分类号：O157.2　　单位代码：10335

学　　号：11235061

浙江大学

博士学位论文

中文论文题目：极值组合与编码理论中的若干问题

英文论文题目：**Several problems in extremal combinatorics and coding theory**

申请人姓名：上官冲

指导教师：葛根年

专业名称：应用数学

研究方向：组合数学与编码理论

所在学院：数学科学学院

论文提交日期　2017年4月1日

极值组合与编码理论中的若干问题

论文作者签名： _____

指导教师签名： _____

论文评阅人1：_____

评阅人2：_____

评阅人3：_____

评阅人4：_____

评阅人5：_____

答辩委员会主席：范更华 教授 福州大学

委员1：范更华 教授 福州大学

委员2：宗传明 教授 天津大学

委员3：符方伟 教授 南开大学

委员4：吴佃华 教授 广西师范大学

委员5：葛根年 教授 浙江大学

答辩日期：2017年5月19日

Several problems in extremal combinatorics and coding theory

Author's signature: _____

Supervisor's signature: _____

External Reviewers: _____

_____

_____

_____

_____

Examining Committee Chairperson:

Prof. Genghua Fan, Fuzhou University

Examining Committee Members:

Prof. Genghua Fan, Fuzhou University

Prof. Chuanming Zong, Tianjin University

Prof. Fangwei Fu, Nankai University

Prof. Dianhua Wu, Guangxi Normal University

Prof. Gennian Ge, Zhejiang University

Date of oral defence: May 19, 2017

浙江大学研究生学位论文独创性声明

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

学位论文作者签名：　　签字日期：　　年　　月　　日

学位论文版权使用授权书

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

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：　　导师签名：

签字日期：　　年　　月　　日　　签字日期：　　年　　月　　日

致　　谢

首先我要感谢我的导师葛根年教授。“古之学者必严其师，师严然后道尊”，在这五年博士学习中他对我严格要求，并给予我很多悉心的指导和帮助，使我与刚入学相比，在各方面都取得了长足的进步。在以后的科研工作中，我将谨记葛老师的教诲，葛老师高瞻远瞩的学术视野和严谨认真的学术作风将使我终身受益。

我要感谢这五年中在学习和生活上给予过我指导的各位老师，特别是筑波大学的缪莹老师，他亲切和蔼，待人以诚，和他交流如沐春风；浙江大学的冯涛老师，他以如履薄冰之心，行勇猛精进之事，他一直都是我榜样。我还要感谢同济大学的杨亦挺老师与西南交通大学的范翠玲老师。

我要感谢亲爱的同门们：张先得师姐、张会师姐、高斐师兄、朱明志师兄、魏恒嘉师兄、胡思煌师兄、李抒行师兄、林浩师兄、张一炜师兄、汪馨、张韬、顾玉杰、马景学、丁报昆、钱昺辰、孔祥梁、韩雪娇、徐子翔、兰昭君等；尤其要感谢魏恒嘉、胡思煌、李抒行、林浩、张一炜、汪馨对我学习和生活上的帮助。我还要感谢林灯、奚元霄，他们在杭州帮我处理了很多与毕业相关的事情。

我要感谢亲爱的好朋友们：在北京的吴金雄、吴利平，上海的周楠，杭州的曹高扬，在深圳的吴艺侃、熊涛，广州的蔡宇、佛山的王鹿平、武汉的倪日文以及余江的宋浩林，他们或与我分享快乐、或与我分担忧虑。

我还要感谢孙蔚楠的理解、支持与陪伴。我要感谢我的亲人们，尤其是我的父亲、母亲和奶奶，“谁言寸草心，报得三春晖”。

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

摘　　要

本论文考虑了极值组合与编码理论中的若干问题。通过使用包括多项式方法、超图移除引理、加法数论在内的强有力的数学工具，研究了若干个具有相当难度的猜想和公开问题。

在第二章中，我们考虑了组合群试领域内由Erdős，Frankl和Füredi提出的、具有三十年历史的一个猜想。给定n个被测样本，其中最多有d个是阳性的，群试理论的目标是采用尽可能少的测试次数找到所有阳性样本，而不是仅仅对所有样本进行逐个检测。一个二元矩阵被称为是d-分离的，如果它的任意d列的布尔和都不包含其它列。分离矩阵在非自适性群试中有着极为重要的应用。用$T(d)$表示最小的t，使得存在一个满足$n > t$的$t \times n$的d-分离矩阵。前人已证明$T(d) \geq \binom{d+2}{2}$，并猜测$T(d) \geq (d+1)^2$。通过技巧性地利用Erdős和Gallai经典的图匹配定理，我们证明$T(d)/d^2 \geq (15+\sqrt{33})/24$，缩小了与猜想值之间的鸿沟。

在第三章中，我们考虑了防诬陷码、父代识别码与追踪码的上界。这些码都是被用来保护具有版权的数字文件的。它们在诸如数字指纹、广播加密方案等场景中都有应用。利用一些组合计数方法中的技巧，我们分别给出了这三种码的上界。这些界都是目前已知的最优界。

在第四章中，我们研究了一个重要的图兰问题，即Brown，Erdős和Sós提出的稀疏超图问题。考虑n个顶点上的r-均衡超图，设其不含仅由v 个顶点张成的e条边，四十多年前，Brown等人用函数$f_r(n,v,e)$ 来表示这个超图所能含有的最大边数。他们提出了一个著名猜想：$n^{k-o(1)} < f_r(n, e(r-k)+k+1, e) = o(n^k)$对所有整数$r > k \geq 2$，$e \geq 3$都成立。注意到，当$r = 3, e = 3, k = 2$时，该猜想的正确性是由著名的Ruzsa-Szemerédi的(6,3)-定理所保证的。我们为该猜想的成立提供了更多的证据。一方面，我们用超图移除引理证明：猜想的右边对所有固定的整数$r \geq k+1 \geq e \geq 3$都成立。我们的结果涵盖了历史上达到猜想上界的所有已知情形。另一方面，通过构造一个合适的加法数论中的sum-free集，我们说明：猜想的左边对$r \geq 3,\ k = 2$与$e = 4, 5, 7, 8$都成立。在$e \geq 4$且$r \geq 4$的范围内，我们的构造是第一个使猜想下界成立的构造。

可分哈希族是一种非常有用的组合结构，它是组合学、密码学和编码理论中很多研究对象的推广。在第五章中，我们解决了关于可分哈希族和完美哈希族的上下界的若干公开问题和猜想。首先，我们发现可分哈希族的大小满足一种Johnson型的迭代不等式。从此出发，我们给出了可分哈希族的改进上界。其次，我们构造了一类完美哈希族的无穷类。它不仅正面回答了Bazrafshan和Trung关于可分哈希族的一个公开问题，而且回答了Alon和Stav关于父代识别码的一个猜想。最后，用$p_t(N,q)$表示q元N长强度为t的完美哈希族的最大可能大小。Walker和Colbourn猜测当q充分大时有$p_3(3,q)=o(q^2)$。通过使用(6,3)-定理，我们证明了$q^{2-o(1)}<p_3(3,q)=o(q^2)$。此外，利用一些加法数论的工具，我们还证明了$q^{2-o(1)}<p_4(4,q)=o(q^2)$。

在第六章和第七章里，我们分别研究了信息科学中的两个编码问题。第一个问题是集中式缓存编码方案，它是由Maddah-Ali和Niesen提出的一种技术，被用来降低无线网络系统中高峰时期的网络负载。设K是系统中用户的数目，则比率$R(K)$和复杂性$F(K)$是缓存方案的主要衡量指标。我们希望设计使$R(K)$和$F(K)$都尽量小的缓存方案。之前的结果都满足$R(K)$是常数而$F(K)$是指数函数。我们把这个问题与3-均衡3-部的(6,3)-free的超图的构造联系起来，并提出了第一个具有常数比率、亚指数复杂性的缓存方案。第二个问题是分布式存储码，它在现代存储系统中有着重要应用。Piggybacking设计被用来构造同时具有好的译码复杂性与修复带宽的存储码。通过引入一个新颖的piggybacking框架，我们所提出的piggyback码具有与现存的码相同的译码复杂性，但是使修复带宽率从$\frac{r-1}{2r-1}$降低到了$\frac{\sqrt{2r-1}}{r}$。

在第八章中，我们考虑了一个有限域上的极值问题。最近，Croot-Lev-Pach和Ellenberg-Gijswijt使用了一种新颖的多项式方法，分别界定了$\mathbb{Z}_4^n$ 与$\mathbb{F}_3^n$上不含3长等差数列的最大子集的大小，这两篇文章都发表在《Annals of Mathematics》上。Terence Tao总结了他们的工作，把其提炼为一种计算某些多变量函数的秩的方法。我们改变了Tao 的计数公式，并用新公式来证明了如下结论：设q 是一个固定的奇素数幂，A为$\mathbb{F}_q^n$的子集，使得不存在三个不同的元素$x,y,z\in A$ 满足$<z-x,y-x>=0$，那么A的大小不超过$\binom{n+q}{q-1}+3$。当q给定而n足够大时，我们的结果显著提高了之前的上界$\mathcal{O}(q^{\frac{n+2}{3}})$。

关键词： 分离矩阵，防诬陷码，父代识别码，追踪码，稀疏超图，超图移除引理，sum-free集，可分哈希族，完美哈希族，集中式编码缓存方案，(6,3)-定理，piggyback码，有限域上的直角

Abstract

This thesis involves various problems in the area of extremal combinatorics and coding theory. We use many powerful tools and deep including polynomial method, hypergraph removal lemma and additive number theory to attack several conjectures and open problems in the literature.

In Chapter 2, we consider a thirty-year-old conjecture of Erdős, Frankl and Füredi in the combinatorial group testing theory. Given n items with at most d of which being positive, instead of testing these items individually, the group testing theory aims to identify all positive items using as few tests as possible. A binary matrix is called d-disjunct if the boolean sum of arbitrary d columns does not contain another column not in this collection. Disjunct matrices have important applications in the nonadaptive group testing. Let $T(d)$ denote the minimal t such that there exists a $t \times n$ d-disjunct matrix with $n > t$. It was known that $T(d) \geq \binom{d+2}{2}$ and was conjectured that $T(d) \geq (d+1)^2$. Using a classical graph matching theorem of Erdős and Gallai, we narrow the gap by proving $T(d)/d^2 \geq (15+\sqrt{33})/24$.

In Chapter 3, we consider the upper bounds of frameproof codes, parent-identifying codes and traceability codes. These codes are introduced to protect the copyrighted digital data. They have applications in the scenarios like digital fingerprinting and broadcast encryption schemes. Using skills from combinatorial counting method, we present three upper bounds for each of these codes. To the best of our knowledge, all the bounds are the best known ones.

In Chapter 4, we deal with an important problem in Turán theory, namely, the sparse hypergraph problem of Brown, Erdős and Sós. More than forty years ago, they introduced the function $f_r(n, v, e)$ to denote the maximum number of edges in an r-uniform hypergraph on n vertices which does not contain e edges spanned by v vertices. They posed a well-known conjecture: $n^{k-o(1)} < f_r(n, e(r-k)+k+1, e) = o(n^k)$ holds for all integers $r > k \geq 2$, $e \geq 3$. Note that for $r = 3, e = 3, k = 2$, this conjecture was solved by the famous Ruzsa-Szemerédi's (6,3)-theorem. We add more evidence for the validity of this conjecture. On one hand, we use the hypergraph removal lemma to prove that the right hand side is true for all fixed integers $r \geq k+1 \geq e \geq 3$.

Our result implies all known upper bounds which match the conjectured magnitude. On the other hand, by constructing an appropriate sum-free set in additive number theory, we show that the left hand side is true for $r \geq 3,\ k = 2$ and $e = 4, 5, 7, 8$. Our construction provides the first lower bound which matches the conjecture in the range $e \geq 4$ and $r \geq 4$.

Separating hash families are useful combinatorial structures which are generalizations of many well-studied objects in combinatorics, cryptography and coding theory. In Chapter 5, we solve several open problems and conjectures about the upper and lower bounds of separating hash families and perfect hash families. Firstly, we discover that the cardinality of a separating hash family satisfies a Johnson-type recursive inequality. As a result, we obtain a new upper bound, which is superior to all previous ones. Secondly, we present a construction for an infinite class of perfect hash families. It provides an affirmative answer to both Bazrafshan-Trung's open problem on separating hash families and Alon-Stav's conjecture on parent-identifying codes. Thirdly, let $p_t(N, q)$ denote the maximal cardinality of a t-perfect hash family of length N over an alphabet of size q. Walker and Colbourn conjectured for sufficiently large q it holds that $p_3(3, q) = o(q^2)$. We verify this conjecture by proving $q^{2-o(1)} < p_3(3, q) = o(q^2)$. Our proof can be viewed as an application of the (6,3)-theorem. We also prove $q^{2-o(1)} < p_4(4, q) = o(q^2)$, using tools from additive number theory.

In Chapters 6 and 7, we study two coding problems in the area of information sciences, respectively. The first one is the centralized coded caching scheme, which is proposed by Maddah-Ali and Niesen as a technique to reduce the network burden in peak times in a wireless network system. The rate $R(K)$ and the complexity $F(K)$ are two major evaluating indicators for a caching scheme, where K is the number of users. The goal is to design caching schemes with $R(K)$ and $F(K)$ both as small as possible. Previous caching schemes have constant $R(K)$ and exponential $F(K)$. We relate this problem to the construction of 3-uniform 3-partite (6,3)-free hypergraphs and present the first caching scheme in the literature, which has constant rate and sub-exponential complexity. The second one is the distributed storage codes, which have important applications in the design of modern storage systems. Piggybacking design is a strategy to construct storage codes with both good decoding complexity and repair bandwidth. By introducing a novel piggybacking framework, we present a piggyback code which has the same decoding complexity as the previous one, while the repair bandwidth rate is reduced from $\frac{r-1}{2r-1}$ to $\frac{\sqrt{2r-1}}{r}$.

In Chapter 8, we discuss an extremal problem over the finite fields. Recently, Croot-Lev-Pach and Ellenberg-Gijswijt used a novel polynomial method to give upper bounds for three-term arith-

metic progression free sets in $\mathbb{Z}_4^n$ and $\mathbb{F}_3^n$, respectively. These two papers have been published in "Annals of Mathematics". Their method was summarized by Terence Tao as a principal which counts the slice-ranks of certain multi-variable polynomials. We develop a variant of Tao's counting formula and use it to prove that, if q is a fixed odd prime power, then the maximal cardinality of a subset A of $\mathbb{F}_q^n$ with no three distinct elements $x, y, z \in A$ satisfying $< z-x, y-x >= 0$ is at most $\binom{n+q}{q-1} + 3$. This bound substantially improves the previously known bound $\mathcal{O}(q^{\frac{n+2}{3}})$ for fixed q and sufficiently large n.

Keywords: disjunct matrix, frameproof code, parent-identifying code, traceability code, sparse hypergraph, hypergraph removal lemma, sum-free set, separating hash family, perfect hash family, centralized coded caching, (6,3)-theorem, piggyback code, right angles over finite field

插　　图

表　格

目　　次

1 绪论

1.1 群试理论和分离矩阵

群试理论是一门关于检测的科学。它最早起源于第二次世界大战。在二战中，为了减少美军中梅毒的发病率，医生们需要对每个士兵进行血液检测。然而，士兵数量以成千上万记，每次检测又需消耗相当的时间和药品。如果逐个检测士兵，所耗时间、费用靡巨。1943年，哈佛大学的经济兼统计学家Dorfman发表了一篇著名论文[56]，彻底改良了从前逐次测试的方法。这篇论文也被认为是组合群试理论的开山之作。

假设每个样本被给予了一个待定的二元状态，阳性（也称被感染态），阴性（也称纯净态）。一次测试可以被看成是一些样本的集合。我们的策略是把所有样品分组，设计成若干个相互独立的测试。如果某次测试结果为0，那么它包含的所有样本都是阴性的；如果测试结果为1，则它至少包含一个阳性样本。因此，我们可以关注那些结果为0的测试集，删去其中包含的所有样本（这些样本都是阴性的），再去考虑剩下的少量样本的状态。通常阳性样本的数量有一个上界d。

通常我们有两种算法，即自适性算法和非自适性算法。自适性算法被设计成具有若干轮，同轮间的测试是相互独立的，但是后轮的测试可以利用前轮的测试结果。反之，非自适性算法同时进行所有测试，并且必须在一轮内识别出所有的阳性样本。由于可以利用更多信息，自适性算法自然得比非自适性算法需要更少的测试次数。然而，非自适性算法也有其自身的优势，他们更节约时间。我们的研究对象主要是非自适性的群试方案。

一个非自适性群试方案可以被表示为一个$t \times n$ 的布尔（二元）矩阵M，其中，我们用测试来标记M的行，用样本来标记它的列，如果第j个样本包含在第i次测试中，$M_{ij} = 1$；否则，$M_{ij} = 0$。M经常被设计成所谓的分离矩阵（Disjunct Matrix）。我们说一个二元矩阵是一个d-分离矩阵(d-DM)，如果其任意d列的布尔和不包含任意其它一列。话句话说，一个矩阵是d- 分离的，如果对任何$d+1$列$c_1, \ldots, c_{d+1}$以及任何$j \in \{1, \ldots, d+1\}$，都存在一行使得该行仅在c_j处取1，其它地方都取0。

我们自然要关心如下的基本问题，给定n、d，求最小的正整数t，使得存在一

个$t \times n$的d-DM。我们把这个最小的t记为$t(d,n)$。自二十世纪六十年代始，编码学家就开始考虑$t(d,n)$的上下界，对于一般的n，我们有$t(d,n) \geq \min\{\binom{d+2}{2}, n\}$。这个界表明了如果$n \leq \binom{d+2}{2}$，那么任何$d$-DM算法都不会优于逐次检测的最简单的算法。上述结果导出了一个有趣的问题：给定d，何时存在一个优于逐次检测算法的非自适性群试算法? 这等价于提问：给定d，求最小的t使得存在一个$t \times n$的d-DM满足$n \geq t+1$。我们记这个最小的t为$T(d)$。1985 年，三位著名的组合学家Erdös，Frankl和Füredi证明$T(d) \geq \binom{d+2}{2}$，并猜测$\lim_{d\to\infty} T(d)/d^2 = 1$，甚至$T(d) \geq (d+1)^2$。三十多年来，这个结果一直没有被改进。最近，我们利用了图论中的一个经典结果，即Erdős 和Gallai 的图匹配定理[70]，极大地改进了$T(d)$的已知值，主要工作可以被表示为如下定理。

定理1.1.1. $T(d)/d^2 \geq (15+\sqrt{33})/24$。

显然，我们的结果极大的提高了从前的结果，但与猜想值还有一定差距。作者在这个主题内已经完成了一篇文章（见主要研究成果中的文献1），发表于《IEEE Transactions on Information Theory》。这个主题对应于本论文的第二章。

1.2 数字指纹码

高带宽网络的普及和多媒体技术的发展，使得多媒体数据成为我们相互沟通的主要载体。然而在多媒体向世界展示其魅力的同时，其赖以成功的技术基础也可能为它带来巨大的威胁。数字文件易于分发和复制，一旦被泄露，其价值将大打折扣。要解决该问题可以采用数字指纹。数字指纹是将不同的标志性识别代码——指纹，利用数字水印技术嵌入到数字媒体中，然后将嵌入了指纹的数字媒体分发给用户。发行商发现盗版行为后，就能通过提取盗版产品中的指纹，确定非法复制的来源，对盗版者进行起诉，从而起到版权保护的作用。

记$\mathcal{C}$为一个(N,n,q)指纹码，即，它是一些q元N长向量的集合，且集合的大小为n。设共有n个用户，每个用户被分配了不同的指纹（或者说是加了指纹的产品）$x \in \mathcal{C}$。设有t 个用户$D = \{x^1, \ldots, x^t\}$ 妄图通过合谋来盗版这一产品，其中，对$1 \leq j \leq t$，我们有$x^j = (x_1^j, \ldots, x_N^j)$。假设他们盗版出的产品为$y = (y_1, \ldots, y_N)$。显然，为了保持产品的有效性，$y_i$的值不能随便取，而是必须符合如下规律：对$1 \leq i \leq N$，我们有$y_i \in \{x_i^1, \ldots, x_i^t\}$。这种规律也被称为是所谓的“marking assumption”，即标记假定，本文所有关于指纹码的讨论都必须符合标记假定。我们的目标是，通过合理地构造指纹码$\mathcal{C}$，使得它能满足如下

条件：当不超过t个用户合谋时，如果已知合谋向量y，我们可以通过y追踪出一个或多个合谋用户。

根据它们的性能强弱，已知的指纹码主要分为以下三种：第一，防诬陷码（Frameproof Codes），这种码没有追踪功能，但是它可以防止诬陷——不超过t个用户合谋而得的向量y不等于$\mathcal{C}$中其它任意不在该合谋集合中的码字，换句话说，防诬陷码可以防止t个违法用户构造出另一个合法用户的码字，进而防止该合法用户被诬陷；第二，父代识别码（Parent-identifying Codes），这种码本身是防诬陷码，但是具有一定的追踪能力——当有不超过t个用户合谋时，我们可以在时间$\mathcal{O}(Nn^t)$内找到至少一个合谋者；第三，追踪码（Traceability Codes），这种码本身既是防诬陷码，又是父代识别码，但是具有更强的追踪能力——当有不超过t个用户合谋时，我们可以在时间$\mathcal{O}(Nn)$内找到至少一个合谋者。如果我们采用列举译码（List Decoding）算法[18,125]，追踪时间可以被进一步减少到$\mathcal{O}(N\log^c n)$，c为某个给定常数。

这三种码的强弱关系显而易见，它们的追踪能力大小是由它们内在的组合结构的强弱所保证的。此外，不同的组合结构也可以给出不同的追踪算法。因此，研究这三种指纹码，就是研究在不同组合结构下组合对象的上下界。我们的成果主要集中在它们上界的改进上，可以分别表示为如下三个定理。

定理1.2.1. *设$\mathcal{C}$为一个强度为t码长为N的二元防诬陷码，则当$t \geq 3$与$N < \frac{15+\sqrt{33}}{24}(t-2)^2$时，有$|\mathcal{C}| \leq N$。*

定理1.2.2. *设$\mathcal{C}$为一个强度为t码长为N的q元父代识别码，令$v = \lfloor (t/2+1)^2 \rfloor$，其中，$0 \leq r \leq v-2$是一个正整数使得$N \equiv r \mod (v-1)$，那么我们有$|\mathcal{C}| \leq rq^{\lceil N/(v-1)\rceil} + (v-1-r)q^{\lfloor N/(v-1)\rfloor}$。*

定理1.2.3. *设$\mathcal{C}$为一个强度为3码长为N的q元追踪码，那么我们有$|\mathcal{C}| \leq cq^{\lceil N/9\rceil}$，其中，$c$是一个仅仅依赖于$N$的常数。*

其中，定理1.2.1极大地提高了从前的结果，把满足$|\mathcal{C}| \leq N$的范围从$N \leq 3t$[81]（线性阶）提高到$N < \frac{15+\sqrt{33}}{24}(t-2)^2$（平方阶），但是与猜想值$N(t) = t^2 + o(t^2)$还有一定距离。定理1.2.2改进了Alon等人[15]从前的结果$|\mathcal{C}| \leq (v-1)q^{\lceil N/(v-1)\rceil}$；当$v-1 \nmid N$时，首项的系数被改进为某个$r < v-1$的常数。追踪码上界的确定一直是一个十分困难的问题，Blackburn等人[36]猜测对强度为t的追踪码，有$|\mathcal{C}| \leq cq^{\lceil N/t^2\rceil}$成立。目前，仅仅知道该猜想对$t = 2$成

立[36]。定理1.2.3第一次证明了该猜想对$t=3$也成立。

关于防诬陷码、父代识别码与追踪码，作者已完成了两篇文章（见主要研究成果中的文献4和文献5）。其中一篇已经投稿至《IEEE Transactions on Information Theory》。这个主题对应于本论文的第三章。

1.3 稀疏超图

稀疏超图问题是Brown，Erdős和Sós[39,40]在七十年代早期提出的一个经典的Turán型问题。这是一个相当难的问题，受到了组合学界甚至数学界的广泛重视。Szemerédi在研究稀疏超图时创造性地发展出了正则性引理（Regularity Lemma），成为其获得Abel奖的重要依据之一。稀疏超图的研究手法糅合了极值方法、概率方法、加法数论等一系列方法，该问题仍然是组合学界的研究热点之一。

超图是指一对点集和边集$\mathcal{H}=(V(\mathcal{H}),E(\mathcal{H}))$，顶点集$V(\mathcal{H})$可以被看做是一个有限集合$X$，边集$E(\mathcal{H})$则是$X$ 的一些子集的集合。一个超图$\mathcal{H}$是r-均衡的，如果对所有$A\in\mathcal{H}$都有$|A|=r$。用$\mathcal{G}_r(v,e)$标记有e条边与v个顶点的r-均衡超图的集合。一般的，我们说这些超图是由v个顶点张成的e条边。Brown，Erdős和Sós引入了函数$f_r(n,v,e)$来表示当n个顶点上的r-均衡超图不含v 个顶点张成的e 条边时，所可能含有的最大边数。这等价于说，对任意e条边$A_1,\ldots,A_e$，成立$|A_1\cup\cdots\cup A_e|\geq v+1$。因为其边的稀疏性，这类超图也被称为稀疏超图。我们感兴趣当r,v,e 是固定的，而n 趋向于无穷大时的情形。已知对每个$r>k\geq 2$与$e\geq 3$，都有$f_r(n,e(r-k)+k,e)=\Theta(n^k)$，上界来自于一个简单的计数，下界来自于标准的概率方法。然而，对$r>k\geq 2$ 与$e\geq 3$决定$f_r(n,e(r-k)+k+1,e)$的渐进表现要难多了，有一个关于$f_r(n,e(r-k)+k+1,e)$的著名猜想。

猜想1.3.1. $n^{k-o(1)}<f_r(n,e(r-k)+k+1,e)=o(n^k)$对所有整数$r>k\geq 2$，$e\geq 3$都成立。

对最简单的情形，$r=3,k=2,e=3$，Ruzsa与Szemerédi[119]证明了著名的(6,3)-引理：$n^{2-o(1)}<f_3(n,6,3)=o(n^2)$。Erdős，Frankl，Rödl[68]把这个结果拓展为：$n^{2-o(1)}<f_r(n,3(r-2)+2+1,3)=o(n^2)$对任意$r\geq 3$ 都成立。Alon与Shapira[14]进一步推广到：$n^{k-o(1)}<f_r(n,3(r-k)+k+1,3)=o(n^k)$对任意$r>k\geq 2$都成立。Sárközy与Selkow[120,121]证明：$f_r(n,4(r-k)+k+1,4)=o(n^k)$。文献[14]的下界与两个零星的例子$n^{2-o(1)}<f_3(n,7,4)$、$n^{2-o(1)}<f_3(n,8,5)$ 是使猜想1.3.1的下界成立的所有已知情形。

我们对猜想1.3.1的上下界都得到了一些新结果，分别表述为如下两个定理。

定理1.3.2. $f_r(n, e(r-k)+k+1, e) = o(n^k)$对所有整数$r \geq k+1 \geq e \geq 3$都成立。

定理1.3.3. $f_r(n, e(r-k)+k+1, e) = o(n^k)$对所有整数$r \geq 3$与$k = 2$在$e = 4, 5, 7, 8$时都成立。

其中，定理1.3.2的证明利用了著名的超图移除引理（Hypergraph Removal Lemma）。我们的结果解决了猜想的上界的所有“简单”情形，因为它可以推出之前所有的已知结果，且第一个未解决的情况就是著名的(7,4)-问题。定理1.3.3说明了猜想的左边对$r \geq 3$和$k = 2$在$e = 4, 5, 7, 8$时都成立。注意到，现存的满足猜想的构造性结果都符合$r = 3$ 或者$e = 3$。我们的构造是历史上第一个打破这个藩篱的。我们的证明依托于图论与加法数论中的两个新概念，即彩虹圈与R-sum-free集合。

关于稀疏超图，作者已经完成了一篇论文（见主要研究成果中的文献9）。该主题对应本论文的第四章。

1.4 哈希函数族

可分哈希族（Separating Hash Family）是一类非常有用的组合结构，它是由Stinson，Wei和Chen[131]提出的。它们是很多组合对象的拓展，例如，完美哈希族，防诬陷码，父代识别码等。

定义1.4.1. 令X和Y分别是大小为n和q的集合。我们称一个包含N个函数$f : X \to Y$的集合$\mathcal{F}$为一个$(N; n, q)$-哈希族。

定义1.4.2. 设$f : X \to Y$是一个函数，取两两互不相交的集合$C_1, C_2, \ldots, C_t \subseteq X$。如果$f(C_1), \ldots, f(C_t)$是两两不相交的，则称$f$分离了$C_1, C_2, \ldots, C_t$。特别的，称$f$分离了一个集合$C \subseteq X$，如果$f(C) \subseteq Y$恰有$|C|$个不同的值。

定义1.4.3. 令X和Y分别是大小为n和q的集合，设$\mathcal{F}$是一个从X到Y的$(N; n, q)$-哈希族。我们说$\mathcal{F}$是一个$(N; n, q, \{w_1, \ldots, w_t\})$-可分哈希族（我们也记为$SHF(N; n, q, \{w_1, \ldots, w_t\})$），如果它满足如下性质：对所有两两互不相交的集合$C_1, C_2, \ldots, C_t \subseteq X$，$|C_i| = w_i$，$1 \leq i \leq t$，都存在至少一个函数$f \in \mathcal{F}$分离了$C_1, C_2, \ldots, C_t$。我们把多重集合$\{w_1, \ldots, w_t\}$称为这个可分哈希族的型。

若$w_1 = w_2 = \cdots w_t = 1$，则一个$SHF(N; n, q, \{1, \ldots, 1\})$就是熟知的$t$-完美哈希族（Perfect Hash Family），也被记为$PHF(N; n, q, t)$。容易看出，完美哈希族满足所有可分哈希族中最强的分离性质。记$u = \sum_{i=1}^{t} w_i$，用$C(N, q, \{w_1, \ldots, w_t\})$与$p_t(N, q)$分别表示最大的$n$，使得一个$SHF(N; n, q, \{w_1, \ldots, w_t\})$或者$PHF(N; n, q, t)$ 存在。我们的主要对研究对象就是可分哈希族与完美哈希族，我们解决了若干关于其上下界的公开问题和猜想。

首先，通过一种被称为分量分组的办法，界定$C(N, q, \{w_1, \ldots, w_t\})$可以被归约于界定$C(u-1, q, \{w_1, \ldots, w_t\})$，这是因为$C(N, q, \{w_1, \ldots, w_t\}) \leq C(u-1, q^{\lceil N/(u-1) \rceil}, \{w_1, \ldots, w_t\})$。研究者们在寻找最小的正实数$\gamma$使得$C(u-1, q, \{w_1, \ldots, w_t\}) \leq \gamma q$对任意的$q$都成立。2011年，Bazrafshan和Trung[19]证明了$C(u-1, q, \{w_1, \ldots, w_t\}) \leq (u-1)q$。并且，他们提出了如下公开问题。

问题1.4.4. *是否存在某个型$\{w_1, \ldots, w_t\}$使得常数$(u-1)$可以被某个严格小于它的常数替换？*

通过给出如下的构造，我们给予他们的问题一个否定的回答，且该构造还回答了Alon和Stav[16]关于父代识别码的一个猜想。

定理1.4.5. *对任何整数$q \geq 2$和$N \geq 2$，都存在一个$PHF(N; Nq^{N-1}, q^{N-1} + (N-1)q^{N-2}, N+1)$。因此，$\gamma = u - 1$是满足$C(u-1, q, \{w_1, \ldots, w_t\}) \leq \gamma q$对任何$q$都成立的最小常数。*

此外，我们还得到了可分哈希族的目前最好的一般界。

定理1.4.6. *假设存在一个$SHF(N; n, q, \{w_1, \ldots, w_t\})$，令$u = \sum_{i=1}^{t} w_i$和$1 \leq r \leq u-1$为正整数，满足$N \equiv r \pmod{u-1}$。如果$C(\lfloor N/(u-1) \rfloor, q, \{w_1, \ldots, w_t\}) \geq u$，则我们有$n \leq rq^{\lceil N/(u-1) \rceil} + (u-1-r)q^{\lfloor N/(u-1) \rfloor}$。*

注意到，当q充分大时，通过一个概率构造可以得知[32]定理1.4.6中的指数$\lceil N/(u-1) \rceil$在$(u-1) | N$时是紧的。但是，当$(u-1) \nmid N$时，指数的紧性非常难以确定，甚至连最简单的情形，$u = 3$和$N = 3$，Walker和Colbourn[141] 提出了如下猜想。

猜想1.4.7. $p_3(3, q) = o(q^2)$.

目前已知的结果仅仅是$\Omega(q^{5/3}) = p_3(3,q) = O(q^2)$。但是，我们利用Ruzsa和Szemerédi[119]的(6,3)-定理与加法数论的技巧，不仅证明了猜想1.4.7 是成立的，而且得到了相当好的构造性结果。实际上，我们得到了如下定理。

定理1.4.8. *对任意给定$\epsilon > 0$，当q充分大时，我们都有$q^{2-\epsilon} < p_3(3,q) = o(q^2)$，且$q^{2-\epsilon} < p_4(4,q) = o(q^2)$。*

关于可分哈希族与完美哈希族，我们已完成了一篇文章（见主要研究成果中的文献3），发表于《SIAM Journal on Discrete Mathematics》。这部分内容对应于本论文的第五章。

1.5 缓存编码方案

视频传播已经成为我们日常生活中无线数据堵塞的一个重要驱动因素，并且，它正面临着引入注目的增长需求。假设我们有一个拥有巨大数据存储的服务器，它与一组用户相连。每个用户都希望从服务器得到某个特定的文件。同一时间的大量需求常常会令无线网络堵塞，这会导致系统的延时和超载，弱化用户体验。缓存是解决这个问题的一种方法。在网络负载很低时，系统把文件的某些部分分发到每个用户的缓存中，因此，在繁忙时段，用户的需求就可以从这些缓存中获益。

缓存方案共有两个阶段：文件布置阶段，这时每个文件的某些数据包依据一个预先设定好的策略被放入每个用户的缓存中；文件分配阶段，这时服务器依据所有用户的不同需求，设计一个方案把这些所需数据包的抑或和（XOR multiplexing）用一个共享的链接广播出去。假设我们有K个用户，N个单位大小的文件，每个用户都含有大小为M的内存空间。在文件发布阶段所需的传输总量被称为这个方案的比率，记作R。为了实现一个缓存方案，每个文件都被划分成一定数量的数据包，我们把这个数目记为F。一般来说，给定K，M，N，R和F这两个参数是一个缓存方案的主要衡量指标。比率R代表了这个方案的效率，而F则表示了它的复杂度。我们把R 和F表示成关于K的函数，一般地说，K的数量会很大。所以，我们通常希望R是与K无关的常数，而F尽可能随着K缓慢增长。一般来说，在这个研究领域我们有如下核心问题。

问题1.5.1. *如果M/N与R都是给定的与K无关的常数，那么，对足够大的K，是否存在F随K多项式增长的缓存方案设计？*

已知编码缓存方案，例如Maddah-Ali-Niesen方案[101]与Yan等人的PDA设计[147]，都满足$R(K)$是常数，但$F(K)$是指数函数。我们分别从上下界两个方面研究了这个问题，主要的结果可以被表示为如下两个定理。

定理1.5.2. *如果M/N与R都是给定的与K无关的常数，那么，对足够大的K，F随K线性增长的PDA设计是不可能存在的。*

定理1.5.3. *如果M/N与R都是给定的与K无关的常数，那么，对足够大的K，存在F随K亚指数增长的PDA设计。*

一些数值实验表明，我们的结果大大改进了文献[101]与文献[147]中的结果。关于缓存方案，作者已完成了一篇文章（见主要研究成果中的文献6），已经投稿至《IEEE Transactions on Information Theory》。这个主题对应于本论文的第六章。

1.6 Piggyback码

分布式存储是一种方兴未艾的存储技术。在分布式存储系统中，整个数据存储在一系列存储节点中。这些节点物理独立并通过一个网络连接。因为每一个节点都有一定的概率损坏，我们必须引入冗余性来确保系统的可靠性。一旦一个单独的存储节点损坏，必须使用存储在幸存节点的数据将其恢复。当修复失败的节点时，有四个参数我们需要考虑，即，计算负载、网络带宽、磁盘I / O 和需访问磁盘的数量。大多数现有的存储编码技术只是考虑这四个参数之一的最优性，本文的主要关心的是优化前两个参数。我们定义平均修复带宽率，γ，为平均修复带宽和原始数据量的比值。

MDS码是数据存储中一种被广泛使用纠删码，修复损坏的存储节点只需利用有限域的加法和乘法，然而，修复一个损坏的节点，它需要下载整个的原始数据。换句话说，MDS存储码的平均修复带宽，γ_{MDS}，等于1。Rashmi等人[114,115]了提出一种piggybacking框架，不仅保持了MDS码的低计算复杂度，且有平均修复带宽率$\gamma_{RSR} = \frac{r-1}{2r-3} \approx \frac{1}{2} < \gamma_{MDS}$。

本文的主要目的是设计一个新的piggybacking框架，以进一步减少存储码的系统节点的修复带宽。通过一系列组合技巧，我们设计的新piggyback码不仅拥有与RSR 码相同的计算复杂度，且其平均修复带宽率可以低至$\gamma_{NEW} = \frac{\sqrt{2r-1}}{r}$。

关于这个主题，作者作者已完成了一篇文章（见主要研究成果中的文献7），已经投稿至《IEEE Transactions on Information Theory》。这个主题对应于本论文的第七章。

1.7 有限域上的直角

从2016年5月开始，随着Croot-Lev-Pach和Ellenberg-Gijswijt等人在多项式方法中的突破性进展，组合学的各个领域产生了一大批重要成果。其中，最显著的成果当属Croot等人[53] 以及Ellenberg和Gijswijt[64]分别证明了$\mathbb{Z}_4^n$与$\mathbb{F}_3^n$上不含三长等差数列的最大子集都是指数小的。这两篇文章都发表在数学界的顶尖期刊《Annals of Mathematics》上。陶哲轩也很关注这个问题，写出了两篇博客文章[137,138]来阐述他的想法。我们也注意到了这种多项式方法，并用它来改进一类有限域上的极值问题的上界，具体问题如下所述。

设q为一个素数幂，$V = \mathbb{F}_q^n$ 是有限域$\mathbb{F}_q$上的n维向量空间。我们将考察V的一个极值性质。我们感兴趣的是V的不包含任何直角的最大子集大小。我们说一个集合$A \subseteq V$ 包含一个直角，如果存在三个不同的元素$x, y, z \in A$使得$< z - x, y - x >= 0$，这里$< \cdot, \cdot >$表示$\mathbb{F}_q$上的内积。记$R(n, q)$为$\mathbb{F}_q^n$的最大的不含直角的子集。在文献[22] 中，Bennett证明了$R(n, q) \leq \mathcal{O}(q^{\frac{n+2}{3}})$。通过改良Tao所提出的一个计数引理，通过计算一些多变量函数的秩，我们得到了如下定理。

定理1.7.1. *令q是一个奇素数幂，A是$\mathbb{F}_q^n$的一个子集，使得不存在三个不同元素$x, y, z \in A$满足$< z - x, y - x >= 0$，那么，$|A| \leq \binom{n+q}{q-1} + 3$。*

可以看出，当q固定时，我们的结果显著地改进了之前的结果。例如，当$q = 3$时，$R(n, 3)$被从$\mathcal{O}(3^{\frac{n+2}{3}})$改进到$(n + 3)^2 + 3$。我们的新上界实际上是$n$的一个多项式函数。这是非常有意思的，因为之前使用类似的多项式方法得到的结果都是n的指数函数。

关于这个主题，作者作者已完成了一篇文章（见主要研究成果中的文献8），已经投稿至《Journal of Combinatorial Theory, Series A》。这个主题对应于本论文的第八章。

2 群试理论和分离矩阵

2.1 简介

给定n个被测样本，假设其中最多d个是阳性的，组合群试理论的目标是用尽可能少的测试次数发现所有的阳性样本。它的历史可以追溯到第二次世界大战，当时，生物学家们需要从大量人口中识别出梅毒的抗原携带者。Dorfman在测试血液样本时[56]，最早提出了组合群试的思想。从那时起，群试理论被极大拓展了，并在很多方面得到了应用；例如，化学泄露测试[126]，电路短路测试[45]，多方通信[25,145]，DNA扫描[58]，模式识别[100]和网络安全[146]。

假设每个样本被给予了一个待定的二元状态，阳性（也称被感染态），阴性（也称纯净态）。我们的策略是把所有样品分组，设计成若干个相互独立的测试。如果某次测试结果为0，那么它包含的所有样本都是阴性的；如果测试结果为1，则它至少包含一个阳性样本。因此，我们可以关注那些结果为0的测试集，删去其中包含的所有样本（这些样本都是阴性的），再去考虑剩下的少量样本的状态。通常阳性样本的数量有一个上界，d。为了找出所有阳性样本，我们可以仅仅独立地检测每个样本，这样总共需要n次测试。另一方面，由信息论导出的上界说明，至少需要$\log \sum_{i=0}^{d} \binom{n}{i} \approx d \log \frac{n}{d}$次测试。当$n$充分大且$d$远小于$n$时，$n$与$d \log \frac{n}{d}$之间有着极大的鸿沟，因此我们需要仔细设计我们的检测算法，以期使用尽可能少的测试数目。

