文[79]中构造了一类CQS$((6n)^4:3s-1)$，其中点集$X=\{a_i:a\in\mathbb{Z}_{6n},i\in\mathbb{Z}_4\}\cup\{\infty_1,\infty_2,\ldots,\infty_{3s-1}\}$，组为$\{\{a_i:a\in\mathbb{Z}_{6n}\}:i\in\mathbb{Z}_4\}$，干为$\{\infty_1,\infty_2,\ldots,\infty_{3s-1}\}$。他们定义了Hanani分解，就是四元组$(D,E,\mathcal{G},\mathcal{H})$，使得$D\subset\{1,3,5,\ldots,6n-1\}$，$E\subset\{0,2,4,\ldots,6n-2\}$，$|D|=|E|=(3s-1)/2$，$\mathcal{G}=\{G_0,G_1,\ldots,G_{3n-1}\}$是点集$\mathbb{Z}_{6n}$上完全图的部分一因子，其中$|G_i|=3n-(3s-1)/2$覆盖了$\mathbb{Z}_{6n}\setminus((D\cup E)+2i)$，$i\in\{0,1,\ldots,3n-1\}$，$\mathcal{H}$是一个一因子的集合，使得$\mathcal{G}\cup\mathcal{H}$是点集$\mathbb{Z}_{6n}$上完全图的一个划分。现在我们修改他们的构造来得到一个4-MHF$_3((2n)^4:s)$。定义Γ是一个覆盖$\mathcal{G}$中所有边的图。由文[79, 定理6.1]中Hanani分解的直接构造，Γ是循环的且不包含长度为$2n$的边。令Υ是有$2n$个部，$\{i,i+2n,i+4n\}$，$i=0,1,\ldots,2n-1$的完全多部图。不难验证Γ在Υ 中的补有一个一因子分解，记为$\mathcal{H}'$。在CQS$((6n)^4:3s-1)$的构造中，用$\mathcal{H}'$替换$\mathcal{H}$。另外，把完全图$\mathbb{Z}_{6n}$的出现在区组

$$\{\{h_i,\overline{h}_i,a_j,\overline{a}_j\}:\{i,j\}\in\{\{0,1\},\{2,3\}\},\{h,\overline{h}\},\{a,\overline{a}\}\in J_k,0\leq k\leq 6n-2\}$$

中的一因子分解$J_0|J_1|\ldots|J_{6n-2}$用Υ替换。

令$G_{i,j}=\{j_i,(j+2n)_i,(j+4n)_i\}$，$i=0,1,2,3$，$j=0,\ldots,2n-1$，$G_{\infty,j}=\{\infty_j,\infty_{j+s},\infty_{j+2s}\}$，$j=1,2,\ldots,s-1$，$G_{\infty,s}=\{\infty_s,\infty_{2s}\}$。那么如上构造的区组集构成一个点集$X$，组集为$\{G_{i,j}:i=0,1,2,3,j=0,\ldots,2n-1\}\cup\{G_{\infty,j}:j=1,2,\ldots,s\}$，四个洞$F_i=\{G_{i,j}:j=0,\ldots,2n-1\}\cup S$，$i=0,1,2,3$，交于一个公共的洞$S=\{G_{\infty,j}:j=1,2,\ldots,s\}$的4-MHF$_3((2n)^4:s)$。□

引理 9.26. *对所有$n\equiv 1\pmod 8$，$n\geq 9$，存在型为3^n的好的$GDC(3,4,3n)$。*

证明. 对任意$n=8k+1$，$k\geq 1$，证明由递归得到。对$k=1$，一个型为3^9的好的GDC$(3,4,27)$由引理9.16得到。当$k>1$时，假设对任意$i<k$，存在型为3^{8i+1}的好的GDC$(3,4,3(8i+1))$。由引理9.22和9.24，我们得到对任意奇数$j<8k+1$，都存在型为3^j的好的GDC$(3,4,3j)$。应用引理9.17，并把一个4-MHF$_3((2k)^4:1)$型为3^{2k+1}的好的GDC$(3,4,3(2k+1))$作为输入设计，就得到了型为3^{8k+1}的好的GDC$(3,4,3(8k+1))$。□

结合引理9.22，9.24和9.26，我们得到：

定理 9.27. *对任意$n\geq 4$，$C(n,3,4,3)=L(n,3,4,3)$。*

9.5　$\mathbb{Z}_{2^m+1}$上的最优常重覆盖码

在本节中，我们将给出一个$\mathbb{Z}_{2^m+1}$上最优$(n,4,3,1)$常重覆盖码的一般结果，即：构造组大小为2^m，$m\geq 2$的最优可分组覆盖。从定理9.1, 对任意$g\equiv 2,4\pmod 6$，$g\neq 10,26\pmod{48}$，$n\equiv 1,2\pmod 3$，存在型为g^n的GDD$(3,4,gn)$，也就是对任意这样的g和n，$C(n,g,4,3)=L(n,g,4,3)$。现在我们考虑$g\equiv 2,4\pmod 6$，$n\equiv 0\pmod 3$的情况。容易计算$L(n,g,4,3)=g^3n(n-1)(n-2)/24+gn/6$。所以如果存在恰好有$\frac{ng}{6}$个大小为6的区组的型$g^n$的GDD$(3,\{4,6\},gn)$，我们用型为$1^6$的OGDC$(3,4,6)$替换大小为6的区组，就得到有$L(n,g,4,3)$个区组的型为$g^n$的GDC$(3,4,gn)$。

与第3节中的定义类似，我们称一个型为g^n的GDD$(3,\{4,6\},gn)$*是好的*，如果它恰好包含$\frac{ng}{6}$个大小为6的区组。

引理 9.28. *如果存在一个型为g^n的好的$GDD(3,\{4,6\},gn)$，那么存在一个型为$(2g)^n$的好的$GDD(3,\{4,6\},2gn)$。*

证明. 令$(X, \mathcal{G}, \mathcal{B})$是给定的型为$g^n$的好的GDD$(3, \{4, 6\}, gn)$，其中恰好有$gn/6$个大小为6的区组。令$X' = X \times \mathbb{Z}_2$，$\mathcal{G}' = \{G \times \mathbb{Z}_2 : G \in \mathcal{G}\}$。对任意大小为4的区组$B \in \mathcal{B}$，在$B \times \mathbb{Z}_2$上构造型为$2^4$的GDD$(3, 4, 8)$，其中组为$\{x\} \times \mathbb{Z}_2$，$x \in B$。记其区组集为$\mathcal{A}_B$。对任意大小为6的区组$B \in \mathcal{B}$，在$B \times \mathbb{Z}_2$上构造型为$2^6$的GDD$(3, 4, 12)$，其中组集为$\{x\} \times \mathbb{Z}_2$，$x \in B$。记其区组集为$\mathcal{C}_B$。容易验证$(X', \mathcal{G}', (\cup_{B\in\mathcal{B},|B|=4}\mathcal{A}_B) \cup (\cup_{B\in\mathcal{B},|B|=6}\mathcal{C}_B))$就是型为$(2g)^n$的GDD$(3, \{4, 6\}, 2gn)$，其中$gn/3$个区组的大小为6。 □

对任意整数$m \geq 2$，显然$2^m \equiv 2, 4 \pmod 6$，$2^m \not\equiv 10, 26 \pmod{48}$。结合定理9.1，引理9.28，和引理9.9，9.13，我们得到如下结果：

定理 9.29. 对任意$m \geq 2$，$n \geq 4$，$C(n, 2^m, 4, 3) = L(n, 2^m, 4, 3)$。

9.6 结论

在本章中，我们对所有$n \geq 4$，$q = 3, 4$或者$q = 2^m + 1$，$m \geq 2$，除了唯一不确定的值$(q, n) = (3, 5)$外，确定了$\mathbb{Z}_q$上的最优$(n, 4, 3, 1)$常重覆盖码的码字个数。

Chapter 10

构造具有分裂性质的认证码

10.1 引言

在认证码的标准模型中[122–124, 127]，一个*发射器*需要在一个不安全信道传送信息给一个*接收器*，而一个*敌人*访问这个信道并想欺骗接收器。敌人可以在这个信道加入一些新的信息，或者从发射器拦截信息并修改成自己的信息。在任意一种情况下，敌人的目标都是欺骗接收器使之相信新的信息是可信的（即来源于发射器）。第一个攻击是基于加入新的信息，称为*身份模拟*，第二个攻击是基于修改来自发射器的信息，称为*身份替换*。