通常我们有两种算法，即自适性算法和非自适性算法。自适性算法被设计成具有若干轮，同轮间的测试是相互独立的，但是后轮的测试可以利用前轮的测试结果。反之，非自适性算法同时进行所有测试，并且必须在一轮内识别出所有的阳性样本。由于可以利用更多信息，自适性算法自然得比非自适性算法需要更少的测试次数。近似地讲，非自适性算法至少需要$\Omega(\frac{d^2}{\log d} \log n)$次测试[59,77,116]。但是自适性算法只需$O(d \log n)$次测试，和最优的信息论界只相差一个常数倍[47]。然而，非自适性算法也有其自身的优势。他们更节约时间，在时间成本很大的应用场景中更能发挥作用，例如，DNA筛选以及网络安全。

关于非自适性群试算法在分子生物学，尤其是DNA筛选中的应用，最近二十年来已经

有很多深入的研究。读者们可以参阅Du和Hwang的综合读本[58]获取更加详细的信息。近年来，Xuan等人[146]发现，组合群试的思想可以被自然地应用于网络安全中。在最简单的网络攻击场景下，我们假设有n个用户连接到t个网络伺服器，在n个用户中，有不超过d个攻击者。类似于检测单次测试的0-1回应，一旦某个攻击者攻击一个伺服器，该伺服器的资源就会被耗尽。因此，我们并不难识别出哪个伺服器正遭受攻击。在网络安全的设定下，非自适性群试比自适性群试更受关注：答案显而易见，我们必须尽可能快地发现攻击者，不然他们可能会给整个网络造成更大的破坏。

一个非自适性群试方案可以被表示为一个$t \times n$的布尔（二元）矩阵M，其中，我们用测试来标记M的行，用样本来标记它的列，如果第j个样本包含在第i次测试中，则$M_{ij} = 1$；否则，$M_{ij} = 0$。M经常被设计成所谓的“分离”矩阵。这个概念是由Kautz和Singleton 提出的[93]，当时他们正在研究信息读取系统中的某些重要问题。随后，Erdős，Frankl和Füredi[67]引入了一个名为“cover-free family”（CFF）的组合结构，CFF的关联矩阵恰好是一个分离矩阵。我们说一个二元矩阵是一个d-分离矩阵(d-DM)，如果任意d列的布尔和不包含任意其它一列。话句话说，一个矩阵是d-分离的，如果对任何$d+1$列$c_1, \ldots, c_{d+1}$以及任何$j \in \{1, \ldots, d+1\}$，都存在一行使得该行仅在c_j处取1，其它地方都取0。一个d-DM可以导出一个非自适性群试方案。另一方面，任何一个非自适性群试方案都必须是一个$(d-1)$-DM[57]。记$t(d,n)$为使一个$t \times n$的d-DM存在的最小的t。D’yachkov 等人[61,62] 近期的结果证明，下面的界渐进成立：

$$\frac{d^2 \log n}{2 \log d}(1 + o(1)) \leq t(d,n) \leq cd^2 \log n(1 + o(1)),$$

其中，c为某个常数。可以看出上下界直接还有一个鸿沟$\log d$，如何消除这个鸿沟是组合群试领域内的主要公开问题。这里，我们关心该领域内的另一个重要公开问题。对于一般的n，我们有$t(d,n) \geq \min\{\binom{d+2}{2}, n\}$，D’yachkov和Rykov[60] 把这个界归功于Bassalygo。这个界表明了如果$n \leq \binom{d+2}{2}$，那么任何d-DM 算法都不会优于逐次检测的最简单的算法。上述结果导出了一个有趣的问题：给定d，何时存在一个优于逐次检测算法的非自适性群试算法? 这等价于提问：给定d，求最小的t使得存在一个$t \times n$的d-DM 满足$n \geq t+1$。我们记这个最小的t为$T(d)$。显然，我们有$T(d) \geq \binom{d+2}{2}$和$t(d,n) \geq \min\{T(d), n\}$。1985 年，Erdös，Frankl 和Füredi猜测[67]：

$$\lim_{d \to \infty} T(d)/d^2 = 1, \qquad (Version\ I),$$
$$T(d) \geq (d+1)^2, \qquad (Version\ II).$$

此外，他们声称版本二对$d \leq 3$都成立，并且$\lim_{d\to\infty} T(d)/d^2 \geq 5/6$，但是没有给出证明。注意到，$d+1$阶仿射平面的关联矩阵是一个$(d+1)^2 \times ((d+1)^2 + (d+1))$的$d$-DM，并且具有常数列重$d+1$。并且，当$d+1$是素数幂时，$d+1$阶的仿射平面总是存在的[41]。这意味着$\lim_{d\to\infty} T(d)/d^2 \leq 1$，且当$d+1$是一个素数幂时有$T(d) \leq (d+1)^2$。2001年，Huang和Hwang[87]证明版本二对$d = 4$成立。2007年，Chen和Hwang[46]证明版本二对$d = 5$也成立。但是关于$T(d)/d^2$的极限值，三十多年来都没有任何改进。本文运用了Erdős 和Gallai 的图匹配定理[70]，说明$T(d) \geq \frac{15+\sqrt{33}}{24}d^2$。我们的主要方法是组合计数，计算分离矩阵的列所包含的某种特定组合结构的数量。显而易见，我们的结论显著提高了之前的结果。值得一提的是，具有常数列重的分离矩阵在DNA筛选中有着特别的应用[58]。Chee的博士论文[42]考察了上述猜想在d-DM具有常数列重$d+1$时的情形，但是并没有将其完全解决。利用一个简单的计数技巧，我们完全解决了这个问题。

我们的主要结果列举如下。

定理2.1.1. *设M是一个$t \times n$的d-DM，并且具有常数列重$d+1$。若$n > t$，则$t \geq (d+1)^2$。*

定理2.1.2. *设M是一个$t \times n$的d-DM。若$n > t$，则$t \geq \frac{15+\sqrt{33}}{24}d^2$。*

我们将在第2.2节证明定理2.1.1，在第2.3节证明定理2.1.2，在第2.4节给出一些小结。

2.2 关于常重矩阵的一个简单界

对一个$t \times n$的二元矩阵M，1和0可以表示一个对应的集合系的关联结构。令$T = [t] := \{1, \ldots, t\}$为一个$t$元集，$\mathcal{F} = \{F_1, \ldots, F_n\} \subseteq 2^T$，那么$M$可以被看成是$(T, \mathcal{F})$的关联矩阵，使得对所有$i \in [t]$，$j \in [n]$，$i \in F_j$当且仅当$M_{ij} = 1$。我们可以用列$c_j$替换子集$F_j$，即，$i \in c_j$当且仅当$M_{ij} = 1$，这也表明第$i$行包含了第$j$ 列。M的某列被称为是孤立的，如果存在一行仅仅与之关联，且不与其它任何列关联。我们称这一行是与该列对应的孤立行。若M是一个d-DM，并含有某个孤立列c，那么，我们可以删去c和其对应的某一个孤立行。我们得到了一个$(t-1) \times (n-1)$的矩阵M'，易见M'保持了d-分离的特性。那么，对M有$n > t$当且仅当对M'有$n-1 > t-1$。由$T(d)$的定义可知，满足$(n-1) > (t-1)$的最小t至少是$T(d)+1$。以上的观察可以被总结为如下引理。

引理2.2.1. *令M为一个$t \times n$的d-DM，若c为M的孤立列。若$n > t$，那么$t > T(d)$。*

证明. 删去列c和与之对应的孤立行，我们得到一个$(t-r_c)\times(n-1)$的d-DM，这里，$r_c \geq 1$是与c关联的孤立行的数目。由于$n-1 > t-r_c$，则由$T(d)$的定义可知，$t-r_c \geq T(d)$，进而可知，$t \geq T(d)+r_c$。 □

因此，为了决定$T(d)$，我们只需考虑不包含孤立列的矩阵。列c的重量$|c|$表示列c所含有的1的数量。d-DM的任何非孤立列的列重都至少为$d+1$，因为它包含的任意1都被包含于其它某列中。因此，对于不含孤立列的d-DM，它的最小列重为$d+1$。定理2.1.1证明了猜想的版本二在最简单的情况下成立，即具有常数列重$d+1$的d-DM。

定理2.1.1的证明如下。

定理2.1.1的证明. 由引理2.2.1可知，我们总是能假定M不含孤立列。那么，对任意不同列c与c'，容易证明$|c \cap c'| \leq 1$。用$C(i)$表示在第i行含有1的列的集合。通过计算整个矩阵包含的所有1的数目，我们可得$\sum_{i=1}^{t}|C(i)| = n(d+1) \geq (t+1)(d+1)$。因此，存在某个$1 \leq i_0 \leq t$使得$|C(i_0)| \geq \lceil \frac{(d+1)(t+1)}{t} \rceil \geq d+2$。注意到，$c \cap c' = \{i_0\}$对所有的$c$，$c' \in C(i_0)$都成立，我们有$t \geq |\vee_{c\in C(i_0)} c| = 1+(d+2)d = (d+1)^2$，这里，$\vee$表示列的布尔和（或者说集合的并）。 □

2.3 关于$T(d)$的一般界

假设K是一个k元集合，我们用$\binom{K}{\lambda}$来表示K的所有λ元子集，其中，$1 \leq \lambda \leq k$是一个正常数。令$\mathcal{G} \subseteq \binom{K}{\lambda}$为$K$的$\lambda$元子集所构成的集族。匹配数$v(\mathcal{G})$被定义为$\mathcal{G}$的最多的互不相交的元素数目。换句话说，任取$\mathcal{G}$中$v(\mathcal{G})+1$个不同元素，其中一定存在两个元素相交不为空。极值集合论的一个经典问题就是当$v(\mathcal{G})$给定时，确定$|\mathcal{G}|$ 的最大值。令$m(k,\lambda,\mu) = \max\{|\mathcal{G}| : \mathcal{G} \subseteq \binom{K}{\lambda},\ |K| = k,\ v(\mathcal{G}) \leq \mu\}$。1959年，Erdős和Gallai[70]确定了当$\lambda = 2$时$m(k,\lambda,\mu)$的值。

引理2.3.1. 当$k \geq 2\mu+1$时，$m(k,2,\mu) \leq \max\{\binom{2\mu+1}{2}, \binom{k}{2} - \binom{k-\mu}{2}\}$。

在研究分离矩阵时，一个很重要的概念是“隐私性”，或者说“私有部分”[67]。对某个给定的矩阵M，$[t]$的某个子集被称为是私有的，如果它仅仅被某一列包含；反之$[t]$的某个子集被称为是非私有的，如果它至少被某两列包含。当证明定理2.1.1时，我们实际上考虑了私有的1-子集，因为某列是孤立的当且仅当它包含一个私有1-子集。为了证明我们关于$T(d)$的一般界，我们考察了私有2-子集的性质。更精确地说，我们

得到了一个下界，即，d-DM的每一列至少要包含若干数量的私有2-子集。对列c，定义$P(c) = \{T \subseteq \{1, \ldots, t\} : |T| = 2,\ T \subseteq c\ and\ T\ is\ private\}$，为$c$所包含的私有2-子集的集合；定义$N(c)$为$c$所含有的非私有2-子集的集合。若列$c$的重量为$k$，即它含有$k$个1，那么我们有$\binom{k}{2} = |P(c)| + |N(c)|$，因为$P(c)$和$N(c)$划分了$c$的所有2-子集。以下引理提供了$N(c)$大小的一个上界。

引理2.3.2. *设M是一个$t \times n$的d-DM，且M没有孤立列。那么对任意的列c满足$|c| = d + s$，其中$1 \leq s \leq d-1$，我们有$|N(c)| \leq m(d+s, 2, s-1) \leq \max\{\binom{2s-1}{2}, \binom{d+s}{2} - \binom{d+1}{2}\}$成立。*

证明. 由$m(d+s, 2, s-1)$的定义可知，我们只需证明$N(c)$不包含s个互不相交的成员。如若不然，c剩下的$(d+s) - 2s = d - s$个1必定包含于M的$d-s$列中，这是因为c不含私有的1-子集。那么，c包含在$s + (d-s) = d$列的并集中，这违反了d-分离的性质。 □

对$s \geq 1$，经过直接计算我们可以验证如下等式成立：

$$\begin{aligned} &\max\{\binom{2s-1}{2}, \binom{d+s}{2} - \binom{d+1}{2}\} \\ &= \begin{cases} \binom{d+s}{2} - \binom{d+1}{2}, & s \leq \frac{2}{3}d + \frac{2}{3}, \\ \binom{2s-1}{2}, & s \geq \frac{2}{3}d + \frac{2}{3}. \end{cases} \end{aligned} \tag{2-1}$$

为了证明定理2.1.2，我们还需要一个引理。

引理2.3.3. *设M是一个$t \times n$的d-DM。假设c是M的任意一列，且c的重量为w_c，那么删去c和所有与之相交的行（即在c的位置含1），我们可以得到一个$(t - w_c) \times (n-1)$的$(d-1)$-DM。*

证明. 见文献[58]的引理2.2.2。 □

定理2.1.2的证明. 根据引理2.2.1，我们可以再一次假设M没有孤立列，则M的最小列重至少为$d+1$。为了证明这个定理，我们对d进行归纳假设。根据之前的结果，我们的结论对$1 \leq d \leq 5$都成立。假设结论对$d-1$也成立。令c是具有最大列重的那一列，为简便起见，令$\kappa = (15 + \sqrt{33})/24$。那么，我们的目标是证明$t \geq \kappa d^2$。我们的证明可以分为两个部分。

情形1： $|c| \geq \lceil 2\kappa d \rceil$。由引理2.3.3可知，删去$c$以及与它相交的行，我们可得一个$(t - |c|) \times (n-1)$的$(d-1)$-DM。显然，由$n > t$可知$n - 1 > t - |c|$。由归纳假设可得$t \geq |c| + \kappa(d-1)^2 \geq 2\kappa d + \kappa(d-1)^2 \geq \kappa d^2$。

情形2： $|c| \leq \lfloor 2\kappa d \rfloor$。这时，$M$每列的列重至多为$\lfloor 2\kappa d \rfloor$。给定某列$u$满足$|u| = d + s$，这里$1 \leq s \leq (2\kappa - 1)d$。我们估计$u$所包含的私有2-子集的数量。一方面，若$|u| \leq \frac{5d}{3} + \frac{2}{3}$，则由公式(2-1)的第一个式子可知$|P(c)| = \binom{d+s}{2} - |N(c)| \geq \binom{d+1}{2}$；另一方面，若$|u| > \frac{5d}{3} + \frac{2}{3}$，则有$2d/3 \leq s \leq (2\kappa - 1)d$，由公式(2-1)的第二个式子可知$|P(c)| \geq \binom{d+s}{2} - \binom{2s-1}{2} \geq (d^2 + 2ds - 3s^2)/2 \geq (3\kappa - 1)(2 - 2\kappa)d^2 = \kappa d^2/2$。注意到，由$\kappa < 1$可知，$|P(c)| \geq \kappa d^2/2$在两种情形下都成立。因为私有2-子集的总数不可能超过$\binom{t}{2}$，我们有$\binom{t}{2} \geq \sum_c |P(c)| \geq n \times \kappa d^2/2 \geq (t+1)\kappa d^2/2$，由此易推出结论，证毕。 □

以下的结论也是显然的。

推论2.3.4. $t(d, n) \geq \min\{\frac{15+\sqrt{33}}{24} d^2, n\}$。

证明. 我们有$t(d, n) \geq \min\{T(d), n\}$，则结论成立。 □

依据证明定理2.1.2类似的方法，我们可以证明如下引理。

推论2.3.5. *设M是一个$t \times n$的d-DM。如果$n > t$，且对M的每列c，都有$|c| \leq \lfloor \frac{5d}{3} \rfloor$。那么，我们有$t > d^2 + d + 1$。*

证明. 由公式(2-1)可知，$|P(c)| \geq \binom{d+1}{2}$对所有非孤立列$c$都成立。那么，由$\binom{t}{2} \geq \sum_c |P(c)| \geq n\binom{d+1}{2} \geq (t+1)\binom{d+1}{2}$可知，结论成立。 □

2.4 结语

在本节中，我们考虑了如下问题，即求最小的t，使得存在一个$t \times n$的d-DM满足$n > t + 1$。我们的结果显著改进了之前的结果。我们方法的创新性在于，考虑了私有2-子集的性质，并利用了Erdős和Gallai的图匹配定理[70]。推广我们方法的一个自然想法是考虑更大的私有子集，那么，这时我们可能需要一个超图版本的图匹配定理[74]。如果这个想法可以行得通，那将是很有趣的。

3 数字指纹码

3.1 简介

盗版追踪方案是由Chor，Fiat和Noar[50]于1994年引入的，他们的初衷是为了打击版权剽窃行为。盗版追踪方案在数字指纹或者加密广播的场景中都非常有用，在这种情况下，只有经过授权的用户才有资格获取分发的文件。我们不妨以一个例子来说明数字指纹码是如何在版权保护中发挥作用的。

在加密广播体系中，商业公司给每个用户都分发一个解密盒。每个解密盒由N把密钥组成，每把密钥有q种可能的取值。一般意义下，不同秘钥的取值集合互不相交。每个解密盒都可以用一个N元组$x = (x_1, \ldots, x_N)$来表示，不失一般性，我们可以设对$1 \leq i \leq N$都有$1 \leq x_i \leq q$。假设有一小部分合谋团体希望构造一个伪造的解密盒$y = (y_1, \ldots, y_N)$，其中，第i把密钥y_i取自该合谋团体所持有的第i把密钥的集合。这一合谋团体可以分发他们的伪造解密盒y以牟利，为了防止这种行为发生，我们希望可以恰当地设计每个合法的解密盒x，使得当y被发现后，我们可以通过y 追踪出一个或多个参与了合谋的用户。

在文献[128]中，Stinson，Staddon和Wei详细讨论了四种盗版追踪方案，即，防诬陷码（Frameproof Codes，简称FP），安全防诬陷码（Secure Frameproof Codes），父代识别码（Parent-identifying Codes，或Identifying Parent Property Codes，简称IPP）和追踪码（Traceability Codes，简称TA）。在这篇论文中，我们主要讨论除了安全防诬陷码之外的三种码。这些码有不同的追踪性能，因此被用于不同的目的。例如，t-FP可以被用来阻止最多t 个合谋者来诬陷某个不在该合谋集合中的合法用户。但是，我们一般认为在数字指纹体系下，FP没有追踪性能——它不能检测出任何合谋者。因此，为了追踪至盗版文件的源头，IPP和TA被引入了，它们具有强度不同的追踪算法。文献中有大量关于这些码的应用和性质的研究，例如文献[10,15,34–37,50,51,128]。这个研究领域的一个主要课题就是决定这些码类的上下界。

不妨考虑一个码$\mathcal{C} \subseteq F^N$，这里，$F$表示一个$q$元集合。不失一般性，我们可以令$F = \{0, 1, \ldots, q-1\}$。若$|\mathcal{C}| = n$，我们把码$\mathcal{C}$称为是一个$(N, n, q)$码。每个码字$c \in \mathcal{C}$可以

被表示为$c=(c_1,\ldots,c_N)$，其中，对所有$1\le i\le N$都有$0\le c_i\le q-1$。有些时候，我们更倾向于用一个矩阵来描述一个码。我们把一个(N,n,q)码表示成一个$N\times n$的q元矩阵，矩阵的每列都一一对应于一个码字。这个矩阵被称为是该码的表示矩阵。本文中，我们经常会用到一个码的表示矩阵，因为这样可以给我们提供很多直观的感受。

对任意集合$D\subseteq\mathcal{C}$与$1\le i\le N$，我们记$desc_i(D)=\{c_i:c\in D\}$。D的后代集（Descendant Set）被记为

$$desc(D)=\{x\in F^N:x_i\in desc_i(D),\ 1\le i\le N\}.$$

我们也能把$desc(D)$看成是

$$desc(D)=desc_1(D)\times desc_2(D)\times\cdots\times desc_N(D).$$

如果我们有$x\in desc(D)$，集合$D\subseteq\mathcal{C}$被称为是一个向量$x\in F^N$的父代集。我们用$\mathcal{P}_t(x)$来表示x的满足如下条件的父代集的集合，即$|D|\le t$且$D\subseteq\mathcal{C}$。

对任意两个向量$x,y\in F^n$，汉明距离（Hamming Distance）$d(x,y)$被定义为它们之间不同位置的个数：

$$d(x,y)=|\{1\le i\le N\mid x_i\ne y_i\}|.$$

有时，使用$I(x,y)=N-d(x,y)$来考量x与y之间的关系会更方便，它表示了x与y相同的位置的个数。码$\mathcal{C}\subseteq F^N$的极小距离被定义为

$$d(\mathcal{C})=\min\{d(x,y)\mid x,y\in\mathcal{C},\ x\ne y\}.$$

对向量$x\in F^N$与子集$D\subseteq\mathcal{C}$，群距离（Group Distance）$d(x,D)$被定义为

$$d(x,D)=|\{i:1\le i\le N,\ x_i\notin desc_i(D)\}|.$$

类似地，我们可以用$I(x,D)=N-d(x,D)$来表示满足$x_i\in desc(D_i)$，$1\le i\le N$的位置i的数目。

我们现在已经做好准备，可以给出本文研究的各种码类的概念。

定义3.1.1. 设$\mathcal{C}$是一个(N,n,q)码，$t\ge 2$是一个整数。

(1) 我们称$\mathcal{C}$为一个t-防诬陷码（或者，t-FP），如果对所有的$D\subseteq\mathcal{C}$且$|D|\le t$，都有

$$desc(D)\cap\mathcal{C}=D.$$

$\mathcal{C}$也会被记为是$FPC(N;n,q,t)$。

(2) 我们称$\mathcal{C}$为一个t-父代识别码（或者，t-*IPP*），如果对所有的$x \in F^N$，都有$\mathcal{P}_t(x) = \emptyset$或者

$$\cap_{D \in \mathcal{P}_t(x)} D \neq \emptyset.$$

$\mathcal{C}$也会被记为是$IPP(N; n, q, t)$。

(3) 我们称$\mathcal{C}$为一个t-追踪码（或者，t-*TA*），如果对所有的$D \subseteq \mathcal{C}$且$|D| \leq t$，和任意的$x \in desc(D)$，都有

$$\min_{c \in D} d(x, c) < \min_{y \in \mathcal{C} \setminus D} d(x, y).$$

$\mathcal{C}$也会被记为是$TA(N; n, q, t)$。

广为人知的是，t-TA性质蕴含了t-IPP性质，t-IPP性质蕴含了t-FP性质。文献[128]详细记载了这几种码类之间的联系。我们已经提到过，如果合谋者的数目不超过t个，那么t-IPP和t-TA 都可以追踪到至少一个合谋者。通俗地讲，假设我们有一个安全码$\mathcal{C}$，一个最多有t个违法用户的合谋者集合$D \subseteq \mathcal{C}$。设$x \in desc(D)$是盗版文件，那么我们的目标是发现某个盗版者$c \in D$。如果$\mathcal{C}$是t-IPP，那么我们可以把$\mathcal{P}_t(x)$ 确定出来——只需把$\mathcal{C}$的所有大小不超过t的子集检测一遍，看看x是否是它的后代；根据定义，我们一定有$\cap_{E \in \mathcal{P}_t(x)} E$是$D$的非空子集。另一方面，如果$\mathcal{C}$是一个$t$-TA，通过计算所有的距离$\{d(x, c) : c \in \mathcal{C}\}$，则我们一定可以找到某个$c \in D$；根据定义，那些有着最小距离的码字一定属于$D$。总而言之，若有$n$个$N$长的$q$元码，且合谋者的数量不超过$t$个，那么IPP和TA一定可以在有限时间内找到一个合谋者，根据性质的不同，它们分别需要时间$\mathcal{O}(N\binom{n}{t})$ 和$\mathcal{O}(Nn)$。值得注意得是，如果我们采用列举译码（List Decoding）算法[18,125]，TA码的追踪时间可以被进一步减少到$\mathcal{O}(N \log^c n)$，c为某个给定常数。

该研究领域的一个核心问题就是确定出满足这些条件的码最多可以含有多少个码字。固定码长N，字母集大小q和码的强度t，我们用$M_{FP}(N, q, t)$，$M_{IPP}(N, q, t)$，$M_{TA}(N, q, t)$来表示对应码类的极大码字数量。此外，我们用$N(t)$来记最小的正整数N使得$M_{FP}(N, 2, t) > N$。最近，$N(t)$的大小引起了可观的研究兴趣[81]。

一般来说，研究这些码类的界主要有两条研究方向。第一，我们考虑小字母集和大码长下的码字个数，即，固定q，让N趋向于无穷大。第二，考虑小码长和大字母集下的码字个数，即，固定N，让q趋向于无穷大。由于具有很大极小距离的纠错码通常可以满足这些指纹码的充分条件[128]，因此，在大字母集上构造码字数量较多的码是相对简单的。然而，由于Plotkin界[139]的限制，在小字母集上构造码字数量较多的码则困难多了，例如，文献[17,18,36,63]都是研究这方面的工作。

本章的动机是改进这些码的上界。我们总共将讨论三个上界。第一个上界（见定理3.2.3）极大地改进了关于二元防诬陷码的已知界，这部分内容包括在第3.2节中；第二个界（见定理3.3.2）改进了父代识别码的一般界，这部分内容包括在第3.3 节中；第三个界（见定理3.4.3）提供了强度为3的追踪码的第一个已知非平凡上界，这部分内容包括在第3.4节中；第3.5 节是一些总结。

3.2 防诬陷码

Blackburn[34]给出了当N小q大时$M_{FP}(N,q,t)$现存的最优界，他证明了如下定理。

定理3.2.1. 令$r \in \{0,\ldots,t-1\}$是一个满足$r \equiv N \pmod t$的整数，那么我们有$M_{FP}(N,q,t) \leq \max\{q^{\lceil N/t\rceil}, r(q^{\lceil N/t\rceil}-1)+(t-r)(q^{\lfloor N/t\rfloor}-1)\}$。

注意到，在很多情况下，常数r和$t-r$都可以被减小。例如，文献[34]的引理9给出了一个更好的界，它改进了$q^{\lceil N/t\rceil}$之前的常数，并把这个常数的决定和极值集合论中的一个问题联系起来。当$r=1$时，文献[140]给出了$M_{FP}(N,q,t) \leq q^{\lceil N/t\rceil}$，这是一个很简洁的上界。

我们曾经提到过，在小字母集上，$M_{FP}(N,q,t)$的决定要比在大字母集上更难。直观地讲，二元防诬陷码是最有趣且最困难的情形。一些近期的论文[80,81]在这个方面取得了一些进展。下面的定理来自于文献[81]。

定理3.2.2. 对所有的$t \geq 3$和$t+1 \leq N \leq 3t$，我们都有$M_{FP}(N,2,t) \leq N$。

注意到$N(t)$是最小的整数N使得存在一个$FPC(N;n,2,t)$满足$n > N$。从定理3.2.1中，我们可以推出$N(t) > t$（只需检查$N \leq t$ 时的上界）。此时，结合定理3.2.2，我们可以得到一个简单界$N(t) > 3t$。

定理3.2.3. 对所有$t \geq 3$与$N < \frac{15+\sqrt{33}}{24}(t-2)^2$，我们都有$M_{FP}(N,2,t) \leq N$，或者，等价地说，$N(t) \geq \frac{15+\sqrt{33}}{24}(t-2)^2$。

我们将在下一个小节中证明这个定理。注意到，我们的结果极大地提高了文献[81]中的结果，将其从线性阶提高到了平方阶。然而，该结论和猜想的界$N(t)=t^2+o(t^2)$还有一定距离。

3.2.1 定理3.2.3的证明

有时，如果我们使用防诬陷码的另一个等价定义，在考虑问题时会更为方便。

定义3.2.4. 一个(N,n,q)码$\mathcal{C}$是一个t-防诬陷码，如果对任何$c \in \mathcal{C}$以及$D \subseteq \mathcal{C}$，使得$c \notin D$和$|D| \leq t$，我们都有$c \notin desc(D)$，这等价于说存在某个$1 \leq i \leq N$使得$c_i \notin desc_i(D)$。

引理3.2.5. 防诬陷码的两种定义是等价的。

证明. 一方面，令$\mathcal{C}$是一个满足定义3.1.1的(N,n,q)码。则给定任意的$c \in \mathcal{C}$以及$D \subseteq \mathcal{C}$，只要满足$c \notin D$和$|D| \leq t$，我们都有$c \notin desc(D)$，如若不然，我们有$desc(D) \cap \mathcal{C} = D \cup \{c\}$，这违反了定义3.1.1。

一方面，令$\mathcal{C}$是一个满足定义3.2.4的(N,n,q)码。那么，给定任意的$D \subseteq \mathcal{C}$，只要$|D| \leq t$，我们就有$desc(D) \cap \mathcal{C} = D$，如果不然，若$desc(D) \cap \mathcal{C} = D \cup \{c\}$对某个$c \notin D$和$c \in \mathcal{C}$成立，那么，我们有$c \in desc(D)$，这违反了定义3.2.4。 □

为了证明定理3.2.3，我们需要引入cover-free集的定义。令X是一个N元集。用2^X来表示由X的所有子集所构成的集合，即$|2^X| = 2^N$。我们说一个集族$\mathcal{F} \subseteq 2^X$是$t$-cover-free 的，如果对任意$\mathcal{F}$ 的$t+1$ 个元素$A_0, A_1, \ldots, A_t$，都有$A_0 \nsubseteq A_1 \cup A_2 \cup \cdots \cup A_t$。假设$|\mathcal{F}| = n$，并且记$X = \{x_1, \ldots, x_N\}$，$\mathcal{F} = \{A_1, \ldots, A_n\}$。$\mathcal{F}$被记为$CFF(N;n,t)$。令$M^*$为$\mathcal{F}$的表示矩阵，这是一个$N \times n$的二元矩阵，其中，行用$X$的元素标记，列用$\mathcal{F}$中的元素标记，在矩阵的第$i$行和第$j$列的位置取1当且仅当$x_i \in A_j$。在一个二元矩阵中，每列的重量是指该列里所含1的个数。

以下引理来自于文献[117]中。

引理3.2.6. 令$\mathcal{F}$是一个$CFF(N;n,t)$，设M^*是它的表示矩阵。固定$\mathcal{F}$的一个元素A，考虑新的集族$\mathcal{F}_1$，定义为

1) $\mathcal{F}_1 \subseteq 2^{X \setminus A}$,

2) $\mathcal{F}_1 = \{B \setminus A : B \in \mathcal{F},\ B \neq A\}$.

则$\mathcal{F}_1$是一个$CFF(N - |A|; n-1, t-1)$。

证明. 我们容易验证$CFF(N-|A|;n-1,t-1)$的前两个参数，因此，只需证明$\mathcal{F}_1$是一个$(t-1)$-cover-free集。如若不然，则存在t个不同的元素$B_0,B_1,\ldots,B_{t-1}$ of $\mathcal{F}_1$，使得$B_0\subseteq B_1\cup\cdots\cup B_{t-1}$。对每个$0\leq i\leq t-1$，记$A_i$为$\mathcal{F}$的元素，它满足$B_i=A_i\setminus A$。那么，我们有$A_0\subseteq B_0\cup A\subseteq(B_1\cup\cdots B_{t-1})\cup A\subseteq A_1\cup\ldots\cup A_{t-1}\cup A$，这违反了$\mathcal{F}$的$t$-cover-free性质。 □

Cover-free集和二元防诬陷码有着紧密的联系。它们的关系可以被表示为如下两个引理。

引理3.2.7. *每个$CFF(N;n,t)$都是$FPC(N;n,2,t)$，并且，每个$FPC(N;n,2,t)$也是一个$CFF(2N;n,t)$。*

证明. 用M和M^*分别标记$FPC(N;n,2,t)$和$CFF(N;n,t)$的表示矩阵。给定M^*，由t-cover-free性质可知，对每列和任意另外t列，都存在一行满足第1列在该行取1，其它列都取0。若我们把M^*的列看成是某些二元防诬陷码的码字，则M^*必然满足定义3.2.4的充分条件，这意味着M^*也代表一个$FPC(N;n,2,t)$。

另一方面，给定M，用10替换0，01替换1。我们得到一个$2N\times n$的矩阵，我们把它记为M_1。我们只需证明M_1是某个$CFF(2N;n,t)$ 的表示矩阵。注意到，M满足t-防诬陷码的性质，考虑M_1，对它的每列和其它任意t列，考虑它们在M中的对应列，由t-防诬陷码的性质可知，存在某行，满足$10\cdots0$或者$01\cdots1$，这也等价于在M_1中有

$$\begin{pmatrix}0&1&\cdots&1\\1&0&\cdots&0\end{pmatrix}\ or\ \begin{pmatrix}1&0&\cdots&0\\0&1&\cdots&1\end{pmatrix}.$$

注意到，第一个子矩阵的第二行或者第二个子矩阵的第一行满足t-cover-free性质。若我们把M_1看成是某个$\mathcal{F}\subseteq 2^X$的表示矩阵，这里$|X|=2N$，那么，由以上讨论我们可以推断出$\mathcal{F}$满足t-cover-free性质。 □

引理3.2.8. *令$N^*(t)$为使得存在一个满足$n>N$的$CFF(N;n,t)$的最小N，同时令$N(t)$为使得存在一个满足$n>N$的$FPC(N;n,2,t)$的最小N，则对$t\geq 3$，我们有$N^*(t-2)\leq N(t)\leq N^*(t)$成立。*

证明. 记M满足$N=N(t)$的$FPC(N;n,2,t)$的表示矩阵，则由$N(t)$的定义可知$n>N$。首先，上述不等式中的上界来自于如下事实，引理3.2.7已经指出，每个$CFF(N;n,t)$同时也

是一个$FPC(N;n,2,t)$。我们只需要证明下界。将M中的0用10替换，1用01替换，我们得到一个$2N\times n$的新矩阵M_1，显而易见，M_1具有恒常列重N，由引理3.2.7可知，M_1是某个$CFF(2N;n,t)$的表示矩阵。又由引理3.2.6，删去M_1的任意一列，以及该列中包含1的行，我们得到一个新矩阵M_2，M_2是一个$CFF(N;n-1,t-1)$的表示矩阵。

我们声明M_2存在一列至少具有重量2。记c为从M_1删去的那一列。如果某个$c'\in M_2$仅有重量1，那么我们可以说明，c与c'在M_1 中恰好含有$N-1$个相同的分量。如果M_2中具有两列重量都为1，那么在M中，存在两个不同列，它们与c都恰好含有$N-1$个相同的分量。这时，我们不难证明，c必然包含在这两列的后代集内。这违反了防诬陷码的基本性质。因此，M_2至多含有一个重量为1的列。由$n-1\geq N>t\geq 3$可得，我们的声明必然成立。

取M_2的任意一个重量为2的列。从M_2中删去该列，以及在该列取值为1的行。再一次，由引理3.2.6可知，新的矩阵是某个$CFF(N';n-2,t-2)$的表示矩阵，同时，我们有$N'\leq N-2<n-2$，因为我们假设了$n>N$，所以，我们可以推出$N'\geq N^*(t-2)$，不等式的下界$N(t)\geq N^*(t-2)$也立即成立。 □

为了证明定理3.2.3，我们只需再说明一个引理，该引理是定理2.1.2的直接结论。

引理3.2.9. $N^*(t)\geq \frac{15+\sqrt{33}}{24}t^2$。

定理3.2.3的证明. 定理3.2.3是引理3.2.8和引理3.2.9的一个直接结论。 □

3.3 父代识别码

在上一节中我们提到了t-FP码的上界大概是$\mathcal{O}(q^{\lceil N/t\rceil})$。然而，为了保证其追踪性，$t$-IPP码只具有小得多的容量，表示为文献[15]中的如下定理。

定理3.3.1. 记$v=\lfloor (t/2+1)^2\rfloor$，那么我们有$M_{IPP}(N,q,t)\leq (v-1)q^{\lceil N/(v-1)\rceil}$。

文献[35]提供了一个稍弱的上界，即，$M_{IPP}(N,q,t)\leq \frac{v(v-1)}{2}q^{\lceil N/(v-1)\rceil}$。在本文中，我们强化了文献[15]的方法，并用该方法来证明如下定理，这个定理也提供了IPP码现存的最好界。

定理3.3.2. 令$v=\lfloor (t/2+1)^2\rfloor$，其中，$0\leq r\leq v-2$是一个正整数使得$N\equiv r \mod (v-1)$，那么我们有$M_{IPP}(N,q,t)\leq rq^{\lceil N/(v-1)\rceil}+(v-1-r)q^{\lfloor N/(v-1)\rfloor}$。

当$v-1 \nmid N$时，我们的定理显然改进了定理3.3.1，因为首项的系数被改进为某个$r<v-1$的常数。

3.3.1 定理3.3.2的证明

在证明之前我们需要一些准备工作。对某个向量$x \in F^N$和集合$V \subseteq \{1,\ldots,N\}$，我们定义$x$被限定于$V$的部分为一个有序的$|V|$-元组，我们把它记为$x|_V=(x_{i_1},\ldots,x_{i_{|V|}})$，其中，对所有$1 \le j \le |V|$和$1 \le i_1 < \cdots < i_{|V|} \le N$，有$i_j \in V$。令$\mathcal{C}$为一个$(N,n,q)$ 码，且c为$\mathcal{C}$的一个码字。我们说$c|_V$是c的一个私有部分，如果$\mathcal{C}$中不含其它码字使得其与c在V的部分完全相同。换句话说，$c|_V$是私有的，当且仅当对所有$c' \in \mathcal{C}\setminus\{c\}$，都有$c'|_V \neq c|_V$。

以下，我们将证明定理3.3.2。

定理3.3.2的证明. 令$\mathcal{C}$为任意一个$IPP(N;n,q,t)$，记$\mathcal{C}$的表示矩阵为M，则M是一个$N \times n$的q-元矩阵。我们将M的行划分成$v-1$个互不相交的部分，记为$V_1,\ldots,V_{v-1}$，这个划分满足条件$|V_1|=\cdots=|V_r|=\lceil N/(v-1)\rceil$，以及$|V_{r+1}|=\cdots=|V_{v-1}|=\lfloor N/(v-1)\rfloor$。我们不难验证$r(\lceil N/(v-1)\rceil)+(v-1-r)(\lfloor N/(v-1)\rfloor)=N$，因此，$\{V_i : 1 \le i \le v-1\}$实际上是$M$的行的一个划分。

我们说一个码字$x \in \mathcal{C}$是特殊的（对应于$\mathcal{C}$来说），如果它包含支撑集为某些V_i的私有部分。假设$|\mathcal{C}| \ge rq^{\lceil N/(v-1)\rceil}+(v-1-r)q^{\lfloor N/(v-1)\rfloor}+1$，我们的目标是找到一个$\mathcal{C}$的子集，使得它违反$t$-IPP的性质。

我们声称一定存在一个非空集合$\hat{\mathcal{C}} \subseteq \mathcal{C}$，使得它不包含任何特殊的（对应于$\hat{\mathcal{C}}$来说）码字。

我们删去$\mathcal{C}$中的特殊码字，把剩下的码字的集合记为$\mathcal{C}^{(1)}$。然后，我们删去$\mathcal{C}^{(1)}$中的特殊码字（对应于$\mathcal{C}^{(1)}$），把剩下的码字的集合记为$\mathcal{C}^{(2)}$。接下来，我们重复这一操作。每一次，无论何时存在一个特殊码字（对应于那些仍未删去的码字的集合），我们就把它删去。我们一直这样做，直到我们得到一个码$\hat{\mathcal{C}}$，使得它不含有任何特殊的码字。我们声明$\hat{\mathcal{C}}$一定是非空的。一方面，任何部分（尤其考虑那些具有支撑集V_i的部分）只能被作为特殊部分删去一次。另一方面，任何被删去的码字（在某个$\mathcal{C}^{(i)}$内是特殊的，$i \ge 1$），包含至少一个支撑集为某个V_i的特殊部分（与$\mathcal{C}^{(i)}$对应）。因此，我们最多能删去不超过$rq^{\lceil N/(v-1)\rceil}+(v-1-r)q^{\lfloor N/(v-1)\rfloor}$ 个特殊码字，因为每个V_i最多可以对应于$q^{|V_i|}$个不同的部分。考虑到我们的假设，$|\mathcal{C}| \ge rq^{\lceil N/(v-1)\rceil}+(v-1-r)q^{\lfloor N/(v-1)\rfloor}+1$，这种删除并不能把$\mathcal{C}$中所有的码字都删去。因此，在删除过程结束之后，我们必然得到一个非空集合，使

得其中的任何码字都不包含支撑集为某个V_i的特殊部分（当然，相对于这些剩余的码字）。那么，我们最后得到的这个集合满足我们声明中所期望的条件。我们把这个集合记为$\hat{\mathcal{C}}$。

在随后的证明里，我们先假设t是一个偶数，那么，我们有$v-1=(t/2+1)^2-1=t^2/4+t$。目前，我们的目标是找到$\hat{\mathcal{C}}$的某个特殊子集，以便推导出我们期望的矛盾。我们从选取某个码字$x_1\in\hat{\mathcal{C}}$开始。然后，选取码字$x_2\in\hat{\mathcal{C}}$满足$x_1|_{V_{t/2+1}}=x_2|_{V_{t/2+1}}$。注意到，$\hat{\mathcal{C}}$的性质保证了这样的$x_2$的存在性。记$m_1=(t/2+1)$。

为了选取x_3，我们考虑x_2以$V_{2(t/2+1)}=V_{t+2}$为支撑集的部分。这一部分必然在$\hat{\mathcal{C}}$的其它码字中出现。我们要检查是否有$x_1|_{V_{t+2}}=x_2|_{V_{t+2}}$。如果成立，我们转去考虑以$V_{t+3}$为支撑集的部分，并去类似地检查它。我们一直这样做直到我们找到某一个V_i满足$i\geq t+2$并且$x_1|_{V_i}\neq x_2|_{V_i}$。我们选取某个码字$x_3$与$x_2$在$V_i$完全相符。记$m_2=i$。

我们一直延续这种操作。第$(k+1)$个码字x_{k+1}的选取方式如下。记m_k是满足$m_k\geq m_{k-1}+(t/2+1)$和$x_k|_{V_{m_k}}\neq x_i|_{V_{m_k}}$对所有$1\leq i\leq k-1$都成立的第一个整数。然后，我们选取$x_{k+1}$为与$x_k$在$V_{m_k}$完全相符的那个码字。如果这样的$m_k$并不存在，我们就说$m_k$是未定义的。

当某个m_k是未定义的，我们就停止这种操作。注意到，用这种方式我们最多可以选出$t/2+1$个码字，因为我们每次选取我们都跳过了至少$t/2+1$个部分，并且，一个N长码字至多被分为$v-1=t^2/4+t=(t/2+1)t/2+t/2<(t/2+1)^2$个部分，因此，我们永远不能找到第$(t/2+2)$个码字。最后，我们得到了一个集合$X\subseteq\hat{\mathcal{C}}$满足如下条件：$|X|\leq t/2+1$，$x_i|_{V_{m_i}}=x_{i+1}|_{V_{m_i}}$对所有$1\leq i\leq|X|-1$都成立。

我们按如下的方式选择X的子代，$s\in desc(X)$。s的最开始的$m_1=t/2+1$个部分（即那些在$V_1\cup\cdots\cup V_{m_1}$中的分量），是取自于$x_1$的，接下来的那些部分，直到$V_{m_2}$都是取自于$x_2$（即那些在延续这个操作。$X$的最后一个元素贡献了至多$t/2$个部分，且这些部分是不属于$X$的其它任何一个元素的。

接下来的观察是我们证明的核心。任何$x_i\in X$贡献了至多$t/2$个不属于其它任何X中元素的部分。固定$x_i\in X$，则$s\in desc(X)$取自于x_i的部分是$V_{m_{i-1}+1},\ldots,V_{m_{i-1}+t/2},\ldots,V_{m_i}$（对$i=1$，我们令$m_0=0$）。由我们对$m_i$和$x_i$的定义可知，仅仅那些$V_i$的前$t/2$个，即，$V_{m_{i-1}+1},\ldots,V_{m_{i-1}+t/2}$，有可能是那些$x_i$在$X$内“私有”的部分。由于$x_i\in\hat{\mathcal{C}}$，并且根据定义，任何$\hat{\mathcal{C}}$中的码字都不包含支撑集为某个$V_i$的私有部分，则存在一个集合$Y_i=\{y_1,\ldots,y_{t/2}\}\subseteq\hat{\mathcal{C}}$，最多有$t/2$个码字使得$y_j|_{V_{m_{i-1}+j}}=x_i|_{V_{m_{i-1}+j}}$对所有$1\leq j\leq t/2$都成立。因此，由$X_i=(X\setminus\{x_i\})\cup Y_i$成立的新集合$X_i$，也能产生后代$s$，这意味着$s\in desc(X_i)$。注意到，$|X_i|=|X|-1+|Y_i|\leq t/2+1-1+t/2=t$，那么我们有$X_i\in\mathcal{P}_t(s)$。

对所有$x_k \in X$我们都可以做类似的替换，我们可以得到对应的Y_k和X_k。令$X_0 = X$，那么由之前的讨论我们可得$s \in desc(X_k)$对所有$0 \leq k \leq |X|$都成立。因此，根据如下简单事实，我们可以推出$\cap_{0\leq k\leq |X|} X_k = \emptyset$，且$|X_k| \leq t$，这违反了$t$-IPP码的性质。

当t是奇数时，我们做完全类似的操作，只需令$m_{k+1} \geq m_k + (t+1)/2$，这时，我们有$|X| \leq (t+1)/2 + 1$。 □

3.4 追踪码

在之前两个章节中我们描述了防诬陷码和父代识别码的上界。然而，决定追踪码的上界是一个困难得多的问题。除开由防诬陷码和父代识别码导出的简单界之外，唯一已知的界是由Blackburn[36]等人给出的。

定理3.4.1. *$M_{TA}(N, q, 2) \leq cq^{\lceil N/4 \rceil}$，其中，$c$是一个仅仅依赖于码长$N$的常数。*

遗憾得是，这个上界并没有我们想得那么好，因为与出现在定理3.2.1和定理3.3.2中的常数相比，这里的常数c实在是太大了（大于$N\binom{N}{\lceil N/4 \rceil}$）。文献[109]给出了一个较为简洁的上界，但是它仅仅对码长为4的2-TA码成立。

在本文中，我们对追踪码的贡献也在于其上界。在文献[36]里，作者提出了下述问题。

问题3.4.2. *令t和N为给定的正整数，满足$t \geq 2$。那么是否存在一个常数c（仅仅依赖于t和N）使得$M_{TA}(N, q, t) \leq cq^{\lceil N/t^2 \rceil}$成立？*

我们在$t = 3$时正面回答了这个问题，我们的结论可以被表述为下面的定理。

定理3.4.3. *令N为一个正整数，则有$M_{TA}(N, q, 3) \leq cq^{\lceil N/9 \rceil}$，这里，$c$是一个仅仅依赖于$N$的常数。*

3.4.1 定理3.4.3的证明

对一个N长码$\mathcal{C}$，一个码字$x \in \mathcal{C}$和一个标示位置的子集$I \subseteq [N]$，其中，$[N] = \{1, 2, \cdots, N\}$,，我们定义：

$$F_{\mathcal{C}}(x, I) = |\{y \in \mathcal{C} : y|_I = x|_I\}|.$$

引理3.4.4. 设t是一个给定的正整数，且令$N = 9t$。假设$\mathcal{C}$是一个q元N长码，且包含*3*个或者更多码字。那么，存在一个子集X，最多含有$c'q^t$个码字，使得子码$\mathcal{C}' = \mathcal{C}\backslash X$满足$d(\mathcal{C}') \geq d(\mathcal{C})+1$，其中，$c'$是一个仅依赖于$N$的常数。注意到，我们简单地说$d(\emptyset) = \infty$。

证明. 假设$d(\mathcal{C}) > N - t$。那么由著名的Singleton界可知，$|\mathcal{C}| \leq q^t$；在这种情况下，我们可以令$X = \mathcal{C}$以及$\mathcal{C}' = \emptyset$。因此，我们假设$d(\mathcal{C}) \leq N - t = 8t$。

假设我们有$d(\mathcal{C}) \leq 2t$。定义$\mathcal{C}$的一个子码$\mathcal{C}'$，它是由移除$\mathcal{C}$的所有含有t个不与其它任意码字共享的位置的码字所构成的；换句话说，我们有

$$X = \{x \in \mathcal{C} : F_{\mathcal{C}}(x, I) = 1 \text{ for some } t\text{-subset } I \subseteq [N]\},$$

且

$$\mathcal{C}' = \{x \in \mathcal{C} : F_{\mathcal{C}}(x, I) \geq 2 \text{ for all } t\text{-subsets } I \subseteq [N]\}.$$

我们有$|X| = |\mathcal{C}\backslash\mathcal{C}'| \leq \binom{N}{t}q^t$，因为在一个$N$长$q$元码中最多有$\binom{N}{t}q^t$不同的$t$元组，并且，每个码字$x \in X$包含至少一个$t$元组，其位置为$I$，满足$F_{\mathcal{C}}(x, I) = 1$；此外，这种$t$元组恰好属于一个$x \in X \subseteq \mathcal{C}$。我们只需证明：不存在不同的码字$x, y \in \mathcal{C}'$满足$d(x, y) = d(\mathcal{C})$。如若不然，存在$x \neq y \in \mathcal{C}'$，使得$d(x, y) = d(\mathcal{C}) \leq 2t$。令$I$ 为$[N]$的一个$2t$元子集，它包含了x与y所有不相同的位置。那么，我们可以选择I_1和I_2，使得$I \subseteq I_1 \cup I_2$，并且$|I_1| = |I_2| = t$。由$\mathcal{C}'$的定义可知，我们有$F_{\mathcal{C}}(x, I_i) \geq 2$，对每个$i \in \{1, 2\}$都成立；因此可以选取$y_1, y_2 \in \mathcal{C}\backslash\{x\}$，使得$x|_{I_i} = y_i|_{I_i}$对$i = 1, 2$都成立。但是，我们则有$x \in desc(y, y_1, y_2)$，这与$\mathcal{C}$是一个3-追踪码相矛盾。因此，我们有$d(\mathcal{C}') > d(\mathcal{C})$，所以在这种情况下引理成立。

如果我们有$2t < d(\mathcal{C}) \leq N - t\ (= 8t)$。记$d(\mathcal{C}) = N - (t + \delta)$，满足$0 \leq \delta < 6t$。定义

$$X = \{x \in \mathcal{C} : F_{\mathcal{C}}(x, I) \leq 2^{\delta+1}\binom{N-t}{\delta+1} \text{ for some } t\text{-subset } I \subseteq [N]\},$$

以及

$$\mathcal{C}' = \{x \in \mathcal{C} : F_{\mathcal{C}}(x, I) > 2^{\delta+1}\binom{N-t}{\delta+1} \text{ for all } t\text{-subsets } I \subseteq [N]\}.$$

注意到$|X| = |\mathcal{C}\backslash\mathcal{C}'| \leq 2^{\delta+1}\binom{N-t}{\delta+1}\binom{N}{t}q^t < 2^{3N}q^t$，因为在一个$N$长$q$元码内至多有$\binom{N}{t}q^t$个不同的$t$元组，并且每个码字$x \in X$包含至少一个$t$元组，位置为$I$，且满足$F_{\mathcal{C}}(x, I) \leq 2^{\delta+1}\binom{N-t}{\delta+1}$，此外，这些$t$元组属于至多$2^{\delta+1}\binom{N-t}{\delta+1}$个码字$x \in X \subseteq \mathcal{C}$。为了证明$d(\mathcal{C}') \geq d(\mathcal{C}) + 1$，我们只需说明不存在不同的码字$x, y \in \mathcal{C}'$满足$d(x, y) = d(\mathcal{C})$。如若不然，存在$y_0 \neq y_1 \in \mathcal{C}'$，满足$I(y_0, y_1) = t + \delta$。定义$I_1 = \{i \in [N] : y_{0,i} = y_{1,i}\}$，那么我们有$y_0|_{I_1} = y_1|_{I_1}$。

取I_2满足$I_1 \cap I_2 = \emptyset$以及$|I_2| = t$。我们声称存在$y_2 \in \mathcal{C}$满足$y_0|_{I_2} = y_2|_{I_2}$与$I(y_1, y_2) \leq \delta$。实际上，$\mathcal{C}$的最小距离蕴含了任何码字都可以被它的$t + \delta + 1$个分量所唯一决定。一旦我们固定了I_2，就有

$$|\{y \in \mathcal{C} : I(y_1, y) \geq \delta + 1,\ y_0|_{I_2} = y|_{I_2}\}| \leq \binom{N-t}{\delta+1} < F_{\mathcal{C}}(y_0, I_2).$$

数值$\binom{N-t}{\delta+1}$表示我们可从$[N]\backslash I_2$中选取$\delta + 1$个分量，使得y_1和y相等，那么，这些分量和I_2唯一决定了y_1。因此，至少存在一个$y_2 \in \mathcal{C}$。我们更新$I_2 = \{i \in [N]\backslash I_1 : y_{0,i} = y_{2,i}\}$，并记$|I_2| = t + \delta_2$，其中，$0 \leq \delta_2 \leq \delta$。注意到，$y_1$和$y_2$在$I_2$中没有相同的分量。因为否则$y_0, y_1, y_2$在这些位置上取值都相等，那么它们都可以被添加到$I_1$。

设$D := [N]\backslash(I_1 \cup I_2)$。若$N - |I_1| - |I_2| \leq t$，由$\mathcal{C}'$的定义可知，我们可以选取某个$y_3 \in \mathcal{C}\backslash\{y_0\}$使得$y_3|_D = y_0|_D$。因此，$y_0 \in desc(y_1, y_2, y_3)$，这与$\mathcal{C}$是一个3-追踪码矛盾。我们可以假设$|D| > t$。令$J = \{i \in [N]\backslash I_1 : y_{1,i} = y_{2,i}\}$。我们有$I(y_0, \{y_1, y_2\}) = |I_1| + |I_2| = 2t + \delta + \delta_2$且$I(y_1, \{y_0, y_2\}) = |I_1| + |J| = t + \delta + |J|$。假设$|J| \leq t + \delta_2$，因为，如若不然，我们可以调换$y_0$和$y_1$的角色。

取一个t元子集$I_3 \subseteq [N]$，使得$I_3 \cap (I_1 \cup I_2) = \emptyset$，让其覆盖$J$的尽可能多的元素。我们声称，存在$y_3 \in \mathcal{C}$ 使得$y_0|_{I_3} = y_3|_{I_3}$且$I(y_3, \{y_1, y_2\}) \leq \delta$。如上文所述，$\mathcal{C}$的任何一个码字由它的$t + \delta + 1$分量所唯一决定，我们有

$$|\{y \in \mathcal{C} : I(y, \{y_1, y_2\}) \geq \delta + 1,\ y_0|_{I_3} = y|_{I_3}\}| \leq 2^{\delta+1}\binom{N-t}{\delta+1} < F_{\mathcal{C}}(y_0, I_3),$$

其中，乘数$2^{\delta+1}$表示选取的分量$i \in [N]\backslash I_3$最多有两种情形，或者$y|_i = y_1|_i$，或者$y|_i = y_2|_i$。因此，存在至少一种选择$y_3 \in \mathcal{C}$。现在，我们重新定义$I_3 = \{i \in [N]\backslash(I_1 \cup I_2) : y_{0,i} = y_{3,i}\}$，并记$|I_3| = t + \delta_3$，这里，$0 \leq \delta_3 \leq \delta$。我们并不难证明$y_1, y_3$与$y_2, y_3$在$I_3$内都没有相同的分量。

对$\{i, j, k\} = \{1, 2, 3\}$，我们记$I_{i,j,k} := \{u \in I_i : y_{j,u} = y_{k,u}\}$，这时，我们可以推出$|I_{1,0,2}| \leq I(y_1, y_2) \leq \delta$，且$|I_{1,0,3}| + |I_{2,0,3}| \leq I(y_3, \{y_1, y_2\}) \leq \delta$。记$E := [N]\backslash(I_1 \cup I_2 \cup I_3)$。容易看出$|E| = 6t - \delta - \delta_2 - \delta_3$以及$|E| > 0$，因为，如若不然，我们有$y_0 \in desc(y_1, y_2, y_3)$，这与3-追踪的性质相矛盾。接下来，我们将考虑两种情形，即，$4t \leq \delta < 6t$与$0 \leq \delta < 4t$。

情形1：$4t \leq \delta < 6t$。

在这种情况下，我们选取一个向量$w \in desc(y_1, y_2, y_3)$，满足$w|_E = y_1|_E$和$w|_{I_j} = y_j|_{I_j}$，这里$j = 1, 2, 3$。我们说$w$这种选取方式是良定义的，因为$E \cup (\cup_{i=1}^{3} I_j) = [N]$，并且他们都是互相不交的。表3-1展示了我们的标记。如下的不等式并不难得出：

	$\overbrace{\quad}^{I_1}$	$\overbrace{\quad}^{I_2}$	$\overbrace{\quad}^{I_3}$	$\overbrace{\quad}^{E}$
$y_0 \in \mathcal{C}'$	$\overbrace{0000\cdots00}$	$\overbrace{0000\cdots00}$	$\overbrace{0000\cdots00}$	$\overbrace{0000\cdots00}$
$y_1 \in \mathcal{C}'$	$0000\cdots00$	$1111\cdots11$	$1111\cdots11$	$1111\cdots11$
$y_2 \in \mathcal{C}$	$****\cdots**$	$0000\cdots00$	$1123\cdots15$	$****\cdots**$
$y_3 \in \mathcal{C}$	$****\cdots**$	$****\cdots**$	$0000\cdots00$	$****\cdots**$
$w \in \mathrm{desc}(y_1,y_2,y_3)$	$\underbrace{0000\cdots00}_{\lvert I_1\rvert=t+\delta}$	$\underbrace{0000\cdots00}_{\lvert I_2\rvert=t+\delta_2}$	$\underbrace{0000\cdots00}_{\lvert I_3\rvert=t+\delta_3}$	$\underbrace{1111\cdots11}_{\lvert E\rvert=6t-\delta-\delta_2-\delta_3}$

表 3-1 当$4t \leqslant \delta < 6t$时

$$
\begin{cases}
I(y_0,w) &= |I_1|+|I_2|+|I_3| = 3t+\delta+\delta_2+\delta_3,\\
I(y_1,w) &= |I_1|+|E| = (t+\delta)+(6t-\delta-\delta_2-\delta_3) = 7t-\delta_2-\delta_3\\
&\leq 7t \leq 3t+\delta \leq I(y_0,w),\\
I(y_2,w) &\leq |I_{1,0,2}|+|I_2|+|E| \leq \delta+(t+\delta_2)+(6t-\delta-\delta_2-\delta_3) = 7t-\delta_3\\
&\leq 7t \leq 3t+\delta \leq I(y_0,w),\\
I(y_3,w) &\leq |I_{1,0,3}|+|I_{2,0,3}|+|I_3|+|E| \leq \delta+(t+\delta_3)+(6t-\delta-\delta_2-\delta_3) = 7t-\delta_2\\
&\leq 7t \leq 3t+\delta \leq I(y_0,w).
\end{cases}
$$

由于$y_0 \notin \{y_1,y_2,y_3\}$，这与$\mathcal{C}$的3-追踪性质相矛盾，得证。

情形2：$0 \leq \delta < 4t$。

在这种情况下，如上所述，我们选择一个向量$w \in desc(y_1,y_2,y_3)$，满足$w|_{I_j} = y_j|_{I_j}$，这里，$j=1,2,3$。然而，对于$w|_E$的选取，我们得更加仔细。

对$1 \leq i < j \leq 3$，定义$J_{i,j} := \{t \in E : y_{i,t} = y_{j,t}\}$与$J_{1,2,3} := J_{1,2} \bigcap J_{1,3} \bigcap J_{2,3}$。我们有$|J_{1,2,3}| \leq |J_{1,2}| \leq \max\{|J|-t,0\} \leq \delta_2$，因为$J_{1,2,3} \subseteq J_{1,2} \subseteq J \setminus I_3$，且我们已经选择了$y_3$使其覆盖$J$的尽可能多的元素。考虑到$|J_{1,3}\setminus J_{1,2,3}| + |J_{2,3}\setminus J_{1,2,3}| \leq I(y_3,\{y_1,y_2\}) \leq \delta < 4t$，我们分别考虑如下的两种情形：

子情形2.1：$|J_{1,3}\setminus J_{1,2,3}| \leq 2t+\delta_3$与$|J_{2,3}\setminus J_{1,2,3}| \leq 2t+\delta_3$。

当$i \in E$时，我们可以按如下的步骤来定义w_i。表3-2标示了我们的记号。

1. 当$i \in J_{1,2} \bigcup J_{2,3}$时，取$w_i = y_{1,i}$；
2. 当$i \in J_{1,3}\setminus J_{1,2,3}$时，取$w_i = y_{2,i}$；
3. 对剩余的位置，即，属于$H := E\setminus(J_{1,2} \bigcup J_{1,3} \bigcup J_{2,3})$的位置，注意到$y_1|_H$，$y_2|_H$和$y_3|_H$的任意一堆都没有相同的分量，我们可以把$H$划分成三个不交的部分，$H_1,H_2,H_3$，满

	$\overbrace{\quad}^{J_{1,2}}$	$\overbrace{\quad}^{J_{1,3}\backslash J_{1,2,3}}$	$\overbrace{\quad}^{J_{2,3}\backslash J_{1,2,3}}$	$\overbrace{\quad}^{H}$
$y_0 \in \mathcal{C}'$	$0000\cdots00$	$0000\cdots00$	$0000\cdots00$	$0000\cdots00$
$y_1 \in \mathcal{C}'$	$1111\cdots11$	$1111\cdots11$	$1111\cdots11$	$1111\cdots11$
$y_2 \in \mathcal{C}$	$1111\cdots11$	$2222\cdots22$	$2222\cdots22$	$2222\cdots22$
$y_3 \in \mathcal{C}$	$1231\cdots23$	$1111\cdots11$	$2222\cdots22$	$3333\cdots33$
$w \in \mathrm{desc}(y_1,y_2,y_3)$	$\underbrace{1111\cdots11}_{\lvert J_{1,2}\rvert\le\delta_2}$	$\underbrace{2222\cdots22}_{\lvert J_{1,3}\backslash J_{1,2,3}\rvert\le 2t+\delta_3}$	$\underbrace{1111\cdots11}_{\lvert J_{2,3}\backslash J_{1,2,3}\rvert\le 2t+\delta_3}$	$\underbrace{****\cdots**}_{\lvert H\rvert=\lvert E\rvert-\lvert J_{1,2}\bigcup J_{1,3}\bigcup J_{2,3}\rvert}$

表 3-2　当$0 \leqslant \delta < 4t$，$|J_{1,3}\backslash J_{1,2,3}| \le 2t+\delta_3$与$|J_{2,3}\backslash J_{1,2,3}| \le 2t+\delta_3$时

足$|H_1| \le 2t+\delta_3-|J_{2,3}\backslash J_{1,2,3}|$，$|H_2| \le 2t+\delta_3-|J_{1,3}\backslash J_{1,2,3}|$，以及$|H_3| = |H|-|H_1|-|H_2| \le 2t$。为了说明这种划分确实存在，我们只需注意到前两个不等式显然是有效的，这由我们对$J_{1,3}\backslash J_{1,2,3}$和$J_{2,3}\backslash J_{1,2,3}$大小的假设可以得到，第三个不等式也成立，因为我们有$|H_3| \le |E|-(|H_1|+|J_{2,3}\backslash J_{1,2,3}|)-(|H_2|+|J_{1,3}\backslash J_{1,2,3}|)$，$|E| = 6t-\delta-\delta_2-\delta_3$，并且我们可以让$|H_1|+|J_{2,3}\backslash J_{1,2,3}|$和$|H_2|+|J_{1,3}\backslash J_{1,2,3}|$尽可能得大，可以取至$2t+\delta_3$。对$w$的未定义的那些分量，我们取$w|_{H_j} = y_j|_{H_j}$，其中$j = 1,2,3$。也能验证这种取法对$w$是良定义的。

现在，对$j \in \{0,1,2,3\}$，我们来计算$I(w,y_j)$的值。注意到，$|J_{1,2}| \le \delta_2, |I_{1,0,2}|+|J_{1,2}| \le I(y_1,y_2) \le \delta$与$|I_{1,0,3}|+|I_{2,0,3}|+|J_{1,2,3}| \le I(y_3,\{y_1,y_2\}) \le \delta$，那么，我们有

$$
\begin{cases}
I(y_0,w) &= |I_1|+|I_2|+|I_3| = 3t+\delta+\delta_2+\delta_3, \\
I(y_1,w) &= |I_1|+|J_{1,2}|+|J_{2,3}\backslash J_{1,2,3}|+|H_1| \le (t+\delta)+\delta_2+(2t+\delta_3) \\
&= 3t+\delta+\delta_2+\delta_3 = I(y_0,w), \\
I(y_2,w) &= |I_{1,0,2}|+|I_2|+|J_{1,2}|+|J_{1,3}\backslash J_{1,2,3}|+|H_2| \le \delta+(t+\delta_2)+(2t+\delta_3) \\
&= 3t+\delta+\delta_2+\delta_3 = I(y_0,w), \\
I(y_3,w) &= |I_{1,0,3}|+|I_{2,0,3}|+|I_3|+|J_{1,2,3}|+|H_3| \le \delta+(t+\delta_3)+2t \\
&= 3t+\delta+\delta_3 \le I(y_0,w).
\end{cases}
$$

由于$y_0 \notin \{y_1,y_2,y_3\}$，这与$\mathcal{C}$的3-追踪性质相矛盾，正如我们所愿。

子情形2.2： 不失一般性，我们假设$|J_{2,3}\backslash J_{1,2,3}| > 2t+\delta_3$。我们可以重新定义$J'_{2,3}$使得$J'_{2,3} \subseteq J_{2,3}\backslash J_{1,2,3}$和$|J'_{2,3}| = 2t+\delta_3$成立。

现在，我们可以按如下步骤定义w_i，这里$i \in E$。表3-3标识了我们所用的记号。

1. 当$i \in J'_{2,3}$时，取$w_i = y_{1,i}$；

	$\overbrace{\quad}^{J'_{2,3}}$	$\overbrace{\quad}^{E\backslash J'_{2,3}}$
$y_0 \in \mathcal{C}'$	$\overbrace{0000\cdots00}$	$\overbrace{0000\cdots00}$
$y_1 \in \mathcal{C}'$	$1111\cdots11$	$****\cdots**$
$y_2 \in \mathcal{C}$	$2222\cdots22$	$2222\cdots22$
$y_3 \in \mathcal{C}$	$2222\cdots22$	$****\cdots**$
$w \in \mathrm{desc}(y_1, y_2, y_3)$	$\underbrace{1111\cdots11}_{\lvert J'_{2,3}\rvert = 2t+\delta_3}$	$\underbrace{2222\cdots22}_{\lvert E\backslash J'_{2,3}\rvert < 2t}$

表 3-3 当$0 \leqslant \delta < 4t$且$|J_{2,3}\backslash J_{1,2,3}| > 2t + \delta_3$时

2. 当$i \in E\backslash J'_{2,3}$，取$w_i = y_{2,i}$；

现在我们可以对$j \in \{0, 1, 2, 3\}$计算$I(w, y_j)$的值。由于$2t+\delta_3 < |J_{2,3}\backslash J_{1,2,3}| \leq I(y_3, \{y_1, y_2\}) \leq \delta < 4t$，且$|E\backslash J'_{2,3}| = \max\{4t - \delta - \delta_2 - 2\delta_3, 0\} < 2t$，我们有

$$
\begin{cases}
I(y_0, w) &= |I_1| + |I_2| + |I_3| = 3t + \delta + \delta_2 + \delta_3, \\
I(y_1, w) &\leq |I_1| + |J_{1,2}| + |J'_{2,3}| \leq (t + \delta) + \delta_2 + (2t + \delta_3) = 3t + \delta + \delta_2 + \delta_3 \\
&= I(y_0, w), \\
I(y_2, w) &= |I_{1,0,2}| + |I_2| + |E\backslash J'_{2,3}| < \delta + (t + \delta_2) + 2t = 3t + \delta + \delta_2 \\
&\leq I(y_0, w), \\
I(y_3, w) &\leq |I_{1,0,3}| + |I_{2,0,3}| + |I_3| + |E\backslash J'_{2,3}| < \delta + (t + \delta_3) + 2t = 3t + \delta + \delta_3 \\
&\leq I(y_0, w).
\end{cases}
$$

由此可知，$y_0 \notin \{y_1, y_2, y_3\}$。这与$\mathcal{C}$的3-追踪性质相矛盾。 □

定理3.4.3的证明. 记$N = 9t - r$，其中，$t \in \mathbb{Z}$且$0 \leq r \leq 8$。通过把所有码字级联向量0^r，我们可以把$\mathcal{C}$看作是一个$9t$长的追踪码。因此，我们总可以假设N能被9整除。令$d = d(\mathcal{C})$。通过重复利用引理3.4.4最多$N - d$次，我们能得到一个极小距离为N的码$\mathcal{C}'$，这个码最多有q个码字。在上面的过程中，为了得到$\mathcal{C}'$我们移除了最多$(N - d)c'q^t$个码字，因此，$|C| \leq (N - d)c'q^t + q \leq cq^t$，这里我们令$c = Nc'$。定理得证。 □

3.5 结语

在这篇论文中，我们用组合计数的方法给出了关于不同追踪方案的若干新的上界。这个方向内还有两个主要的公开问题。

第一个问题是决定$N(t)$的精确值或近似值。Erdős，Frankl和Füredi[67]曾经猜测$N^*(t) = t^2 + o(t^2)$。如果这个猜想是成立的，那么由引理3.2.8立即可以推出$N(t) = t^2 + o(t^2)$。已知界和猜想界仍然存在一个鸿沟。

第二个问题是回答问题3.4.2。防诬陷码和父代识别码都遵守一个有趣的性质是，它们都服从所谓的复合规律，该定律指出$M_{FP}(aN, q, t) < M_{FP}(N, q^a, t)$ 与$M_{IPP}(aN, q, t) < M_{IPP}(N, q^a, t)$对所有正整数$a$都成立。该性质指出一个$FPC(N; n, q, t)$ （$IPP(N; n, q^a, t)$）存在当一个$FPC(aN; n, q, t)$（$IPP(aN; n, q, t)$）存在。通过把一个aN长的码拆分成N块a元组的并，我们可以把它看成是一个N 长q^a元码，该复合规律可以通过这个观察直接得到。遗憾得是，由于定义中极小距离条件的限制，追踪码似乎并不满足该规律。这也许是追踪码的上界如此难估计的一个原因。我们证明定理3.4.3办法似乎可以被延拓去证明更多结果，当然，讨论将会更加复杂。

4 稀疏超图

4.1 简介

在本章中，我们将考虑一个由Brown，Erdős和Sós在七十年代早期提出一个稀疏超图问题。我们从一些必要的定义出发。当我们说到一个超图时，我们实际是在说一对点集和边集$\mathcal{H} = (V(\mathcal{H}), E(\mathcal{H}))$，顶点集$V(\mathcal{H})$可以被看做是一个有限集合$X$，边集$E(\mathcal{H})$则是$X$ 的一些子集的集合。我们通常记$|V(\mathcal{H})| = v(\mathcal{H})$与$|E(\mathcal{H})| = e(\mathcal{H})$。为了简便起见，我们用$\mathcal{H}$来表示边集$E(\mathcal{H})$，因此，$|\mathcal{H}|$ 也表示$|E(\mathcal{H})|$。一个超图$\mathcal{H}$是线性的，如果对不同的$A, B \in \mathcal{H}$，都有$|A \cap B| \leq 1$。此外，我们说$\mathcal{H}$是r-均衡的，如果对所有$A \in \mathcal{H}$都有$|A| = r$。

给定一个r-均衡超图的集合$\mathscr{H}$，则一个$\mathscr{H}$-free r-均衡的超图不包含$\mathscr{H}$中的任何元素。Turán数$ex_r(n, \mathscr{H})$表示一个n 个顶点的$\mathscr{H}$-free r-均衡的超图所能含有的最大边数。Turán型的问题在极值组合领域内扮演了重要的角色，见综述文章[54,76,94,124,132]。

用$\mathcal{G}_r(v, e)$标记有e条边与v个顶点的r-均衡超图的集合。一般的，我们说这些超图是由v个顶点张成的e条边。我们将着眼于一个由Brown，Erdős和Sós[39,40]提出的Turán型问题。他们引入了函数$f_r(n, v, e)$来表示n个顶点上r-均衡超图，当其不含v 个顶点张成的e 条边时，所可能含有的最大边数。这等价于说，对任意e条边$A_1, \ldots, A_e$，成立$|A_1 \cup \cdots \cup A_e| \geq v+1$。由定义知，$f_r(n, v, e) = ex_r(n, \mathcal{G}_r(v, e))$。有时，$\mathcal{G}_r(v, e)$-free超图也被称为稀疏超图[78]，这是因为它的边是稀疏的。我们只感兴趣当r, v, e时固定的，而n趋向于无穷大的情形。已知对每个$r > k \geq 2$与$e \geq 3$，都有$f_r(n, e(r-k)+k, e) = \Theta(n^k)$，上界来自于一个简单的计数，下界来自于标准的概率方法。然而，对$r > k \geq 2$与$e \geq 3$决定$f_r(n, e(r-k)+k+1, e)$的渐进表现要难多了。在文献中，有一个关于$f_r(n, e(r-k)+k+1, e)$的著名猜想。

猜想4.1.1. $n^{k-o(1)} < f_r(n, e(r-k)+k+1, e) = o(n^k)$对所有整数$r > k \geq 2$，$e \geq 3$都成立。

最简单的情形，$r = 3$，$k = 2$，$e = 3$，即(6,3)-问题，直到Ruzsa与Szemerédi[119]证明

了如下著名的(6,3)-引理才被解决：

$$n^{2-o(1)} < f_3(n,6,3) = o(n^2). \tag{4-1}$$

Erdős，Frankl，Rödl[68]把这个结果拓展为

$$n^{2-o(1)} < f_r(n,3(r-2)+2+1,3) = o(n^2) \tag{4-2}$$

对任意$r \geq 3$都成立。Alon与Shapira[14]进一步推广到

$$n^{k-o(1)} < f_r(n,3(r-k)+k+1,3) = o(n^k) \tag{4-3}$$

对任意$r > k \geq 2$都成立。文献[14]的下界意味着$n^{2-o(1)} < f_3(n,7,4)$与$n^{2-o(1)} < f_3(n,8,5)$。这两个零星的例子以及(4-3)的左边是猜想4.1.1下界成立的所有已知情形。关于猜想的上界，Sárközy与Selkow[120,121]也得到了一些结果：

$$f_r(n,4(r-k)+k+1,4) = o(n^k) \tag{4-4}$$

对$r > k \geq 3$成立，且

$$f_r(n,e(r-k)+k+\lfloor \log_2 e \rfloor, e) = o(n^k) \tag{4-5}$$

对所有$r > k \geq 2$与$e \geq 3$都成立。容易看出，(4-5)蕴含了(4-1)，(4-2)与(4-3)的左边部分，因为$\lfloor \log_2 3 \rfloor = 1$。但是，当$e \geq 4$时，与猜想值仍然有一条鸿沟。Solymosi和Solymosi[127]最近的工作证明了$f_3(n,14,10) = o(n^2)$，这个结果在$r = 3$，$k = 2$和$e = 10$的特殊情形改进了(4-5)。这也是十年来渐进界(4-5)第一个被改进的情形。

我们对函数$f_r(n,v,e)$的改进包含了以下三个方面：

- 第一，我们证明了猜想4.1.1的右边对所有固定整数$r \geq k+1 \geq e \geq 3$都成立（见下面的定理4.2.2）。我们的结论利用了著名的超图移除引理（Hypergraph Removal Lemma）。我们的结果解决了猜想的上界的所有“简单”情形，因为它蕴含了所有(4-1)，(4-2)，(4-3)，(4-4)的右边作为其特殊情形，且第一个为解决的情况就是著名的(7,4)-问题。

- 第二，我们给出了一个新的渐进界（见下面的定理4.2.3），这个界说明$f_r(n, e(r-k)+k+i+1, e) = o(n^k)$对所有满足$i \geq 0$，$r \geq k+i+1 \geq 2$，$\binom{k+i+1}{k} \geq e \geq 3$的整数$r$，$k$，$e$，$i$都成立。在很多情形下这个界都比(4-5)要好。

- 第三，我们给出了若干构造性的结果（见第4.5节中的若干个定理），说明了猜想4.1.1的左边在$r \geq 3$和$k = 2$在$e = 4, 5, 7, 8$时都成立。注意到，现存的满足猜想的构造性结果都符合$r = 3$ 或者$e = 3$。我们的构造是历史上第一个打破这个藩篱的。我们的证明依托于图论与加法数论中的两个新概念，即，彩虹圈与R_L-sum-free集。我们的出发点在于，我们首先发现不含彩虹圈的超图是稀疏超图的良好候选；其次，我们幸运地发现可以利用加法数论的工具来构造足够大的不含彩虹圈的超图。

本章剩余内容安排如下。我们将在第4.2节证明$f_r(n, e(r-k)+k+1, e) = o(n^k)$对所有整数$r \geq k+1 \geq e \geq 3$都成立。新的渐进界也将在这一节被证明。接下来的三个小节中，我们将致力于稀疏超图的构造。在第4.3节，我们将介绍彩虹圈与R_L-sum-free的概念，以及它们在构造稀疏超图时的应用。在第4.4节中，我们将解释利用sum-free集来构造稀疏超图的基本想法。第4.5节是关于$r \geq 3$，$k = 2$与$e = 4, 5, 7, 8$时$f_r(n, e(r-k)+k+1, e)$的具体构造。我们将在第4.6节做一些总结。

4.2 稀疏超图与超图移除引理

本节的主要任务是证明猜想4.1.1的右边对所有整数$r \geq k+1 \geq e \geq 3$都成立。我们仅利用了如下的超图移除引理[52]。

引理4.2.1 (Hypergraph removal lemma). *对任何r-均衡超图G与任何$\epsilon > 0$，都存在$\delta > 0$使得任何n个顶点的r-均衡超图，若其包含G的最多$\delta n^{v(G)}$份拷贝，则通过移除最多ϵn^r条边，可以让它变为是不含有G的（G-free）。*

通过超图移除引理，容易推出如下事实：对任何给定的常数$\epsilon > 0$，都存在某个$\delta(\epsilon) > 0$，使得如果要使一个n个顶点的r-均衡超图$\mathcal{H}$变为G-free需删去至少ϵn^r条边，那么$\mathcal{H}$一定包含G的至少$\delta(\epsilon) n^{v(G)}$份拷贝。

定理4.2.2. *$f_r(n, e(r-k)+k+1, e) = o(n^k)$对所有整数$r \geq k+1 \geq e \geq 3$都成立。*

证明. 对满足定理条件的r,k,e，令$\mathcal{H}$是一个$\mathcal{G}_r(e(r-k)+k+1,e)$-free的$r$-均衡超图。假设对某个$\epsilon>0$有$|\mathcal{H}|\geq\epsilon n^k$。

首先，我们声明对任意$A_0\in\mathcal{H}$，只存在$\mathcal{H}\setminus\{A_0\}$的最多$e-2$条边，使得它们交$A_0$于至少$k$个顶点。如若不然，存在$e-1$条边$A_1,\ldots,A_{e-1}$使得$|A_0\cap A_i|\geq k$对每个$1\leq i\leq e-1$都成立。那么我们有$|\cup_{i=0}^{e-1}A_i|\leq er-(e-1)k<er-(e-1)k+1$，这与事实$\mathcal{H}$是$\mathcal{G}_r(e(r-k)+k+1,e)$-free相矛盾。因此，存在一个超图$\mathcal{H}'\subseteq\mathcal{H}$，$|\mathcal{H}'|\geq\frac{\epsilon}{e-1}n^k$满足对所有不同的$A,B\in\mathcal{H}'$，都有$|A\cap B|\leq k-1$。

接下来，我们将构造一个辅助的k-均衡超图$\mathcal{H}^*$来帮助我们证明该定理。顶点集$V(\mathcal{H}^*)$满足$V(\mathcal{H}^*)\subseteq V(\mathcal{H}')\subseteq V(\mathcal{H})$。边集$E(\mathcal{H}^*)$是按如下方式构成的：对每条$r$-均衡的边$A\in\mathcal{H}'$，我们构造一个超图$K_r^k(A)$，它表示顶点集$A$上的$k$-均衡完全超图。$K_r^k(A)$是由取$A$的所有$k$元子集而构成的。容易看出，$A\in\mathcal{H}'$与$K_r^k(A)\subseteq\mathcal{H}^*$之间是有一一对应的。$E(\mathcal{H}^*)$是由全部$K_r^k(A)$的所有边之并所形成的，即$E(\mathcal{H}^*)=\cup_{A\in\mathcal{H}'}K_r^k(A)$。一个重要的观察是，对任意两条边$A,B\in\mathcal{H}'$，$k$-均衡超图$K_r^k(A)$与$K_r^k(B)$是不含公共边的。这个观察来自于简单的事实，对$A,B\in\mathcal{H}'$有$|A\cap B|\leq k-1$。

总而言之，我们构造了一个k-均衡超图$\mathcal{H}^*$，它包含K_r^k的至少$|\mathcal{H}'|\geq\frac{\epsilon}{e-1}n^k$个边不交的拷贝。因此需要删去至少$\frac{\epsilon}{e-1}n^k$条边才能使得$\mathcal{H}^*$是$K_r^k$-free的。由超图移除引理可知，$\mathcal{H}^*$含有$K_r^k$的至少$\delta_\epsilon n^r$份拷贝。现在，让我们估计如下$K_r^k$的数量：它含有两条来自于同一个$A\in\mathcal{H}'$的边。首先，注意到$K_r^k$的两条边决定了它至少$k+1$个顶点，且这样的$A\in\mathcal{H}'$有$\mathcal{O}(n^k)$种选择。其次，待定$K_r^k$的剩下的$r-k-1$个顶点有最多$n^{r-k-1}$种选择。因此，这种$K_r^k$的数量至多为$\mathcal{O}(n^k)\cdot n^{r-k-1}=\mathcal{O}(n^{r-1})$，当$n$足够大时将小于$\delta(\epsilon)n^r$（其中$\delta(\epsilon)$是由超图移除引理所保证的常数）。