一般地，令$\mathcal{S}$表示所有*源状态*的集合，$\mathcal{M}$为所有*信息*的集合，$\mathcal{E}$是所有*编码规则*的集合。这些都是有限集。一个源状态是发射器想要传给接收器的信息。一个编码规则是一个从$\mathcal{S}$到$2^{\mathcal{M}}$的一个单射。发射器和接收器事先约定一个秘密的编码规则$e \in \mathcal{E}$。为了传递一个源状态$s \in \mathcal{S}$，传递器确定$M = e(s)$（这里$M \subseteq \mathcal{M}$），并选择一个信息$m \in M$发送给接收器。接收器认为收到的信息是可信的如果e的像中存在一个M包含收到的信息。为了使接收器能恢复源状态，每个编码规则需要满足条件：

$$e(s) \cap e(s') = \varnothing，\text{对不同的} s, s' \in \mathcal{S}。$$

三元组$(\mathcal{S}, \mathcal{M}, \mathcal{E})$被称为是一个*认证码*，或者简称为*A-码*。

一个A-码$(\mathcal{S}, \mathcal{M}, \mathcal{E})$可以表示成一个$|\mathcal{E}| \times |\mathcal{S}|$矩阵，其中行是由编码规则标记，列是由源状态标记，使得在第$e \in \mathcal{E}$行，$s \in \mathcal{S}$列的元素是$e(s)$。

关于认证码的研究主要是集中在每个编码规则都是从$\mathcal{S}$到$\binom{\mathcal{M}}{c}$的单射的情况，其中c为某个正整数。这样的一个A-code被称为是*c-分裂A-码*。一个1-分裂A-码也称为*无分裂A-码*。当$c \geq 2$，一个c-分裂A-code码也称为一个*有分裂A-码*。一个有分裂A-码对Simmons在文[125, 126]中提出的认证码的推广的模型非常有用。

在一个阶数为i的欺骗攻击 [108]中，敌人在非安全信道中观察到由发射器发出的在相同编码规则下的i个不同的信息。敌人加入一个新的信息（与已发送的i个信息不同），并希望被接收器认为是可信的。在这种框架下，当对A-码的身份模拟和身份替换攻击只是阶数为0和1的欺骗攻击时，已经有了很多研究工作，然而当阶数$i \geq 2$时，尤其是当$c \geq 2$时，对c-分裂A-码的研究却很少。

源状态集合$\mathcal{S}$上的概率分布产生了$\binom{\mathcal{S}}{i}$，$i \geq 0$的概率分布。给定了这些概率分布，发射器和接收器选择了$\mathcal{E}$上的概率分布，称为编码策略。对任意$s \in \mathcal{S}$和$e \in \mathcal{E}$，发射器选择$e(s)$上的概率分布，称为分裂策略。假设敌人已经知道编码和分裂策略。发射器和接收器通过选择编码和分裂策略来使被敌人欺骗的概率最小。我们把敌人用一个阶数为i的欺骗攻击误导接收器的概率记为P_{d_i}。已知如下关于P_{d_i}的下界。

命题 10.1 (Huber [92]). 在一个c-分裂A-码$(\mathcal{S}, \mathcal{M}, \mathcal{E})$中，对任意$i \geq 0$，$P_{d_i} \geq c \cdot \frac{|\mathcal{S}|-i}{|\mathcal{M}|-i}$。

一个c-分裂A-码被称为是$(t-1)$-倍安全防欺骗的如果对任意i，$0 \leq i < t$，$P_{d_i} = c(|\mathcal{S}| - i)/(|\mathcal{M}| - i)$。为了简明，我们称这种码为$(t, c)$-分裂$A$-码。

Huber在文[92]中指出了如果一个A-码是$(t-1)$-倍安全防欺骗的，编码规则的数目一定要足够大。

命题 10.2 (Huber [92]). 在一个(t, c)-分裂A-码$(\mathcal{S}, \mathcal{M}, \mathcal{E})$中，$|\mathcal{E}| \geq \frac{1}{c^t} \cdot \frac{\binom{|\mathcal{M}|}{t}}{\binom{|\mathcal{S}|}{t}}$。

考虑到效率，我们需要一个A-码中的编码规则的数目越小越好。我们称一个(t, c)-分裂A-码是最优的，如果它能达到命题10.2中的下界。

本章中的主要结果是对$c \geq 2$，$t \in \{2, 3\}$，构造了具有三个源状态的最优(t, c)-分裂A-码。特别的，我们证明了存在如下两个新的无穷类：

(i) 对任意$v \equiv 1 \bmod 150$，$v \neq 301$，存在具有三个源状态和v个信息的$(2, 5)$-分裂A-码。

(ii) 对任意$v \equiv 2 \bmod 8$，存在具有三个源状态和v个信息的$(3, 2)$-分裂A-码。

我们得到的$(3, 2)$-分裂A-码是当$t > 2$和$c > 1$时，(t, c)-分裂A-码的第一个已知的无穷类。我们还证明了具有k个源状态和v个信息的$(2, c)$-分裂A-码对任意充分大的v（当k和c固定时）都是存在的。

这一章的结构如下：在第10.2节中，我们将介绍一些基本概念和基本结果；在第10.3节中，我们给出一个渐近性的存在结果；在第10.4节中，我们将推进$t = 2$时，分裂A码的结果；在第10.5节中，我们给出$t = 3$时，一个新的分裂A码的无穷类；在第10.6节中，将对本章的主要结果进行总结。

10.2 准备知识

本节中我们将介绍在下面几节构造中用到的基本定义和结果。

Huber在文[92]中定义了分裂t-设计，推广了Ogata等在[114]中定义的分裂2-设计。

定义 10.3. 令t，v，k，c和λ是正整数，且$t \le k$，$ck \le v$。一个分裂t-设计，或者分裂t-$(v, k \times c, \lambda)$设计，是一个二元组$(X, \mathcal{A})$使得

(i) X是一个v个元素的集合，称为点；

(ii) $\mathcal{A}$是一个$k \times c$阵列的集合，称为区组，其中的元素属于X，使得X中的每个点在每个区组中最多出现一次；

(iii) 对任意$\{x_i : 1 \le i \le t\} \in \binom{X}{t}$，恰好有$\lambda$个区组，使得$x_i$，$1 \le i \le t$，恰好出现在每个区组的$t$个不同的行。

注意到分裂t-$(v, k \times 1, \lambda)$设计与t-(v, k, λ)设计的经典定义一致。Huber在文[92]中证明了分裂t-设计与最优分裂A-码的等价性。

定理 10.4 (Huber [92]). 存在一个分裂t-$(v, k \times c, 1)$设计当且仅当存在一个具有k个源状态，v个信息和$\binom{v}{t}/c^t\binom{k}{t}$个编码规则的最优$(t, c)$-分裂$A$-码。

一个分裂t-设计存在的必要条件如下：

命题 10.5 (Huber [92]). 存在一个分裂t-$(v, k \times c, \lambda)$设计的必要条件是，对任意s，$0 \le s \le t$，

$$\lambda\binom{v-s}{t-s} \equiv 0 \bmod c^{t-s}\binom{k-s}{t-s}。$$

有时，一个分裂t-设计$(X, \mathcal{A})$的点可以取加法群Γ中的元素，使得$X = \Gamma$。如果区组集$\mathcal{A}$是由一个集合$\mathcal{B} \subseteq \mathcal{A}$生成，即：$\mathcal{A} = \cup_{B \in \mathcal{B}}\{B + g : g \in \Gamma\}$，那么$\mathcal{B}$就称为$(X, \mathcal{A})$的基区组。

例 10.6. 令$X = \mathbb{Z}_{151}$。把下面的阵列

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 5 & 13 & 59 & 105 & 118 \\ 28 & 67 & 73 & 112 & 134 \end{pmatrix}$$

作为基区组展开生成区组集$\mathcal{A}$，就得到了一个分裂2-$(151, 3 \times 5, 1)$设计$(X, \mathcal{A})$。

下面定理总结了当$\lambda = 1$时，分裂t-设计存在的一些已知结果。

定理 10.7 (Du [53]，Ge等[72]，Wang [141]，Wang等[143]). *在下面情况下，一个分裂2-$(v, k \times c, 1)$设计存在的必要条件（命题10.5）也是充分的：*