根据以上的讨论，我们可以总结到，总是存在一个$K_r^{k*}\subseteq\mathcal{H}^*$，它的$\binom{r}{k}$条$k$-均衡边来自于$\mathcal{H}'$的$\binom{r}{k}$条不同的$r$-均衡边。特别的，对$r\geq k+1\geq e$，我们可以选择一个$K_{k+1}^k\subseteq K_r^{k*}$，并取这样一个$K_{k+1}^k$的$e$条边，记作$B_1,\ldots,B_e$。考虑$\mathcal{H}'$中对应的$e$条边$A_1,\ldots,A_e$，满足$B_i\subseteq A_i$，$1\leq i\leq e$。那么，$B_1,\ldots,B_e$是由$k+1$个顶点所张成的$e$条边，所以我们可以推出$|A_1\cup\cdots\cup A_e|\leq re-(ek-(k+1))=e(r-k)+k+1$，这与事实$\mathcal{H}'$是$\mathcal{G}_r(e(r-k)+k+1,e)$-free的相矛盾。因此，定理由反证法得证。 □

我们对定理4.2.2实际上蕴含了如下更一般的结果。

定理4.2.3. 对满足$i\geq0$，$r\geq k+i+1\geq2$，$\binom{k+i+1}{k}\geq e\geq3$的整数$r,k,e,i$，我们有$f_r(n,e(r-k)+k+i+1,e)=o(n^k)$。

证明. 令$\mathcal{H}$是一个$\mathcal{G}_r(e(r-k)+k+i+1,e)$-free的$r$-均衡超图。假设$|\mathcal{H}|\geq \epsilon n^k$对某个常数$c$成立。我们跟随定理4.2.2的证明思路。正如证明的最后一步，可以选择一个$K^k_{k+i+1}\subseteq K^{k*}_r$ 与它的e条边，记作$B_1,\ldots,B_e$。考虑$\mathcal{H}'$ 中对应的e条边$A_1,\ldots,A_e$，满足$B_i\subseteq A_i$，$1\leq i\leq e$。那么，$B_1,\ldots,B_e$是由$k+i+1$个顶点张成的e条边，因此我们可以推出$|A_1\cup\cdots\cup A_e|\leq re-(ek-(k+i+1))=e(r-k)+k+i+1$，这与$\mathcal{H}'$是$\mathcal{G}_r(e(r-k)+k+i+1,e)$-free的相矛盾。 □

不妨让我们比较定理4.2.2与定理4.2.3，以及之前的结果。可以验证定理4.2.2包含(4-4)以及(4-3)的右边作为其特殊情形。猜想中第一个未能覆盖的情形是$r=3,\ k=2,e=4$，这也是熟知的(7,4)-问题。为了解决更困难的情形，例如，(7,4)-问题，我们有两种可能的方法，一种是利用比超图移除引理更强的工具，另一种是建立一个更好的禁止构型模型。如果我们对比定理4.2.3与(4-5)，并不难看出当r,e,k,i满足$r\geq k+i+1\geq 2$，$\binom{k+i+1}{k}\geq e$与$\lfloor\log_2 e\rfloor\geq i+2$时，我们的结果更好。

4.3 禁止构型与sum-free集

我们将归纳一些稀疏超图中肯定不能出现的基本结构。这些基本结构被称为是禁止构型。当构造不含小的禁止构型的超图时，加法数论是一类重要的工具。在本节中，我们将收集一些必要的知识。

4.3.1 彩虹圈

我们从彩虹圈的定义开始，它是作者在研究完美哈希族时引入的。一个r-均衡超图$\mathcal{H}$是r-部的如果它的顶点集$V(\mathcal{H})$可以用r种颜色染色，使得$\mathcal{H}$ 中没有边包含两种相同颜色的点。在这样一个染色中，颜色集$V(\mathcal{H})$，即，相同颜色的顶点集，被称为是$\mathcal{H}$的部，我们用$V_1,\ldots,V_r$来表示$V(\mathcal{H})$的r种颜色集。那么，$V(\mathcal{H})$是所有V_i的不交并，且对每个$1\leq i\leq r$都有$A\in\mathcal{H}$，$|A\cap V_i|=1$。

我们也将用到Berge[23,24]引进的超图圈的定义。对$k\geq 2$，超图$\mathcal{H}$中的一个圈是顶点与边的交错列，$v_1,A_1,v_2,A_2,\ldots,v_k,A_k,v_1$，且有如下性质

(a) $v_1,v_2,\ldots,v_k$是$\mathcal{H}$的不同顶点，

(b) $A_1,A_2,\ldots,A_k$是$\mathcal{H}$的不同边，

(c) 对$1\leq i\leq k-1$和$v_k,v_1\in E_k$有$v_i,v_{i+1}\in A_i$。

可以验证，对$2 \leq i \leq k$有$A_{i-1} \cap A_i = \{v_i\}$，且$A_k \cap A_1 = \{v_1\}$。

接下来我们将给出彩虹圈的定义。令$\mathcal{H}$是一个线性的r-均衡超图。一个k-圈

$$v_1, A_1, v_2, A_2, \ldots, v_k, A_k, v_1$$

被称为是彩虹k- 圈，如果$v_1, \ldots, v_k$落在$V(\mathcal{H})$的k个不同的部中。对r-均衡超图来说，一个彩虹k-圈存在仅当$k \leq r$。本文的一个创新点就是我们发现对某些参数，不含彩虹圈的超图也是稀疏超图。

我们最感兴趣的是长度为三或四的彩虹圈。一个彩虹3-圈有形式$v_1, A_1, v_2, A_2, v_3, A_3, v_1$。从几何上来说，我们可以把彩虹3-圈看成是一个三角形，它的三个顶点落在三个不同的顶点集中。

引理4.3.1. *设$\mathcal{H}$是一个线性的r-部r-均衡超图。那么，$\mathcal{H}$是$\mathcal{G}_r(3r-3, 3)$-free的当且仅当它不包含彩虹3-圈。*

证明. 只需证明若三条边$A_1, A_2, A_3 \in \mathcal{H}$满足$|A_1 \cup A_2 \cup A_3| \leq 3r-3$，那么它们肯定会形成一个彩虹3-圈。首先，注意到$\mathcal{H}$ 是一个线性超图，由鸽笼原理可知，

$$\begin{aligned}|A_1 \cup A_2 \cup A_3| =& |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_3 \cap A_1| + |A_1 \cap A_2 \cap A_3| \\ \geq& 3r - 3 + |A_1 \cap A_2 \cap A_3|.\end{aligned}$$

从而，我们可以推出$|A_1 \cup A_2 \cup A_3| = 3r-3$，$|A_1 \cap A_2| = |A_2 \cap A_3| = |A_3 \cap A_1| = 1$且$A_1 \cap A_2 \cap A_3 = \emptyset$。不失一般性，假设$A_1 \cap A_2 = \{a\}$，$A_2 \cap A_3 = \{b\}$且$A_3 \cap A_1 = \{c\}$。由于$a, b, c$各不相同，它们必属于三个不同的顶点集。令$a \in V_1$，$b \in V_2$与$c \in V_3$。那么我们将得到一个彩虹3-圈$b, A_1, a, A_2, c, A_3, b$，它可以用表4-1表示出来。

	A_1	A_2	A_3
V_1	a	a	
V_2		b	b
V_3	c		c

表 4-1　彩虹3-圈

□

若一个超图$G=\{A_1,A_2,A_3,A_4\}$形成一个彩虹4-圈$d,A_1,a,A_2,b,A_3,c,A_4,d$，就像上面的引理一样，$G$可以表示为表4-2。

	A_1	A_2	A_3	A_4
V_1	a	a		
V_2		b	b	
V_3			c	c
V_4	d			d

表 4-2　彩虹4-圈

4.3.2　Sum-free集

考虑一个线性方程$\sum_{i=1}^{s}a_im_i=0$，有整系数$a_1,\ldots,a_s$，未知数x_i。如果有$\sum_{i=1}^{s}a_i=0$，我们说这个方程是齐次的。我们说集合$M\subseteq[n]$不含上述方程的非平凡解，如果$m_i\in M$且$\sum_{i=1}^{s}a_im_i=0$，则能推出所有m_i相等。这里关于非平凡解的定义是Ruzsa[118]原始定义的一个简化版本。给定一个集合$R=\{b_1,\ldots,b_r\}$，这是r个不同的非负整数。一个集合M被称为是R_L-sum-free的当且仅当对任何l满足$3\leq l\leq L\leq r$与任何l-子集$S=\{b_{j_1},b_{j_2},\ldots,b_{j_l}\}\subseteq R$，方程

$$(b_{j_2}-b_{j_1})m_1+(b_{j_3}-b_{j_2})m_2+\cdots+(b_{j_l}-b_{j_{l-1}})m_{l-1}+(b_{j_1}-b_{j_l})m_l=0$$

在M中除了平凡解$m_1=m_2=\cdots=m_l$之外都无解。

注记4.3.2. *R_L-sum-free集的概念是传统sum-free集的推广，传统sum-free集已经被广泛的研究过了（见文献[118]）。作者在研究完美哈希族时曾经考虑了$r=4$和$L=4$时的情况。*

引理4.3.3. *令$0<a<1$为一个给定的常数。则$2^{\mathcal{O}(\log^a n)}=o(n^\epsilon)$对所有小常数$\epsilon>0$都成立。*

证明. 该引理由如下直接计算可得：

$$\lim_{n\to+\infty}\frac{2^{\mathcal{O}(\log^a n)}}{n^\epsilon}=\lim_{n\to+\infty}\frac{2^{\mathcal{O}(\log^a n)}}{2^{\epsilon\log n}}=\lim_{n\to+\infty}2^{\mathcal{O}(\log^a n)-\epsilon\log n}=2^{-\infty}=0.$$

□

引理4.3.4. 令$l \geq 2$为一个给定的整数。令$a_1, \ldots, a_l \in [n]$为l个正整数（并不是固定的，可能会是n的函数）。那么存在一个集合$M \subseteq [n]$，$|M| \geq \frac{n}{2^{\mathcal{O}(\sqrt{\log n \log \sum_{i=1}^{l} a_l})}}$，不含下述方程的非平凡解

$$a_1 m_1 + \cdots + a_l m_l = (a_1 + \cdots + a_l) m_{l+1}.$$

证明. 该证明是Behrend[21]构造的一个直接应用，见文献[10]中引理3.2的第一部分。 □

引理4.3.5. 令$a_1, a_2, a_3, a_4 \in [n]$为四个不同的正整数（并不是固定的，可能会是$n$的函数），满足

(1) $a_1 < a_2 < a_3 < a_4$，

(2) $a_1 + a_4 = a_2 + a_3$，

(3) 对任意的小常数$\epsilon > 0$，都有$a_1 = o(a_3^{\epsilon})$，$a_2 = o(a_3^{\epsilon})$，$a_4 - a_3 = o(a_3^{\epsilon})$与$a_4 = o(n^{\epsilon})$，

(4) 存在两个常数$0 < a, b < 1$，使得$\log a_2 = \mathcal{O}((\log a_3)^a)$且$\log a_3 = \mathcal{O}((\log n)^b)$，

则存一个集合$M \subseteq [n]$，$|M| \geq \frac{n}{2^{\mathcal{O}((\log n)^{1+\frac{b(a-1)}{2}})}} > n^{1-o(1)}$，不含如下方程的非平凡解

$$a_1 x + a_4 y = a_2 u + a_3 v.$$

注记4.3.6. 注意到由于$a < 1$且$b < 1$，所以我们有$1 + \frac{b(a-1)}{2} < 1$。因此由引理*4.3.3*可知$2^{\mathcal{O}((\log n)^{1+\frac{b(a-1)}{2}})} = n^{o(1)}$。

证明. 令$\mathcal{B} \subseteq [0, \frac{a_3+1}{a_2})$为一个整数集合，且不含下面辅助方程的非平凡解：

$$a_1 x + (a_4 - a_3 - 1) y + v = a_2 u. \tag{4-6}$$

注意到，由引理的第二个条件可知，$a_1 + a_4 - a_3 - 1 + 1 = a_2$。由引理4.3.4，存在$\mathcal{B}$使得

$$|\mathcal{B}| \geq \frac{\frac{a_3+1}{a_2}}{2^{\mathcal{O}(\sqrt{\log \frac{a_3+1}{a_2} \log a_2})}} > \frac{a_3^{1-o(1)}}{2^{\mathcal{O}((\log a_3)^{\frac{1+a}{2}})}} > a_3^{1-o(1)},$$

其中最后一个不等式由引理4.3.3推出。令M为包含如下整数的集合：如果把该整数写成$a_3 + 1$进展开的形式，基底中的元素仅仅包含那些属于$\mathcal{B}$中的。那么我们有

$$M \geq |\mathcal{B}|^{\lfloor \log_{a_3+1} n \rfloor} = \Omega(|\mathcal{B}|^{\frac{\log n}{\log(a_3+1)}}) = \Omega(n^{\frac{\log |\mathcal{B}|}{\log(a_3+1)}}) > n^{1-o(1)}.$$

我们声明方程$a_1x+(a_4-a_3-1)y+v=a_2u$在M内没有非平凡解。

如若不然，x,y,u,v形成一个上述方程的非平凡解。让我们把它们按a_3+1进制展开，使得$x=\sum x_i(a_3+1)^i$，$y=\sum y_i(a_3+1)^i$，$u=\sum u_i(a_3+1)^i$与$v=\sum v_i(a_3+1)^i$。因为x,y,u,v构成一个非平凡解，则必存在某个整数i使得x_i,y_i,u_i,v_i不全相等。令j为满足这个条件的最小i。那么，我们有

$$a_1x_j(a_3+1)^j+a_4y_j(a_3+1)^j\equiv a_2u_j(a_3+1)^j+a_3v_j(a_3+1)^j \pmod{(a_3+1)^{j+1}}.$$

这意味着

$$a_1x_j+(a_4-a_3-1)y_j\equiv a_2u_j-v_j \pmod{a_3+1},$$

即

$$a_1x_j+(a_4-a_3-1)y_j+v_j\equiv a_2u_j \pmod{a_3+1}.$$

由我们的构造可知，$x_j,y_j,u_j,v_j<\frac{a_3+1}{a_2}$，上面的同余关系作为下面的等式必也成立

$$a_1x_j+(a_4-a_3-1)y_j+v_j=a_2u_j.$$

这是一个矛盾，因为x_j,y_j,u_j,v_j是不全相等的，且$\mathcal{B}$不含方程(4-6)的非平凡解。

仔细计算$n^{\frac{\log|\mathcal{B}|}{\log(a_3+1)}}$后可得我们的引理。 □

引理4.3.7. 令$\sum_{i=1}^s a_ix_i=0$为一个线性方程。若$M\subseteq[n]$不含其非平凡解，则这对任何平移$(M+b)\cap[n]$，$b\in\mathbb{Z}$，也成立；其中$M+b:=\{m+b:m\in M\}$。

证明. 如果不然，存在某个$b\in\mathbb{Z}$使得$M+b$包含方程的非平凡解。记这组解为$\{b_1,\dots,b_s\}$，其中$b_i=m_i+b$，$1\le i\le s$。那么$m_1,\dots,m_s$是不全相等的。我们有

$$0=\sum_{i=1}^s a_ib_i=\sum_{i=1}^s a_i(m_i+b)=\sum_{i=1}^s a_im_i+b\sum_{i=1}^s a_i=\sum_{i=1}^s a_im_i.$$

因此，$\{m_1,\dots,m_s\}\subseteq M$也是方程的一个非平凡解，这与引理的假设是矛盾的。 □

引理4.3.8. 令$0<a<1$为一个给定的常数，t为一个给定的正整数。令$\sum_{i=1}^s a_{ij}x_i=0$，$1\le j\le t$，为t个齐次线性方程。如果对每个整数$1\le j\le t$，都存在一个集合$M_j\subseteq[n]$，$|M_j|\ge\frac{n}{2^{\mathcal{O}(\log^a n)}}$不含方程$\sum_{i=1}^s a_{ij}x_i=0$的非平凡解。那么，存在一个集合$M\subseteq[n]$，$|M|\ge\frac{n}{2^{\mathcal{O}(\log^a n)}}$不含任意一个方程的非平凡解。

证明. 随机、平均且独立地选取$t-1$个整数$\mu_2,\ldots,\mu_t \in \{-n,\ldots,n\}$。则由引理4.3.7可知，$M = M_1 \cap (M_2+\mu_2) \cap \cdots \cap (M_t+\mu+t)$对$t$个方程都不含非平凡解。现在，让我们计算任何一个$m \in M_1$属于上述交集的概率。对每个$2 \le j \le t$，我们有$-n \le m - m_j \le n$，$m_j \in M_j$。因此可以推出

$$Pr[m \in (M_i+\mu_i)] = Pr[\exists\, m_i \in M_i,\ s.t.\ \mu_i = m - m_i] = \frac{|M_i|}{2n} = \Omega(2^{-\mathcal{O}(\log^a n)}).$$

所以，成立

$$Pr[m \in (M_2+\mu_2) \cap \cdots \cap (M_t+\mu+t)] = \Omega(2^{-\mathcal{O}(\log^a n)})^t = \Omega(2^{-\mathcal{O}(\log^a n)}),$$

这意味着$|M|$的期望至少是$E[|M|] = |M_1|\Omega(2^{-\mathcal{O}(\log^a n)}) = \frac{n}{2^{\mathcal{O}(\log^a n)}}$。 □

下面的定理是本节的主要内容。

定理4.3.9. *对每个整数$r \ge 4$，都存在一个r-子集$R \subseteq [n]$和一个关于R的R_4-sum-free集$M \subseteq [n]$，满足$|M| > n^{1-o(1)}$。*

证明. 为了构造所期望的sum-free集，我们取$R = \{b_1,\ldots,b_r\}$，其中，$b_1 = 2^{(\log n)^{\frac{1}{2^r}}}$，$b_{i+1} = 2^{(\log b_i)^2}$，$1 \le i \le r-1$。那么$\log b_{i+1} = (\log b_i)^2$，且不难计算$\log b_i = (\log b_1)^{2^{i-1}}$和$b_i = 2^{(\log b_1)^{2^{i-1}}} = 2^{(\log n)^{\frac{1}{2^{r-i+1}}}}$ 对$1 \le i \le r$都成立。由引理4.3.3可知，$b_i = o(b_{i+1}^{\epsilon})$对$1 \le i \le r-1$与任意给定的正常数$\epsilon > 0$都成立，这是因为$b_i = 2^{\sqrt{\log b_{i+1}}}$。此外，$b_r = 2^{\sqrt{\log n}} = o(n^{\epsilon})$。

对$3 \le l \le 4$与任意l-子集$S = \{b_{j_1}, b_{j_2}, \ldots, b_{j_l}\} \subseteq R$，让我们计算如下形式的方程的不等价类个数：

$$(b_{j_2} - b_{j_1})m_1 + (b_{j_3} - b_{j_2})m_2 + \cdots + (b_{j_l} - b_{j_{l-1}})m_{l-1} + (b_{j_1} - b_{j_l})m_l = 0. \tag{4-7}$$

情形1： 若$l = 3$，则考虑方程

$$(b_{j_2} - b_{j_1})m_1 + (b_{j_3} - b_{j_2})m_2 + (b_{j_1} - b_{j_3})m_3 = 0.$$

由对称性可知，我们总能假设$b_{j_1} < b_{j_2} < b_{j_3}$。因此方程可以被转化为如下等价的形式

$$(b_{j_2} - b_{j_1})m_1 + (b_{j_3} - b_{j_2})m_2 = (b_{j_3} - b_{j_1})m_3. \tag{4-8}$$

我们把这个方程称为是Type 1的，当$l = 3$时，所有方程都是Type 1的。Type 1方程的总数为$\binom{r}{3}$。

情形2： 若$l=4$，给定任意四个元素$b_{j_1},b_{j_2},b_{j_3},b_{j_4}\in R$。假设$b_{j_1}<b_{j_2}<b_{j_3}<b_{j_4}$，则通过列举所有的可能组合，不难看出所有的方程都等价于下面的三种类型之一

$$(b_{j_2}-b_{j_1})m_1+(b_{j_3}-b_{j_2})m_2+(b_{j_4}-b_{j_3})m_3=(b_{j_4}-b_{j_1})m_4, \tag{4-9}$$

$$(b_{j_2}-b_{j_1})m_1+(b_{j_4}-b_{j_2})m_2=(b_{j_4}-b_{j_3})m_3+(b_{j_3}-b_{j_1})m_4, \tag{4-10}$$

$$(b_{j_4}-b_{j_1})m_1+(b_{j_3}-b_{j_2})m_2=(b_{j_3}-b_{j_1})m_3+(b_{j_4}-b_{j_2})m_4. \tag{4-11}$$

我们把上面三个方程分别称为Type 2，Type 3和Type 4。每种类型是由$\binom{r}{4}$个不同的方程组成的。

我们可以总结到所有形式为(4-7)的方程含有最多$t:=\binom{r}{3}+3\binom{r}{4}$种不同的可能构型，它们分别被记作$Eq_1,\dots,Eq_t$。下面的步骤可以被归纳如下：我们首先利用引理4.3.4与引理4.3.5来构造t个足够大的集合$M_1,\dots,M_t\subseteq[n]$使得对$1\le i\le t$集合$M_i$都不含方程$Eq_i$的非平凡解。然后我们再利用引理4.3.8来构造一个我们所期望的集合M，它不含$Eq_1,\dots,Eq_t$中任意一个方程的非平凡解。细节如下。

由引理4.3.4可知，对每个Type 1或者Type 2的方程，都存在一个集合$M\subseteq[n]$，

$$|M|\ge\frac{n}{2^{\mathcal{O}(\sqrt{\log n\log b_r})}}=\frac{n}{2^{\mathcal{O}((\log n)^{\frac{3}{4}})}}$$

使得其不含有非平凡解。现在我们只需考虑Type 3与Type 4的方程。比较方程(4-10) 与引理4.3.5。我们可以选取$a_1:=b_{j_2}-b_{j_1}$，$a_2:=b_{j_3}-b_{j_1}$，$a_3:=b_{j_4}-b_{j_3}$与$a_4:=b_{j_4}-b_{j_2}$。由R的定义可知，容易验证a_1,a_2,a_3,a_4满足引理4.3.5的四个条件。回想引理4.3.5中a与b的定义，容易验证$a\le\frac{1}{2}$与$b\ge\frac{1}{2^{r-3}}$都成立，当$j_4=j_3+1$与$j_4=3$时等号成立。因此，我们有对任何Type 3与Type 4的方程，都存在一个集合$M\subseteq[n]$，

$$|M|\ge\frac{n}{2^{\mathcal{O}((\log n)^{1+\frac{b(a-1)}{2}})}}\ge\frac{n}{2^{\mathcal{O}((\log n)^{1+\frac{1/2^{r-3}(1/2-1)}{2}})}}=\frac{n}{2^{\mathcal{O}((\log n)^{1-\frac{1}{2^{r-1}}})}}$$

不含其非平凡解。

总而言之，如果我们记$c=\max\{\frac{3}{4},1-\frac{1}{2^{r-1}}\}$，则由上面的讨论可知，对$1\le i\le t$，存在一个集合$M_i\subseteq[n]$，$|M_i|\ge\frac{n}{2^{\mathcal{O}((\log n)^a)}}$，不含$Eq_i$的非平凡解。由引理4.3.8，我们可以推知存在一个集合$M\subseteq[n]$，$|M|\ge\frac{n}{2^{\mathcal{O}((\log n)^a)}}$不含$t$个方程$Eq_1,\dots,Eq_t$中任何一个的非平凡解。这相当于是说$M\subseteq[n]$是一个$R_4$-sum-free集，其中$R=\{b_1,\dots,b_r\}$；其大小$|M|>n^{1-o(1)}$由引理4.3.3保证。 □

定理4.3.9的证明蕴含了如下较弱一点的结论。

定理4.3.10. *对每个整数$r \geq 3$，都存在一个r元集合$R \subseteq [n]$与一个R_3-sum-free集$M \subseteq [n]$，满足$|M| > n^{1-o(1)}$。*

4.4 利用sum-free集来构造超图

广为人知的是加法数论的工具可以被用来构造满足一些图兰性质的超图，例如文献[10,78,119]。给定一个正整数r，一个合适的sum-free集合$M \subseteq [n]$，我们可以按如下方式构造一个r-均衡r-部超图。顶点集是由$V(\mathcal{H}) = V_1 \times \cdots \times V_r$所构成的，其中，$V_1, \ldots, V_r$是待定的正整数集，满足对每个$1 \leq i \leq r$都有$|V_i| = \mathcal{O}(n^{1+o(1)})$。边集被定义为

$$\mathcal{H} = \{A(y,m) : A(y,m) = (y + b_1 m, y + b_2 m, \ldots, y + b_r m),\ y \in [n], m \in M\},$$

这里$A(y,m)$是一个有序的r-元组，使得对每个$1 \leq j \leq r$都有$y + b_j m \in V_i$。$\mathcal{B} := \{b_1, b_2, \ldots, b_r\} \subseteq [n]$ 是一个给定的r 元集合，它对$\mathcal{H}$ 的每条边都是一样的，我们称$\mathcal{B}$为超图$\mathcal{H}_M$的斜率集。

注记4.4.1. *容易验证$|\mathcal{H}| = n|M|$，且$|\mathcal{H}| > n^{2-o(1)}$，如果我们能构造一个足够大的sum-free集$M$满足$|M| > n^{1-o(1)}$。*

我们立即可以得到下面的引理。

引理4.4.2. *按照上面的方式构造的超图永远都是线性的。*

证明. 假设$|A(y,m) \cap A(y',m')| \geq 2$，则存在$0 \leq i, j \leq r-1$与$i \neq j$使得

$$\begin{cases} y + b_i m = y' + b_i m', \\ y + b_j m = y' + b_j m'. \end{cases}$$

可以推出$y - y' = b_i(m' - m) = b_j(m' - m)$，这意味着$m = m'$与$y = y'$（注意到$b_i - b_j \neq 0$）。

□

定理4.4.3. *若M是一个R_L-sum-free集，满足$3 \leq L \leq r$，那么按照上述方式构造的超图$\mathcal{H}_M$是一个r-均衡r-部的线性超图，且不包含长度小于$L+1$的彩虹圈。*

证明. 首先，$\mathcal{H}_M$显然是一个r-均衡r-部的超图，它的线性性也由引理5.5.2所保障了。根据我们的定义可知，一个超圈的长度至少为3。那么我们只需证明$\mathcal{H}_M$不含有长度满足$3 \leq l \leq L$的l-圈。

如若不然，存在一个彩虹l-圈，且$3 \leq l \leq L$，不失一般性，此圈可以被记作为如下的形式：$v_1, A(y_1, m_1), v_2, A(y_2, m_2), \ldots, v_l, A(y_l, m_l), v_1$，其中，对$1 \leq i \leq l$和$1 \leq j_i \leq r$有$v_i \in V_{j_i}$。此外，根据彩虹圈的定义，对$i_1 \neq i_2$我们有$j_{i_1} \neq j_{i_2}$。不难验证$A(y_1, m_1) \cap A(y_2, m_2) \cap V_{j_2} = \{v_2\}, \ldots, A(y_{l-1}, m_{l-1}) \cap A(y_l, m_l) \cap V_{j_l} = \{v_l\}, A(y_l, m_l) \cap A(y_1, m_1) \cap V_{j_1} = \{v_1\}$。另外，对$1 \leq j \leq r$，由我们的构造可知$A(y, m) \cap V_j = \{y + b_j m\}$，则如下$l$个方程同时成立

$$\begin{cases} y_1 + b_{j_2} m_1 = y_2 + b_{j_2} m_2, \\ y_2 + b_{j_3} m_2 = y_3 + b_{j_3} m_3, \\ \vdots \\ y_{l-1} + b_{j_l} m_{l-1} = y_l + b_{j_l} m_l, \\ y_l + b_{j_1} m_l = y_1 + b_{j_1} m_1. \end{cases}$$

根据一个简单的消去法，我们可以推知

$$(b_{j_2} - b_{j_1}) m_1 + (b_{j_3} - b_{j_2}) m_2 + \cdots + (b_{j_l} - b_{j_{l-1}}) m_{l-1} + (b_{j_1} - b_{j_l}) m_k = 0,$$

这意味着$m_1 = \cdots = m_l$，这是因为M是R_L-sum-free的。因此，$y_1 = \cdots = y_l$且$A(y_1, m_1) = \cdots = A(y_l, m_l)$，这显然是一个矛盾。因此，我们可以总结到$\mathcal{H}_M$不含有长度小于$L+1$的彩虹圈。 □

推论4.4.4. *对任何$r \geq 4$，都存在一个r-均衡r-部超图$\mathcal{H}$满足$|\mathcal{H}| > |v(\mathcal{H})|^{2-o(1)}$，且不包含任何长度为3或4的彩虹圈。*

证明. 这个推论是定理4.3.9与定理4.4.3的直接结论。 □

4.5　稀疏超图的构造

我们将利用上节所展示的结论来构造我们所期望的稀疏超图。我们首先证明$\mathcal{G}_r(4r-5, 4)$-free与$\mathcal{G}_r(5r-7, 5)$-free超图都可以由$\mathcal{G}_r(3r-3, 3)$-free超图得到。然而，$e = 6$是一个特殊的情形，$\mathcal{G}_r(6r-9, 6)$-free性质并不能由$\mathcal{G}_r(3r-3, 3)$-free性质推出。实际上，对$r \geq 3$，$e = 6$和$k = 2$我们并不能构造出满足猜想下界的$\mathcal{G}_r(6r-9, 6)$-free超图。但令人惊奇地

是，当$e=7$与$e=8$时，我们可以构造足够大的$\mathcal{G}_r(7r-11,7)$-free与$\mathcal{G}_r(8r-13,8)$-free超图，对$r\geq 3$，$k=2$和$e=7,8$，它都可以符合猜想的下界。下面我们从一些对我们的证明非常有帮助的引理开始。

引理4.5.1. 令$e\geq 3$是一个正整数，$\mathcal{H}$是一个r-均衡r-部的线性超图。假设$\mathcal{H}$是$\mathcal{G}_r(3r-3,3)$-*free*与$\mathcal{G}_r(e(r-2)+3,e)$-*free* 的，但它不是$\mathcal{G}_r((e+1)(r-2)+3,e+1)$-*free*的。则对任何$e+1$条不同的边$A_1,\ldots,A_{e+1}\in\mathcal{H}$ 满足$|\cup_{i=1}^{e+1}A_i|\leq(e+1)(r-2)+3$，且对任何$A_i\in\{A_1,\ldots,A_{e+1}\}$，都存在三条不同的边$A_{i_1},A_{i_2},A_{i_3}\in\{A_1,\ldots,A_{e+1}\}\setminus\{A_i\}$，使得

(1) A_i每个A_{i_1},A_{i_2}和A_{i_3}于不同的顶点，即，$|A_i\cap(A_{i_1}\cup A_{i_2}\cup A_{i_3})|=3$，

(2) A_{i_1},A_{i_2}和A_{i_3}是两两不交的，

(3) $|A_{i_1}\cup A_{i_2}\cup A_{i_3}\cup A_i|=4r-3$。

证明. 令$A_1,\ldots,A_{e+1}\in\mathcal{H}$为$e+1$条不同的边，满足$|\cup_{i=1}^{e+1}A_i|\leq(e+1)(r-2)+3$。由$\mathcal{H}$的$\mathcal{G}_r(e(r-2)+3,e)$-free性质可知，我们有$|\cup_{i=1}^{e}A_i|\geq e(r-2)+4$。记$X=\cup_{i=1}^{e}A_i$，则有

$$(e+1)(r-2)+3\geq|X\cup A_{e+1}|=|X|+|A_{e+1}|-|X\cap A_{e+1}|\geq e(r-2)+4+r-|X\cap A_{e+1}|.$$

根据一个简单的消去，可以推知$|A_{e+1}\cap(\cup_{i=1}^{e}A_i)|\geq 3$。由于$\mathcal{H}$是一个线性超图，这个交错限制意味着存在三条不同的边$A_{i_1},A_{i_2},A_{i_3}\in\{A_1,\ldots,A_e\}$使得$A_{e+1}$交它们中的每一个于不同的顶点。我们总可以假设$i_1=1,i_2=2,i_3=3$，且$A_1\cap A_{e+1}=\{a\}$，$A_2\cap A_{e+1}=\{b\}$，$A_3\cap A_{e+1}=\{c\}$。注意到$\mathcal{H}$也是$r$-部的，$a,b,c$必须属于$\mathcal{H}$ 的不同顶点集中。我们分别设$a\in V_1$，$b\in V_2$和$c\in V_3$。A_1,A_2,A_3与A_{e+1}的相交关系可以用如下表4-3表示出来。

	A_1	A_2	A_3	A_e
V_1	a			a
V_2		b		b
V_3			c	c

表 4-3　引理4.5.1的图示

我们声称A_1,A_2与A_3是两两不交的。如果$A_1\cap A_2=\{d\}\neq\emptyset$。则由$\mathcal{H}$的线性性，容易看出$d\notin\{a,b,c\}$，这意味着$A_1\cap A_{e+1}=\{a\},A_2\cap A_{e+1}=\{b\}$且$A_1\cap A_2=\{d\}$。

那么我们有$|A_1 \cup A_2 \cup A_{e+1}| \leq 3r-3$，这与假设$\mathcal{H}$是$\mathcal{G}_r(3r-3,3)$-free相矛盾。因此，我们的声明成立了。剩下的只需证明$|A_1 \cup A_2 \cup A_3 \cup A_{e+1}| = 4r-3$，它可以由事实$|A_1 \cup A_2 \cup A_3| = 3r$与$|A_{e+1} \cap (A_1 \cup A_2 \cup A_3)| = 3$推出。令$i_1 = 1, i_2 = 2, i_3 = 3$和$i = e+1$即可以得到我们的引理。 □

引理4.5.2. *假设$\mathcal{H}$是一个$\mathcal{G}_r(3r-3,3)$-free的r-均衡线性超图。令A和B为$\mathcal{H}$的两条边，它们满足$A \cap B \neq \emptyset$。若存在另外一条边$C \in \mathcal{H} \setminus \{A,B\}$与$A$和$B$的交都不是空集，那么一定有$C \cap A = C \cap B = A \cap B$，即$A$，$B$，$C$包含一个公共的顶点。*

证明. 该引理是$\mathcal{H}$的$\mathcal{G}_r(3r-3,3)$-free性质与线性性质的一个直接结论。 □

引理4.5.3. *令$e \geq 4$是一个正整数，$\mathcal{H}$是一个由恰好e条边构成的r-均衡r-部的线性超图。假设$\mathcal{H}$是$\mathcal{G}_r(3r-3,3)$-free且$\mathcal{G}_r((e-1)(r-2)+3, e-1)$-free，但不是$\mathcal{G}_r(e(r-2)+3,e)$-free的，即$|V(\mathcal{H})| \leq e(r-2)+3$。那么对任意顶点$a \in V(\mathcal{H})$都有$\deg(a) \leq \lfloor \frac{e}{3} \rfloor$。*

证明. 不失一般性，我们可以假设：$\max\{\deg(v) : v \in V(\mathcal{H})\} = l$。选取一个顶点$a \in V(\mathcal{H})$满足$\deg(a) = l$。令$a \in V_1$且设$A_1, \ldots, A_l$为包含顶点$a$的$l$条边。由$\mathcal{H}$的线性性可知，$A_1 \setminus \{a\}, \ldots, A_l \setminus \{a\}$是两两互不相交的。对每个$1 \leq i \leq l$，我们把引理4.5.1应用于每一个$A_i$，那么，可以推知对任意$A_i$都存在三条边$B_{i_1}$，$B_{i_2}$与$B_{i_3}$满足引理4.5.1的三条性质。注意到对每个$i$，$\{A_1, \ldots, A_l\} \setminus \{A_i\}$中的最多一条边可以充当$\{B_{i_1}, B_{i_2}, B_{i_3}\}$中的一条边。因此，对任意$A_i$，都存在至少两条取自$\mathcal{H} \setminus \{A_1, \ldots, A_l\}$的不同边$B_{i_1}, B_{i_2}$，满足$\emptyset \neq B_{i_1} \cap A_i \neq B_{i_2} \cap A_i \neq \{a\}$。实际上，$2l$条边$\{B_{i_j} : 1 \leq i \leq l,\ 1 \leq j \leq 2\}$是全不相同的。如若不然，则存在$1 \leq i \neq i' \leq l$与某个$B \in \{B_{i_j} : 1 \leq i \leq l,\ 1 \leq j \leq 2\}$使得$B \cap A_i \neq \emptyset$和$B \cap A_{i'} \neq \emptyset$都成立。因此，由引理4.5.2可知，唯一可能的情形就是$B \cap A_i \cap A_{i'} = \{a\}$，这是一个矛盾。

现在，边A_i与边B_{i_j}给我们带来了至少$3l$条不同的边，这意味着$3l \leq e$；进而，由l是一个整数可知$l \leq \lfloor \frac{e}{3} \rfloor$。 □

4.5.1 $\mathcal{G}_r(4r-5,4)$-free与$\mathcal{G}_r(5r-7,5)$-free超图

这个小节的主要任务是证明如一个r-均衡r-部的线性超图是$\mathcal{G}_r(3r-3,3)$-free的，则它肯定也是$\mathcal{G}_r(4r-5,4)$-free的与$\mathcal{G}_r(5r-7,5)$-free的。让我们从下面的引理开始。

定理4.5.4. *令$\mathcal{H}$为一个r-均衡r-部的线性超图。如果$\mathcal{H}$是$\mathcal{G}_r(3r-3,3)$-free的，则它也是$\mathcal{G}_r(4r-$*

$5,4)$-*free*的。

证明. 如若不然，$\mathcal{H}$不是$\mathcal{G}_r(4r-5,4)$-free的。那么存在四条不同的边$A_1,A_2,A_3,A_4\in\mathcal{H}$，使得$|A_1\cup A_2\cup A_3\cup A_4|\leq 4r-5$。由引理4.5.1可知，$A_1,A_2,A_3,A_4$也满足$|A_1\cup A_2\cup A_3\cup A_4|=4r-3$，这显然是一个矛盾。 □

定理4.5.5. *令$\mathcal{H}$为一个r-均衡r-部的线性超图。如果$\mathcal{H}$是$\mathcal{G}_r(3r-3,3)$-free的，则它也是$\mathcal{G}_r(5r-7,5)$-free的。*

证明. 如若不然，$\mathcal{H}$不是$\mathcal{G}_r(5r-7,5)$-free的。那么有五条不同的边$A_1,A_2,A_3,A_4,A_5\in\mathcal{H}$，使得$|A_1\cup A_2\cup A_3\cup A_4\cup A_5|\leq 5r-7$。由定理4.5.4可知，$\mathcal{H}$是$\mathcal{G}_r(4r-5,4)$-free的。那么存在$\{A_1,A_2,A_3,A_4,A_5\}$的四条边满足引理4.5.1。令这四条边为$A_1,A_2,A_3$与$A_4$，使得$A_1,A_2$和$A_3$是两两不交的。再一次，由$\mathcal{G}_r(4r-5,4)$-free 性质，我们有$|A_2\cup A_3\cup A_4\cup A_5|\geq 4r-4$。记$X=A_2\cup A_3\cup A_4\cup A_5$。那么$|A_1\cap X|\leq 2$，这是因为$A_1\cap(A_2\cup A_3)=\emptyset$，$|A_1\cap A_4|=1$，$|A_1\cap A_5|\leq 1$。因此，我们可以推出

$$|A_1\cup X|=|A_1|+|X|-|A_1\cap X|\geq 4r-4+r-2=5r-6>5r-7,$$

这与我们的假设相矛盾。 □

以下的推论是上面两个定理的直接结果。

命题4.5.6. *$f_r(n,4(r-2)+3,4)>n^{2-o(1)}$，$f_r(n,5(r-2)+3,5)>n^{2-o(1)}$。换句话说，猜想4.1.1的左边对$r\geq 3$，$e=4$，$k=2$与$r\geq 3$，$e=5$，$k=2$成立。*

证明. 由定理4.5.4与定理4.5.5可知，我们只需证明存在一个足够大的r-均衡r-部的线性$\mathcal{G}_r(3r-3,3)$-free超图。引理4.3.1，注记4.4.1和定理4.4.3指出这样的超图确实是存在的，如果存在一个相应的足够大的R_3-sum-free 集，而R_3-sum-free集的存在性是由定理4.3.10保证的。 □

4.5.2 不是$\mathcal{G}_r(6r-9,6)$-free的超图的分类

上面小节的结果指出，所有r-均衡r-部的线性$\mathcal{G}_r(3r-3,3)$-free超图也是$\mathcal{G}_r(4r-5,4)$-free与$\mathcal{G}_r(5r-7,5)$-free的。然而，当$e=6$时，这个性质却不能成立。例如，我们可以考虑如下表4-4所示的超图。

	A_1	A_2	A_3	A_4	A_5	A_6
V_1	a_1	b_1	c_1	a_1	b_1	c_1
V_2	a_2	b_2	c_2	b_2	c_2	a_2
V_3	a_3	b_3	c_3	c_3	a_3	b_3

表 4-4 (6,3)-free但不是(9,6)-free的超图

这个超图有六条边，并且是一个3-均衡3-部的线性超图。容易验证它满足$\mathcal{G}_3(6,3)$-free，$\mathcal{G}_3(7,4)$-free与$\mathcal{G}_3(8,5)$-free的性质。但是，我们有$|\cup_{i=1}^{6} A_i| = 9$，因此，它不是$\mathcal{G}_3(9,6)$-free的。令人惊奇的是，如果我们给满足$\mathcal{G}_r(3r-3,3)$-free而不满足$\mathcal{G}_r(6r-9,6)$-free的超图添加一些限制条件，我们可以证明所有六条边之并不超过$6r-9$个顶点的情形仅仅有一种可能的构型（考虑同构性）。

定理4.5.7. *令$r \geq 3$，$\mathcal{H}$是一个r-均衡r-部的线性超图。假设$\mathcal{H}$没有三长且没有四长的彩虹圈。若存在$\mathcal{H}$的六条边$A_1,\ldots,A_6$使得$|A_1\cup\cdots\cup A_6| \leq 6r-9$，那么$|A_1\cup\cdots\cup A_6| = 6r-9$且$A_1,\ldots,A_6$只有一种可能的构型（考虑同构性）。*

注记4.5.8. *引理4.3.1说明了$\mathcal{H}$不含彩虹3-圈当且仅当它是$\mathcal{G}_r(3r-3,3)$-free的。*

注记4.5.9. *记$W = A_1\cup\cdots\cup A_6$且$\mathcal{H}_W = \{A_1,\ldots,A_6\}$。由引理4.5.3可以推知顶点$x\in W$的最大度数为2。假设$W$含有$\lambda$个度数为2的顶点且$\mu$个度数为1的顶点。那么我们有$\lambda+\mu \leq 6r-9$。更进一步，自然我们有*

$$6r = \sum_{x\in W}\deg(x) = 2\lambda+\mu \leq 2\lambda+(6r-9-\lambda) = 6r-9+\lambda.$$

所以可以推知$\lambda \geq 9$。我们将证明确实会成立$|W| = 6r-9$且W包含恰好9个度数为2的顶点，以及$6r-18$个度数为1的顶点。我们还将说明9个度数为2的顶点只有一种可能的构型，这个构型等价于表4-4所描述的超图。

证明. 为了证明我们的定理，基本的出发点是利用反证法。通过若干条仔细设计的声明后，我们会达到目标。

假设$\mathcal{H}$不是$\mathcal{G}_r(6r-9,6)$-free的。则存在$\mathcal{H}$的六条边$A_1,\ldots,A_6$，使得$|A_1\cup\cdots\cup A_6| \leq 6r-9$。又由于$\mathcal{H}$不包含彩虹3-圈，它是$\mathcal{G}_r(3r-3,3)$-free的；进而，它也是$\mathcal{G}_r(4r-5,4)$-free与$\mathcal{G}_r(5r-7,5)$-free的。不失一般性，我们取$A_1,A_2,A_3$与$A_6$为满足引理4.5.1条件的四

条边。令A_1, A_2与A_3为互不相交的三条边。设$A_1 \cap A_6 = \{a\} \in V_1$，$A_2 \cap A_6 = \{b\} \in V_2$与$A_3 \cap A_6 = \{c\} \in V_3$。记$X = A_1 \cup A_2 \cup A_3 \cup A_6$与$Y = A_4 \cup A_5$。

声明1： $|X \cap Y| = 6$，且这六个不同的交点有如下形式：$A_i \cap A_j$，$i \in \{1,2,3\}$，$j \in \{4,5\}$。

证明：首先我们显然有$|X \cap Y| \leq 6$，这是因为$|X \cap Y| \leq |X \cap A_4| + |X \cap A_5| \leq 3+3 = 6$。那么只需证明$|X \cap Y| \geq 6$。对$A_1$，$A_2$，$A_3$分别使用引理4.5.1（分别取引理4.5.1中的“A_i”为A_1，A_2，A_3）。那么，必定存在$A_{11}, A_{12}, A_{13}, A_{21}, A_{22}, A_{23}, A_{31}, A_{32}, A_{33}$（不一定全不同）满足

$$|A_1 \cup (A_{11} \cup A_{12} \cup A_{13})| = 3,\ |A_2 \cup (A_{21} \cup A_{22} \cup A_{23})| = 3,\ |A_3 \cup (A_{31} \cup A_{32} \cup A_{33})| = 3.$$

由于A_1，A_2，A_3是两两不交的，不难得出上面三个式子成立当且仅当

$$|A_1 \cup (A_4 \cup 5 \cup A_6)| = 3,\ |A_2 \cup (A_4 \cup 5 \cup A_6)| = 3,\ |A_3 \cup (A_4 \cup 5 \cup A_6)| = 3.$$

A_1，A_2，A_3的不相交性也意味着上述交集中牵涉到的九个顶点都是不同的。因此，声明立刻得证。

声明2： A_4，A_5，A_6是互不相交的。

证明：如若不然。例如，假设$A_4 \cap A_5 \neq \emptyset$。任取一个$i \in \{1,2,3\}$。由于$A_i \cap A_4 \neq \emptyset$且$A_i \cap A_5 \neq \emptyset$，由引理4.5.2可知$A_i$，$A_4$和$A_5$一定包含一个公共顶点，根据声明1，这是不可能的。

注意到，我们假设了$A_1 \cap A_6$，$A_2 \cap A_6$和$A_3 \cap A_6$分别是落在V_1，V_2和V_3内的。下一个声明是非常重要的：我们说明了如果$\mathcal{H}$不包含彩虹4-圈，那么$(A_1 \cup A_2 \cup A_3) \cap (A_4 \cup A_5)$中的其它六个顶点一定也会落在$V_1 \cup V_2 \cup V_3$内。

声明3： 交集$A_4 \cap (A_1 \cup A_2 \cup A_3)$和$A_5 \cap (A_1 \cup A_2 \cup A_3)$牵涉到的六个顶点都落在顶点集$V_1, V_2, V_3$中，我们已经假设了$a \in V_1$，$b \in V_2$与$c \in V_3$。

证明：我们将只对A_4证明声明3，这是因为对A_5的证明也是类似的。只需验证$A_4 \cap A_1 \in V_1 \cup V_2 \cup V_3$，这是因为$A_4 \cap A_2$和$A_4 \cap A_1$的证明都是类似的。注意到这个声明对3-均衡的超图是自动成立的。若$r \geq 4$，假设存在某个d，使得$A_4 \cap A_1 = \{d\} \notin V_1 \cup V_2 \cup V_3$。令$d \in V_4$对某个顶点集$V_4$成立。

我们将首先证明$A_4 \cap A_2$和$A_4 \cap A_3$ 一定落在$V_1 \cup V_2 \cup V_3$内。显然，这两个交点都不能落在V_4中，因为它们都必须与d不同，且$\mathcal{H}$是r-部的线性超图。因此，这个结

论对4-部超图（即$r = 4$）是自动成立的。对$r \geq 5$，假设$A_4 \cap A_2 = \{e\} \in V_5$，这里$V_5$是某个不属于$\{V_1, V_2, V_3, V_4\}$的顶点集。表4-5刻画了这些边的相交关系。不难看出，$d, A_1, a, A_6, b, A_2, e, A_4, d$将形成一个彩虹4-圈，这与定理的假设是矛盾的。用类似的办法，也能够说明$A_4 \cap A_3 \in V_1 \cap V_2 \cap V_3$。

	$\boldsymbol{A_1}$	$\boldsymbol{A_2}$	A_3	$\boldsymbol{A_4}$	A_5	$\boldsymbol{A_6}$
V_1	a					a
V_2		b				b
V_3			c			c
V_4	d			d		
V_5		e		e		

表 4-5　$A_4 \cap A_1 \in V_4$且$A_4 \cap A_2 \in V_5$，加粗的边形成彩虹4-圈

注意到$A_4 \cap \{a, b, c\} = \emptyset$以及$b = A_2 \cap V_2$。那么$A_2 \cap A_4$不是落在$V_1$中，就是落在$V_3$ 中。一方面，如果$A_2 \cap A_4 = \{e\} \in V_3$，则下面的表4-6说明$d, A_1, a, A_6, b, A_2, e, A_4, d$再一次形成一个彩虹4-圈，矛盾。

	$\boldsymbol{A_1}$	$\boldsymbol{A_2}$	A_3	$\boldsymbol{A_4}$	A_5	$\boldsymbol{A_6}$
V_1	a					a
V_2		b				b
V_3		e	c	e		c
V_4	d			d		

表 4-6　$A_4 \cap A_1 \in V_4$且$A_4 \cap A_2 \in V_3$，加粗的边形成彩虹4-圈

另一方面，如果$A_2 \cap A_4 = \{e\} \in V_1$，那么$A_3 \cap A_4$一定落在$V_2$中（它不能落在$V_1$内，因为$A_2 \cap A_4$已经在$V_1$内；它也不能落在$V_3$内，因为$A_3 \cap V_3 = \{c\}$且$c \notin A_4$）。令$A_3 \cap A_4 = \{f\} \in V_2$，那么下面的表4-7说明了$d, A_1, a, A_6, c, A_3, f, A_4, d$形成一个彩虹4-圈，矛盾。

因此，我们可以总结到：所有出现在交集$A_4 \cap (A_1 \cup A_2 \cup A_3)$和$A_5 \cap (A_1 \cup A_2 \cup A_3)$中的六个点都落在$V_1, V_2$与$V_3$内。声明得证。

现在，我们可以证明定理的主要部分。声明3说明$\{A_1, \ldots, A_6\}$中任意两个集合的交集落在$V_1 \cup V_2 \cup V_3$中。因此，$A_1 \setminus (V_1 \cup V_2 \cup V_3), \ldots, A_6 \setminus (V_1 \cup V_2 \cup V_3)$是两两不交的。因此，

	$\boldsymbol{A_1}$	A_2	$\boldsymbol{A_3}$	$\boldsymbol{A_4}$	A_5	$\boldsymbol{A_6}$
V_1	a	e		e		a
V_2		b	f	f		b
V_3			c			c
V_4	d			d		

表 4-7 $A_4 \cap A_1 \in V_4$，$A_4 \cap A_2 \in V_1$，$A_3 \cap A_4 \in V_2$，**加粗的边形成彩虹4-圈**

在讨论中我们可以忽略它们。假设把A_1, A_2, A_3限制到V_1, V_2, V_3上可以得到表4-8中表示的图。

	A_1	A_2	A_3
V_1	a	f	h
V_2	d	b	i
V_3	e	g	c

表 4-8 A_1, A_2, A_3**限制到**V_1, V_2, V_3**上所得的超图**

注意到我们假设了$A_6 \cap A_1 \cap V_1 = \{a\}$，$A_6 \cap A_2 \cap V_2 = \{b\}$，$A_6 \cap A_3 \cap V_3 = \{c\}$。根据$\mathcal{H}$的线性性与声明1、2，容易验证（仅仅通过列举所有的可能性）当考虑在$V_1 \cup V_2 \cup V_3$上的限制时，A_4和A_5仅有两种可能，即

	A_1	A_2	A_3	A_4	A_5	A_6
V_1	a	f	h	f	h	a
V_2	d	b	i	i	d	b
V_3	e	g	c	e	g	c

或者

	A_1	A_2	A_3	A_4	A_5	A_6
V_1	a	f	h	h	f	a
V_2	d	b	i	d	i	b
V_3	e	g	c	g	e	c

.

注意到这两种构型实际上是等价的。也容易看出$|A_1 \cup \cdots \cup A_6| = 6r - 9$。定理得证。 □

注意到上面的构型也能被表示一个3×3的格，即

	A_1	A_2	A_3
A_4	a	f	h
A_5	d	b	i
A_6	e	g	c

我们把这个构型称为$G_{3\times 3}$。

注记4.5.10. 可以看出定理*4.5.7*所决定的唯一的构型满足如下三条重要的性质。

(1) 对每个$i \in \{1,2,3\}$与$j \in \{4,5,6\}$，都有$A_i \cap A_j \neq \emptyset$。此外，出现在交集中的九个点是不同的。

(2) 对$\{i,j\} \subseteq \{1,2,3\}$或者$\{i,j\} \subseteq \{4,5,6\}$，$A_i \cap A_j = \emptyset$。

(3) A_1, A_2, A_3与A_4, A_5, A_6在$V_1 \cup V_2 \cup V_3$中具有相同的九个顶点。

4.5.3 $\mathcal{G}_r(7r-11,7)$-free超图

引理4.5.11. 令$r \geq 3$是一个正整数且$\mathcal{H}$为r-均衡r-部的线性超图。假设$\mathcal{H}$不含三长且不含四长的彩虹圈。若存在$\mathcal{H}$的六条边$A_1, \ldots, A_6$使得$|A_1 \cup \cdots \cup A_6| \leq 6r-9$，那么对任意$A_7 \in \mathcal{H} \setminus \{A_1, \ldots, A_6\}$，都有$|A_7 \cap (A_1 \cup \cdots \cup A_6)| \leq 1$。

证明. 我们的假设意味着$\mathcal{H}$是$\mathcal{G}_r(3r-3,3)$-free，$\mathcal{G}_r(4r-5,4)$-free与$\mathcal{G}_r(5r-7,5)$-free的。由定理4.5.7下面的讨论可知，$\{A_1, \ldots, A_6\}$的唯一构型等价于$G_{3\times 3}$。

记$X = A_1 \cup \cdots \cup A_6$。若存在某个$A_7 \in \mathcal{H} \setminus \{A_1, \ldots, A_6\}$使得$|A_7 \cap X| \geq 2$.。则由$\mathcal{H}$的线性性可知，存在$i,j \in \{1, \ldots, 6\}$与$i \neq j$使得$A_7 \cap A_i \neq \emptyset$，$A_7 \cap A_j \neq \emptyset$且$A_7 \cap A_i \neq A_7 \neq A_j$。因此，可以推出$A_i \cap A_j = \emptyset$，否则，$A_7, A_i$与$A_j$将违反$\mathcal{H}$的$\mathcal{G}_r(3r-3,3)$-free性质。由注记4.5.10的(1)和(2)可知，我们有$\{i,j\} \subseteq \{1,2,3\}$或$\{i,j\} \subseteq \{4,5,6\}$。假设$\{i,j\} \subseteq \{1,2,3\}$。记$y_i = A_7 \cap A_i$及$y_j = A_7 \cap A_j$。我们的证明可以被划分为以下三种情形，依据$y_i, y_j$与$V_1 \cup V_2 \cup V_3$之间的关系。

情形1： $y_i \in V_1 \cup V_2 \cup V_3$且$y_j \in V_1 \cup V_2 \cup V_3$。

注意到，我们已经假设了$\{i,j\} \subseteq \{1,2,3\}$。若$y_j \in V_1 \cup V_2 \cup V_3$，由注记4.5.10的(3)可知，我们可以找到一个$j' \in \{4,5,6\}$ 满足$y_j \in A_{j'}$。那么，我们有$A_7 \cap A_i = \{y_i\}$，

$A_7 \cap A_{j'} = \{y_j\}$，$y_i \neq y_j$与$A_i \cap A_{j'} \neq \emptyset$（由注记4.5.10的(1)），这意味着$|A_7 \cup A_i \cup A_{j'}| = 3r-3$，违反了$\mathcal{G}_r(3r-3,3)$-free的性质。下面的表4-9直观地展示了我们的证明过程。

	$\boldsymbol{A_i}$	A_j	$\boldsymbol{A_{j'}}$	$\boldsymbol{A_7}$
V_1	y_i			y_i
V_2		y_j	y_j	y_j
V_3	$A_i \cap A_{j'}$		$A_i \cap A_{j'}$	

表 4-9　引理4.5.11的情形1，$i,j \in \{1,2,3\}$且$j' \in \{4,5,6\}$，加粗的边形成彩虹3-圈

情形2： $y_i \in V_1 \cup V_2 \cup V_3$且$y_j \notin V_1 \cup V_2 \cup V_3$。

再一次，由注记4.5.10的(3)可知，存在一个$i' \in \{4,5,6\}$满足$y_i \in A_{i'}$。那么，我们有$A_7 \cap A_{i'} = \{y_i\}$，$A_7 \cap A_j = \{y_j\}$，$y_i \neq y_j$与$A_{i'} \cap A_j \neq \emptyset$（由注记4.5.10的(1)），这意味着$|A_7 \cup A_{i'} \cup A_j| = 3r-3$，违反了$\mathcal{G}_r(3r-3,3)$-free的性质。下面的表4-10直观地展示了我们的证明过程。

	$\boldsymbol{A_i}$	A_j	$\boldsymbol{A_{j'}}$	$\boldsymbol{A_7}$
V_1				
V_2		y_j	y_j	y_j
V_3	$A_i \cap A_{j'}$		$A_i \cap A_{j'}$	
V_i	y_i			y_i

表 4-10　引理4.5.11的情形2，$i,j \in \{1,2,3\}$且$j' \in \{4,5,6\}$，加粗的边形成彩虹3-圈

情形3： $y_i \notin V_1 \cup V_2 \cup V_3$且$y_j \notin V_1 \cup V_2 \cup V_3$。

在这个条件下，y_i与y_j不能落在相同的顶点集中，这是因为$\mathcal{H}$是r-部的且$y_i \neq y_j$。假设$y_i \in V_{l_i}$与$y_j \in V_{l_j}$，其中，$\{l_i,l_j\} \cap \{1,2,3\} = \emptyset$且$l_i \neq l_j$（这时，$\mathcal{H}$包含至少五个顶点集，这意味着$r \geq 5$，对$r=4$，我们只需考虑前两种情形）。任取一个$k \in \{4,5,6\}$使得$A_k \cap A_i = x_i$且$A_k \cap A_j = x_j$。这时，利用注记4.5.10 的结论不难知道$x_i, A_i, y_i, A_7, y_j, A_j, x_j, A_k, x_i$构成一个彩虹4-圈，这与定理的假设相矛盾。下面的表4-11直观地展示了我们的证明过程。

对$\{i,j\} \subseteq \{4,5,6\}$，证明是类似的。因此，定理得证。 □

为了证明我们的主要结论，我们还需要一个引理。

	$\boldsymbol{A_i}$	$\boldsymbol{A_j}$	$\boldsymbol{A_k}$	$\boldsymbol{A_7}$
V_1	x_i		x_i	
V_2		x_j	x_j	
V_3				
V_{l_i}	y_i			y_i
V_{l_j}		y_j		y_j

表 4-11　引理4.5.11的情形3，$i,j\in\{1,2,3\}$且$k\in\{4,5,6\}$，加粗的边形成彩虹4-圈

引理4.5.12. 令$r\geq 4$是一个正整数，$\mathcal{H}$是一个r-均衡r-部的线性超图。假设$\mathcal{H}$不含三长且不含四长的彩虹圈。再假设$\mathcal{H}$不含度数大于2的顶点。令A_1,A_2,A_3,A_4为$\mathcal{H}$的四条互不相交的边，则存在至多一条边$B\in\mathcal{H}\setminus\{A_1,A_2,A_3,A_4\}$满足$|B\cap(A_1\cup A_2\cup A_3\cup A_4)|=4$。

证明. 如若不然，假设存在两条不同的边$B,C\in\mathcal{H}\setminus\{A_1,A_2,A_3,A_4\}$满足$|B\cap(A_1\cup A_2\cup A_3\cup A_4)|=4$与$|C\cap(A_1\cup A_2\cup A_3\cup A_4)|=4$。交集中牵涉到的八个顶点一定是不同的，否则$\mathcal{H}$将包含度数大于2的顶点。由$\mathcal{H}$的$\mathcal{G}_r(3r-3,3)$-free性质可知，不难验证$B\cap C=\emptyset$。我们的目标是说明$\{A_1,A_2,A_3,A_4,B,C\}$中必有四条边会形成一个彩虹4-圈。令$V_1,\ldots,V_r$为$\mathcal{H}$的$r$个顶点部分。不失一般性，对$1\leq i\leq 4$我们设$B\cap A_i=\{b_i\}\in V_i$且$C\cap A_i=\{c_i\}$。注意到，对不同的$1\leq i_1\neq i_2\leq 4$，我们有$\{c_{i_1},c_{i_2}\}\cap(V_{i_1}\cup V_{i_2})\neq\emptyset$，否则$\{b_{i_1},b_{i_2},c_{i_1},c_{i_2}\}$将落在四个不同的顶点部中，进而$b_{i_1},A_{i_1},c_{i_1},C,c_{i_2},A_{i_2},b_{i_2},B,b_{i_1}$形成一个彩虹4-圈。另一方面，由于我们有$a_{i_1}\in V_{i_1}$，$a_{i_2}\in V_{i_2}$且$B\cap C=\emptyset$，容易看出$c_{i_1}\notin V_{i_1}$且$c_{i_2}\notin V_{i_2}$。因此我们有$c_{i_1}\in V_{i_2}$或者$c_{i_2}\in V_{i_1}$两者之一成立。对每个$1\leq i\leq 4$，令$1\leq x_i\leq r$为四个满足$c_i\in V_{x_i}$的整数。那么以上的讨论意味着对每个$\{i_1,i_2\}\subseteq\{1,2,3,4\}$，我们有$x_{i_1}=i_2$或者$x_{i_2}=i_1$。令$\{i_1,i_2\}$取遍$\{1,2,3,4\}$的所有二元子集。可以推知，下面的六个方程必定同时成立。

$$\begin{cases}(x_1-2)(x_2-1)=0, & i_1=1,\ i_2=2,\\ (x_1-3)(x_3-1)=0, & i_1=1,\ i_2=3,\\ (x_1-4)(x_4-1)=0, & i_1=1,\ i_2=4,\\ (x_2-3)(x_3-2)=0, & i_1=2,\ i_2=3,\\ (x_2-4)(x_4-2)=0, & i_1=2,\ i_2=4,\\ (x_3-4)(x_4-3)=0, & i_1=3,\ i_2=4.\end{cases}$$

不难验证这是不可能的。因此，$\{A_1,A_2,A_3,A_4,B,C\}$一定会诱导出一个彩虹4-圈，这是一个矛盾。我们的引理得证了。　□

定理4.5.13. 令$r \geq 3$为一个正整数，$\mathcal{H}$是r-均衡r-部线性超图。假设$\mathcal{H}$不包含三长且不包含四长的彩虹圈，则$\mathcal{H}$是$\mathcal{G}_r(7r-11,7)$-*free* 的。

证明. 假设$\mathcal{H}$不是$\mathcal{G}_r(7r-11,7)$-free的，则存在$\mathcal{H}$ de 七条边$A_1,\ldots,A_7$使得$|A_1\cup\cdots\cup A_7|\leq 7r-11$。由于$\mathcal{H}$不含有彩虹3-圈，它是$\mathcal{G}_r(3r-3,3)$-free的，进而是$\mathcal{G}_r(4r-5,4)$-free与$\mathcal{G}_r(5r-7,5)$-free的。记$\mathcal{H}'$为$\{A_1,\ldots,A_7\}$构成的子图。证明被分为两个部分，依据$\mathcal{H}'$是否为$\mathcal{G}_r(6r-9,6)$-free的。

若$\mathcal{H}'$不是$\mathcal{G}_r(6r-9,6)$-free的，那么令$A_1,\ldots,A_6$为六条边使得$|A_1\cup\cdots\cup A_6|\leq 6r-9$。记$X=A_1\cup\cdots\cup A_6$。由定理4.5.7可知，$|X|=6r-9$且这六条边必形成一个$G_{3\times 3}$。因此，我们有

$$7r-11\geq|X\cup A_7|=|X|+|A_7|-|X\cap A_7|=6r-9+r-|X\cap A_7|,$$

这意味着$|X\cap A_7|\geq 2$，根据引理4.5.11，这是一个矛盾。

因此，为了证明这个定理，只需验证$\mathcal{H}'$是$\mathcal{G}_r(6r-9,6)$-free的情形。引理4.5.3说明$\mathcal{H}'$不包含度数为3的顶点。假设$\mathcal{H}'$含有λ个度数为2的顶点与μ个度数为1的顶点。那么我们有$\lambda+\mu\leq 7r-11$。进一步，自然成立

$$7r=\sum_{x\in W}\deg(x)=2\lambda+\mu\leq 2\lambda+(7r-11-\lambda)=7r-11+\lambda.$$

因此，可以推知$\lambda\geq 11$。让我们计算如下二元组的数目：$N:=\{(v,A):v\in A,A\in\mathcal{H},\ v\in V(\mathcal{H}),\ \deg(v)=2\}$。注意到$N=2\lambda\geq 22$，且仅有七条边。因此，存在至少一条边包含至少四个度数为2的顶点（注意到这四个点必定落在四个不同的顶点部中，因此这个定理对$r=3$显然成立）。若$r\geq 4$，不失一般性，假设A_7为这么一条边，且A_1,A_2,A_3,A_4为与A_7有着公共度数为2顶点的四条边。对$1\leq i\leq 4$，令$A_7\cap A_i=\{a_i\}$。现在我们可以作出一个辅助的表4-12。

	A_1	A_2	A_3	A_4	A_5	A_6	A_7
V_1	a_1						a_1
V_2		a_2					a_2
V_3			a_3				a_3
V_4				a_4			a_4

表 4-12　有四个度数为2的点包含在一条边内

采用一个类似于引理4.5.1中(2)的证明技巧，可以得到A_1, A_2, A_3, A_4是互不相交的。我们对$i = 1,2,3,4$重复地使用引理4.5.1。每一次对$i \in \{1,2,3,4\}$，都存在三条不交的边$A_{i_1}, A_{i_2}, A_{i_3} \in \{A_1, \ldots, A_7\} \setminus \{A_i\}$满足$|A_{i_l} \cap A_i| = 1$对每个$1 \leq l \leq 3$都成立。由于$A_1, A_2, A_3, A_4$的不交性，上述情况成立的唯一一种可能就是$\{A_{i_1}, A_{i_2}, A_{i_3}\} = \{A_5, A_6, A_7\}$对所有$1 \leq i \leq 4$都成立。再一次，由$A_1, A_2, A_3, A_4$的不交性可知，$A_5 \cap (A_1 \cup A_2 \cup A_3 \cup A_4)$，$A_6 \cap (A_1 \cup A_2 \cup A_3 \cup A_4)$，$A_7 \cap (A_1 \cup A_2 \cup A_3 \cup A_4)$牵涉到的12个交点都是不同的，这意味着我们有$|A_5 \cap (A_1 \cup A_2 \cup A_3 \cup A_4)| = 4$，$|A_6 \cap (A_1 \cup A_2 \cup A_3 \cup A_4)| = 4$与$|A_7 \cap (A_1 \cup A_2 \cup A_3 \cup A_4)| = 4$。因此，由引理4.5.12可知$\mathcal{H}'$一定包含一个彩虹4-圈，矛盾。 □

4.5.4 $\mathcal{G}_r(8r-13, 8)$-free的超图

在这个小节中，我们将研究$\mathcal{G}_r(8r-13, 8)$-free的超图。我们的目标是构造一个足够大的$\mathcal{G}_r(8r-13, 8)$-free超图，以达到猜想在$r \geq 3, k = 2$与$e = 8$时的下界。

定理4.5.14. *令$r \geq 3$为一个正整数，且$\mathcal{H}$是一个r-均衡r-部的线性超图。假设$\mathcal{H}$不含三长且不含四长的彩虹圈，则$\mathcal{H}$一定是$\mathcal{G}_r(8r-13, 8)$-free的。*

证明. 定理4.5.13说明$\mathcal{H}$是$\mathcal{G}_r(7r-11, 7)$-free的。如果它不是$\mathcal{G}_r(8r-13, 8)$-free的，则令$\mathcal{H}' = \{A_1, \ldots, A_8\}$为一个含有八条边的子图，且满足$|A_1 \cup \cdots A_8| \leq 8r-13$。引理4.5.3说明$\mathcal{H}'$不含度数为3的顶点。假设$\mathcal{H}'$包含$\lambda$个度数为2的顶点和$\mu$个度数为1的顶点。我们有$\lambda + \mu \leq 8r-13$。更进一步，自然有

$$8r = \sum_{x \in W} \deg(x) = 2\lambda + \mu \leq 2\lambda + (8r - 13 - \lambda) = 8r - 13 + \lambda.$$

因此，可以推出$\lambda \geq 13$。让我们计算如下二元组的数目：$N := \{(v, A) : v \in A, A \in \mathcal{H}, v \in V(\mathcal{H}), \deg(v) = 2\}$。注意到$N = 2\lambda \geq 26$且我们只有八条边。因此存在至少一条边含有至少四个度数为2的顶点（注意到这四个点必定落在四个不同的顶点部中，因此这个定理对$r = 3$显然成立）。若$r \geq 4$，不失一般性，令A_8为这么一条边，且令A_1, A_2, A_3, A_4为与A_8交于一个公共的度数为2的顶点的四条边。对$1 \leq i \leq 4$，令$A_8 \cap A_i = \{a_i\}$。我们可以画一个辅助的表4-13。

容易验证A_1, A_2, A_3, A_4都是互不相交的。我们声称A_5, A_6与A_7也是互不相交的。如若不然，不失一般性，假设suppose $A_6 \cap A_7 \neq \emptyset$。我们对$i = 1,2,3,4$重复使用引理4.5.1 repeatedly for $i = 1,2,3,4$。每一次对$i \in \{1,2,3,4\}$都存在三条不交的边$A_{i_1}, A_{i_2}, A_{i_3} \in$

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
V_1	a_1							a_1
V_2		a_2						a_2
V_3			a_3					a_3
V_4				a_4				a_4

表 4-13　有四个度数为2的点包含在一条边内

$\{A_1,\ldots,A_8\}\setminus\{A_i\}$满足$|A_{i_l}\cap A_i|=1$对每个$1\le l\le 3$都成立。由$A_1,A_2,A_3,A_4$的不交性可知，对每个$i\in\{1,2,3,4\}$，$A_{i_1},A_{i_2},A_{i_3}$的可能候选只可能从$\{A_5,A_6,A_7,A_8\}$中选取。由于$A_i\cap A_8\neq\emptyset$，$\{A_5,A_6,A_7\}$中的至少两条边都必须与$A_i$有非空交集。称这样的两条边为$A_i$的一个相交对（如果三条边$A_5,A_6,A_7$都与$A_i$有非空交集，我们仅仅从它们中任意选取两条边构成$A_i$ 的相交对）。注意到包含在一个相交对中的两条边是不交的。因此在$A_6\cap A_7\neq\emptyset$的假设之下，对每个$i\in\{1,2,3,4\}$，A_i的相交对只可能是(A_5,A_6)或者(A_5,A_7)。观察到这两对都包含A_5，这意味着$A_5\cap A_i\neq\emptyset$对每个$1\le i\le 4$都成立。因此，我们有$|A_5\cap(A_1\cup A_2\cup A_3\cup A_4)|=4$且$|A_8\cap(A_1\cup A_2\cup A_3\cup A_4)|=4$，这与引理4.5.12相矛盾。因此，我们的声明是正确的。我们可以总结到A_5,A_6,A_7是互不相交的。

对每个$j\in\{5,6,7\}$，通过对A_j使用引理4.5.1，可以推知存在至少一个$i\in\{1,2,3,4\}$满足$A_i\cap A_j\neq\emptyset$。注意到我们也有$A_i\cap A_8\neq\emptyset$。因此，我们有$A_j\cap A_8=\emptyset$，否则我们要不然会得到一个度数为3的顶点，要不然会存在三条边包含至多$3r-3$个顶点。实际上，我们已经证明了A_5,A_6,A_7,A_8是互不相交的。一方面，对A_5,A_6 和A_7反复使用引理4.5.1。从而对$1\le j\le 4$，每个A_j与$A_1\cup A_2\cup A_3\cup A_4$都至少有三个交点。另一方面，引理4.5.12说明交集的大小至多为三。因此，实际上我们有$|A_j\cap(A_1\cup A_2\cup A_3\cup A_4)|=3$对每个$j\in\{5,6,7\}$都成立。甚至，交集中牵涉到的所有九个顶点都是不同的。在下面我们能将说明$A_1\cup A_2\cup A_3\cup A_4$与$A_5\cup A_6\cup A_7\cup A_8$有着太多的交点（多达$3\times3+4=13$个），这导致无法避免彩虹4-圈的出现。为简洁起见，接下来我们记$X=A_1\cup A_2\cup A_3\cup A_4$和$Y=A_5\cup A_6\cup A_7$。

由于$|X\cap Y|=9$且$|A_i\cap Y|\ge 2$对每个$1\le i\le 4$都成立，存在恰好一个$i_0\in\{1,2,3,4\}$满足$|A_{i_0}\cap Y|=3$且$|A_k\cap Y|=2$，$k\in\{1,2,3,4\}\setminus\{j\}$。让我们把这个特殊的边设为$A_4$（即假设$i_0=4$）。现在，注意到$\{A_1,A_2,A_3\}$中的每条边与$\{A_5,A_6,A_7\}$中的恰好两条边相交；反之，$\{A_5,A_6,A_7\}$中的每条边也恰好与$\{A_1,A_2,A_3\}$中的两条边相交。通过穷举，容易看出在$\{A_1,A_2,A_3\}$与$\{A_5,A_6,A_7\}$之间在等价意义上说仅仅有一种可能的相交关系。不失一般

性，假设

$$A_5 \cap A_1 \neq \emptyset, \qquad A_5 \cap A_2 \neq \emptyset,$$
$$A_6 \cap A_1 \neq \emptyset, \qquad A_6 \cap A_3 \neq \emptyset,$$
$$A_7 \cap A_2 \neq \emptyset, \qquad A_7 \cap A_3 \neq \emptyset.$$

此外，令$1 \leq x_1, x_2, x_4, y_1, y_3, y_4, z_2, z_3, z_4 \leq r$为满足如下条件的九个整数

$$A_5 \cap A_1 \in V_{x_1}, \qquad A_5 \cap A_2 \in V_{x_2}, \qquad A_5 \cap A_4 \in V_{x_4},$$
$$A_6 \cap A_1 \in V_{y_1}, \qquad A_6 \cap A_3 \in V_{y_3}, \qquad A_6 \cap A_4 \in V_{y_4},$$
$$A_7 \cap A_2 \in V_{z_2}, \qquad A_7 \cap A_3 \in V_{z_3}, \qquad A_7 \cap A_4 \in V_{z_4}.$$

注意到我们已经假设了$A_i \cap A_8 \in V_i$对每个$1 \leq i \leq 4$成立。因此，如同引理4.5.12的证明一样，为了避免彩虹4-圈的出现，如下九个方程必须同时成立。

$$(x_1 - 2)(x_2 - 1) = 0, \qquad (x_1 - 4)(x_4 - 1) = 0, \qquad (x_2 - 4)(x_4 - 2) = 0,$$
$$(y_1 - 3)(y_3 - 1) = 0, \qquad (y_1 - 4)(y_4 - 1) = 0, \qquad (y_3 - 4)(y_4 - 3) = 0,$$
$$(z_2 - 3)(z_3 - 2) = 0, \qquad (z_2 - 4)(z_4 - 2) = 0, \qquad (z_3 - 4)(z_4 - 3) = 0.$$

另一个重要的观察就是，对每个$1 \leq i \leq 4$，三元组x_i, y_i, z_i中的任意两个都不能有相同的值，这是因为超图本身是r-部的。在这种意义下，我们可以验证只要给定其中一个未知数的值，那么九个未知数的值就可以被同时确定下来。例如，$(x_1 - 2)(x_2 - 1) = 0$意味着$x_1 = 2$或者$x_2 = 1$。令$x_1 = 2$。那么为了保证第一行剩下两个方程成立，我们必须令$x_4 = 1$与$x_2 = 4$。让我们检查第二行的第二个方程。由于$x_4 = 1$且$y_4 \neq x_4$，我们必须令$y_1 = 4$，这意味着$y_3 = 1$且$y_4 = 3$。现在我们必须令$x_1 = 2$，$y_1 = 4$且$x_4 = 1$，$y_4 = 3$，这意味着$A_5 \cap A_1 \in V_1$，$A_6 \cap A_1 \in V_4$，$A_5 \cap A_4 \in V_1$，$A_6 \in A_4 \in V_3$。容易看出，这四个交点落在四个不同的顶点部中，并且四条边A_5, A_1, A_6, A_4一定会形成一个彩虹4-圈，矛盾。因此，我们已经证明了$|A_1 \cup \cdots \cup A_8| > 8r - 13$且$\mathcal{H}$一定是$\mathcal{G}_r(8r - 13, 8)$-free的。 □

4.6 结语

在这一章中我们考虑了Brown，Erdős和Sós在稀疏超图上的著名猜想。对猜想的上界，我们用超图移除引理证明$f_r(n, e(r-k)+k+1, e) = o(n^k)$对所有正整数$r \geq k+1 \geq e$都成立。第一个未能覆盖的情形就是$r = 3$，$k = 2$和$e = 4$。在文献中，$f_3(n, 7, 4)$的阶的确定通常被称为是(7,4)-问题。我们称$G \in \mathcal{G}_3(e+3, e)$为一个$(e+3, e)$-构型。可以说明，要证明$f_3(n, 7, 4) = o(n^2)$等价于证每个有$\Omega(n^2)$条边的3-均衡超图都包含两个有两条公共边

的(6,3)-构型。然而，利用移除引理我们只能保证存在两个有一条公共边的(6,3)-构型。因此，我们怀疑我们需要更强的工具才能去研究(7,4)-问题。

对猜想的下界部分，一方面我们证明不含彩虹圈的超图是稀疏超图的很好候选；另一方面，通过使用来自加法数论的工具，我们发展出了一套方法来构造不含彩虹圈的超图。我们猜测我们所给出的构造方法可以在更多的情况下达到猜想的下界。在这个方向做出新的成果将会是很有意思的。

最后，我们提出两个公开问题。

问题1： 确定$f_3(n,7,4)=o(n^2)$是否成立。

问题2： 构造出大小为$\Omega(n^{2-o(1)})$的n个顶点上的r-均衡$\mathcal{G}_r(6r-9,6)$-free超图，即，证明$f_r(n,6r-9,6)>n^{2-o(1)}$。

实际上，$f_r(n,6r-9,6)$的上界也是未知的，我们姑且不考虑它的上界，只关心其下界。如果想要用加法数论的办法来构造下界，我们会碰到一个棘手的问题，即要求最大的$M\subseteq[n]$（希望M大至$n^{1-o(1)}$），不含形如

$$sx+ty=(s-1)u+(t+1)v$$

的方程的非平凡解，其中，$s\neq t+1$。最简单的情形，$s=t=2$时，方程为$2x+2y=u+3v$，根据文献[118]的讨论，此时要考虑这种问题都是很困难的。

5 可分哈希族

5.1 简介

可分哈希族（Separating Hash Family）是一类非常有用的组合结构，它是由Stinson，Wei和Chen[131]提出的。它们是很多组合对象的拓展，例如，完美哈希族，防诬陷码，父代识别码等。我们从一些定义开始叙述。

定义5.1.1. 令X和Y分别是大小为n和q的集合。我们称一个有N个函数$f : X \to Y$的集合$\mathcal{F}$为一个$(N; n, q)$-哈希族。

定义5.1.2. 设$f : X \to Y$是一个函数，取两两互不相交的集合$C_1, C_2, \ldots, C_t \subseteq X$。如果$f(C_1), \ldots, f(C_t)$是两两不相交的，则称$f$分离了$C_1, C_2, \ldots, C_t$。特别的，称$f$分离了一个集合$C \subseteq X$，如果$f(C) \subseteq Y$恰有$|C|$个不同的值。

定义5.1.3. 令X和Y分别是大小为n和q的集合，设$\mathcal{F}$是一个从X到Y的$(N; n, q)$-哈希族。我们说$\mathcal{F}$是一个$(N; n, q, \{w_1, \ldots, w_t\})$- 可分哈希族（我们也记为$SHF(N; n, q, \{w_1, \ldots, w_t\})$），如果它满足如下性质：对所有两两互不相交的集合$C_1, C_2, \ldots, C_t \subseteq X$，$|C_i| = w_i$，$1 \leq i \leq t$，都存在至少一个函数$f \in \mathcal{F}$分离了$C_1, C_2, \ldots, C_t$。我们把多重集合$\{w_1, \ldots, w_t\}$称为这个可分哈希族的型。

给定一个正整数q，我们记$[q]$代表集合$\{1, \ldots, q\}$。不失一般性，我们固定字母集Y为前q个正整数的集合。此外，为了简便起见，本文中我们一直记$u = \sum_{i=1}^{t} w_i$。为了避免简单的情形，假设$n > q$，$q \geq t \geq 2$且$u \leq n$。

可分哈希函数的定义最初是在$t = 2$时由Stinson，Trung和Wei[129]提出的，后来Stinson，Wei和Chen[131]对这个概念进行了推广。这个结构与很多被深入研究过的组合对象都有关系，这些对象在组合学、密码学和编码理论中都有应用，文献[32,131]提供了详细的介绍。下面归纳一些我们感兴趣的对象。

- 若$w_1 = w_2 = \cdots w_t = 1$，则一个$SHF(N; n, q, \{1, \ldots, 1\})$就是熟知的$t$-完美哈希族（Perfect Hash Family），也被记为$PHF(N; n, q, t)$。完美哈希族是基本的组合结构，它在密码学[29,31,128,129]、数据库管理[104]、回路设计[106]、概率算法的确定性设计[13]中都着重要的应用。

- 若$t = 2$满足$w_1 = 1$和$w_2 = w$，一个$SHF(N; n, q, \{1, w\})$也被称为w-防诬陷码（Frameproof Codes）。我们已经提到过，防诬陷码是一类指纹码，在版权保护中有着应用，文献[34,38,128,130]是一些关于防诬陷码的结果。

- 强度为2的父代识别码（Identifiable Parent Property Codes）是同时满足型$\{1, 1, 1\}$和型$\{2, 2\}$的可分哈希族，见文献[8,10,11,16,30]。

可分哈希族的界和构造是这个研究方向的核心问题。给定正整数N，q和$w_1, \ldots, w_t$，我们对如下问题感兴趣：原像集X的阶n最大能多大？用$C(N, q, \{w_1, \ldots, w_t\})$来记这个最大的阶。

通过一种被称为分量分组（Grouping Coordinates）的办法，界定$C(N, q, \{w_1, \ldots, w_t\})$可以被归约于界定$C(u-1, q, \{w_1, \ldots, w_t\})$，这是因为文献[19,32,131]已经注意到

$$C(N, q, \{w_1, \ldots, w_t\}) \leq C(u-1, q^{\lceil N/(u-1) \rceil}, \{w_1, \ldots, w_t\}).$$

在该研究领域内，研究者们在寻找最小的正实数γ使得$C(u-1, q, \{w_1, \ldots, w_t\}) \leq \gamma q$对任意的$q$都成立。我们建议读者阅读文献[19,32,128,129,131]，以查找之前研究者们已经做过的努力。在2008年，Stinson，Wei和Chen[131]证明了$C(3, q, \{1, 1, 2\}) \leq 3q + 2 - 2\sqrt{3m+1}$以及$C(3, q, \{2, 2\}) \leq 4q - 3$这两种特殊的情况成立。同一年，Blackburn，Etizon，Stinson和Zaverucha[32]证明了$C(u-1, q, \{w_1, \ldots, w_t\}) \leq (w_1 w_2 + u - w_1 - w_2)q$，其中，$w_1, w_2 \leq w_i$，$3 \leq i \leq t$。2011年，Bazrafshan和Trung[19]证明了如下定理。

定理5.1.4. $C(u-1, q, \{w_1, \ldots, w_t\}) \leq (u-1)q$.