(i) $(k, c) = (2, 2n)$，对任意正整数n；

(ii) $(k, c) = (2, 3)$，除了确定的值$v = 10$外；

(iii) $(k, c) = (3, 2)$，除了确定的值$v = 9$外；

(iv) $(k, c) = (3, 3)$，除了不确定的值$v = 55$外；

(v) $(k, c) = (4, 2)$，除了不确定的值$v \in \{49, 385\}$外。

另外，对任意$v \equiv 1 \bmod 96$，存在2-$(v, 3 \times 4, 1)$设计。

与分裂t-设计类似，可以定义“分裂”类型的GDD。当$t = 2$时，Wang给出了这样的定义[141]。这里，我们要推广到一般的t。一个分裂可分组t-设计，记为分裂GDD$(t, k \times c, v)$，是一个满足如下条件的三元组$(X, \mathcal{G}, \mathcal{A})$：

(i) X是一个v个点的集合，称为点；

(ii) $G = \{G_1, \ldots, G_s\}$是X的划分，称为组；

(iii) $\mathcal{A}$是一个$k \times c$阵列的集合，称为区组，元素从X中取值，使得每个点在每个区组中至多出现一次；

(iv) 对任意包含每个组至多一个点的$\{x_i : 1 \le i \le t\} \in \binom{X}{t}$，恰好有一个区组使得$x_i$，$1 \le i \le t$出现在$t$个不同的行中。

分裂GDD的型与GDD的定义类似，一个分裂GDD的型为$g_1^{n_1}\dots g_s^{n_s}$表示有n_i个大小为g_i的组，$1\le i\le s$。分裂GDD在分裂设计的循环构造中起了重要作用。下面我们给出GDD的Wilson's基本构造法[145, 146]的一个推广。

定理 10.8 (基本构造法). 令$(X,\mathcal{G},\mathcal{A})$是一个GDD$(t,k,v)$。假设对任意区组$A\in\mathcal{A}$，存在一个型为$c^k$的分裂GDD$(t,k'\times c,kc)$ $(X_A,\mathcal{G}_A,\mathcal{B}_A)$，其中$X_A=A\times\{1,\dots,c\}$，$\mathcal{G}_A=\{\{x\}\times\{1,\dots,c\}:x\in A\}$。那么存在一个型为$\{c|G|:G\in\mathcal{G}\}$的分裂GDD$(t,k'\times c,vc)$ $(X',\mathcal{G}',\mathcal{A}')$，其中$X'=X\times\{1,\dots,c\}$，$\mathcal{G}'=\{G\times\{1,\dots,c\}:G\in\mathcal{G}\}$，$\mathcal{A}'=\cup_{A\in\mathcal{A}}\mathcal{B}_A$。

因为对任意t，k，c，型为c^k的分裂GDD$(t,k\times c,kc)$（只包含一个区组）总是存在的。我们有：

推论 10.9. 若存在型为$g_1^{n_1}\dots g_s^{n_s}$的GDD(t,k,v)，则存在型为$(cg_1)^{n_1}\dots(cg_s)^{n_s}$的分裂GDD$(t,k\times c,vc)$。

如Ge等在文[72]中所述，我们也可以在分裂GDD的组上填入分裂2-设计来得到新的分裂2-设计。

命题 10.10 (填组). 令$(X,\mathcal{G},\mathcal{A})$是一个分裂GDD$(2,k\times c,v)$。如果对任意$G\in\mathcal{G}$，存在一个分裂2-$(|G|+1,k\times c,1)$设计，那么存在一个分裂2-$(v+1,k\times c,1)$设计。

10.3　非存在性和渐近结果

令λ是一个正整数。v个顶点的完全多重图，记为λK_v，是一个每对不同的顶点恰好有λ条边的图。令G是一个没有孤立点的简单图。一个阶数为v，指数为λ的G-设计是把λK_v的边集划分成与G同构的子图。如果$e(G)$表示G中边的个数，$d(G)$表示G中顶点度数的最大公因子，那么通过简单的计算可以得出：

(i) $\lambda v(v-1)\equiv 0 \bmod 2e(G)$，

(ii) $\lambda(v-1)\equiv 0 \bmod d(G)$，

是一个阶数为v，指数为λ的G设计存在的必要条件。Wilson在文[148]证明了这些必要条件也是渐近充分的。

定理 10.11 (Wilson [148]). 令G是一个没有孤立点的简单图。那么存在一个只依赖G和λ的常数v_0，使得对任意$v \geq v_0$，存在一个阶数为v指数为λ的G-设计，满足$\lambda v(v-1) \equiv 0 \bmod 2e(G)$，$\lambda(v-1) \equiv 0 \bmod d(G)$。

令$K_{k\times c}$表示一个完全k-部图，每个部分有c个顶点。一个分裂2-$(v, k \times c, \lambda)$设计$(X, \mathcal{A})$等价于一个阶数为v，指数为λ的$K_{k\times c}$-设计，通过建立如下联系：

(i) X中的点对应λK_v中的顶点，

(ii) 一个区组$A \in \mathcal{A}$对应一个完全k部图，其中第i个包含c个顶点的部对应A的第i行的c个元素，$1 \leq i \leq k$。

应用定理10.11，令$G = K_{k\times c}$就得到了如下分裂2-设计存在的渐近结果。

推论 10.12. 存在一个只依赖于k，c和λ的常数v_0，使得对任意$v \geq v_0$，存在一个分裂2-$(v, k \times c, \lambda)$设计，满足：$\lambda v(v-1) \equiv 0 \bmod c^2k(k-1)$，$\lambda(v-1) \equiv 0 \bmod c(k-1)$。

我们用一个非存在性结果结束本节。Huang在文[91]中指出划分K_v的边集的完全k部图的个数至少是$\lceil (v-1)/(k-1) \rceil$。

命题 10.13. 对任意$k, c \geq 2$，不存在一个分裂2-$((k-1)c^2+1, k \times c, 1)$设计。

证明. 假设存在一个分裂2-$((k-1)c^2+1, k \times c, 1)$设计。这个分裂2-设计的区组数是$((k-1)c^2+1)/k$。这意味着我们可以把$K_{(k-1)c^2+1}$的边集划分成$((k-1)c^2+1)/k$个完全$k$部子图。由Huang的结果这是不可能的，因此$\lceil (k-1)c^2/(k-1) \rceil = c^2 > ((k-1)c^2+1)/k$。 □

定理10.7中确定的例外是命题10.13中的特例。

10.4 分裂2-设计

在本节中，我们将建立分裂2-$(v, 3 \times 5, 1)$设计的一个无穷类，并去掉定理10.7(v)中的不确定的值$v = 385$。

命题 10.14. *对任意*$v \equiv 1 \bmod 150$*，除了不确定的值*$v = 301$*以外，存在一个分裂*2-$(v, 3 \times 5, 1)$*设计。*

证明. 由例10.6存在一个2-$(151, 3\times5, 1)$设计，所以令$v \geq 451$。令$v = 150m+1$，对任意整数$m \geq 3$，存在一个型为30^m的GDD$(2, \{3\}, 30m)$（见[66]）。应用推论10.9来得到一个型为150^m的分裂GDD$(2, 3 \times 5, 150m)$。在这个分裂GDD的组上填入分裂2-$(151, 3 \times 5, 1)$设计（例10.6）就得到了一个分裂2-$(150k + 1, 3 \times 5, 1)$设计。 □

命题 10.15. *存在一个分裂*2-$(385, 4 \times 2, 1)$*设计。*

证明. 存在一个型为48^4的GDD$(2, \{4\}, 192)$（见[66]）。应用推论10.9得到一个型为96^4的分裂GDD$(2, 4 \times 2, 384)$。在这个GDD的组上填入一个分裂2-$(97, 4 \times 2, 1)$设计（定理10.7）就得到一个分裂2-$(385, 4 \times 2, 1)$设计。 □

10.5　分裂3-设计

在本节中，我们将建立当$c > 1$时，一个分裂3-设计的第一个已知的无穷类。这里，我们先介绍分裂烛台设计的定义。

一个阶数为v的**分裂**$(t, k \times c)$**烛台设计**是一个四元组$(X, S, \mathcal{G}, \mathcal{A})$，满足如下性质：

(i) X是一个v个元素的集合，称为**点**；

(ii) $S \subseteq X$，称为**干**；

(iii) $\mathcal{G} = \{G_1, \ldots, G_m\}$是$X \setminus S$的一个划分（$\mathcal{G}$中的元素称为**组**）；

(iv) $\mathcal{A}$是一个$k \times c$阵列的集合，称为**区组**，元素从X中取值，使得X中的每个点在每个区组中最多出现一次；

(v) 对任意$\{x_i : 1 \leq i \leq t\} \in \binom{X}{t}$，其中对任意$i$，$|T \cap (S \cup G_i)| < t$，恰好存在一个区组，使得$x_i$，$1 \leq i \leq t$，出现在这个区组的$t$个不同的行。