此外，他们猜测（见问题5.1.6）$\gamma = u - 1$是最小的实数使得上面的界对任意的q都成立。

我们在很多方面改进了定理5.1.4，包括一些更紧的界和一些渐进最优的构造。我们工作的创新性在于，之间的组合学家研究这类问题采用的方法多为组合设计、代数组合、有限几何与概率方法，而我们发展两种新的工具，即加法数论与极值组合，来研究具有可分离性质的码和集族。我们将在本章的小结中详细论述这个观点。

我们的主要结论展示如下。

5.1.1 可分哈希族

跟随之前一些文章的步伐[19,32,131]，我们发现了可分哈希族的一个重要的性质，即$C(N,q,\{w_1,\ldots,w_t\})$的增长满足一种Johnson型的不等式。简单地讲，$C(N,q,\{w_1,...,w_t\}) \leq q^l + \max\{u-1, C(N-l,q,\{w_1-1,...,w_t\})\}$对每个正整数$l$都成立（见下面的引理5.3.1）。作为一个结果，我们得到了如下的关于可分哈希族的一个最新的界。

定理5.1.5. *假设存在一个$SHF(N;n,q,\{w_1,\ldots,w_t\})$，令$u=\sum_{i=1}^{t} w_i$和$1 \leq r \leq u-1$为正整数，满足$N \equiv r \pmod{u-1}$。如果$C(\lfloor N/(u-1)\rfloor,q,\{w_1,\ldots,w_t\}) \geq u$，则我们有$n \leq rq^{\lceil N/(u-1)\rceil} + (u-1-r)q^{\lfloor N/(u-1)\rfloor}$。*

我们的证明的一个创新性在于，我们没有用到所谓的分量分组的办法，之前所有的证明都用了这个方法。如果$N \geq u-1$且$q \geq u$，则限制$C(\lfloor N/(u-1)\rfloor,q,\{w_1,\ldots,w_t\}) \geq u$可以被略去。

对于定理5.1.4定义的系数γ，文献[19]的作者提出了如下的问题。

问题5.1.6. *是否存在某个型$\{w_1,\ldots,w_t\}$使得定理5.1.4中的常数$(u-1)$可以被某个严格小于它的常数替换?*

通过给出如下的构造，我们给予他们的问题一个否定的回答。

定理5.1.7. *对任何整数$q \geq 2$和$N \geq 2$，都存在一个$PHF(N;Nq^{N-1},q^{N-1}+(N-1)q^{N-2},N+1)$。因此，$\gamma = u-1$是满足$C(u-1,q,\{w_1,\ldots,w_t\}) \leq \gamma q$对任何$q$都成立的最小常数。*

为了说明我们的构造确实是问题5.1.6的一个否定回答，只需注意到一个u-完美哈希族也是$\{w_1,\ldots,w_t\}$-可分哈希族，这对任何$\sum_{i=1}^{t} w_i = u$都成立。如果我们设$N=u-1$，则我们的构造意味着存在一个$SHF(u-1;n,q,\{w_1,\ldots,w_t\})$使得$\lim_{q\to\infty}\frac{n}{q} = u-1$对任意$\sum_{i=1}^{t} w_i = u$都成立。因此，常数$\gamma$永远不能比$u-1$小。

5.1.2 父代识别码

我们提到过强度为2的父代识别码，该定义在文献[128]中被推广到强度为t的情形。用$i_t(N,q)$标记N长q元的t-IPP码的最大码字数目。令$v=\lfloor (t/2+1)^2\rfloor$。可以证明$i_t(N,q) \leq$

$i_t(v-1, q^{\lceil N/(v-1)\rceil})$（这与可分哈希族的情形是一致的）。因此，界定$i_t(N,q)$可以被归约于界定$i_t(v-1,q)$。Alon和Stav[16]证明了$i_t(v-1,q) \le (v-1)q$，他们猜测

猜想5.1.8. *必定有构造可以说明$(v-1)$是满足不等式$i_t(v-1,q) \le (v-1)q$的最小常数。*

我们的定理5.1.7不仅回答了问题5.1.6，而且还验证了上述猜想，这是因为文献[16,128]指出了一个v-完美哈希族也满足t-父代识别性。

5.1.3 完美哈希族

如文献[32]中所称的，定理5.1.5中的指数$\lceil N/(u-1)\rceil$是实际的。我们可以从两个方面理解这一点。一方面，Blackburn[28]的一个概率构造说明对任何给定的u和任何正的实数δ，$\delta < N/(u-1)$，只要q足够大，则都存在一个$PHF(N; \lfloor q^\delta \rfloor, q, u)$。另一方面，令$p_t(N,q)$为$PHF(N;n,q,t)$的最大容量，文献[16]和[96,108]都说明了$p_u(N,q) \ge (c_u q)^{N/(u-1)}$对某个常数$c_u$成立。因此，我们可以总结到，当$q$充分大时，指数$\lceil N/(u-1)\rceil$在$(u-1)|N$时是紧的。

但是，当$(u-1) \nmid N$时，这个问题要难得多。我们并不知晓这个指数是否是紧的。甚至连最简单的情形，$u=3$和$N=3$，Walker和Colbourn[141]提出了如下猜想。

猜想5.1.9. $p_3(3,q) = o(q^2)$。

注意到，定理5.1.5说明$p_3(3,q) = O(q^2)$。最近的一篇论文[75]指出$p_3(3,q) = \Omega(q^{5/3})$。他们运用了有限几何的方法来构造这样的集族。但是在上界和下界之间仍然有着巨大的鸿沟。对一般型的可分哈希族，Blackburn等人[32]提出了一个类似的问题。

问题5.1.10. ([32]) *令N和w_i为固定的整数。若$(u-1) \nmid N$，那么对充分大的q和任意小的$\epsilon > 0$，问是否存在一个$SHF(N;n,q,\{w_1,\ldots,w_t\})$满足$n \ge q^{\lceil N/(u-1)\rceil - \epsilon}$?*

实际上，下面我们证明了猜想5.1.9，（见定理5.5.4和定理5.5.7）。我们发现完美哈希族与一类Turán问题有着紧密的联系。通过一些变形，Walker-Colbourn的猜想可以由著名的Ruzsa和Szemerédi[119]的(6,3)定理直接给出。事实上，我们证明了

$$q^{2-\epsilon} < p_3(3,q) = o(q^2)$$

对所有足够大的q与任意小的$\epsilon > 0$都成立。我们也证明了

$$q^{2-\epsilon} < p_4(4, q) = o(q^2)$$

（见下面的定理5.6.2）。我们引入了图论和加法数论中的两个新概念，即，彩虹圈和R-sum-free集，来证明这个结果。上述两个结果表明，问题5.1.10也许存在一个正面的回答。

5.2 准备工作

在这一节中，我们将介绍一些记号和概念，我们也会介绍一些简单引理，这些引理在下面的小节中会被用到。

5.2.1 可分哈希族

在考虑可分哈希族的性质时，表示矩阵是一个十分有用的工具。一个$(N; n, q)$-哈希族可以被表示成一个$N \times n$的q元矩阵，这个矩阵常常被记为M。M的行表示哈希族中的函数，列表示X中的元素。M中行$f \in \mathcal{F}$和列$x \in X$的元素是$f(x) \in Y$。我们记M的角标为$M(f, x)$，其中，$f \in \mathcal{F}$，$x \in X$；也可记为$M(i, j)$，其中，$1 \le i \le N$，$1 \le j \le n$。

$SHF(N; n, q, \{w_1, \ldots, w_t\})$的矩阵表示满足如下性质：给定互不相交的列集$C_1, \ldots, C_t$，满足$|C_i| = w_i$，$1 \le i \le t$，存在$M$的一行$r$，使得

$$\{M(r, x) : \ x \in C_i\} \cap \{M(r, x) : \ x \in C_j\} = \emptyset$$

对所有$i \neq j$都成立。我们说行r区分了一个列子集$C \subseteq X$，如果$\{M(r, x) : x \in C\}$在Y中恰好有$|C|$个不同值。M的列x可以被写成一个N长q向量，$x = (x(1), x(2), \ldots, x(N))$，其中，$x(i) \in [q]$，$i \in [N]$。对$M$的一个行子集$L$，$x$被限制在$L$ 的分量是一个$|L|$长的向量，被记为是$x|_L = (x(i_1), x(i_2), \ldots, x(i_{|L|}))$，这里$i_j$, $1 \le j \le |L|$是行标。我们说某列$x \in X$在M中有一个独特的分量i，如果对任何其它的$y \in X$，$y \neq x$，都有$y(i) \neq x(i)$。若不会引起矛盾得话，我们不会特别区分一个哈希族和它的表示矩阵。

5.2.2 图论

在构造完美哈希族时，我们将利用到汉明图（Hamming Graphs）。设k和q为正整数，汉明图$H(k, q)$以所有q元集上的k元组为顶点集，两个k元组是相连的当且仅当它们恰好在一个位置不同。这个图也被称为是k维q元超立方体。这里不妨令该q元集为$[q]$。

我们会用到很多第四章中已经介绍的图论知识。当我们谈论到超图时，实际上是说一对$\mathcal{G}=(V(\mathcal{G}),E(\mathcal{G}))$，其中顶点集$V(\mathcal{G})$被当做前$n$ 个正整数的集合$[n]$，边集被当做是$[n]$ 的一些子集之并。图$\mathcal{G}$是线性的当且仅当对所有不同的边$A,B\in E(\mathcal{G})$，都有$|A\cap B|\leq 1$。我们说图$\mathcal{G}$是r-均衡的，如果对所有边$A\in E(\mathcal{G})$，都有$|A|=r$。

一个r-均衡的超图$\mathcal{G}$是r-部的，如果它的顶点集$V(\mathcal{G})$可以被染成r种颜色，使得$\mathcal{G}$中没有边含有颜色相同的两个顶点。在这样一个染色中，$V(\mathcal{G})$的那些颜色集，即相同颜色的顶点集，被称为是$\mathcal{G}$的不同顶点部。本文主要考虑r-均衡r-部的超图，且每个部分都具有相同的大小q。随后，我们会发现这类超图的边集与某个$r\times|E(\mathcal{G})|$的q元矩阵是等价的。

给定一个r-均衡超图的集合$\mathcal{H}$，一个$\mathcal{H}$-free r-均衡的超图是指这样一个图，它不含$\mathcal{H}$中的任何元素。图兰数（Turán Numbers）$ex_r(n,\mathcal{H})$表示n个顶点上的$\mathcal{H}$-free r-均衡超图的最大边数。在本章中，我们会讨论若干个超图上的图兰问题。

以下稀疏超图的内容第四章已经提到过，我们不妨复习一遍。Brown，Erdős和Sós[39,40]引入了函数$f_r(n,v,e)$来表示n个顶点的r-均衡超图，若其不包含由v 个点张成的e 条边，则其能含有的最大边数。换句话说，在这种超图中，任意e条边的并都含有至少$v+1$个顶点。这类超图被称为是$G(v,e)$-free 的超图。Ruzsa 和Szemerédi[119]著名的(6,3)-定理指出

$$n^{2-o(1)}<f_3(n,6,3)=o(n^2). \tag{5-1}$$

这被Alon和Shapira[14]推广至

$$n^{k-o(1)}<f_r(n,3(r-k)+k+1,3)=o(n^k). \tag{5-2}$$

当后文考虑完美哈希族的一些问题时，我们会用到这些界。若要阅读有关图兰问题的更多信息，文献[78]及其参考文献是不错的选择。

当$f_r(n,v,e)$的定义被限定于r-均衡r-部且每部恰好有q个顶点的超图时，我们使用记号$f_r^*(q,v,e)$来表示对应的最大边数。注意到，$f_r^*(q,v,e)\leq f_r(rq,v,e)$。

接下来，我们不妨重温超图圈与彩虹圈的定义。对$k\geq 2$，超图$\mathcal{G}$中的一个圈是顶点与边的交错列，$v_1,A_1,v_2,A_2,\ldots,v_k,A_k,v_1$，且有如下性质

(a) $v_1,v_2,\ldots,v_k$是$\mathcal{G}$的不同顶点，

(b) $A_1,A_2,\ldots,A_k$是$\mathcal{G}$的不同边，

(c) 对$1\leq i\leq k-1$和$v_k,v_1\in E_k$有$v_i,v_{i+1}\in A_i$。

可以验证，对$2 \leq i \leq k$有$A_{i-1} \cap A_i = \{v_i\}$，且$A_k \cap A_1 = \{v_1\}$。

接下来我们将给出彩虹圈的定义。令$\mathcal{G}$是一个线性的r-均衡超图。一个k-圈

$$v_1, A_1, v_2, A_2, \ldots, v_k, A_k, v_1$$

被称为是彩虹k-圈，如果$v_1, \ldots, v_k$落在$V(\mathcal{G})$的k个不同的部中。对r-均衡超图来说，一个彩虹k-圈存在仅当$k \leq r$。

令$\mathcal{G}$是一个r-均衡r-部的线性超图，且每部的大小为q。假设$\mathcal{G}$没有彩虹圈，则我们用$g_r^*(q)$来表示$g_r^*(q)$所能含有的最大边数。引理5.6.1说明了$g_r^*(q)$大的超图可以被用来构造好的完美哈希族。

5.2.3 加法数论

文献[11,78]中已经证明了人们可以利用一些加法数论的方法来构造具有分离性质的码或集族。这里我们要用到4.3.2节中一些sum-free集的知识。考虑一个线性方程$\sum_{i=1}^{s} a_i m_i = 0$，有整系数$a_1, \ldots, a_s$，未知数$x_i$。这个方程是齐次的如果有$\sum_{i=1}^{s} a_i = 0$。我们说集合$M \subseteq [n]$不含上述方程的非平凡解，如果$m_i \in M$且$\sum_{i=1}^{s} a_i m_i = 0$，则所有$m_i$相等。这里关于非平凡解的定义是Ruzsa[118] 原始定义的一个简化版本。给定一个集合$R = \{b_1, \ldots, b_r\}$，这是r个不同的非负整数。一个集合M被称为是R_L-sum-free的当且仅当对任何$3 \leq l \leq L \leq r$与任何l-子集$S = \{b_{j_1}, b_{j_2}, \ldots, b_{j_l}\} \subseteq R$，方程

$$(b_{j_2} - b_{j_1})m_1 + (b_{j_3} - b_{j_2})m_2 + \cdots + (b_{j_l} - b_{j_{l-1}})m_{l-1} + (b_{j_1} - b_{j_l})m_l = 0$$

在M中除了平凡解$m_1 = m_2 = \cdots = m_l$之外都无解。

我们将使用R_3-sum-free集来构造三行强度为三的完美哈希族，使用R_4-sum-free集来构造四行强度为四的完美哈希族。关于R_3-sum-free集，我们会用到Erdős，Frankl和Rödl[68]以及Ruzsa[118] 的经典结果（证明可以参考引理4.3.10）。

引理5.2.1. *对任意正整数r，都存在一个$\gamma_r > 0$，使得对任何整数q，都能找到一个R_3-sum-free集$M \subseteq [q]$满足$|M| > qe^{-\gamma_r \sqrt{\log q}}$。*

关于R_4-sum-free集，通过一些变形，我们可以联合Alon，Fischer与Szegedy[11]的引理3.2和推论3.3，用引理4.3.7与引理4.3.8的方法证明如下结果。

引理5.2.2. 存在一个集合$M \subseteq \{0, 1, \ldots, \lfloor (q-1)/(\mu+5) \rfloor\}$满足

$$|M| \geq q e^{-\gamma(\log q)^{3/4}},$$

使得M不含以下任何一个方程的非平凡解。

$$\begin{cases} 2m_1 + 3m_2 + \mu m_3 - (\mu+5)m_4 & = 0 \\ 5m_1 + (\mu+3)m_2 - 3m_3 - (\mu+5)m_4 & = 0 \\ 5m_1 + \mu m_2 - 2m_3 - (\mu+3)m_4 & = 0 \\ 2m_1 + 3m_2 - 5m_3 & = 0 \\ 5m_1 + \mu m_2 - (\mu+5)m_3 & = 0 \\ 2m_1 + (\mu+3)m_2 - (\mu+5)m_3 & = 0 \\ 3m_1 + \mu m_2 - (\mu+3)m_3 & = 0 \end{cases} \tag{5-3}$$

这里γ是一个常数，且$\mu = \lceil 2^{\sqrt{\log q}} \rceil$。

5.2.4 一些引理

下面的引理是Erdös和Kleitman[71]的一个结果的变形。

引理5.2.3. 任何r-均衡的超图$\mathcal{G}$都包含一个r-均衡r-部超图$\mathcal{H}$，使其每部的大小为q或$q+1$，并满足

$$\frac{|E(\mathcal{H})|}{|E(\mathcal{G})|} \geq \frac{r!}{r^r}.$$

证明. 令$|V(\mathcal{G})| = n$，取q为满足$rq \leq n < r(q+1)$的整数。我们仅对$n = rq$证明该引理，其它情况下我们可以把每部大小设为$q+1$。只需找到一个$V(\mathcal{G})$的划分π，满足$\pi = \{B_1, \ldots, B_r\}$且$|B_i| = q$对$1 \leq i \leq r$，使得$\mathcal{F}_\pi = \{A \in E(\mathcal{G}) : |A \cap B_i| = 1 \; for \; all \; 1 \leq i \leq r\}$ 包含我们所期望的边的数目。令$P(\mathcal{G})$为$V(\mathcal{G})$的所有可能划分的集合。让我们计算$N := |\{(A, \pi) : A \in E(\mathcal{G}),\, \pi \in P(\mathcal{G}),\, |A \cap B_i| = 1 \; for \; every \; B_i \in \pi\}|$的数量。可以算出，任何$A \in E(\mathcal{G})$被包含在$P(\mathcal{G})$的$\frac{|P(\mathcal{G})| \cdot q^r}{\binom{rq}{r}}$个满足条件的元素中。因此，通过“算两次”的方法，存在某个$\pi \in P(\mathcal{G})$使得$\mathcal{F}_\pi$包含至少

$$\frac{|E(\mathcal{G})| \cdot |P(\mathcal{G})| \cdot q^r / \binom{rq}{r}}{|P(\mathcal{G})|} = \frac{|E(\mathcal{G})| \cdot q^r}{\binom{rq}{r}}$$

条$E(\mathcal{G})$的边。那么，这个特殊的π将诱导出一个r-均衡r-部的超图$\mathcal{H}$包含我们所期望的边的数目。 □

这个引理意味着对任何r-均衡的超图$\mathcal{G}$，只要$|V(\mathcal{G})|$足够大，那么就存在一个r-部子图$\mathcal{H} \subseteq \mathcal{G}$使得$|E(\mathcal{H})|$和$|E(\mathcal{G})|$拥有相同的数量级。换句话说，由引理5.2.3我们可以推知$f_r(rq, v, e) = \Theta(f_r^*(q, v, e))$。

我们还会用到下面的简单结论。

引理5.2.4. *加入G是一个n个顶点的有限图。若G不含圈，则G有最多$n-1$条边。*

证明. G肯定含有一个顶点的度为1，这是因为G中的每条路径都是有限的，都必须含有一个终点。从G中选取一个度为1的顶点，则删去它，通过对$|V|$进行归纳假设容易推出我们的结论。 □

5.3 Johnson型上界

本节的目的是为可分哈希族建立一个Johnson型的上界，我们会用它来证明定理5.1.5。为了得到这个界，我们的想法是删去可分哈希族的表示矩阵的某些行以及仔细挑选的某些列，然后证明剩下的矩阵会满足某些更弱的可分性质。我们把这个用迭代方法得到的界称为Johnson型的界，是因为它与编码理论中的Johnson界很相近。我们常用M来表示一个可分哈希族的表示矩阵。

引理5.3.1. *设$1 \leq l \leq N$为一个正整数，那么我们有$C(N, q, \{w_1, ..., w_t\}) \leq q^l + \max\{u - 1, C(N-l, q, \{w_1 - 1, ..., w_t\})\}$。实际上，在不等式的右边我们可以把“$-1$”放在任何一个$w_i$, $1 \leq i \leq t$之后。*

证明. 选出M的l行，用L表示这些行的集合。记$\mathcal{A} \subseteq Y^l$为极大的列的集合，使得这些列限定到$L$都是不同的。我们只需一列如果有若干列限定到$L$上是相同的。容易得出，$|\mathcal{A}| \leq q^l$，这是因为最多有$q^l$个不同的$l$长向量。把所选的$l$行和$\mathcal{A}$中所含的向量都从$M$中删去。用$M'$表示剩下的矩阵。那么，$M'$是一个$q$元$(N-l) \times (n - |\mathcal{A}|)$矩阵。若$n - |\mathcal{A}| \leq u - 1$，结论成立。反之，只需证明$M'$是某个$\{w_1, \ldots, w_i - 1, \ldots, w_t\}$型可分哈希族的表示矩阵，其中，$1 \leq i \leq t$可以任意的。

如若不然，对某个i，M'不是$\{w_1, \ldots, w_i - 1, \ldots, w_t\}$-可分的。不失一般性，我们令$i = 1$。那么，存在$t$个$M'$的列的子集$C_1, \ldots, C_t$，$|C_1| = w_1 - 1$且$|C_i| = w_i$，$2 \leq i \leq t$，使得$M'$的任何一行都不能区分$C_1, \ldots, C_t$。令$c$为$C_2$的任意一列，并令$c'$是$\mathcal{A}$中的一列，使

得$c'|_L = c|_L$。我们对$\mathcal{A}$的定义保证了这样的$c' \in \mathcal{A}$一定存在。因此，在原矩阵M中，没有行可以区分$C_1 \cup \{c'\}, C_2, \ldots, C_t$。这与$M$是$\{w_1, \ldots, w_t\}$-可分的相矛盾。因此，$M'$满足我们所期望的可分性，该引理可以由事实$n - |\mathcal{A}| \leq C(N - l, q, \{w_1 - 1, ..., w_t\}$与$|\mathcal{A}| \leq q^l$证出。 □

注记5.3.2. 我们认为该*Johnson*型界是十分有趣且重要的，因为它指出了可分哈希族的结构中所隐含的信息。

作为引理5.3.1的第一个应用，我们将用它来证明定理5.1.5。

注意到，通过在上界的表达式中引入一个求较大值的函数我们可以略去制约条件$C(\lfloor N/(u-1) \rfloor, q, \{w_1, \ldots, w_t\}) \geq u$（就如引理5.3.1中的情形一样）。此外，当$N \geq u - 1$与$q$足够大，例如$q \geq u$时，$C(\lfloor N/(u-1) \rfloor, q, \{w_1, \ldots, w_t\}) \geq u$总是成立的。

定理*5.1.5*的证明. 可以验证$N = r\lceil N/(u-1) \rceil + (u - 1 - r)\lfloor N/(u-1) \rfloor$。我们重复利用引理5.3.1$u-1$次，其中，分别令$l$等于$\lceil N/(u-1) \rceil$ r次，等于$\lfloor N/(u-1) \rfloor$ $u - 1 - r$次。则定理可以由一个简单的事实$C(0, q, \{1\}) = 0$推得。 □

注记5.3.3. 并不难看出，我们的界是改进了定理*5.1.4*，也改进了文献[19]和文献[32]的结论。我们发现$\lceil N/(u-1) \rceil$是用我们的方法能得到的最好的指数项，这是因为要降低指数项，就必须降低在删除过程中牵涉到的l的最大值。换句话说，我们需要对N行进行更加细致地划分，因此就需要更多的删除轮数。然而，我们最多可以进行$u-1$次删除，这是因为若$t - 1$且$N > 0$时，$C(N, q, \{w_1, \ldots, w_t\})$可以为任意大。

注记5.3.4. 由于防诬陷码是一类特殊的可分哈希族，并不难发现我们的界包含文献[34]的定理*1*。由文献[34]中的构造*2*和构造*3*可知，定理*5.1.5*在$q \geq N$，$\{w_1, \ldots, w_t\} = \{1, w\}$，$N \equiv 1 \pmod{w}$或$q = \Omega(N^2)$，$\{w_1, \ldots, w_t\} = \{1, 2\}$时是近似最优的。接下来的小节里，我们将给出一个构造，这个构造表明当$N = u - 1$时定理*5.1.5*也是近似最优的。

5.4 $t-1$行的t-完美哈希族的构造

本节的目标是对任意正整数$q \geq 2$和$N \geq 2$构造出一个$PHF(N; Nq^{N-1}, q^{N-1} + (N-1)q^{N-2}, N+1)$。我们构造的一个优点是它推广了之前的许多构造。当$N = 2$时，$PHF(2; 2q, q+1, 3)$的构造已经出现于文献[103]和文献[141]内。当$N = 3$时，$PHF(3; 3q^2, q^2+$

$2q, 4)$的构造也出现于众多的文献里，例如，Hollmann 等人[85]，Blackburn[27]，Stinson等人[131]以及Bazrafshan等人[19]。

让我们从$N = 3$开始，把它作为一个阐释我们想法的简单例子。

例5.4.1. ([19,27,85,131]) 对任何整数$q \geq 2$，都存在一个$PHF(3; 3q^2, q^2 + 2q, 4)$。

证明. 我们首先构造一个$3\times q^2$的子矩阵，其中，字母集是一个(q^2+2q)元的集合$\{(x, y), (x, 0), (0, y) : 1 \leq x, y \leq q,\ x, y \in \mathbb{Z}\}$，

$$\begin{pmatrix} (1,1) & (1,2) & \cdots & (1,q) & (2,1) & \cdots & (2,q) & \cdots & (q,1) & \cdots & (q,q) \\ (0,1) & (0,2) & \cdots & (0,q) & (0,1) & \cdots & (0,q) & \cdots & (0,1) & \cdots & (0,q) \\ (1,0) & (1,0) & \cdots & (1,0) & (2,0) & \cdots & (2,0) & \cdots & (q,0) & \cdots & (q,0) \end{pmatrix}.$$

我们把这个子矩阵的三行分别$A_0,\ A_1,\ A_2$，那么，我们期望构造的完美哈希族的表示矩阵可以被表示如下

$$\begin{pmatrix} A_0 & A_2 & A_1 \\ A_1 & A_0 & A_2 \\ A_2 & A_1 & A_0 \end{pmatrix}.$$

不难看出，这是一个$q^2 + 2q$元字母集上的$3 \times 3q^2$矩阵。不难证明这确实是一个4-完美哈希族的表示矩阵。 □

在上面的矩阵中，A_0的作用就像一个恒等映射一样，它保持了$\{(x, y) : 1 \leq x, y \leq q,\ x, y \in \mathbb{Z}\}$中的每个元素不变，同时，$A_i$，$i = 1,\ 2$的作用就像一个映射，它们把$(x, y)$的第$i$个分量映射为0。实际上，这个简单的构造背后蕴含的想法可以被进一步推广。

不妨回忆之前汉明图的定义。取一个k维的q元超立方体，则$|V(\mathcal{A})| = q^k$。对$1 \leq i \leq k$与任意的$\alpha = (\alpha(1), \ldots, \alpha(k)) \in V(\mathcal{A})$，定义$\pi_i$为一个映射，它使$\alpha(i)$为零，但保持$\alpha$的其它所有位置。我们说$\pi_i$分离了一个集合$S \subseteq V(\mathcal{A})$，如果$\pi_i(\alpha) \neq \pi_i(\beta)$对任意不同的$\alpha,\ \beta \in S$都成立。文献[27]的命题1建立了一个关于这些映射的重要性质。我们将其列举如下。

引理5.4.2. ([27]) 设$S \subseteq V(\mathcal{A})$是任意一个$t$元子集，满足$t \leq k$，则$S$被$\pi_1, \ldots, \pi_k$中的至少$k - t + 1$个函数所分离。

下面的引理是上述引理的一个简单结论。

引理5.4.3. 令π_i $(1 \le i \le k)$为上述定义的函数，用π_0标记恒等映射，它满足$\pi_0(\alpha) = \alpha$对每个$\alpha \in V(\mathcal{A})$都成立。假如$S \subseteq V(\mathcal{A})$是一个$t$元子集，使得$t \le k+1$，则$\pi_0, \pi_1, \ldots, \pi_k$中的至多$t-1$个函数不能分离$S$。

证明. 利用引理5.4.2，且考虑事实π_0分离$V(\mathcal{A})$的每个子集。 □

现在我们可以证明定理5.1.7。

定理5.1.7的证明. 取一个q元的$N-1$维超立方体$\mathcal{A}$。显然$|V(\mathcal{A})| = q^{N-1}$。令$\pi_0, \pi_1, \ldots, \pi_{N-1}$为上述定义的映射。我们期望的完美哈希族可以被表示为如下矩阵。

$$\begin{pmatrix} \pi_0(\mathcal{A}) & \pi_{N-1}(\mathcal{A}) & \cdots & \cdots & \pi_1(\mathcal{A}) \\ \pi_1(\mathcal{A}) & \pi_0(\mathcal{A}) & \cdots & \cdots & \pi_2(\mathcal{A}) \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ \pi_{N-1}(\mathcal{A}) & \pi_{N-2}(\mathcal{A}) & \cdots & \cdots & \pi_0(\mathcal{A}) \end{pmatrix},$$

对每个$0 \le i \le N-1$，$\pi_i(\mathcal{A}) := (\pi_i(\alpha))_{\alpha \in V(\mathcal{A})}$是一个$1 \times |V(\mathcal{A})|$的子矩阵。记这个表示矩阵为$M$，则$M$是一个$N \times Nq^{N-1}$的矩阵。记$Y = \cup_{i=0}^{N-1} \pi_i(\mathcal{A})$为字母集。不难看出对每个$1 \le i \le N-1$都有$|\{\pi_i(\alpha) : \alpha \in V(\mathcal{A})\}| = q^{N-2}$与$|\{\pi_0(\alpha) : \alpha \in V(\mathcal{A})\}| = q^{N-1}$。则可以验证$|Y| = q^{N-1} + (N-1)q^{N-2}$。从而可以得知$M$是一个$(N; Nq^{N-1}, q^{N-1} + (N-1)q^{N-2})$-哈希族的表示矩阵。

现在我们只需证明这个哈希族实际上是一个$(N+1)$-完美哈希族。把M看作是N个列块的级联，记为$(C_1|C_2|\cdots|C_N)$，其中$|C_1| = |C_2| = \cdots = |C_N| = q^{N-1}$。取$M$的列的任意一个$(N+1)$元子集$S$。我们将证明必存在$M$的一行分离$S$。若$S \subseteq C_i$对某个$1 \le i \le N$成立，那么$C_i$的第$i$行，即对应于$\pi_0$的那一行，可以分离$S$，这是因为对任意不同的$\alpha, \beta \in V(\mathcal{A})$都有$\pi_0(\alpha) \ne \pi_0(\beta)$。如若不然，令$C_{i_1}, \ldots, C_{i_j}$为与$S$有非空交集的列块，其中$j \ge 2$是一个正整数。对$1 \le l \le j$，记$C_{i_l} \cap S = S_l$。那么有$\sum_{l=1}^{j} |S_l| = N+1$与$|S_l| \le N$对每个$l$都成立。由引理5.4.3可知，$C_{i_l}$的最多$|S_l|-1$行不能分离$S_l$。由于$\sum_{l=1}^{j}(|S_l|-1) = N+1-l \le N+1-2 = N-1 < N$，则必存在$(C_1|C_2|\cdots|C_N)$的一行可以分离$\cup_{i=1}^{l} S_l = S$。 □

注记5.4.4. 我们的构造有一个重要的性质，它满足

$$\lim_{q\to\infty}\frac{Nq^{N-1}}{q^{N-1}+(N-1)q^{N-2}}=N$$

且该构造是渐进最优的，因为定理*5.1.5*给出了$p_{N+1}(N,q)\le Nq$。注意到，对任意w_i满足$w_i\ge 1$与$\sum_{i=1}^{t}w_i=u$，一个u-完美哈希族都是$\{w_1,\dots,w_t\}$-可分的。联合定理*5.1.5*与定理*5.1.7*可得

$$\lim_{q\to\infty}\frac{C(u-1,q,\{w_1,\dots,w_t\})}{q}=u-1,$$

这给予问题*5.1.6*一个否定的回答。此外，考虑到事实上任何$(\lfloor(t/2+1)^2\rfloor)$-完美哈希族也是$t$-*IPP*码，可以看出我们的构造也验证了猜想*5.1.8*的正确性。

注记5.4.5. 值得注意的是文献*[27]*（一篇未发表的手稿）的命题*2*也注意到了$\lim_{q\to\infty}\frac{p_u(u-1,q)}{q}=u-1$。但是作者使用了优化的方法，没有给出确切的构造。

引理5.4.2的证明也给出了一个汉明图的结论，该结论似乎也很有意思。

推论5.4.6. 将$H(k,q)$的边集用k种颜色染色，使得边(α,β)被染为颜色i，如果α与β在他们的第i个位置不同。那么$H(k,q)$不包含一个两两边都不同色的圈。

5.5 三行且强度为三的完美哈希族

我们已经提到过若$(u-1)\nmid N$，则很难决定定理5.1.5中的指数$\lceil N/(u-1)\rceil$是否是紧的。在接下来的两节中，我们将处理这类问题的两个小例子，即，$N=u=3$与$N=u=4$。当$N=u=3$时，对应的可分哈希族只有两种可选的类型，即，$\{1,2\}$-可分与3-完美哈希。Bazrafshan和Trung[20]证明了$C(3,q,\{1,2\})\le q^2$且$SHF(3;q^2,q,\{1,2\})$对$q\ge 2$是存在的。Walker和Colbourn[141]猜测$p_3(3,q)=o(q^2)$。在这一节中，我们将证明这个猜想，并说明$q^{2-o(1)}<p_3(3,q)=o(q^2)$。此外，上界可以被拓展到$p_t(t,q)$与$C(u,q,\{w_1,\dots,w_t\})$，其中$\sum_{i=1}^{t}w_i=u$。

让我们从一个简单的引理开始。注意到我们将不区分完美哈希族与其表示矩阵。我们说哈希族的一个向量x（即表示矩阵的一列）有一个特殊的位置i，如果对其它任何向量（列），y，$y\ne x$，都有$y(i)\ne x(i)$。

引理5.5.1. *用X记$PHF(N;n,q,t)$的列集。通过删去最多Nq个向量，我们可以得到一个子集$X^* \subseteq X$使得X^*中不含含有特殊位置（在新集合X^*中）的向量。*

证明. 我们用一个贪婪算法来构造X^*。从X中删去x_1，如果x_1在X中有一个特殊位置。记$X_1 = X - \{x_1\}$。一般的，如果$x_{i+1} \in X_i$在X_i内有一个特殊位置，我们从X_i中删去x_{i+1}，并记$X_{i+1} = X_i - \{x_{i+1}\}$。一直延续这个步骤，直到我们得到一个$X^*$，它的任何一个向量都不含有特殊位置。由于我们对每个位置$i \in [N]$可以删去每个元素$y \in [q]$最多一次，我们将删去最多Nq个向量。 □

因为接下来要考虑的完美哈希族大小都至少为$q^{1+\epsilon}$，这里ϵ为某个正常数。那么当N固定，q足够大时，从X中删去Nq个向量的做法可以被忽略。用$PHF^*(N;n,q,t)$标记满足每个向量都不含特殊位置的完美哈希族（来自于$PHF(N;n,q,t)$）。我们用$p_t^*(N,q)$来标记n对应的最大值。

引理5.5.2. *在一个$PHF^*(t;n,q,t)$中，任意两个向量最多有两个位置相同。*

证明. 如若不然，下面的子矩阵必被包含在这样的$PHF^*(t;n,q,t)$的表示矩阵中

$$\begin{pmatrix} \boldsymbol{\alpha_1(1)} & \boldsymbol{\alpha_2(1)} & * & * & * & * \\ \boldsymbol{\alpha_1(2)} & \boldsymbol{\alpha_2(2)} & * & * & * & * \\ \boldsymbol{\alpha_1(3)} & * & \boldsymbol{\alpha_3(3)} & * & * & * \\ \vdots & * & * & \ddots & * & * \\ \vdots & * & * & * & \ddots & * \\ \boldsymbol{\alpha_1(t)} & * & * & * & * & \boldsymbol{\alpha_t(t)} \end{pmatrix},$$

其中，每一行的粗体元素是相同的。α_1, α_2是两个向量，满足$\alpha_1(i) = \alpha_2(i)$对$i = 1, 2$都成立，因为$\alpha_1$不含有特殊位置，存在$\alpha_3, \ldots, \alpha_t$使得$\alpha_j(j) = \alpha_1(j)$对$3 \leq j \leq t$都成立。因此，子矩阵的所有行都不能分离$\{\alpha_1, \ldots, \alpha_t\}$，这违反了$t$-完美哈希的性质。 □

下面的两个观察是非常有用的。

观察1: 一方面，任何$N \times n$的q元矩阵M都可以被看成是一个N-均衡N-部超图，$\mathcal{G} = (V(\mathcal{G}), E(\mathcal{G}))$，每个顶点部的大小都是$q$，且顶点集被定义为$V(\mathcal{G}) = \cup_{i=1}^{N} V_i$，对$1 \leq i \leq N$，我们有$V_i = \{(i,j) : 1 \leq j \leq q\}$，边集被定义为$E(\mathcal{G}) = \{\{(i, x(i))\}_{i=1}^{N} : x = \{x(i)\}_{i=1}^{N} \; is \; a \; column \; of \; M\}$。

观察2: 另一方面，给定一个N-均衡N-部超图$\mathcal{G}=(V(\mathcal{G}),E(\mathcal{G}))$，每部的大小为$q$。我们可以把$E(\mathcal{G})$当做是某个$N\times|E(\mathcal{G})|$的$q$元矩阵$M$。注意到$V(\mathcal{G})$可以被划分为$N$个两两不交的$q$元集。我们可以令$V_i=\{(i,j):1\leq j\leq q\}$，$1\leq i\leq N$，其中，第一个位置$i$对应于第$i$部$V_i$，第二个位置$j$对应于$V_i$中的第$j$个顶点。那么，矩阵$M$可以由如下方式构成，其列集为$\{x=\{x(i)\}_{i=1}^N:\{(i,x(i))\}_{i=1}^N\in E(\mathcal{G})\}$。这样的$M$被称为是$E(\mathcal{G})$的表示矩阵。

上面两个观察建立了多部图与q元矩阵的桥梁。回忆$f_r^*(n,v,e)$的定义。我们有

引理5.5.3. $p_3^*(3,q)\leq f_3^*(q,6,3)\leq p_3(3,q)$.

证明. 不难看出，$PHF^*(3;n,q,3)$存在当且仅当下面的构型不包含在其表示矩阵中。

$$\begin{pmatrix} a & * & a \\ b & b & * \\ * & c & c \end{pmatrix},$$

这些星号都不属于$\{a,b,c\}$.