一个分裂(t, k)烛台设计$(X, S, \mathcal{G}, \mathcal{A})$的**型**是一个多重集$\{|G| : G \in \mathcal{G}\}$。一个型为$g_1^{n_1} \cdots g_r^{n_r}$，干的大小为$s$的分裂$(t, k)$烛台设计，记为$(t, k)$-CS$(g_1^{n_1} \cdots g_r^{n_r} : s)$。

如下定理是文[87]中对一般的烛台设计的Hartman's基本构造法推广到分裂$(3, k \times c)$烛台设计的情况。

定理 10.16. 如果分别存在一个$(3,k)$-CS$(g_1^{n_1} \cdots g_r^{n_r} : s)$，一个分裂$(3, k' \times c)$-CS$(m^{k-1} : a)$和一个型为$m^k$的分裂GDD$(3, k' \times c, mk)$，那么存在一个分裂$(3, k' \times c)$-CS$((g_1 m)^{n_1} \cdots (g_r m)^{n_r} : m(s-1)+a)$。

证明. 令$(X, S, \mathcal{G}, \mathcal{A})$是一个$(3,k)$-CS$(g_1^{n_1} \cdots g_r^{n_r} : s)$，且$\infty \in S$。对$Y \subseteq X$，定义集合

$$P(Y) = ((Y \setminus \{\infty\}) \times \mathbb{Z}_m) \cup (\{\infty\} \times \mathbb{Z}_a)。$$

进一步定义：

$$S' = ((S \setminus \{\infty\}) \times \mathbb{Z}_m) \cup (\{\infty\} \times \mathbb{Z}_a)，$$
$$\mathcal{G}' = \{G \times \mathbb{Z}_m : G \in \mathcal{G}\}。$$

对任意一个包含点∞的$A \in \mathcal{A}$，令

$$(P(A), \{\infty\} \times \mathbb{Z}_a, \{\{x\} \times \mathbb{Z}_m : x \in A \setminus \{\infty\}\}, \mathcal{B}_A)$$

是一个分裂$(3, k' \times c)$-CS$(m^{k-1} : a)$，且对任意不包含点∞的$A \in \mathcal{A}$，令

$$(A \times \mathbb{Z}_m, \{\{x\} \times \mathbb{Z}_m : x \in A\}, \mathcal{C}_A)$$

是一个型为m^k的分裂GDD$(3, k' \times c, mk)$。

很容易验证$(P(X), S', \mathcal{G}', \mathcal{A}')$，其中

$$\mathcal{A}' = \left(\bigcup_{A \in \mathcal{A}: \infty \in A} \mathcal{B}_A \right) \cup \left(\bigcup_{A \in \mathcal{A}: \infty \notin A} \mathcal{C}_A \right),$$

是所需的分裂$(3, k' \times c)$-CS$((g_1 m)^{n_1} \cdots (g_r m)^{n_r} : m(s-1)+a)$。 □

我们也可以在分裂烛台设计的组上填入分裂3-设计得到更大的分裂3-设计。

命题 10.17. 如果存在一个分裂$(3, k \times c)$-CS$(g_1^{n_1} \cdots g_r^{n_r} : s)$，其中$s \leq 2$，并且对任意$1 \leq i \leq r$，存在一个分裂3-$(g_i + s, k \times c, 1)$设计，那么存在一个分裂3-$(s + \sum_{i=1}^{r} g_i n_i, k \times c, 1)$设计。

证明. 令$(X,S,\mathcal{G},\mathcal{A})$是一个分裂$(3,k\times c)$-CS$(g_1^{n_1}\cdots g_r^{n_r}:s)$，其中$s\le 2$。对任意$G\in\mathcal{G}$，令$(G\cup S,\mathcal{B}_G)$是一个分裂3-$(|G|+s,k\times c,1)$设计。那么$(X,\mathcal{A}\cup(\cup_{G\in\mathcal{G}}\mathcal{B}_G))$就是所需的分裂3-$(s+\sum_{i=1}^{r}g_in_i,k\times c,1)$设计。 □

为了应用定理10.16和命题10.17，我们需要一些分裂烛台设计。

引理 10.18. *存在一个分裂*$(3,3\times 2)$-CS$(8^2:0)$*和一个分裂*$(3,3\times 2)$-CS$(8^2:2)$。

证明. 令$X=\mathbb{Z}_{16}$，$\mathcal{G}=\{\{2i+j:0\le i\le 7\}:j\in\{0,1\}\}$。令

$$\mathcal{B}=\left\{\begin{pmatrix}0&4\\6&9\\7&11\end{pmatrix},\begin{pmatrix}0&14\\1&4\\11&13\end{pmatrix},\begin{pmatrix}0&5\\8&10\\13&15\end{pmatrix},\begin{pmatrix}0&2\\4&1\\7&15\end{pmatrix},\begin{pmatrix}0&13\\1&15\\2&12\end{pmatrix},\begin{pmatrix}0&13\\1&9\\4&6\end{pmatrix},\begin{pmatrix}0&6\\9&7\\14&15\end{pmatrix}\right\}。$$

那么$(X,\mathcal{G},\varnothing,\mathcal{A})$，其中$\mathcal{A}=\cup_{B\in\mathcal{B}}\{B+2i \bmod 16:0\le i<8\}$，就是一个分裂$(3,3\times 2)$-CS$(8^2:0)$。

现在令$S=\{x,y\}$，使得$S\cap X=\varnothing$，并令

$$\mathcal{C}=\left\{\begin{pmatrix}x&y\\2i&2i+2\\2j+1&2j+3\end{pmatrix}:i,j\in\{0,2,4,6\}\right\}。$$

那么$(X\cup\{x,y\},S,\mathcal{G},\mathcal{A}\cup\mathcal{C})$就是一个分裂$(3,3\times 2)$-CS$(8^2:2)$。 □

我们建立了分裂3-设计存在性的一个新的无穷类。

定理 10.19. *存在一个分裂*3-$(v,3\times 2,1)$*设计当且仅当*$v\equiv 2 \bmod 8$。

证明. 必要条件$v\equiv 2 \bmod 8$由命题10.5得到。

Huber在文[92]中指出存在一个分裂3-$(10,3\times 2,1)$设计，所以我们将考虑$v>10$的情况。记$v=8m+2$，对某个整数$m\ge 2$。令X是一个$m+1$个点的集合，包含点∞。很容易验证$(X,\{\infty\},\{\{x\}:x\in X\setminus\{\infty\}\},\binom{X}{3})$是一个$(3,3)$-CS$(1^m:1)$。应用定理10.16，输入一个分裂$(3,3\times 2)$-CS$(8^2:2)$（引理10.18）

和一个型为8^3的分裂GDD$(3, 3 \times 2, 24)$（由型为4^3的平凡GDD$(3, 3, 12)$和推论10.9得到）来得到一个分裂$(3, 3 \times 2)$-CS$(8^m : 2)$。现在对这个分裂$(3, 3 \times 2)$-CS$(8^m : 2)$应用命题10.17，结合一个分裂3-$(10, 3 \times 2, 1)$设计就得到了一个分裂3-$(8m + 2, 3 \times 2, 1)$设计。 □

10.6 结论

当k，c和t较大时，确定有k个源状态，$(t-1)$-倍安全防欺骗的最优c-分裂认证码的存在性是一个困难的问题，需要新的直接和递归构造方法来推进这个问题。在本章中，我们通过构造分裂设计，得到了两类新的分裂认证码。

Bibliography

[1] R. J. R. Abel and F. E. Bennett, *Super-simple Steiner pentagon systems*, Discrete Appl. Math. **156** (2008), no. 5, 780–793.

[2] R. J. R. Abel, F. E. Bennett and G. Ge, *Super-simple holey Steiner pentagon systems and related designs*, J. Combin. Des. **16** (2008), no. 4, 301–328.

[3] R. J. R. Abel, C. J. Colbourn and J. H. Dinitz, *Mutually orthogonal Latin squares (MOLS)*, C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs (2nd ed.), Chapman and Hall/CRC, Boca Raton (2007), 160–193.

[4] R. J. R. Abel, C. J. Colbourn, J. Yin and H. Zhang, *Existence of incomplete transversal designs with block size five and any index* λ, Des. Codes Cryptogr. **10** (1997), no. 3, 275–307.

[5] P. Adams, D. E. Bryant and A. Khodkar, *On the existence of super-simple designs with block size* 4, Aequationes Math. **51** (1996), no. 3, 230–246.

[6] E. Agrell, A. Vardy and K. Zeger, *Upper bounds for constant-weight codes*, IEEE Trans. Inform. Theory **46** (2000), no. 7, 2373–2395.

[7] A. M. Assaf, *The packing of pairs by quadruples*, Discrete Math. **90** (1991), no. 3, 221–231.

[8] R. D. Baker, *Partitioning the planes of* $\mathrm{AG}_{2m}(2)$ *into* 2*-designs*, Discrete Math. **15** (1976), no. 3, 205–211.

[9] T. Beth, D. Jungnickel and H. Lenz, *Design theory*, Cambridge University Press, Cambridge, 1986.

[10] S. Blake-Wilson and K. T. Phelps, *Constant weight codes and group divisible designs*, Des. Codes Cryptogr. **16** (1999), no. 1, 11–27.

[11] E. J. Billington, R. G. Stanton and D. R. Stinson, *On λ-packings with block size four* ($v \not\equiv 0 \bmod 3$), Ars Combin. **17** (1984), no. A, 73–84.

[12] I. Bluskov, *New designs*, J. Combin. Math. Combin. Comput. **23** (1997), 212–220.

[13] I. Bluskov and H. Hämäläinen, *New upper bounds on the minimum size of covering designs*, J. Combin. Des. **6** (1998), no. 1, 21–41.

[14] G. T. Bogdanova, *Bounds for the Maximum Size of Ternary Constant-Composition Codes*, Proc. of the International Workshop on Optimal Codes, Jun. (1998), 15–18.

[15] G. Bogdanova, *New bounds for the maximum size of ternary constant weight codes*, Serdica Math. J. **26** (2000), no. 1, 5–12.

[16] G. T. Bogdanova and S. N. Kapralov, *Enumeration of optimal ternary codes with a given composition*, Problemy Peredachi Informatsii **39** (2003), no. 4, 35–40.

[17] G. T. Bogdanova and D. S Ocetarova, *Some Ternary Constant-Composition Codes*, Proc. Sixth Int. Workshop Algebraic and Combinatorial Coding Theory, Pskov, Russia, Sep. (1998), 41–45,

[18] A. E. Brouwer, A. Schrijver and H. Hanani, *Group divisible designs with block-size four*, Discrete Math. **20** (1977), 1–10.

[19] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane and W. D. Smith, *A new table of constant weight codes*, IEEE Trans. Inform. Theory **36** (1990), no. 6, 1334–1380.

[20] D. de Caen, *Extension of a theorem of Moon and Moser on complete subgraphs*, Ars Combin. **16** (1983), 5–10.

[21] H. Cao, K. Chen and R. Wei, *Super-simple balanced incomplete block designs with block size* 4 *and index* 5, Discrete Math. **309** (2009), no. 9, 2808–2814.

[22] H. Cao, L. Ji and L. Zhu, *Constructions for generalized Steiner systems* GS$(3, 4, v, 2)$, Des. Codes Cryptogr. **45** (2007), no. 2, 185–197.

[23] Y. M. Chee, S. H. Dau, A. C. H. Ling and S. Ling, *The sizes of optimal q-ary codes of weight three and distance four: a complete solution*, IEEE Trans. Inform. Theory **54** (2008), no. 3, 1291–1295.

[24] Y. M. Chee, S. H. Dau, A. C. H. Ling and S. Ling, *Linear size optimal q-ary constant-weight codes and constant-composition codes*, IEEE Trans. Inform. Theory **56** (2010), no. 1, 140–151.

[25] Y. M. Chee, G. Ge and A. C. H. Ling, *Group divisible codes and their application in the construction of optimal constant-composition codes of weight three*, IEEE Trans. Inform. Theory **54** (2008), no. 8, 3552–3564.

[26] Y. M. Chee and S. Ling, *Constructions for q-ary constant-weight codes*, IEEE Trans. Inform. Theory **53** (2007), no. 1, 135–146.

[27] Y. M. Chee and S. Ling, *Improved lower bounds for constant GC-content DNA codes*, IEEE Trans. Inform. Theory **54** (2008), no. 1, 391–394.

[28] Y. M. Chee, A. C. H. Ling, S. Ling and H. Shen, *The PBD-closure of constant-composition codes*, IEEE Trans. Inform. Theory **53** (2007), no. 8, 2685–2692.

[29] K. Chen, *On the existence of super-simple* $(v, 4, 3)$*-BIBDs*, J. Combin. Math. Combin. Comput. **17** (1995), 149–159.

[30] K. Chen, *On the existence of super-simple* $(v, 4, 4)$*-BIBDs*, J. Statist. Plann. Inference **51** (1996), no. 3, 339–350.

[31] K. Chen, Z. Cao and R. Wei, *Super-simple balanced incomplete block designs with block size* 4 *and index* 6, J. Statist. Plann. Inference **133** (2005), no. 2, 537–554.

[32] K. Chen, G. Ge and L. Zhu, *Generalized Steiner triple systems with group size five*, J. Combin. Des. **7** (1999), no. 6, 441–452.

[33] K. Chen, G. Ge and L. Zhu, *Starters and related codes*, J. Statist. Plann. Inference **86** (2000), no. 2, 379–395.

[34] K. Chen and R. Wei, *Super-simple* $(v, 5, 5)$ *designs*, Des. Codes Cryptogr. **39** (2006), no. 2, 173–187.

[35] K. Chen and R. Wei, *Super-simple* $(v, 5, 4)$ *designs*, Discrete Appl. Math. **155** (2007), no. 8, 904–913.

[36] K. Chen and L. Zhu, *On the existence of skew Room frames of type* t^u, Ars Combin. **43** (1996), 65–79.

[37] W. Chu, C. J. Colbourn and P. Dukes, *Constructions for permutation codes in powerline communications*, Des. Codes Cryptogr. **32** (2004), no. 1-3, 51–64.

[38] W. Chu, C. J. Colbourn and P. Dukes, *On constant composition codes*, Discrete Appl. Math. **154** (2006), no. 6, 912–929.

[39] G. Cohen, M. G. Karpovsky, H. Mattson and J. Schatz, *Covering radius—survey and recent results*, IEEE Trans. Inform. Theory **31** (1985), no. 3, 328–343.

[40] C. J. Colbourn and J. H. Dinitz, *Mutually orthogonal Latin squares: a brief survey of constructions*, J. Statist. Plann. Inference **95** (2001), no. 1-2, 9–48.

[41] C. J. Colbourn and J. H. Dinitz (eds.), *Handbook of combinatorial designs*, second ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2007.

[42] C. J. Colbourn, D. G. Hoffman and R. Rees, *A new class of group divisible designs with block size three*, J. Combin. Theory Ser. A **59** (1992), no. 1, 73–89.

[43] C. J. Colbourn, T. Kløve and A. C. H. Ling, *Permutation arrays for powerline communication and mutually orthogonal Latin squares*, IEEE Trans. Inform. Theory **50** (2004), no. 6, 1289–1291.

[44] C. J. Colbourn, E. R. Lamken, A. C. H. Ling and W. H. Mills, *The existence of Kirkman squares—doubly resolvable* $(\nu, 3, 1)$*-BIBDs*, Des. Codes Cryptogr. **26** (2002), no. 1-3, 169–196.

[45] C. J. Colbourn and A. C. H. Ling, *Pairwise balanced designs with block sizes* $8, 9$ *and* 10, J. Combin. Theory Ser. A **77** (1997), no. 2, 228–245.

[46] D. J. Costello and G. D. Forney, *Channel coding: The road to channel capacity*, Proc. IEEE **95** (2007), no. 6, 1150–1177.

[47] C. Ding, *Optimal Constant Composition Codes From Zero-Difference Balanced Functions*, IEEE Trans. Inform. Theory **54** (2008), no. 12, 5766–5770.

[48] C. Ding and J. Yin, *Algebraic constrctions of constant-composition codes*, IEEE Trans. Inform. Theory **51** (2005), no. 4, 1585–1589.

[49] C. Ding and J. Yin, *Combinatorial constructions of optimal constant-composition codes*, IEEE Trans. Inform. Theory **51** (2005), no. 10, 3671–3674.

[50] C. Ding and J. Yin, *A construction of optimal constant composition codes*, Des. Codes Cryptogr. **40** (2006), no. 2, 157–165.

[51] C. Ding and J. Yuan, *A family of optimal constant-composition codes*, IEEE Trans. Inform. Theory **51** (2005), no. 10, 3668–3671.

[52] Y. Ding, *A construction for constant-composition codes*, IEEE Trans. Inform. Theory **54** (2008), no. 10, 3738–3741.