我们把这个构型称为是三角形，因为这三列都不含公共的元素且两列恰好有一个公共元素。一方面，我们有$f_3^*(q,6,3)\leq p_3(3,q)$，这是因为对哈希族的任意三列，如果没有行可以分离它们，那么对每一行都存在两个相等的元素。因此，这些列（或者说对应的边）必是由最多六个顶点所张成的。故边数达到$f_3^*(q,6,3)$的对应超图必是3-完美哈希的。另一方面，若$PHF^*(3;n,q,3)$的某三列含最多六个顶点，那么要不存在两列有两个相同的元素，要不这三列构成一个三角形。这两种情形在$PHF^*(3;n,q,3)$中都是被禁止的。因此我们有$p_3^*(3,q)\leq f_3^*(q,6,3)$。引理得证。 □

定理5.5.4. $p_3(3,q)=f_3(3q,6,3)+O(q)$，且对任意$\epsilon>0$，$q^{2-\epsilon}<p_3(3,q)=o(q^2)$对足够大的$q$都成立。

证明. 利用引理5.2.3，引理5.5.1，引理5.5.3与不等式(5-1)。 □

作为引理5.3.1的第二个应用，$p_3(3,q)$的上界可以被拓展到$p_t(t,q)$和$C(u,q,\{w_1,\ldots,w_t\})$。

推论5.5.5. 对任何$t\geq 3$，$\sum_{i=1}^t w_i=u$，有$C(u,q,\{w_1,\ldots,w_t\})=o(q^2)$。特别的，对任何$t\geq 3$有$p_t(t,q)=o(q^2)$。

证明. 利用引理5.3.1与定理5.5.4。 □

注记5.5.6. 利用图移除引理[9]也能证明$p_t(t,q) = o(q^2)$，文献[11]和[16]提到了图移除引理在这类问题中的应用。但是，我们利用引理5.3.1给出的证明要简单多了。当$1 + w \leq q$时，文献[20]说明了$C(1 + w, q, \{1, w\}) \leq q^2$。此外，对任意素数幂$q$，都存在一个$SHF(w + 1; q^2, q, \{1, w\})$。因此，对$C(u, q, \{w_1, \ldots, w_t\})$，$t = 2$，我们不能决定$C(w_1 + w_2, q, \{w_1, w_2\}) = \Omega(q^2)$或者$C(w_1 + w_2, q, \{w_1, w_2\}) = o(q^2)$。决定$C(w_1 + w_2, q, \{w_1, w_2\})$的确切阶将会是一个很有趣的问题。

结合4.4节中提到的超图构造方法，由引理5.2.1（或者直接由推论4.4.4）可知如下定理。

定理5.5.7. 存在一个常数γ满足$p_3(3, q) > q^2 e^{-\gamma\sqrt{\log q}}$。

5.6 四行且强度为四的完美哈希族

构造满足$p_4(4, q) > q^{2-o(1)}$的4-完美哈希族要困难得多了。在构造中我们会用到彩虹圈与R-sum-free集，实际上，我们希望证明如下引理。

引理5.6.1. $p_t^*(t, q) \leq g_t^*(q) \leq p_t(t, q)$.

证明. 首先，我们将证明任何$PHF^*(t; n, q, t)$ 都能导出一个t-均衡t-部的线性超图$\mathcal{G}$，且其不含有任何彩虹圈。用M记该哈希族的表示矩阵，则M也能被看作是$E(\mathcal{G})$的表示矩阵。由引理5.5.2，M（或者说$E(\mathcal{G})$）已经是线性的了。只需证明M不包含彩虹圈。如若不然，M的被标记为$\alpha_1, \ldots, \alpha_k$的列（也是$E(\mathcal{G})$对应的边）形成一个彩虹$k$-圈$v_1, \alpha_1, v_2, \alpha_2, \ldots, v_k, \alpha_k, v_1$，且$k \leq t$。由观察1可知，$V(\mathcal{G})$的第$i$部可以被定义为$V_i = \{(i, j) : j \in [q]\}$，其中，第一个分量对应于$M$的第$i$行，第二个分量对应于$[q]$的第$j$个元素。不失一般性，我们可以假设$v_i$取自第$i$个顶点集。那么，可以推出$\alpha_i(i) = \alpha_{i+1}(i)$对$1 \leq i \leq k - 1$与$\alpha_k(k) = \alpha_1(k)$成立。下面由这样一个彩虹$k$-圈导出的矩阵必定被包含在$M$中

$$\begin{pmatrix} \boldsymbol{\alpha_1(1)} & \boldsymbol{\alpha_2(1)} & \alpha_3(1) & \alpha_4(1) & & \alpha_{k-1}(1) & \alpha_k(1) \\ \alpha_1(2) & \boldsymbol{\alpha_2(2)} & \boldsymbol{\alpha_3(2)} & \alpha_4(2) & & \alpha_{k-1}(2) & \alpha_k(2) \\ \alpha_1(3) & & \boldsymbol{\alpha_3(3)} & \boldsymbol{\alpha_4(3)} & & \alpha_{k-1}(3) & \alpha_k(3) \\ \vdots & & & \ddots & & \vdots & \vdots \\ \vdots & & & & \ddots & \boldsymbol{\alpha_{k-1}(k-1)} & \boldsymbol{\alpha_k(k-1)} \\ \boldsymbol{\alpha_1(k)} & & & & & & \boldsymbol{\alpha_k(k)} \end{pmatrix},$$

其中，每一行的两个加粗的元素是相等的。注意到，在矩阵中，列表示了边且每列的元素表示了包含在对应边中的顶点。容易看出，M的前k行中任何一行都不能分离$\{\alpha_1, \ldots, \alpha_k\}$。注意到$M$的列都不含特殊位置，从而存在$\alpha_{k+1}, \ldots, \alpha_t$使得对$k+1 \leq j \leq t$有$\alpha_j(j) = \alpha_1(j)$，这个关系也能被表示为

$$\begin{pmatrix} \boldsymbol{\alpha_1(k+1)} & \boldsymbol{\alpha_{k+1}(k+1)} & * & * & * & * \\ \boldsymbol{\alpha_1(k+2)} & * & \boldsymbol{\alpha_{k+2}(k+2)} & * & * & * \\ \vdots & * & * & \ddots & * & * \\ \vdots & * & * & * & \ddots & * \\ \boldsymbol{\alpha_1(t)} & * & * & * & * & \boldsymbol{\alpha_t(t)} \end{pmatrix}.$$

因此，M中剩下的$t-k$行不能分离$\{\alpha_1, \alpha_{k+1}, \ldots, \alpha_t\}$。故我们可以总结到$M$没有行可以分离$\{\alpha_1, \ldots, \alpha_t\}$，这与$t$-完美哈希的性质矛盾了。

接下来只需说明对任何t-均衡t-部线性超图（每部大小都是q）$\mathcal{G}$，若它没有彩虹圈，则可以导出一个$PHF(t; n, q, t)$满足$n = |E(\mathcal{G})|$。我们仍然用M来记$E(\mathcal{G})$的表示矩阵。我们声明如果存在一个M的$t \times t$子矩阵T使得没有行可以分离它，那么由T诱导的超图会包含一个彩虹k-圈，$k \leq t$。

我们将对t使用数学归纳法。当$t = 2$时，一个2×2的子矩阵总是可以被两行中的一行分离，如果子矩阵的两列是不同的。当$t = 3$时，如果一个3-均衡3-部线性超图的3×3子矩阵不能被它的任何一行分离，那么，这个子矩阵实际上会形成一个如同引理5.5.3所定义的三角形。可以验证，这个三角形可以被表示为一个彩虹3-圈，$\{a, E_1, b, E_2, c, E_3\}$，其中$E_1, E_2, E_3$为三角形的三条边。现在，我们假设声明对$t-1$是正确的。取一个$t \times t$的矩阵$T$，它的列集被标记为$C = \{\alpha_1, \ldots, \alpha_t\}$，行集被标记为$R = \{r_1, \ldots, r_t\}$，且满足没有行可以分离$C$。对每个$1 \leq i \leq t$，我们记$C_i = C - \{\alpha_i\}$以及$R_i = R - \{r_i\}$。此外，我们用$T_{ij}$来记由$R_i$和$C_j$所形成的$(t-1) \times (t-1)$子矩阵。此时，对任何子矩阵$T_{ij}$，一定存在

一行可以分离它的所有列，否则，由归纳假设可知，T_{ij}必包含某个长度为$k \leq t-1$的彩虹k-圈。

不失一般性，假设r_1分离了C_t。注意到这一行不能分离C，因此，我们能假设$\alpha_t(1) = \alpha_1(1)$。再考虑$T_{11}$，存在$R-\{r_1\}$中的一行可以分离$C-\{\alpha_1\}$。我们令这一行为$r_2$。类似的，存在$2 \leq j \leq t$使得$\alpha_1(2) = \alpha_j(2)$，这是由于$r_2$不能分离$C$。由于$\alpha_1$和$\alpha_t$已经有了某个相等的位置，即，$\alpha_t(1) = \alpha_1(1)$，则有$j \neq t$。假设$\alpha_1(2) = \alpha_2(2)$。现在考虑$T_{22}$，存在$R-\{r_2\}$中的一行可以分离$C-\{\alpha_2\}$。注意到这一行不能是$r_1$，因为$\alpha_1$和$\alpha_t$在它们的第一个位置相等。我们可以设这一行为$r_3$。出于同样的原因，存在$j \in [t], j \neq 2$使得$\alpha_2(3) = \alpha_j(3)$。那么，由$\alpha_1(2) = \alpha_2(2)$可知$j \neq 1$。若$j = t$，我们得证了，因为$\{\alpha_1, \alpha_2, \alpha_t\}$将形成一个彩虹3-圈。因此，我们令$j = 3$。

上述讨论可以由下面的矩阵所表示出来

$$
\begin{pmatrix}
\boldsymbol{\alpha_1(1)} & \alpha_2(1) & \alpha_3(1) & \alpha_4(1) & \cdots & \cdots & \alpha_{t-1}(1) & \boldsymbol{\alpha_t(1)} \\
\boldsymbol{\alpha_1(2)} & \boldsymbol{\alpha_2(2)} & \alpha_3(2) & \alpha_4(2) & \cdots & \cdots & \alpha_{t-1}(2) & \alpha_t(2) \\
\alpha_1(3) & \boldsymbol{\alpha_2(3)} & \boldsymbol{\alpha_3(3)} & \alpha_4(3) & \cdots & \cdots & \alpha_{t-1}(3) & \alpha_t(3) \\
\alpha_1(4) & \alpha_2(4) & \boldsymbol{\alpha_3(4)} & \boldsymbol{\alpha_4(4)} & \cdots & \cdots & \alpha_{t-1}(4) & \alpha_t(4) \\
 & & & \ddots & & & & \\
 & & & & \ddots & & & \\
\alpha_1(i-1) & \cdots & \boldsymbol{\alpha_{i-2}(i-1)} & \boldsymbol{\alpha_{i-1}(i-1)} & & \cdots & \cdots & \alpha_t(i+1) \\
\alpha_1(i) & \cdots & & \boldsymbol{\alpha_{i-1}(i)} & \boldsymbol{\alpha_i(i)} & & \cdots & \alpha_t(i+1) \\
\alpha_1(i+1) & \cdots & & & \boldsymbol{\alpha_i(i+1)} & \boldsymbol{\alpha_{i+1}(i+1)} & \cdots & \alpha_t(i+1) \\
 & & & \ddots & & & & \\
 & & & & \ddots & & &
\end{pmatrix},
$$

其中，每一行中加粗的两个元素是相等的。我们对$T_{i,i}$，$i \geq 3$继续上面的步骤。由我们的选择可知，对所有的$1 \leq j \leq i$，在行r_j中成立$\alpha_{j-1}(j) = \alpha_j(j)$（$\alpha_0$被认为是$\alpha_t$）。因此，$\{r_1, \ldots, r_i\}$中没有行可以分离$T_{i,i}$。我们总是可以假设$r_{i+1} \in R-\{r_i\}$就是分离$C-\{\alpha_i\}$的那一行。所有存在某个$j \in [t], j \neq i$使得$\alpha_i(i+1) = \alpha_j(i+1)$，这是因为$r_{i+1}$不能分离整个的$C$。显然地，$j \neq i-1$。若$j \in \{1, \ldots, i-2\}$或者$j = t$，$j$的这种选择会诱导出一个由$\{\alpha_j, \ldots, \alpha_i\}$形成的彩虹$(i-j+1)$-圈

$$\begin{pmatrix} \boldsymbol{\alpha_j(j+1)} & \boldsymbol{\alpha_{j+1}(j+1)} & * & & * & * \\ * & \boldsymbol{\alpha_{j+1}(j+2)} & \boldsymbol{\alpha_{j+2}(j+2)} & & * & * \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & & \ddots & \vdots \\ & & & & & \\ * & * & * & & \boldsymbol{\alpha_{i-1}(i)} & \boldsymbol{\alpha_i(i)} \\ \boldsymbol{\alpha_j(i+1)} & * & * & & * & \boldsymbol{\alpha_i(i+1)} \end{pmatrix}$$

或者一个由$\{\alpha_1, \ldots, \alpha_i, \alpha_t\}$形成的一个彩虹$(i+1)$-圈

$$\begin{pmatrix} \boldsymbol{\alpha_1(1)} & * & * & & & & \cdots & \boldsymbol{\alpha_t(1)} \\ \boldsymbol{\alpha_1(2)} & \boldsymbol{\alpha_2(2)} & * & & & & \cdots & * \\ * & \boldsymbol{\alpha_2(3)} & \boldsymbol{\alpha_3(3)} & & & & \cdots & * \\ \vdots & \vdots & & \ddots & & & \cdots & \vdots \\ \vdots & \vdots & \vdots & & \ddots & & \cdots & \vdots \\ & & & & & & & \\ * & * & * & & \boldsymbol{\alpha_{i-1}(i)} & \boldsymbol{\alpha_i(i)} & & * \\ * & * & * & & & \boldsymbol{\alpha_i(i+1)} & \cdots & \boldsymbol{\alpha_t(i+1)} \end{pmatrix}.$$

如果以上两种情形都不成立，我们总可以假设$j = i+1$，并继续这个过程。

但是，当进行到$T_{t-1,t-1}$，$\alpha_{t-1}(t) = \alpha_t(t)$时，上述过程将停止。此时，$\{\alpha_1, \ldots, \alpha_t\}$会形成一个彩虹$t$-圈，我们期望的矛盾就达到了。 □

由第4.4节的构造方式，以及引理5.2.2与引理5.6.1（或直接由推论4.4.4）可得如下定理。

定理5.6.2. *存在一个常数γ使得$p_4(4,q) > q^2 e^{-\gamma(\log q)^{3/4}}$。*

5.7 与超图Turán问题的联系

在本节中，我们将从超图Turán问题的观点出发来研究完美哈希族。

定理5.7.1. *对任意正整数t, N, q，我们有$f_N^*(q, tN-N, t) \le p_t(N,q)$。此外，$\frac{N!}{N^N} f_N(Nq, tN-N, t) \le p_t(N,q)$。*

证明. 由引理5.2.3，只需说明定理的第一个声明。回忆如果一个超图$\mathcal{G}$是N-均衡N-部的，且每部的大小为q，则$E(\mathcal{G})$可以被表示为一个$N \times |E(\mathcal{G})|$的$q$元矩阵$M$。若$\mathcal{G}$是$G(tN-N,t)$-free的，那么给定任何$t$条边的集合$S \subseteq E(\mathcal{G})$，不难验证它的表示矩阵中必然存在一行可以分离$S$，否则$S$能包含最多$tN-N$个顶点，与$\mathcal{G}$是$G(tN-N,t)$-free的相矛盾。因此，$M$可以被视为是所需的完美哈希族的表示矩阵。 □

定理5.7.1的一个直接应用可以给出如下结果。

推论5.7.2. *若$2 \nmid N$，则对任意$\epsilon > 0$，都有$p_3(N,q) > q^{\lceil N/2 \rceil - \epsilon}$。*

证明. 该推论可以由不等式(5-2)，$n^{k-o(1)} < f_r(n, 3(r-k)+k+1, 3) = o(n^k)$所推出。设$N = 2k-1$与$t = 3$，由定理7-7可以推出

$$p_3(N,q) \geq p_3^*(N,q) \geq f_N^*(q, 3N-N, 3) \geq \frac{N!}{N^N} f_N(Nq, 3N-N, 3) > \frac{N!}{N^N}(Nq)^{\lceil N/2 \rceil - o(1)}.$$

□

5.8 结语

在本章中我们主要研究了满足一定分离性的码和哈希族。我们解决了若干关于其下界或上界的猜想和公开问题。我们主要有两种方式去研究这一类问题。第一种方法是发掘出分离性中蕴含的结构性质。例如，我们的Johnson型界被用来证明定理5.1.5和推论5.5.5。第二种方法是我们建立了完美哈希族，图论和加法组合之间的桥梁。例如，通过考虑一个相关的超图Turán问题，我们解决了猜想5.1.9。我们也说明了加法组合的工具可以被用来构造好的完美哈希族。

除了这些新方法，我们认为我们在第四节的构造也是很有意义的。因为它推广可很多已知的构造。该方法的进一步推广是令人期待的。

作为总结，我们提出以下较为有趣且十分有意义的公开问题。

问题1: 若$2 \nmid N$，引理5.7.2说明$p_3(N,q) > q^{\lceil N/2 \rceil - o(1)}$。决定$p_3(N,q) = o(q^{\lceil N/2 \rceil})$还是$p_3(N,q) = \Theta(q^{\lceil N/2 \rceil})$成立。

问题2: 对一个r-均衡r-部线性超图，若它没有彩虹圈，我们已经对$i = 3, 4$证明了$g_r^*(q) = o(q^2)$与$g_i^*(q) > q^{2-o(1)}$。那么，是否对所有$r \geq 3$都有$g_r^*(q) > q^{2-o(1)}$?

问题3: 定理5.7.1证明了$p_t(N,q) \geq f_N^*(q, tN-N, t)$，然而是否存在一个$p_t(N,q)$的上界且仅仅利用$f_N^*(q,v,t)$来表示?

6 缓存方案

6.1 简介

视频传播已经成为我们日常生活中无线数据堵塞的一个重要驱动因素，并且，它正面临着引人注目的增长需求[1]。假设我们有一个拥有巨大数据存储的服务器，它与一组用户相连。每个用户都希望从服务器得到某个特定的文件。同一时间的大量需求常常会令无线网络堵塞，这会导致系统的延时和超载，弱化用户体验。因此，不管是学术界还是工业界都有很大的兴趣来解决这个问题。解决的办法就是充分利用分布在整个网络的内存——尤其是那些靠近末端用户的——来复制文件。我们把文件的复制品称为缓存。在网络负载很低时，系统把文件的某些部分分发到每个用户的缓存中，因此，在繁忙时段，用户的需求就可以从这些缓存中获益。用这种方式，我们可以减轻网络负载并舒缓其拥塞。

在Maddah-Ali和Niesen关于编码缓存的开创性文章[101]中，他们提出了集中式缓存方案（Centralized Coded Caching Scheme，简记为CCC方案），其中，“集中式”的意思表示在网络中有一个服务器负责调配所有的传输。CCC方案共有两个阶段：文件布置阶段，这时每个文件的某些数据包依据一个预先设定好的策略被放入每个用户的缓存中；和文件分配阶段，这时服务器依据所有用户的不同需求，设计一个方案把这些所需数据包的抑或和（XOR multiplexing）用一个共享的链接广播出去。从这时起，编码缓存成为了一个活跃的科研领域，在这个方面产出了很多文章，例如文献[89,90,92,102,107,112]。

CCC方案的核心的想法是设计一个适合的文件布置策略，使得在发布阶段所有用户各种各样的需求可以用有限多次的多路广播传送来满足。每个用户都可以恢复他所需的文件，通过同时利用他所收到的广播文件与本地缓存里已经存储好的文件。假设我们有K个用户，N个单位大小的文件（这时整个数据库的大小也是N），每个用户都含有大小为M的内存空间。注意在本文中我们仅考虑$N \geq K$时的情形。在文件发布阶段所需的总共传输总量被称为这个方案的比率，记作R。为了实行一个缓存方案，每个文件都被划分成一定数量的数据包，我们把这个数目记为F。一般来说，给定K，M，N，R和F 这两个参数是一个缓存体系的主要衡量指标。比率R代表了这个方案的效率，而F则表示了它的

复杂度。为了衡量一个方案的好坏，我们通常假设比例M/N是固定的常数，把R和F表示成关于K的函数，来考察它们的表现。

对一个简单的未编码的缓存方案来说，每个用户在他的缓存里存储了每个文件的M/N部分。根据用户的需求，服务器把剩下的$(1-\frac{M}{N})$部分以广播的形式分发出去。因此，对未编码的缓存方案来说，它的比率是$R_U = K\cdot(1-\frac{M}{N})$，其中第一个因子$K$表示完全没有缓存时的比率，第二个因子$(1-\frac{M}{N})$被称为局部缓存增益[101]。$R_U$是随着$K$线性增长的。为了实现这个方案，容易看出我们只需把每个文件分割成$F_U = N$个数据包。因此，F_U是一个与K无关的常数。

通过在文件布置阶段和分发阶段同时使用好的策略，Maddah-Ali-Niesen方案可以把比率显著地降低为$R_{AN} = K\cdot(1-\frac{M}{N})\frac{1}{1+KM/N}$。当$K$越来越大时，$R_{AN}$的极限是$\frac{N-M}{M}$，这是一个与$K$无关的常数。Maddah-Ali-Niesen方案的比率对不加任何编码的布置阶段来说是最优的，不管是对$K \leq N$[142]，还是$K > N$[150]；这里的不加任何编码是指文件布置阶段是被局限于非编码的。然而，为了实行Maddah-Ali-Niesen 的方案，每个文件必须被分割成F_{AN}个数据包，这里$F_{AN} = \binom{K}{KM/N}$，这个数是随着K呈指数级增长的。当K相对较大时，这显然是不合时宜的。

为了减小F_{AN}的大小，Yan 等人[147]提出了一个新的概念，称之为布置分发阵列设计（Placement Delivery Array Design，简称为PDA 设计），并用它来构造一些合适的CCC方案。PDA清楚地表明了在布置阶段每个用户需要缓存什么，以及在发布阶段服务器应该广播什么。从这个观点出发，Yan等人提出了两类缓存方案。与Maddah-Ali-Niesen之前的方案相比，Yan等人的F_{PDA} 显著地小于F_{AN}，然而比率R_{PDA}仅比R_{AN}高出一点点。然而，F_{PDA}仍然是随着K呈指数级增长的。

就在最近，Shanmugam等人[123]利用Ruzsa-Szeméredi图构造出了F随着K线性增长的缓存方案。他们的构造对任何常数M/N都是可能实行的。不幸的是，他们的比率R不是一个常数，而是K^{δ}这种形式的，这里，$\delta > 0$是一个可以任意小的常数。实际上我们将证明当R和M/N都是固定的常数时，F随K线性增长的缓存方案是不存在的。我们的结论说明，Shanmugam等人的构造在$F = \Theta(K)$时实际上是渐进最优的了，因为在这种情况下，R不可能是一个常数。我们也会讨论与Ruzsa-Szeméredi图相关的内容，并说明如何用它们去构造具有常数比率的缓存方案。

从以上的方案中我们可以看出，直觉上来说，在两个参数F和R之间肯定有一个权衡关系。文献[122]最早开始考虑F作为K, M, N的函数的最小值，但它是从随机化的去中心化缓存方案着手的。从那时起，这个问题在编码缓存的研究领域里就扮演了一个重要的角色，文献[123,136,147,148] 都考虑了相关的内容。如之前提到的，本文的出发点是假设M/N是

固定的，且试图将F和R表示为K个函数。然而，一个很重要的考虑就是，如果R不是一个常数而是与K相关的一个函数，那么当有很多个用户时，R就会变得太大了，这将使这个缓存方案不切实际。因此，我们更加青睐于码率是常数的缓存方案。当我们考虑常数码率的CCC方案时，在Maddah-Ali-Niesen方案和Yan等人的方案中，F都是一个随着K指数增长的函数，这也使得这些方案是不切实际的。一个亟待解决且十分有趣的问题构造F 尽可能小的常数码率缓存方案。我们的终极目标是证明是否存在一个$F = f(K)$是多项式的常数码率缓存方案。换句话说，我们试图构造在如下约束条件下的最优CCC 方案：

1. 缓存布置被限定是未经编码的，
2. 分发阶段使用了二元码，即抑或运算，
3. $K \gg 1$。

总而言之，我们希望优化如下函数：

$$F(K) := \min\{F \in \mathbb{Z}^+ : for\ fixed\ M/N \in \mathbb{R}^+, there\ exists\ a\ (K, M, N)\ CCC\ scheme\ with\ constant\ R.\}$$

本文跟随了文献[147]的步伐，我们发现PDA的概念与极值组合中的一个重要问题有着自然地联系。我们证明，一个PDA存在当且仅当一个对应的线性(6, 3)-free3-均衡3-部超图存在。以这个为出发点，我们可以很直观也很简单地理解如何去构造一个CCC方案。通过运用著名的(6, 3)-定理，我们首先证明了常比率且F随K线性增长的CCC方案是不存在的（见定理6.3.4）。随后，我们给出了两个无穷类的构造（或者说满足对应条件的超图），一类构造来自于不交集合的并（见定理6.4.1），它包含了Maddah-Ali-Niesen方案作为其一个特殊情形；另一类来自于延拓的q元序列（见定理6.5.2），它包含了Yan等人的方案作为其特殊情形。我们并没有得到关于$F(K)$的一般表达式。但是通过分析我们的方案，我们得出F随K亚指数增长的常比率缓存方案是存在的。

6.2 CCC方案与PDA设计

首先让我们回忆文献[101]中定义的CCC方案。考虑一个缓存系统，其中有K 个用户通过一个无错误的链接（Error-free Shared Link）连接到一个服务器上，把K 个用户记为$\mathcal{K} = \{1, \ldots, K\}$。$N$个被记作$\{W_1, W_2, \ldots, W_N\}$的文件被存储在服务器里，并假设这些文件都是单位大小的，则CCC 方案可以用如下图片表示出来。

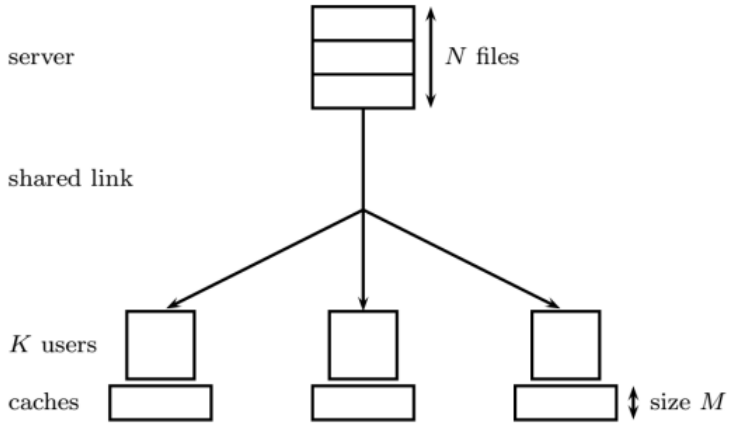

图 6-1　缓存系统

我们把该缓存体系叫做(K, M, N) 缓存体系。

现在我们简单介绍文献[147]所引入的PDA设计，它仅仅利用一个简单的阵列就表示了整个CCC方案。一个大小为$F \times K$的PDA，被记作为$\mathcal{P} = [p_{j,k}]_{F\times K}$，这里$F$是一个整数使得$FM/N$也是一个整数，该阵列是由一个特定的符号“$*$”和$S$个整数$\mathcal{S} = \{1, 2, \ldots, S\}$构成。我们假设每个整数$s \in \mathcal{S}$在阵列中都出现了至少一次。此外，我们记$\mathcal{F} = \{1, \ldots, F\}$与$\mathcal{N} = \{1, \ldots, N\}$ 。我们有如下约束条件：

C1. 符号$*$在每列中都恰好出现$Z = FM/N$ 次，因此每列都含有$F - Z$个整数元素；

C2. 每行或者每列都不含有相等的整数；

C3. 对任意两个不同的位置，若果有$p_{j_1,k_1} = p_{j_2,k_2} = s \in \mathcal{S}$，$j_1 \neq j_2$，$k_1 \neq k_2$，则我们有$p_{j_1,k_2} = p_{j_2,k_1} = *$。

我们把满足以上限制条件的阵列称为一个(K, F, Z, S)-PDA。如果每个$\mathcal{S}$中的整数在$\mathcal{P}$中出现恰好g次，进一步把这个阵列称为g-正则的，被记为g-(K, F, Z, S) PDA。如前所述，每个编码缓存方案都有两个阶段，即，布置阶段和分发阶段。给定一个PDA，与两个阶段相对应的操作策略如下所述。

1. 布置阶段：把每个文件分割成F个数据包，即，$W_i = \{W_{i,j} : j \in \mathcal{F}\}$。每个用户$k \in \mathcal{K}$在他的缓存中存储如下数据包：

$$Z_k = \{W_{i,j} : p_{j,k} = *, i \in \mathcal{N}\}.$$

容易看出每个用户含有一个容量为$Z \cdot \frac{1}{F} \cdot N = M$的缓存。

2. 分发阶段：一旦服务器接到了用户的请求$d=(d_1,\ldots,d_K)$，这里$d_k\in\mathcal{N}$表示用户k所需求的文件的指标，服务器在时间点s广播如下的数据包的抑或运算：

$$\bigoplus_{p_{j,k}=s,j\in\mathcal{F},k\in\mathcal{K}} W_{d_k,j}.$$

每个用户的解码算法如下所述。对某个用户$k\in\mathcal{K}$，所需某个文件W_{d_k}，$d_k\in\mathcal{N}$，由布置阶段可知，该用户已经知道$\{W_{d_k,j}:p_{j,k}=*\}$。为了恢复W_{d_k}，他只需解码未知的数据包$\{W_{d_k,j}:p_{j,k}\in\mathcal{S}\}$。注意到，对每个$s\in\mathcal{S}$，在广播的信息$\bigoplus_{p_{j,k}=s,j\in\mathcal{F},k\in\mathcal{K}}W_{d_k,j}$中，由约束条件C3可得，用户$k$ 知道所有数据包$\{W_{d_{k'},j}:p_{j,k'}=s,\ k'\neq k\}$，这些都在布置阶段被放入他的缓存中。那么，未知的值$W_{d_k,j},\ p_{j,k}=s$可以通过从$\bigoplus_{p_{j,k}=s,j\in\mathcal{F},k\in\mathcal{K}}W_{d_k,j}$中减去$\bigoplus_{p_{j,k'}=s,j\in\mathcal{F},k'\in\mathcal{K},k'\neq k}W_{d_{k'},j}$而解出。这并不难。因此，通过一个简单的运算每个用户都能恢复他所需的文件。因此这个缓存方案是可以运行的。

例6.2.1. 作为一个例子，我们给出*(2,1,2) CCC*方案的*(2,4,2,2)-PDA*设计。并不难验证如下阵列确实是一个*(2,4,2,2)-PDA*。

$$\mathcal{P}_{4,2}=\begin{pmatrix} * & 1\\ 1 & *\\ * & 2\\ 2 & * \end{pmatrix}$$

假设我们给定了两个文件W_1和W_2。把每个文件划分成四个数据包，使得成立$W_1=\{W_{1,1},W_{1,2},W_{1,3},W_{1,4}\}$ 与$W_2=\{W_{2,1},W_{2,2},W_{2,3},W_{2,4}\}$。记$Z_1$和$Z_2$分别为两个用户的缓存。在布置阶段，第一个用户存储$Z_1=\{W_{1,1},W_{1,3},W_{2,1},W_{2,3}\}$，且第二个用户存储$Z_2=\{W_{1,2},W_{1,4},W_{2,2},W_{2,4}\}$。根据上面描述的*PDA*，服务器所广播的内容被表示于表*6-1*中。

Request d	Time slot 1	Time slot 2
(1,1)	$W_{1,2}\bigoplus W_{1,1}$	$W_{1,4}\bigoplus W_{1,3}$
(1,2)	$W_{1,2}\bigoplus W_{2,1}$	$W_{1,4}\bigoplus W_{2,3}$
(2,1)	$W_{2,2}\bigoplus W_{1,1}$	$W_{2,4}\bigoplus W_{1,3}$
(2,2)	$W_{2,2}\bigoplus W_{2,1}$	$W_{2,4}\bigoplus W_{2,3}$

表 6-1 例6.2.1中的分发阶段

为了解释该解码算法，不妨假设$d=(1,2)$。第一个用户可以通过解码$W_{1,2}$ 和$W_{1,4}$来

恢复W_1。注意到$W_{1,2}$和$W_{1,4}$可以通过从$W_{1,2} \bigoplus W_{2,1}$中减去$W_{2,1}$，以及从$W_{1,4} \bigoplus W_{2,3}$中减去$W_{2,3}$而得到。同理，第二个用户可以通过解码$W_{2,1}$和$W_{2,3}$来恢复$W_2$。$W_{2,1}$与$W_{2,3}$可以通过分别从$W_{1,2} \bigoplus W_{2,1}$与$W_{1,4} \bigoplus W_{2,3}$中减去$W_{1,2}$和$W_{1,4}$得到。对于用户其它的请求，我们有类似的解码算法。

不管用户的需求是什么，PDA所代表的缓存方案会广播S个数据包，每个数据包的大小是$1/F$。因此，这个方案的比率恰好是$R = S/F$。除此之外，如果每个文件都被分成F个数据包，那么这个方案被称为是一个F-划分方案。在文献[147]中，作者证明了PDA设计里的一个基本定理。

定理6.2.2 ([147]). *一个(K, M, N)缓存系统的F-划分方案可以用一个(K, F, Z, S)-PDA $\mathcal{P} = [p_{j,k}]_{F \times K}$表达出来，其中，$Z/F = M/N$。不管需求如何，每个用户都可以通过比率$R = S/F$正确地恢复出他所需的文件。.*

注记6.2.3. 文献[101]中的Maddah-Ali-Niesen方案等价于一个$(K, \binom{K}{t}, \binom{K-1}{t-1}, \binom{K}{t+1})$-PDA，其中$t = KM/N$是一个整数。

注记6.2.4. 文献[147]中，Yan等人给出的第一个方案是一个$(q(m+1), q^m, q^{m-1}, q^{m+1} - q^m)$-PDA。

简而言之，设计一个CCC方案可以被转化为设计某个满足给定条件的PDA。在本文中，我们考虑M/N固定，$N \geq K$，且K趋于无穷的情况。我们通过考察F与R同K的关系来分析一个缓存方案。

6.3 超图模型

现在我们转入使用超图的额观点来研究CCC方案或者PDA设计。我们首先给出一些必要的定义。当我们谈论到超图时，实际上是说一对$\mathcal{G} = (V(\mathcal{G}), E(\mathcal{G}))$，其中顶点集$V(\mathcal{G})$被当做前$n$ 个正整数的集合$[n]$，边集被当做是$[n]$ 的一些子集之并。图$\mathcal{G}$是线性的当且仅当对所有不同的边$A, B \in E(\mathcal{G})$，都有$|A \cap B| \leq 1$。我们说图$\mathcal{G}$是r-均衡的，如果对所有边$A \in E(\mathcal{G})$，都有$|A| = r$。

一个r-均衡的超图$\mathcal{G}$是r-部的，如果它的顶点集$V(\mathcal{G})$可以被染成r种颜色，使得$\mathcal{G}$中没

有边含有颜色相同的两个顶点。在这样一个染色中，$V(\mathcal{G})$的那些颜色集，即相同颜色的顶点集，被称为是$\mathcal{G}$的不同顶点部。在这章中我们主要关心3-均衡3-部超图，三个顶点集为$\mathcal{F}$，$\mathcal{K}$，$\mathcal{S}$使得$|\mathcal{F}| = F$，$|\mathcal{K}| = K$，$|\mathcal{S}| = S$。

Brown，Erdős和Sós[39,40]引入了函数$f_r(n, v, e)$来表示n 个顶点的r-均衡超图，若其不包含由v 个点张成的e 条边，则其能含有的最大边数。换句话说，在这种超图中，任意e条边的并都含有至少$v + 1$个顶点。这类超图被称为是$G_r(v, e)$-free 的超图。Ruzsa和Szemerédi[119]著名的(6,3)-定理指出

引理6.3.1.

$$n^{2-o(1)} < f_3(n, 6, 3) = o(n^2).$$

这个引理也说明，如果一个3-均衡的n顶点超图是(6, 3)-free的，那么它的边数的阶就不可能是n^2的线性阶。

请回想关于$\mathcal{F}$，$\mathcal{K}$，$\mathcal{S}$的定义。下面的观察是我们研究方法的出发点。每个PDA都是一个$F \times K$的阵列$\mathcal{P}$，其元素都从属于一个大小为$S + 1$的字母集（“+1”表示符号“*”）。我们不妨考虑一个线性的3-均衡3-部超图$\mathcal{H}$，它的三个部分为$\mathcal{F}$，$\mathcal{K}$，$\mathcal{S}$，并满足$|\mathcal{F}| = F$，$|\mathcal{K}| = K$以及$|\mathcal{S}| = S$。我们连一条边$\{j, k, s\}$，其中$j \in \mathcal{F},\ k \in \mathcal{K},\ s \in \mathcal{S}$当且仅当在第$j$行第$k$列的元素恰好是$s \in \mathcal{S}$。这时，这个超图$\mathcal{H}$被阵列$\mathcal{P}$所唯一决定了，反之亦然（在另一个方向，假如我们有一个线性的3-均衡3-部超图$\mathcal{H}$，三个部分为$\mathcal{F}$，$\mathcal{K}$，$\mathcal{S}$，那么我们可以构造一个对应的$F \times K$阵列$\mathcal{P}$，使得其元素从属于$\mathcal{S} \cup \{*\}$）。此时，$\mathcal{H}$称为是由$\mathcal{P}$所定义的超图。容易验证，超图的边数恰好等于PDA中整数的个数。可以计算$|E(\mathcal{H})| = K(F - Z) = KF(1 - \frac{M}{N})$。

我们使用超图的观点的一个重要原因是PDA的三个限制条件都可以被简单地翻译为超图里对应的条件。下面的定理建立了PDA和(6, 3)-free超图的等价关系。

定理6.3.2. *一个满足条件C1，C2，C3的(K, F, Z, S)-PDA存在当且仅当由它定义的超图是一个线性的(6, 3)-free 3-均衡3-部超图$\mathcal{H}$，它的三个部分为$\mathcal{F}$，$\mathcal{K}$，$\mathcal{S}$，并满足$|\mathcal{F}| = F$，$|\mathcal{K}| = K$以及$|\mathcal{S}| = S$。此外，每个顶点$k \in \mathcal{K}$恰好与$F - Z$条边相连。*

证明. 令$\mathcal{H}$为一个由(K, F, Z, S)-PDA $\mathcal{P}$所表示的一个超图。一方面，为了证明必要性，只需说明$\mathcal{H}$满足定理中所提到的限制条件。

1. 容易验证$\mathcal{H}$是一个3-均衡3-部的超图，三个顶点集为$\mathcal{F}$，$\mathcal{K}$，$\mathcal{S}$。

2. $\mathcal{H}$的线性性质可以由限制条件C2推出。首先，我们没有如下形式的两边，$\{j,k,s\}$和$\{j,k,s'\}$，这是因为$p_{j,k}$是良定义的且只有一个特定的值。第二，我们没有两边如$\{j,k,s\}$和$\{j,k',s\}$，因为如若不然，$p_{j,k} = p_{j,k'} = s$，这是被C2所禁止的。最后，我们没有两边如$\{j,k,s\}$与$\{j',k,s\}$，否则$p_{j,k} = p_{j',k} = s$，这也是被条件C2所禁止的。

3. $k \in \mathcal{K}$中的每个顶点都恰好与$F - Z$条边相连，因为由C1可知，$\mathcal{P}$的每列含有恰好$F - Z$个整数，这推出了$\mathcal{H}$的$F - Z$条边。

4. $\mathcal{H}$是(6, 3)-free的。换句话说，$\mathcal{H}$中任意三条边的并含有至少七个顶点。如若不然，设存在三条边是由最多六个顶点张成的。若顶点数不超过五个，则容易推出必存在两边有两个公共顶点，这违反了超图的线性性。只需考虑，三条边由六个顶点张成的情形。考察这六个点从三个部分中选取的方式。我们说，这些顶点被划分成$a/b/c$这种形式，如果我们从第一部分中选出a个点，从第二部分中选出b个点，从第三部分中选出c个点。如果它们被划分成4/1/1或者3/2/1这种形式（考虑划分的置换），则我们依旧可以通过超图的线性性推出矛盾。对剩下的情形2/2/2，我们总能把这些顶点记为$j_1, j_2, k_1, k_2, s_1, s_2$。假设我们有三条边，那么，不失一般性，假设$s_1$出现在两条边$\{j_1,k_1,s_1\}$与$\{j_2,k_2,s_1\}$之中。那么，第三条边的候选者可能是$\{j_1,k_2,s_2\}$或者$\{j_2,k_1,s_2\}$.。然而，由C3可知，$p_{j_1,k_1} = p_{j_2,k_2} = s_1$ 意味着$p_{j_1,k_2} = p_{j_2,k_1} = *$。因此，对任何$s_2 \in \mathcal{S}$没有边是$\{j_1,k_2,s_2\}$或者$\{j_2,k_1,s_2\}$这两种形式的。因此，不存在三条边由六个顶点张成的。