[53] B. Du, *Splitting balanced incomplete block designs with block size* 3×2, J. Combin. Des. **12** (2004), 404–420.

[54] A. G. D'yachkov, *Random constant composition codes for multiple access channels*, Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform. **13** (1984), no. 6, 357–369.

[55] T. Ericson and V. Zinoview, *Spherical codes generated by binary partitions of symmetric pointsets*, IEEE Trans. Inform. Theory **41** (1995), no. 1, 107–129.

[56] T. Etzion, *Optimal constant weight codes over Z_k and generalized designs*, Discrete Math. **169** (1997), no. 1-3, 55–82.

[57] T. Etzion, V. Wei and Z. Zhang, *Bounds on the sizes of constant weight covering codes*, Des. Codes Cryptogr. **5** (1995), no. 3, 217–239.

[58] M. K. Fort and G. A. Hedlund, *Minimal coverings of pairs by triples*, Pacific J. Math. **8** (1958), 709–719.

[59] F.-W. Fu, T. Kløve, Y. Luo and V. K. Wei, *On the Svanström bound for ternary constant-weight codes*, IEEE Trans. Inform. Theory **47** (2001), no. 5, 2061–2064.

[60] F.-W. Fu, A. J. H. Vinck and S. Y. Shen, *On the constructions of constant-weight codes*, IEEE Trans. Inform. Theory **44** (1998), no. 1, 328–333.

[61] F. Gao and G. Ge, *Optimal ternary constant composition codes of weight four and distance five*, IEEE Trans. Inform. Theory **57** (2011), no. 6, 3742–3757.

[62] G. Ge, *Generalized Steiner triple systems with group size $g \equiv 1, 5 \pmod 6$*, Australas. J. Combin. **21** (2000), 37–47.

[63] G. Ge, *Generalized Steiner triple systems with group size $g \equiv 0, 3 \pmod 6$*, Acta Math. Appl. Sin. Engl. Ser. **18** (2002), no. 4, 561–568.

[64] G. Ge, *Further results on the existence of generalized Steiner triple systems with group size $g \equiv 1, 5 \pmod 6$*, Australas. J. Combin. **25** (2002), 19–27.

[65] G. Ge, *On $(g, 4; 1)$-difference matrices*, Discrete Math. **301** (2005), no. 2-3, 164–174.

[66] G. Ge, *Group divisible designs*, C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs (2nd ed.), Chapman and Hall/CRC, Boca Raton (2007), 255–260.

[67] G. Ge, *Construction of optimal ternary constant weight codes via Bhaskar Rao designs*, Discrete Math. **308** (2008), no. 13, 2704–2708.

[68] G. Ge and A. C. H. Ling, *A systematic approach to some block design constructions*, J. Combin. Theory Ser. A **108** (2004), no. 1, 89–97.

[69] G. Ge and A. C. H. Ling, *Group divisible designs with block size four and group type $g^u m^1$ for small g*, Discrete Math. **285** (2004), no. 1-3, 97–120.

[70] G. Ge and A. C. H. Ling, *Group divisible designs with block size four and group type $g^u m^1$ with minimum m*, Des. Codes Cryptogr. **34** (2005), no. 1, 117–126.

[71] G. Ge and A. C. H. Ling, *Asymptotic results on the existence of 4-RGDDs and uniform 5-GDDs*, J. Combin. Des. **13** (2005), no. 3, 222–237.

[72] G. Ge, Y. Miao and L. Wang, *Combinatorial constructions for optimal splitting authentication codes*, SIAM J. Discrete Math. **18** (2005), 663–678.

[73] G. Ge and D. Wu, *Generalized Steiner triple systems with group size ten*, J. Math. Res. Exposition **23** (2003), no. 3, 391–396.

[74] G. Ge and D. Wu, *4-*GDDs(3^n) and generalized Steiner systems* GS$(2, 4, v, 3)$, J. Combin. Des. **11** (2003), no. 6, 381–393.

[75] G. Ge and D. Wu, *Some new optimal quaternary constant weight codes*, Sci. China Ser. F **48** (2005), no. 2, 192–200.

[76] G. Ge and R. S. Rees, *On group-divisible designs with block size four and group-type $g^u m^1$*, Des. Codes Cryptogr. **27** (2002), no. 1-2, 5–24.

[77] G. Ge and R. S. Rees, *On group-divisible designs with block size four and group-type $6^u m^1$*, Discrete Math. **279** (2004), no. 1-3, 247–265.

[78] G. Ge, R. S. Rees and L. Zhu, *Group-divisible designs with block size four and group-type $g^u m^1$ with m as large or as small as possible*, J. Combin. Theory Ser. A **98** (2002), no. 2, 357–376.

[79] A. Granville and A. Hartman, *Subdesigns in Steiner quadruple systems*, J. Combin. Theory Ser. A **56** (1991), no. 2, 239–270.

[80] R. M. Gray and L. D. Davisson, *Source coding theorems without the ergodic assumption*, IEEE Trans. Information Theory **IT-20** (1974), 502–516.

[81] H.-D. O. F. Gronau, *Super-simple designs*, C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs (2nd ed.), Chapman and Hall/CRC, Boca Raton (2007), 633–635.

[82] H.-D. O. F. Gronau, D. L. Kreher and A. C. H. Ling, *Super-simple* $(v, 5, 2)$*-designs*, Discrete Appl. Math. **138** (2004), no. 1-2, 65–77.

[83] H.-D. O. F. Gronau and R. C. Mullin, *On super-simple* 2-$(v, 4, \lambda)$ *designs*, J. Combin. Math. Combin. Comput. **11** (1992), 113–121.

[84] H. Hanani, *On quadruple systems*, Canad. J. Math. **12** (1960), 145–157.

[85] H. Hanani, *Balanced incomplete block designs and related designs*, Discrete Math. **11** (1975), 255–369.

[86] A. Hartman, *A general recursive construction for quadruple systems*, J. Combin. Theory Ser. A **33** (1982), no. 2, 121–134.

[87] A. Hartman, *The fundamental construction for* 3*-designs*, Discrete Math. **124** (1994), 107–132.

[88] A. Hartman, W. H. Mills and R. C. Mullin, *Covering triples by quadruples: an asymptotic solution*, J. Combin. Theory Ser. A **41** (1986), no. 1, 117–138.

[89] K. Heinrich and J. Yin, *On group divisible covering designs*, Discrete Math. **202** (1999), no. 1-3, 101–112.

[90] I. S. Honkala, *Modified bounds for covering codes*, IEEE Trans. Inform. Theory **37** (1991), no. 2, 351–365.

[91] Q. X. Huang, *On the decomposition of* K_n *into complete* m*-partite graphs*, J. Graph Theory **15** (1991), 1–6.

[92] M. Huber, *Combinatorial bounds and characterizations of splitting authentication codes*, Crypt. Commun. **2** (2010), 173–185.

[93] S. Huczynska, *Equidistant frequency permutation arrays and related constant composition codes*, Des. Codes Cryptogr. **54** (2010), no. 2, 109–120.

[94] S. Huczynska and G. L. Mullen, *Frequency permutation arrays*, J. Combin. Des. **14** (2006), no. 6, 463–478.

[95] L. Ji, *An improvement on covering triples by quadruples*, J. Combin. Des. **16** (2008), no. 3, 231–243.

[96] L. Ji, *An improvement on H design*, J. Combin. Des. **17** (2009), no. 1, 25–35.

[97] L. Ji, D. Wu and L. Zhu, *Existence of generalized Steiner systems* $\mathrm{GS}(2, 4, v, 2)$, Des. Codes Cryptogr. **36** (2005), no. 1, 83–99.

[98] J. G. Kalbfleisch and R. G. Stanton, *Maximal and minimal coverings of* $(k-1)$*-tuples by* k*-tuples*, Pacific J. Math. **26** (1968), 131–140.

[99] A. Khodkar, *Various super-simple designs with block size four*, Australas. J. Combin. **9** (1994), 201–210.

[100] H. K. Kim and V. Lebedev, *Cover-free families, superimposed codes and key distribution patterns*, J. Combin. Des. **12** (2004), 79–91.

[101] O. D. King, *Bounds for DNA codes with constant GC-content*, Electron. J. Combin. **10** (2003), Research Paper 33, 13 pp. (electronic).

[102] D. S. Krotov, *Inductive constructions of perfect ternary constant-weight codes with distance* 3, Problemy Peredachi Informatsii **37** (2001), no. 1, 3–11.

[103] K. Kurosawa and S. Obana, *Combinatorial bounds on authentication codes with arbitration*, Des. Codes Cryptogr. **22** (2001), 265–281.

[104] A. C. H. Ling, X. J. Zhu, C. J. Colbourn and R. C. Mullin, *Pairwise balanced designs with consecutive block sizes*, Des. Codes Cryptogr. **10** (1997), no. 2, 203–222.

[105] Y. Luo, F. W. Fu, A. J. H. Vinck and W. Chen, *On constant-composition codes over* $\mathbb{Z}_q$, IEEE Trans. Inform. Theory **49** (2003), no. 11, 3010–3016.

[106] J. Luo and T. Helleseth, *Constant composition codes as subcodes of cyclic codes*, IEEE Trans. Inform. Theory **57** (2011), no. 11, 7482–7488.

[107] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[108] J. L. Massey, *Cryptography, a selective survey*, in "Digital Communications '85: Proceedings of the Second Tirrenia International Workshop on Digital Communications" (eds. E. Biglieri and G. Prati), Elsevier, (1986), 3–25.

[109] E. Mendelsohn, *Mendelsohn Designs*, C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs (2nd ed.), Chapman and Hall/CRC, Boca Raton (2007), 528–534.

[110] O. Milenkovic and N. Kashyap, *On the design of codes for DNA computing*, Coding and cryptography, Lecture Notes in Comput. Sci., vol. 3969, Springer, Berlin, 2006, pp. 100–119.

[111] W. H. Mills, *On the covering of triples by quadruples*, Proceedings of the Fifth Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1974) (Winnipeg, Man.), Utilitas Math., 1974, pp. 563–581.

[112] W. H. Mills, *A covering of triples by quadruples*, Proceedings of the Twelfth Southeastern Conference on Combinatorics, Graph Theory and Computing, Vol. II (Baton Rouge, La., 1981), vol. 33, 1981, pp. 253–260.

[113] W. H. Mills, *On the existence of H designs*, Proceedings of the Twenty-first Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1990), vol. 79, 1990, pp. 129–141.

[114] W. Ogata, K. Kurosawa, D. R. Stinson and H. Saido, *New combinatorial designs and their applications to authentication codes and secret sharing schemes*, Discrete Math. **279** (2004), 383–405.

[115] P. R. J. Östergård and M. Svanström, *Ternary constant weight codes*, Electron. J. Combin. **9** (2002), no. 1, Research Paper 41, 23 pp. (electronic).

[116] K. Phelps and C. Yin, *Generalized Steiner systems with block size three and group size $g \equiv 3 \pmod 6$*, J. Combin. Des. **5** (1997), no. 6, 417–432.

[117] K. Phelps and C. Yin, *Generalized Steiner systems with block size three and group size four*, Ars Combin. **53** (1999), 133–146.

[118] R. Rees and D. R. Stinson, *On the existence of incomplete designs of block size four having one hole*, Utilitas Math. **35** (1989), 119–152.

[119] C. A. Rodger, *Linear spaces with many small lines*, Discrete Math. **129** (1994), no. 1-3, pp. 167–180, linear spaces (Capri, 1991).

[120] C. A. Rodger, E. B. Wantland, K. Chen and L. Zhu, *Existence of certain skew Room frames with application to weakly 3-chromatic linear spaces*, J. Combin. Des. **2** (1994), 311–324.

[121] J. Schönheim, *On coverings*, Pacific J. Math. **14** (1964), 1405–1411.

[122] G. J. Simmons, *A game theory model of digital message authentication*, Congr. Numer. **34** (1982), 413–424.

[123] G. J. Simmons, *Message authentication: a game on hypergraphs*, Congr. Numer. **45** (1984), 161–192.

[124] G. J. Simmons, *Authentication theory/coding theory*, in "Advances in Cryptology – CRYPTO '84" (eds. G.R. Blakely and D. Chaum), Springer-Verlag, (1985), 411–432.

[125] G. J. Simmons, *Message authentication with arbitration of transmitter/receiver disputes*, in "Advances in Cryptology – EUROCRYPT '87," Springer-Verlag, (1987), 151–165.

[126] G. J. Simmons, *A Cartesian product construction for unconditionally secure authentication codes that permit arbitration*, J. Cryptology **2** (1990), 77–104.

[127] G. J. Simmons, *A survey of information authentication*, in "Contemporary Cryptology — The Science of Information Integrity "(ed. G.J. Simmons), IEEE Press, (1992), 379–419.

[128] D. H. Smith, L. A. Hughes and S. Perkins, *A new table of constant weight codes of length greater than 28*, Electron. J. Combin. **13** (2006), no. 1, pp. Article 2, 18 pp. (electronic).

[129] D. R. Stinson, R. Wei and J. Yin, *Packings*, C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs (2nd ed.), Chapman and Hall/CRC, Boca Raton (2007), 550–556.

[130] D. R. Stinson, R. Wei and L. Zhu, *New constructions for perfect hash families and related structures using combinatorial designs and codes*, J. Combin. Des. **8** (2000), no. 3, 189–200.

[131] M. Svanström, *A lower bound for ternary constant weight codes*, IEEE Trans. Inform. Theory **43** (1997), no. 5, 1630–1632.

[132] M. Svanström, *A class of perfect ternary constant-weight codes*, Des. Codes Cryptogr. **18** (1999), no. 1-3, 223–229.

[133] M. Svanström, *Ternary Codes with Weight Constraints*, Ph.D dissertation, Linköpings Universitet, Linköping, Sweden, 1999.

[134] M. Svanström, *Constructions of ternary constant-composition codes with weight three*, IEEE Trans. Inform. Theory **46** (2000), no. 7, 2644–2647.

[135] M. Svanström, P. R. J. Östergård and G. T. Bogdanova, *Bounds and constructions for ternary constant-composition codes*, IEEE Trans. Inform. Theory **48** (2002), no. 1, 101–111.

[136] J. D. Swift, *A generalized Steiner problem*, Rend. Mat. (6) **2** (1969), 563–569.

[137] L. Teirlinck, *Some new* 2*-resolvable Steiner quadruple systems*, Des. Codes Cryptogr. **4** (1994), no. 1, 5–10.

[138] I. E. Telatar and R. G. Gallager, *Zero error decision feedback capacity of discrete memoryless channels*, Proc. Bilkent Int. Conf. New Trends Commun. Control Signal Process., E. Arikan, Ed., 1990, pp. 228–233, Elsevier.

[139] P. Turán, *On the theory of graphs*, Colloquium Math. **3** (1954), 19–30.

[140] S. A. Vanstone, D. R. Stinson, P. J. Schellenberg, A. Rosa, R. Rees, C. J. Colbourn, M. W. Cater and J. E. Carter, *Hanani triple systems*, Israel J. Math. **83** (1993), no. 3, pp. 305–319.

[141] J. Wang, *A new class of optimal 3-splitting authentication codes*, Des. Codes Cryptogr. **38** (2006), 373–381.

[142] J. Wang and L. Ji, *A class of group divisible* 3*-designs and their applications*, J. Combin. Des. **17** (2009), no. 2, 136–146.

[143] J. Wang and R. Su, *Further results on the existence of splitting BIBDs and application to authentication codes*, Acta Appl. Math. **109** (2010), 791–803.

[144] B. Wen, J. Wang and J. Yin, *Optimal grid holey packings with block size* 3 *and* 4, Des. Codes Cryptogr. **52** (2009), no. 1, 107–124.

[145] R. M. Wilson, *An existence theory for pairwise balanced designs. I. Composition theorems and morphisms*, J. Combin. Theory Ser. A **13** (1972), 220–245.

[146] R. M. Wilson, *An existence theory for pairwise balanced designs. II. The structure of PBD-closed sets and the existence conjectures*, J. Combin. Theory Ser. A **13** (1972), 246–273.

[147] R. M. Wilson, *Constructions and uses of pairwise balanced designs*, Math. Centre Tracts **55** (1974), 18–41.

[148] R. M. Wilson, *Decompositions of complete graphs into subgraphs isomorphic to a given graph*, in "Proceedings of the Fifth British Combinatorial Conference (Univ. Aberdeen, Aberdeen, 1975)," Winnipeg, Man., (1976), 647–659.

[149] H. Wu and J. Chang, *Constructing constant composition codes via distance-increasing mappings*, SIAM J. Discrete Math. **26** (2012), no. 1, 375–383.

[150] D. Wu and P. Fan, *Constructions of optimal quaternary constant weight codes via group divisible designs*, Discrete Math. **309** (2009), no. 20, 6009–6013.

[151] D. Wu, G. Ge and L. Zhu, *Generalized Steiner triple systems with group size* $g = 7, 8$, Ars Combin. **57** (2000), 175–191.

[152] D. Wu and L. Zhu, *Generalized Steiner systems* $\mathrm{GS}(2, 4, \nu, 2)$ *with* ν *a prime power* $\equiv 7 \pmod{12}$, Des. Codes Cryptogr. **24** (2001), no. 1, 69–80.

[153] J. Yan and J. Yin, *Constructions of optimal GDRP(*$n, \lambda; v$*)'s of type* $\lambda^1\mu^{m-1}$, Discrete Appl. Math. **156** (2008), no. 14, 2666–2678.

[154] J. Yan and J. Yin, *A class of optimal constant composition codes from GDRPs*, Des. Codes Cryptogr. **50** (2009), no. 1, 61–76.

[155] J. Yin and A. M. Assaf, *Constructions of optimal packing designs*, J. Combin. Des. **6** (1998), no. 4, 245–260.

[156] J. Yin, Y. Lu and J. Wang, *Maximum distance holey packings and related codes*, Sci. China Ser. A **42** (1999), no. 12, 1262–1269.

[157] J. Yin and Y. Tang, *A new combinatorial approach to the construction of constant composition codes*, Sci. China Ser. A **51** (2008), no. 3, 416–426.

[158] J. Yin, J. Yan and C. Wang, *Generalized balanced tournament designs and related codes*, Des. Codes Cryptogr. **46** (2008), no. 2, 211–230.

[159] H. Zhang and G. Ge, *Optimal ternary constant-weight codes of weight four and distance six*, IEEE Trans. Inform. Theory **56** (2010), no. 5, 2188–2203.

[160] H. Zhang and G. Ge, *Completely reducible super-simple designs with block size four and related super-simple packings*, Des. Codes Cryptogr. **58** (2011), 321–346.

[161] H. Zhang and G. Ge, *Optimal quaternary constant-weight codes of weight four and distance five*, IEEE Trans. Inform. Theory **59** (2012), no. 3, 2706–2718.

[162] H. Zhang, X. Zhang and G. Ge, *Optimal ternary constant-weight codes of weight four and distance five*, IEEE Trans. Inform. Theory **58** (2013), no. 5, 1617–1629.

[163] X. Zhang and G. Ge, *On the existence of partitionable skew Room frames*, Discrete Math. **307** (2007), no. 22, 2786–2807.

[164] M. Zhu and G. Ge, *Quaternary constant-composition codes with weight* 4 *and distances* 5 *or* 6, IEEE Trans. Inform. Theory **58** (2012), no. 9, 6012–6022.

[165] M. Zhu and G. Ge, 4-$*GDD(6^n)$*s and related optimal quaternary constant-weight codes*, J. Combin. Des. **20** (2012), no. 12, 509–526.

附录

对攻读博士期间完成的其他研究成果，鉴于篇幅限制，我们将只列出结果，而省略证明过程。

令$A_q(n,d,w)$表示长度为n，重量为w，最小汉明距离为d的最优q元常重码的码字个数。我们确定了：

(i) $A_4(6t+2,6,4)=3t(3t+1)$，对任意$t\geq 2$。$A_4(23,6,4)=120$。

(ii) $A_3(n,8,5)=\left\lfloor \frac{2n}{5}\left\lfloor \frac{n-1}{n}\right\rfloor\right\rfloor$，对任意$n\equiv 0,1 \pmod{20}$或$n\equiv 25 \pmod{100}$，$n\notin\{125,225,325\}$。

令$A_q(n,d,\overline{w})$表示长度为n，常复合为$\overline{w}$，最小汉明距离为d的最优q元常重复合码的码字个数。

(i) 对任意整数$n\geq 4$，

$$A_3(n,6,[3,1])=\begin{cases}\left\lfloor \frac{n}{3}\left\lfloor \frac{n-1}{3}\right\rfloor\right\rfloor, & \text{当}n\equiv 0,1,2,3,6 \pmod 9\text{时，}\\ \frac{n^2-2n+1}{9}+\left\lfloor \frac{n-1}{36}\right\rfloor, & \text{当}n\equiv 4,22,31 \pmod{36}\text{，}n\notin \\ & \quad\{40,67,94,103,130,139,229,\\ & \quad\ 247,373,382,391\}\text{时，}\\ \frac{n^2-3n-1}{9}+\left\lfloor \frac{n+4}{36}\right\rfloor, & \text{当}n\in\{5,14,23,32\}\text{时，}\\ \frac{n^2-3n-1}{9}+\left\lfloor \frac{n+2}{18}\right\rfloor, & \text{当}n\in\{16,61\}\text{时，}\\ 28, & \text{当}n=17\text{时。}\end{cases}$$

攻读博士学位期间论文完成情况

[1] H. Zhang and G. Ge, *Optimal ternary constant-weight codes of weight four and distance six*, IEEE Trans. Inform. Theory **56** (2010), no. 5, 2188–2203. (SCI)

[2] Y. M. Chee, X. Zhang and H. Zhang, *Infinite families of optimal splitting authentication codes secure against spoofing attacks of higher order*, Adv. Math. Commun. **5** (2011), no. 1, 59–68. (SCI)

[3] H. Zhang and G. Ge, *Completely reducible super-simple designs with block size four and related super-simple packings*, Des. Codes Cryptogr. **58** (2011), no. 3, 321–346. (SCI)

[4] X. Zhang, H. Zhang and G. Ge, *Optimal constant weight covering codes and nonuniform group divisible 3-designs with block size four*, Des. Codes Cryptogr. **62** (2012), no. 2, 143–160. (SCI)

[5] H. Zhang, X. Zhang and G. Ge, *Optimal ternary constant-weight codes with weight* 4 *and distance* 5, IEEE Trans. Inform. Theory **58** (2012), no. 5, 2706–2718. (SCI)

[6] H. Zhang and G. Ge, *Optimal quaternary constant-weight codes with weight four and distance five*, IEEE Trans. Inform. Theory **59** (2013), no. 3, 1617–1629. (SCI)

[7] Y. M. Chee, H. M. Kiah, H. Zhang and X. Zhang, *Optimal Codes in the Enomoto-Katona Space*, to appear in Proceedings of the 2013 International Symposium on Information Theory.

[8] Y. M. Chee, H. Zhang and X. Zhang, *Complexity of Dependencies in Bounded Domains, Armstrong Codes, and Generalizations*, to appear in Proceedings of the 2013 International Symposium on Information Theory.

[9] Y. M. Chee, G. Ge, H. Zhang and X. Zhang, *Linear size optimal q-ary constant-weight codes with weight three*, in manuscript.

[10] G. Ge, H. Zhang and M. Zhu, *Ternary constant-composition codes with composition* $[2, 2]$ *and distance six*, in manuscript.

简　　历

基本情况

张会：女，1984年10月生，浙江大学数学系在读博士研究生。

教育状况

2003 年 9 月至2007 年 7 月, 东北大学理学院，本科，专业：信息与计算科学。

2007 年 9 月至2013 年 6 月，浙江大学数学系，直博研究生，专业：应用数学。

工作经历

2012 年 8 月至2013 年 8 月，南洋理工大学数学系，Project Officer。

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: hzhangzju@126.com

致　　谢

时光飞逝，在浙大攻读博士学位的日子马上就要结束了，我也从对组合数学几乎一无所知到即将成为组合数学方向的博士毕业生。首先我要感谢恩师葛根年教授，当初是葛老师带领我们走入这个领域，并手把手地教我们做问题，写文章，使我们对这个领域的知识日益加深。还要感谢他还给了我们很多机会去参加各种会议，学习各种不同知识，接触各种不同的问题，并总是尽心尽力地给我们提供了很多发展的机遇。攻读博士期间葛老师言传身教，他教给我们的做学问的态度会让我们受益终生。

我要感谢南洋理工大学的李耀明教授，在我读博士最后一年提供了南洋理工大学数学系工作一年的机会。

我要感谢师姐张先得博士，和她一起做问题让我收获颇多。还要感谢在新期间她对我生活和工作上的许多帮助。

我还要感谢浙江大学在我读博期间提供的补助、奖学金等，还有教育部的“博士研究生学术新人奖”，这些在很大程度上改善了我们的生活和科研条件，使我们能安心做研究。

我还要感谢博士研究生朱明志、高斐、胡思煌、魏恒嘉、李抒行、张一炜等，和他们在一起的日子使我们辛苦的攻读博士学位的生活有了很多乐趣。

最后，还要感谢父母家人对我的支持理解。