另一方面，为了证明充分性，如下的观察是至关重要的。如果我们有一个线性的3-均衡3-部超图$\mathcal{H}$，顶点集为$\mathcal{F}$，$\mathcal{K}$，$\mathcal{S}$，那么我们可以构造一个对应的$F \times K$阵列$\mathcal{P}$，它的元素从属于$\mathcal{S} \cup \{*\}$。$\mathcal{P}$中第j行与第k列的值是$s \in \mathcal{S}$，如果$\{j,k,s\}$构成$\mathcal{H}$的一条边，否则为*。可以发现，由线性性可知，并没有如下形式的两条边，即，$\{j,k,s\}$与$\{j,k,s'\}$，因此，$p_{j,k}$是良定义的。容易证明$\mathcal{P}$满足C1和C2，C3也可以用反证法证明。 □

例6.3.3. *为了阐释定理6.3.2，我们考虑例6.2.1中的PDA所定义的超图。令$\mathcal{H}$是一个由三个顶点集$\mathcal{F}$，$\mathcal{K}$，$\mathcal{S}$构成的超图，且满足$\mathcal{F} = \{j_1, j_2, j_3, j_4\}$，$\mathcal{K} = \{k_1, k_2\}$与$\mathcal{S} = \{s_1, s_2\}$。$\mathcal{H}$有四条边，因为例6.2.1中的$\mathcal{P}_{4,2}$恰好有四个整数元素。由定理6.3.2及其之前的讨论可知，$\mathcal{H}$的四条边是$\{j_2,k_1,s_1\}$，$\{j_1,k_2,s_1\}$，$\{j_3,k_2,s_2\}$与$\{j_4,k_1,s_2\}$。可以验证$\mathcal{H}$是一个线性的(6, 3)-free3-均衡3-部超图。也能看出，$\mathcal{K}$的每个顶点恰与两条边相连。那么，$\mathcal{H}$可以被看作是满足条件C1，C2，C3的如下(2,4,2,2)-PDA。*

$$\mathcal{P}^*_{4,2} = \begin{array}{|c|c|c|}\hline & k_1 & k_2 \\ \hline j_1 & * & s_1 \\ \hline j_2 & s_1 & * \\ \hline j_3 & * & s_2 \\ \hline j_4 & s_2 & * \\ \hline \end{array}$$

可以看出，$\mathcal{P}_{4,2}$与$\mathcal{P}^*_{4,2}$实际上是等价的。

为了说明我们超图观点的巨大作用，我们首先证明如下定理，该定理是引理6.3.1 与定理6.3.2的一个直接推论。

定理6.3.4. *如果$R = S/F$与M/N都是给定的与K无关的常数，那么，对足够大的K，F随K线性增长的(K, F, Z, S)-PDA 是不可能存在的。*

证明. 对足够大的K，假如存在一个满足定理所述条件的(K, F, Z, S)-PDA。注意到，$Z/F = M/N$。考察由这个PDA定义的超图$\mathcal{H}$，我们有$|V(\mathcal{H})| = |\mathcal{F}|+|\mathcal{K}|+|\mathcal{S}| = F+K+S = \Theta(K)+K+RF = \Theta(K)$ 且$|E(\mathcal{H})| = K(F-Z) = KF(1-M/N) = \Theta(K^2) = \Theta(|V(\mathcal{H})|^2)$。

另一方面，由定理6.3.2可知，$\mathcal{H}$是(6, 3)-free的，因此，由引理6.3.1可知，$|E(\mathcal{H})| = o(|V(\mathcal{H})|^2)$，这是一个矛盾。 □

如同我们在介绍里提到的那样，本文的动机是考虑什么是最小的F使得存在一个常数比率R的方案。定理6.3.4实际上提供了一个下界，即，F随K 线性增长的常比率方案是不存在的。Maddah-Ali-Niesen与Yan等人的方案说明，F随K呈指数增长的方案是存在的。那么，我们可以降低F的阶吗? 作为这个方向迈出的第一步，接下来，我们会给出两个方案，它们满足F是随着K呈亚指数增长的。我们的构造是直接由超图观点给出的，我们实际上构造了两类线性(6, 3)-free3-均衡3-部的超图。

6.4 由不交子集的并得出的构造

这一节中我们给出第一个方案。

方案1:
令n, a, b是满足$n \geq a+b$的正整数。令$[n]=\{1,2,\ldots,n\}$，且用$\binom{[n]}{a}=\{A\subseteq[n]:|A|=a\}$表示$[n]$的所有$a$元子集。我们按如下要求构造一个超图$\mathcal{H}_1$。令$V_1,\ V_2,\ V_3$为$V(\mathcal{H}_1)$的三个顶点集，满足$V_1=\binom{[n]}{a}$，$V_2=\binom{[n]}{b}$与$V_3=\binom{[n]}{a+b}$。三个顶点$A\in V_1,\ B\in V_2,\ C\in V_3$构成一条边$\{A,B,C\}$当且仅当$|A|=a$，$|B|=b$，$|C|=c$且$A\cup B=C$（这也意味着$A\cap B=\emptyset$）。可以得出，$\mathcal{H}_1$包含$\binom{n}{a}\binom{n-a}{b}$条边（注意到$\binom{n}{a}\binom{n-a}{b}=\binom{n}{b}\binom{n-a}{b}$）。

定理6.4.1. *$\mathcal{H}_1$是一个线性的(6, 3)-free3-均衡3-部超图。*

证明. 可以看出，该超图是3-均衡3-部的。对一条边$\{A,B,C\}$，每两个顶点唯一决定了第三个，因此，我们可以得出它的线性性。假设有三条边是由六个顶点张成的，那么由定理6.3.2的证明可知，我们只需考虑六个顶点是均匀地从三部中取出的情形。对六个顶点A, A', B, B', C, C'，若它们包含三条边，则不失一般性，我们可以假设一定存在两条边$\{A,B,C\}$与$\{A',B',C\}$。然而，$A\cup B=A'\cup B'=C$与$A\neq A'$意味着$A\cap B'\neq\emptyset$且$A'\cap B\neq\emptyset$，因此，$|A\cup B'|<a+b$且$|A'\cup B|<a+b$。所以，对任何$C'\in V_3$，我们没有有形如$\{A,B',C'\}$或者$\{A',B,C'\}$的边。因此，并不存在由六个顶点张成的三条边。 □

定理6.4.2. *对任意三个正整数$a,\ b,\ n$使得$a+b\leq n$，都存在一个$\binom{a+b}{a}$-正则$(\binom{n}{b},\binom{n}{a},\binom{n}{a}-\binom{n-b}{a},\binom{n}{a+b})$-PDA.*

证明. 取$\mathcal{F}=V_1,\ \mathcal{K}=V_2$且$\mathcal{S}=V_3$，那么，由方案1的构造可知，容易看出$\mathcal{K}$的每个顶点都与恰好$\binom{n-b}{a}$边相连。因此，由定理6.3.2与定理6.4.1我们可以推导出存在一个(K,F,Z,S)-PDA，满足$K=\binom{n}{b},\ F=\binom{n}{a},\ Z=\binom{n}{a}-\binom{n-b}{a}$与$S=\binom{n}{a+b}$。此外，它是$\binom{a+b}{a}$-正则的，因为对任意$C\in\binom{[n]}{a+b}$，都有$|\{(A,B):A\in\binom{[n]}{a},\ B\in\binom{[n]}{b},\ A\cup B=C\}|=\binom{a+b}{a}$。 □

例6.4.3. 我们给出一个例子，以说明方案1与上面的定理，我们取$n=4$，$a=2$，$b=1$。由定义可知，$V_1=\binom{[4]}{2}=\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$，$V_2=\binom{[4]}{1}=\{\{1\},\{2\},\{3\},\{4\}\}$与$V_3=\binom{[n]}{3}=\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$。根据方案1中的构造，$A\in V_1$，$B\in V_2$与$C\in V_3$形成一条边当且仅当$A\cap B=\emptyset$且$A\cup B=C$。这导致了超图$\mathcal{H}_1$包含了12条边，即，$\{\{2,3\},\{1\},\{1,2,3\}\}$，$\{\{2,4\},\{1\},\{1,2,4\}\}$，$\{\{3,4\},\{1\},\{1,3,4\}\}$；$\{\{1,3\},\{2\},\{1,2,3\}\}$，$\{\{1,4\},\{2\},\{1,2,4\}\}$，$\{\{3,4\},\{2\},\{2,3,4\}\}$；$\{\{1,2\},\{3\},\{1,2,3\}\}$，

$\{\{1,4\},\{3\},\{1,3,4\}\}$，$\{\{2,4\},\{3\},\{2,3,4\}\}$；$\{\{1,2\},\{4\},\{1,2,4\}\}$，$\{\{1,3\},\{4\},\{1,3,4\}\}$，$\{\{2,3\},\{4\},\{2,3,4\}\}$。那么定理*6.5.1*保证了$\mathcal{H}_1$是一个线性的*(6, 3)-free3-*均衡*3-*部超图。为了构造一个对应的*PDA*，我们取$\mathcal{K}=V_2$，$\mathcal{F}=V_1$与$\mathcal{S}=V_3$。那么由定理*6.3.2*与定理*6.4.2*，我们可以推出$\mathcal{H}_1$导出了如下的*3-(4,6,3,4)-PDA*，其中，行是由$\mathcal{F}=V_1=\binom{[4]}{2}$所标记的，列是由$\mathcal{K}=V_2=\binom{[4]}{1}$所标记的，并且所有的元素从属于$\mathcal{S}=V_3=\binom{[4]}{3}$。

$\mathcal{P}_{6,4}=$

	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$
$\{1,2\}$	*	*	$\{1,2,3\}$	$\{1,2,4\}$
$\{1,3\}$	*	$\{1,2,3\}$	*	$\{1,3,4\}$
$\{1,4\}$	*	$\{1,2,4\}$	$\{1,3,4\}$	*
$\{2,3\}$	$\{1,2,3\}$	*	*	$\{2,3,4\}$
$\{2,4\}$	$\{1,2,4\}$	*	$\{2,3,4\}$	*
$\{3,4\}$	$\{1,3,4\}$	$\{2,3,4\}$	*	*

不难看出，如果取$b=1$，$n=K$与$a=KM/N$，那么方案1显然包含Maddah-Ali-Niesen方案作为其一个特殊情形。实际上，我们的超图观点体现了Maddah-Ali-Niesen方案的本质结构。

对于一般的情形，我们有$R=S/F=\binom{n}{a+b}/\binom{n}{a}$，$F=\binom{n}{a}$，$M/N=Z/F=1-\binom{n-b}{a}/\binom{n}{a}$与$K=\binom{n}{b}$。一般地来说，衡量这个方案的表现并不是简单的事，因为很难去把R或F表示为一个K的函数。然而，R比未经编码的方案要好得多了；因为，$R_U=K(1-\frac{M}{N})=\binom{n}{b}\binom{n-b}{a}/\binom{n}{a}$，且$R_U/R=\binom{a+b}{a}\gg 1$。因此，我们的新方案在这种情况下是有意义的，因为它极大的降低了未经编码的方案的码率。实际上，通过选取适当的参数，我们的方案1可以导出若干个常比率的方案，其中F是随着K呈亚指数增长的。我们给出如下的例子。

注记6.4.4. 如果取$b=2$，那么我们可以得到一个$(\binom{n}{2},\binom{n}{a},\binom{n}{a}-\binom{n-2}{a},\binom{n}{a+2})$-*PDA*。若令$n=\lambda a$对某个常数$\lambda>1$成立，那么，我们有$R=S/F=\binom{n}{a+2}/\binom{n}{a}\approx(\lambda-1)^2$且$M/N=Z/F=(\binom{n}{a}-\binom{n-2}{a})/\binom{n}{a}\approx\frac{2\lambda-1}{\lambda^2}$，由斯特林公式可以求得

$$F=\binom{n}{\lambda^{-1}n}=\frac{1+o(1)}{\sqrt{2\pi\lambda^{-1}(1-\lambda^{-1})n}}\cdot 2^{nH(\lambda^{-1})}=\mathcal{O}(K^{-1/4}\cdot 2^{\sqrt{2K}H(\lambda^{-1})}),$$

其中，$H(x)=-x\log_2 x-(1-x)\log_2(1-x)$，$0<x<1$是二元熵函数。容易看出，在这样的参数下，$R$与$M/N$都是与$K$无关的常数，且$F$是随着$K$呈亚指数增长的。

6.5 由延拓的q元序列所得出的构造

在本节中我们给出第二个方案。

方案2:

令$q \geq 2, m, t$为正整数，满足$t \leq m$。令$\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$。如下构造一个3-均衡3-部的超图。第一个顶点集是$W_1 = \{A = (a_1, \ldots, a_m) : a_i \in \mathbb{Z}_q\}$，即，$W_1$包含所有长为$m$的$q$元向量，且$|W_1| = q^m$。第二个顶点集是$W_2 = \{B = (\delta_1, \ldots, \delta_t, b_{\delta_1}, \ldots, b_{\delta_t}) : 1 \leq \delta_1 < \cdots < \delta_t \leq m, b_{\delta_i} \in \mathbb{Z}_q\}.$，即，$W_2$包含长为$2t$的向量，前$t$个位置是从1到$m$严格递增的$t$个整数，后$t$个位置是$\mathbb{Z}_q$中的元素。因此，$|W_2| = \binom{m}{t} q^t$。最后，$W_3 = \{C = (c_1, \ldots, c_m, c_{m+1}, \ldots, c_{m+t}) : c_i \in \mathbb{Z}_q \text{ for } 1 \leq i \leq m \text{ and } c_{m+j} \in \mathbb{Z}_q \backslash \{q-1\} \text{ for } 1 \leq j \leq t\}$。显然，$|W_3| = q^m (q-1)^t$且对每个$1 \leq j \leq t$，都有$c_{m+j} + 1 \not\equiv 0 \pmod{q}$。

三个顶点$A \in W_1,\ B \in W_2,\ C \in W_3$形成一条边$\{A, B, C\}$当且仅当下面的条件同时成立。注意到，所有运算是在$\mathbb{Z}_q$中进行的。

1. $a_i = c_i$，$i \notin \{\delta_1, \ldots, \delta_t\}$，$1 \leq i \leq m$;
2. $a_{\delta_j} = c_{\delta_j} + c_{m+j} + 1$，$j = 1, 2, \ldots, t$;
3. $b_{\delta_j} = c_{\delta_j}$，$j = 1, 2, \ldots, t$。

我们有如下的观察。比较C与A的前m个位置。对$i \notin \{\delta_1, \ldots, \delta_t\}$，对应的元素是相等的。对其它的位置，由$c_{m+j} \in \mathbb{Z}_q \backslash \{q-1\}$，$1 \leq j \leq t$可知，$c_{m+j} + 1 \neq 0$，因此由第二个约束条件可知它们对应的位置都是不等的。因此，A与C属于一条边的一个必要条件是$(a_1, \ldots, a_m)$与$(c_1, \ldots, c_m)$恰好有t个不同的元素。此外，我们有$a_{\delta_j} \neq b_{\delta_j}$，$j = 1, 2, \ldots, t$。

定理6.5.1. *$\mathcal{H}_2$是一个线性的(6, 3)-free3-均衡3-部超图。*

证明. 容易验证这个超图是3-均衡3-部的。只需证明线性性和(6, 3)-free的性质。

1. 我们首先证明线性性。只需验证，对形如$\{A, B, C\}$的边，每两个顶点（如果它们确实在一条边上）唯一地决定了第三个。对给定的A和B，从$\delta_1, \ldots, \delta_t$，$C$的前$m$个位置可以由第一个和第三个约束条件得出。$C$的最后$t$个位置可以由第二个约束条件计算出。类似的，对给定的B和C，反解出A也是自然的。当A和C给定，决定B，这种情形与上述两种稍微有所不同。通过以上观察，$\{\delta_1, \ldots, \delta_t\}$可以由对比$(a_1, \ldots, a_m)$与$(c_1, \ldots, c_m)$得出，只需找到那些对应元素不同的位置。那么，

$\{b_{\delta_1}, \ldots, b_{\delta_t}\}$可以有第三个约束条件得出。超图的线性性得证了。

2. 对于(6, 3)-性质，由定理6.3.2的证明可知，我们只需考虑六个顶点均匀地取自三个顶点集的情形。对六个顶点A, A', B, B', C, C'，加入它们可以导出三条边，那么不失一般性，我们可以假设有三条边$\{A, B, C\}$，$\{A', B, C'\}$与$\{A, B', C'\}$。通过一些角标的置换，我们也能假设$B = (1, 2, \ldots, t, b_1, \ldots, b_t)$，那么，则有$C = (b_1, \ldots, b_t, c_{t+1}, \ldots, c_{m+t})$, $A = (b_1 + c_{m+1} + 1, \ldots, b_t + c_{m+t} + 1, c_{t+1}, \ldots, c_m)$与$C' = (b_1, \ldots, b_t, c'_{t+1}, \ldots, c'_{m+t})$。对比$A$和$C'$的前$t$个元素，它们是全然不同的，这是因为$c_j + 1 \neq 0$，$m + 1 \leq j \leq m + t$。因此，为了保证$\{A, B', C'\}$确实构成一条边，我们必须有$B' = (1, 2, \ldots, t, b'_1, \ldots, b'_t)$，那么$C' = (b'_1, \ldots, b'_t, c'_{t+1}, \ldots, c'_{m+t})$。这意味着$b_i = b'_i$，$1 \leq i \leq t$，即，$B$与$B'$是完全相等的，矛盾。

□

定理6.5.2. *对任意三个正整数q, t, m满足$t \leq m$，都存在一个$\binom{m}{t}$-正则$(\binom{m}{t}q^t, q^m, q^m - q^{m-t}(q-1)^t, q^m(q-1)^t)$-PDA。*

证明. 取$\mathcal{F} = W_1$, $\mathcal{K} = W_2$且$\mathcal{S} = W_3$。首先，由方案2的构造过程可知$\mathcal{K}$中的每个顶点恰好在$q^{m-t}(q-1)^t$条边中，这是由于每个位置a_i, $i \notin \{\delta_1, \ldots, \delta_t\}$都有$q$种选择，每个位置$a_{\delta_j}$, $1 \leq j \leq t$都有$q-1$种选择（$a_{\delta_j} \neq b_{\delta_j}$，$1 \leq j \leq t$）。因此，由定理6.3.2 与定理6.5.1，我们可以推出存在一个(K, F, Z, S)-PDA，$K = \binom{m}{t}q^t$, $F = q^m$, $Z = q^m - q^{m-t}(q-1)^t$，$S = q^m(q-1)^t$。此外，它是$\binom{m}{t}$-正则的，因为对任何$C \in \mathcal{S}$，对$\{\delta_1, ..., \delta_t\}$都有$\binom{m}{t}$种选择，并且，一旦$C$与$\{\delta_1, ..., \delta_t\}$都固定下来了，我们来就可以用三个约束条件来决定$A$和$B$。 □

例6.5.3. 为了更好地说明方案2以及上述定理，我们选取$t = 1$, $m = 2$与$q = 2$作为一个例子。由定义可知，$W_1 = \{(0,0), (0,1), (1,0), (1,1)\}$，$W_2 = \{(1,0), (1,1), (2,0), (2,1)\}$以及$W_3 = \{(0,0,0), (0,1,0), (1,0,0), (1,1,0)\}$。由方案2的构造方式可知，得到的超图$\mathcal{H}_2$是由八条边组成的。定理6.3.2，定理6.5.1，定理6.5.2保证了$\mathcal{H}_2$可以导出如下的2-(4,4,2,4)-PDA，其中行是由$\mathcal{F} = W_1$标记，列是由$\mathcal{K} = W_2$标记，并且其中的元素从属于$\mathcal{S} = W_3$。

$\mathcal{P}_{4,4} =$

	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
$(0,0)$	$*$	$(1,0,0)$	$*$	$(0,1,0)$
$(0,1)$	$*$	$(1,1,0)$	$(0,0,0)$	$*$
$(1,0)$	$(0,0,0)$	$*$	$*$	$(1,1,0)$
$(1,1)$	$(0,1,0)$	$*$	$(1,0,0)$	$*$

可以看出，如果选取$t=1$，则方案2可以导出一个$(mq, q^m, q^{m-1}, q^m(q-1))$-PDA，这与Yan等人构造出的第一个方案是十分相近的仅仅缺失了q个用户。但是，如果我们固定q，并让m趋向于无穷大，这个误差是可以忽略不计的。

对于一般的情形，我们有$R = S/F = (q-1)^t$，$F = q^m$且$K = \binom{m}{t}q^t$。我们也有$M/N = Z/F = 1-(1-1/q)^t$。固定q和t，令m趋向于无穷，则有R和M/N是与K无关的常数。而且，利用不等式$(m/t)^t < \binom{m}{t} < (em/t)^t$，我们可以从$K$中解出$m$，即，

$$\frac{tK^{\frac{1}{t}}}{eq} < m < \frac{tK^{\frac{1}{t}}}{q},$$

那么我们可以得到F的一个上界$F = \mathcal{O}(q^{tK^{1/t}/q})$。如果我们设定$t \geq 2$，则$F$显然是随着$K$呈亚指数增长的。

我们还可以指出超图观点的另一个优势。在文献[147]中，作者们给出了两个对称的构造，即，一个$(q(m+1), q^m, q^{m-1}, q^{m+1}-q^m)$-PDA，$M/N = 1/q$与一个$(q(m+1), q^{m+1}-q^m, (q-1)^2q^{m-1}, q^m)$-PDA，$M/N = (q-1)/q$。在文献[147]中，作者花了不少位置来分别地给出这两种构造。然而，从我们的超图观点出发，这两种构造实际上是一样的：如果我们知道它们两者中的任何一个，我们就可以马上知道另一个。假设第一个构造是被超图$\mathcal{G}_1$表示的，三个顶点集为$V_1 = \mathcal{F}$, $V_2 = \mathcal{K}$与$V_3 = \mathcal{S}$，那么第二个构造则是对一个对称的超图$\mathcal{G}_2$所表示的，它的顶点集为$V_1 = \mathcal{S}$, $V_2 = \mathcal{K}$与$V_3 = \mathcal{F}$。因此，如果$\mathcal{G}_1$是线性且(6, 3)-free的，$\mathcal{G}_2$显然也是。从一个给定的由超图表示的PDA设计，我们可以立即推出另一个，仅仅需要通过调换顶点集$\mathcal{F}$与$\mathcal{S}$的角色。因此，我们可以得到如下推论。

推论6.5.4. *对任意三个正整数$q \geq 2$, t, m，都存在一个$(\binom{m}{t}q^t, q^m(q-1)^t, q^m(q-1)^t - q^{m-t}(q-1)^t, q^m)$-PDA，其中，$R = 1/(q-1)^t$，$M/N = Z/F = 1-1/q^t$。*

注记6.5.5. *在引理6.5.4中，如果我们令$K = \binom{m}{t}q^t$，那么可以得出$m < tK^{1/t}/q$。所以，$F = q^m(q-1)^t < q^{tK^{1/t}/q+t}$，当$t \geq 2$时是随着$K$呈亚指数增长的。*

6.6 与从前的构造的对比

在本节中，我们把我们的构造与存在的一些构造进行对比。首先，我们把所有的构造都放在下面的表格里。

		K	M/N	F	R
Construction 1	M-N[101]	K	$\frac{1}{q}$	$\binom{K}{\frac{K}{q}}$	$\frac{K}{K+q}(q-1)$
Construction 2	M-N[101]	K	$\frac{q-1}{q}$	$\binom{K}{\frac{K}{q}}$	$\frac{K}{q+K(q-1)}$
Construction 3	Yan et al.[147]	K	$\frac{1}{q}$	$q^{\frac{K}{q}-1}$	$q-1$
Construction 4	Yan et al.[147]	K	$\frac{q-1}{q}$	$(q-1)q^{\frac{K}{q}-1}$	$\frac{1}{q-1}$
Construction 5	Scheme 1	$\binom{n}{b}$	$1-\frac{\binom{n-b}{a}}{\binom{n}{a}}$	$\binom{n}{a}$	$\frac{\binom{n}{a+b}}{\binom{n}{a}}$
Construction 6	Scheme 1: $b=2,\ n=\lambda a$	$\binom{n}{2}$	$\approx \frac{2\lambda-1}{\lambda^2}$	$\binom{n}{\frac{n}{\lambda}}$	$\approx (\lambda-1)^2$
Construction 7	Scheme 2	$\binom{m}{t}q^t$	$1-(\frac{q-1}{q})^t$	q^m	$(q-1)^t$
Construction 8	Scheme 2: symmetric form	$\binom{m}{t}q^t$	$1-\frac{1}{q^t}$	$q^m(q-1)^t$	$\frac{1}{(q-1)^t}$

表 6-2 一些CCC方案的总结

表格6-2包含了若干种不同的PDA。直接比较它们的优劣性是不太可行的，这是因为这些参数都具有一些迷惑性。因此，我们希望在某些统一的参数下来对比这些方案。我们会比较注记6.4.4 （构造6）引理6.5.4（构造8）的构造，因为注记6.4.4给出了具有小的M/N的PDA，引理6.5.4给出了具有大的M/N的PDA。对$M/N=1/q$，我们比较构造1，3，6。对构造6，我们选取$K:=\binom{n}{2}$，$\lambda:=2q$，则$n\approx\sqrt{2K}$，$M/N\approx\frac{2\lambda-1}{\lambda^2}=1/q-1/4q^2\approx 1/q$且$R\approx(2q-1)^2$，由注记6.4.4我们有$F\approx\sqrt{\frac{2^{1/2}q^2}{\pi(2q-1)K^{1/2}}}\cdot 2^{\sqrt{2K}H(\frac{1}{2q})}$。对$M/N=(q^t-1)/q^t$，$t\geq 2$，我们对比构造2，4，8。对构造8，我们选取$K:=\binom{m}{t}q^t$，那么$m<\frac{tK^{\frac{1}{t}}}{q}$，$F<q^{tK^{1/t}/q+t}$且$R=1/(q-1)^t$。对比被表示在表6-3与表6-4中。

对$M/N=1/q$，从表6-3中，我们可以看出构造6的比率大概是构造1，3的平方的四倍，但是F的大小下降地很快。固定q，则F从$\Omega(q^{K/q})$ 降低到$\mathcal{O}(q^{\sqrt{8K}/q})$（通过直接计算可知，$2^{\sqrt{2K}H(\frac{1}{2q})}<q^{\sqrt{8K}/q}$ for $q\geq 2$）。对$M/N=(q^t-1)/q^t$，我们的构造的优势就更引人注目了。表6-4中，K充分大时，构造2，4，8的比率是十分相近的。然而，F从$\Omega(q^{tK/q^t})$降低到了$\mathcal{O}(q^{tK^{1/t}/q})$。

下面，我们将给出这些构造更多的数值比较。例如，在注记6.4.4中，我们分别取$\lambda=4$和$n=12,16,20$。那么，$K=\binom{12}{2},\binom{16}{2},\binom{20}{2}$，$F=\binom{12}{3},\binom{16}{4},\binom{20}{5}$且$S=\binom{12}{5},\binom{16}{6},\binom{20}{7}$。我们有如下的表6-5。

我们可以考虑构造1，3在K大至66时的表现，取$M/N=0.5$。构造1得出$F_{1,60}=\binom{66}{33}=$

	K	M/N	F	R
Construction 1	K	$\frac{1}{q}$	$\approx \frac{q}{\sqrt{2\pi K(q-1)}} \cdot q^{\frac{K}{q}} \cdot (\frac{q}{q-1})^{K(1-\frac{1}{q})}$	$\frac{K}{K+q}(q-1)$
Construction 3	K	$\frac{1}{q}$	$q^{\frac{K}{q}-1}$	$q-1$
Construction 6	K	$\approx \frac{1}{q} - \frac{1}{4q^2}$	$\approx \sqrt{\frac{2^{1/2}q^2}{\pi(2q-1)K^{1/2}}} \cdot 2^{\sqrt{2K}H(\frac{1}{2q})}$	$\approx (2q-1)^2$

表 6-3 $M/N = 1/q$时的对比

	K	M/N	F	R
Construction 2	K	$\frac{q^t-1}{q^t}$	$\approx \frac{q^t}{\sqrt{2\pi K(q^t-1)}} \cdot q^{\frac{tK}{q^t}} \cdot (\frac{q^t}{q^t-1})^{K(1-\frac{1}{q^t})}$	$\frac{K}{q^t+K(q^t-1)}$
Construction 4	K	$\frac{q^t-1}{q^t}$	$(q^t-1)q^{\frac{tK}{q^t}-1}$	$\frac{1}{q^t-1}$
Construction 8	K	$\frac{q^t-1}{q^t}$	$< q^{tK^{1/t}/q+t}$	$\frac{1}{(q-1)^t}$

表 6-4 $M/N = (q^t-1)/q^t$时的对比

K	M/N	F	R
66	0.4545	220	3.6
120	0.45	1820	4.4
190	0.4473	15504	5

表 6-5 构造6的一些数值结果

7219428434016266000，构造3得出$F_{3,60} = 2^{32} = 4294967296$。对$K = 120$，构造1和3分别给出$F_{1,120} = \binom{120}{60}$与$F_{3,120} = 2^{59}$。我们的结论显然比它们好多了。

对构造2，4，8我们也能进行类似的比较。在引理6.5.4中，我们取$t = 2,\ q = 2$与$m = 3, 4, 5, 6, 7$。那么，通过直接计算可知有如下表6-6。

K	M/N	F_2	F_4	F_8	R_2	R_4	R_8
12	0.75	220	48	8	0.3	0.3333	1
24	0.75	134596	3072	16	0.3258	0.3333	1
40	0.75	847660528	786432	32	0.3226	0.3333	1
60	0.75	53194089192720	805306308	64	0.3261	0.3333	1
84	0.75	32719234717090660000	3298534883328	128	0.3281	0.3333	1

表 6-6 构造2，4，8的一些数值比较

6.7 相关课题

除了超图的观点，我们也提供了其它三个研究PDA的有趣的途径。

满足Blackburn性质的部分拉丁方： 拉丁方是一个$n \times n$的矩阵$\mathcal{L}$，被填充以n个不同的元素$\{1, \ldots, n\}$，每个元素在每行出现一次，每列也出现一次。一个部分拉丁方是由$\mathcal{L}$的若干行或列构成的子矩阵。我们说一个部分拉丁方$\mathcal{P}$满足Blackburn性质，如果两个不同的位置$p_{a,b}$与$p_{c,d}$有相同的元素，则对应的二角$p_{a,d}$和$p_{b,c}$为空格。我们把这个部分拉丁方称为是正则的，如果每一列都有相同数量的元素。我们希望填充尽可能多的位置而不违反这个规律，这个问题由Blackburn[33]提出，Wanless[144]也研究了它。可以验证PDA 的阵列的定义实际上等价于一个正则的满足Blackburn性质的部分拉丁方。例如，可以验证约束条件C1，C2与C3分别等价于正则性，拉丁性与Blackburn性质。

例6.7.1. 接下来，我们给出一个简单的例子来说明部分拉丁方与*PDA*之间的联系。让我们从一个4×4的拉丁方开始，

$$\begin{pmatrix} 3 & 1 & 2 & 4 \\ 1 & 4 & 3 & 2 \\ 4 & 2 & 1 & 3 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

上面拉丁方的前两列可以导出一个满足*Blackburn*性质的部分拉丁方，

$$\begin{pmatrix} * & 1 \\ 1 & * \\ * & 2 \\ 2 & * \end{pmatrix},$$

它与*(2,4,2,2)-PDA*是等价的。

二部图的边的强染色： 图的边染色是指边的着色使得任意两个相连的边都被染成不同的颜色。图$\mathcal{G}$边的强染色是一个边染色，并且满足每个染色集是一个诱导匹配，即，任意两个属于同色的边的顶点是不相连的。强染色数$S(\mathcal{G})$是最小的颜色数使得一个图$\mathcal{G}$边的强染色存在。文献[4] 是关于边的强染色的简单介绍。一般来说，通过

边的强染色有两种方式来构造PDA。如果一个二部图$\mathcal{G}$有顶点集X, Y，且有边的强染色，其颜色集为$C = \{c_1, \ldots, c_t\}$。那么，我们可以构造一个3-均衡3-部超图$\mathcal{H}$，其边集是由$\{\{x, y, c\} : x \in X,\ y \in Y,\ c \in C,\ \{x, y\}\ is\ an\ edge\ of\ \mathcal{G}\ colored\ by\ color\ c\}$构成的。直接可以验证$\mathcal{H}$是一个线性的(6, 3)-free超图（只需用到定义）。

一方面，假设$\mathcal{G}$在顶点集Y中是d-正则的，就是说Y的每个顶点都恰好与X的d个顶点相连。则超图$\mathcal{H}$在顶点集Y中也是d-正则的。它可以构造一个PDA $\mathcal{P}$满足$\mathcal{F} = X$，$\mathcal{K} = Y$与$\mathcal{S} = C$，使得对$x \in \mathcal{F}$与$y \in \mathcal{K}$，都有

1) $p_{x,y} = *$，若$\{x, y\}$不是$\mathcal{G}$的一条边，

2) $p_{x,y} = c \in \mathcal{S}$，若$\{x, y\}$是$\mathcal{G}$的一条边，且它被染成颜色$c$，即，$\{x, y, c\}$是$\mathcal{H}$的一条边。

因为$\mathcal{H}$是线性且(6, 3)-free的，它在Y中也是正则的，则由定理6.3.2可知，我们有$\mathcal{P}$是一个$(|Y|, |X|, |X| - d, |C|)$-PDA。相反的，给定一个PDA，我们也能构造出一个对应的二部图，它有一个对应的强边染色。Yan等人在文献[148]利用了这个观察。利用一个图论中的结果[88]，他们构造出了具有更多参数的PDA。

另一方面，假设对每个$c \in C$，$\mathcal{G}$包含μ_c条不同的边被染成颜色c。令$\mu = \min_{c \in C}\{\mu_c\}$。我们可以从每个颜色集中选取$\mu$ 条边。那么超图$\mathcal{H}$也能构成一个PDA $\mathcal{P}$，它具有参数$\mathcal{F} = X$，$\mathcal{K} = C$与$\mathcal{S} = Y$，使得对$x \in \mathcal{F}$与$c \in \mathcal{K}$ 有

1) $p_{x,c} = *$，若$\mathcal{H}$中没有边包含$\{x, c\}$，

2) $p_{x,c} = y \in \mathcal{S}$，若$\{x, y\}$是$\mathcal{G}$的一条边，且它被染成颜色$c$，即，$\{x, y, c\}$是$\mathcal{H}$的一条边。

注意到对每个$c \in \mathcal{K} = C$，我们仅选取提前选择好的μ条边，这也意味着我们总是可以让超图$\mathcal{H}$在$\mathcal{K} = C$这个顶点集是μ-正则的。由于$\mathcal{H}$是线性且(6, 3)-free的，并在$\mathcal{K}$是μ-正则的，那么，由定理6.3.2可知，$\mathcal{P}$是一个$(|C|, |X|, |X| - \mu, |Y|)$-PDA。如果我们想要构造一个常比率的CCC，我们认为第二种构造也许会比第一种更好。这是因为这种情形下有$R = |Y|/|X|$。因此，要使比率为常数，我们只需选取一个二部图使得其两个顶点集几乎拥有相同数量的顶点数。我们将在Ruzsa-Szeméredi图的构造中用到这个观察。

来自于Ruzsa-Szeméredi图的构造： 一个二部图被称为是(r, t)-Ruzsa-Szeméredi图，如果它的边集可以被看做是t个边不交的诱导匹配$M_1, \ldots, M_t$的并，使得$|M_1| = \cdots = |M_t| = r$。有时，条件“$= r$”与“$= s$”会被替换为“$\geq r$”与“$\geq s$”。注意到Ruzsa-Szeméredi图实际上就是二部图的特殊的强边染色。我们只需把$M_1, \cdots, M_t$ 染上t种不同的颜色$c_1, \ldots, c_t$。那

么，由定义可知我们会得到一个图$\mathcal{G} = M_1 \cup M_1 \cdots \cup M_t$的强边染色。投稿这篇论文之后，作者注意到从Ruzsa-Szeméredi图构造CCC方案的方法被一篇最近的文章[123]所使用了，他们了利用Alon等人[12]关于Ruzsa-Szeméredi图的构造，得到的CCC方案中，F是随K线性增长的。然而，他们的缓存方案的比率不是一个常数，而是有着$R = K^{\delta}$的形式，$\delta > 0$是一个任意小的正实数。这里，我们会用到Ruzsa-Szeméredi图的另一个已经存在的构造[73]，来构造一个常比率的CCC方案。在文献[73]中，作者构造了一个$(\frac{(1-o(1))}{3}N, N^{\Omega(\frac{1}{\log\log N})})$-Ruzsa-Szeméredi图，其中，$N$是每个顶点集的顶点数。因此，根据上一个段落的讨论，如果我们$\mu = r$与$\mathcal{K} = \{c_1, \ldots, c_t\}$，那么这样一个Ruzsa-Szeméredi图会导出一个PDA，具有参数$F = S = N$，$R = \frac{S}{F} = 1$，$\frac{M}{N} = \frac{N-\mu}{N} = \frac{N-\frac{(1-o(1))}{3}N}{N} = \frac{2}{3} + o(1)$，且$K = N^{\Omega(\frac{1}{\log\log N})}$。可以说明$\log K = \Omega(\frac{\log N}{\log\log N})$，注意到构造6和8给出的是$\log K = \Omega(\log\log N)$ 。然而，这个新构造有一个缺陷，它仅对$\frac{M}{N} = \frac{2}{3} + o(1)$成立。如何拓展这个构造，是一个有趣的问题。此外，下面的公开问题也很有趣。

问题1：是否存在一个二部(r, t)-Ruzsa-Szeméredi图$\mathcal{G}$，顶点集为X，Y，满足$|X| = |Y| = N$，$r = \Theta(N)$，$t = \Omega(N^a)$对某个$0 < a < 1$成立?

这个公开问题在Ruzsa-Szeméredi图的构造研究中也很有趣，见文献[12]。它也可以导出一个$(t, N, N-r, N)$-PDA，其中$N = \mathcal{O}(t^{1/a})$是t的多项式函数。

6.8 结语

在这篇文章中，我们把构造一个CCC方案或者PDA设计的问题转化为超图的观点。该问题与极值组合学中著名的(6, 3)-问题产生了联系。从这个观点出发，构造缓存方案转变为构造线性的(6, 3)-free3-均衡3-部超图。我们提供了两种方案，分别拓展了Maddah-Ali-Niesen方案与Yan等人的方案。我们方案中的参数很灵活，因此，我们实际上贡献了两大类缓存方案。

什么才是最小的F使得存在一个常比率的缓存方案? 我们的构造表明F随K 亚指数增长就足够了。定理6.3.4也说明，常比率的CCC方案F随K线性增长是不可能的。我们仍然不知道，是否存在F随K多项式增长的常比率方案。我们把它作为一个公开问题。

问题2：令M/N和R为与K无关的常数。找出最小的$F = f(K)$使得存在一个(K, F, Z, S)-PDA，满足$S = RF$，$Z = FM/N$。特别的，证明或否定存在一个F随着K多项式增长的构造。

7 Piggyback码

7.1 简介

由于其可靠性和有效性，分布式存储系统在上二十年吸引了很多的关注。在分布式存储系统中，整个数据存储在一系列存储节点中。这些节点物理独立并通过一个网络连接。因为每一个节点都有一定的概率损坏，我们必须引入冗余性来确保系统的可靠性。在文献中，有两种策略来保证冗余：复制和纠删编码。直观地说，复制很简单，但效率低下。相反，纠删编码提供了更好的存储效率。因此，为了处理大量的信息，纠删编码技术一直被应用于许多现代分布式存储系统中，例如，Google Colossus[2]，HDFS Raid[3]，Total Recall[26]，Microsoft Azure[86]与OceanStore[97]。

一旦一个单独的存储节点损坏，必须使用存储在幸存节点的数据将其恢复。当修复失败的节点时，有四个参数我们需要考虑，即，计算负载、网络带宽、磁盘I / O 和需访问磁盘的数量。在文献中，大多数现有的存储编码技术只是考虑这四个参数之一的最优性，例如，MDS码对计算负荷，再生编码对网络带宽[55]，局部修复代码对需访问磁盘的数量[110] [134]。本文的主要关心的是优化前两个参数。我们定义平均修复带宽率，γ，为平均修复带宽和原始数据量的比值。接下来，我们将简要地回顾三类存储码的修复复杂性和修复带宽，即，MDS存储码，MSR码和piggyback码。

MDS码是数据存储中一种被广泛使用纠删码，例如，文献[135,143]。它达到了最佳的冗余与效率之间的的权衡。一个$(k+r,k)$MDS 存储码包含$k+r$个存储节点，满足性质原始数据可以被$k+r$个节点中的任何k个所恢复。它可以容忍任何r个节点的损坏。这个属性被称为MDS性质。一个节点被称为是系统的，如果它存储了部分不加编码的原始数据。系统的MDS码是一个MDS码，且满足原始数据以不加编码的形式存储在k个系统节点中。剩下的r 个节点，被称为校验节点，存储k个系统节点的校验数据。从实用的角度来看，存储码最好是个系统码，因为在正常情况下，数据可以直接从系统节点中读取，而不需要执行解码。许多实际问题也需要高效的存储码，即，$r \ll k$。因此，在分布式存储系统的设计中，一个损坏的系统节点的修复效率是非常重要的。

在MDS存储码的情形下，修复损坏的存储节点只需利用有限域的加法和乘法，使其在修复过程中有合理的计算负载。然而，修复一个损坏的节点，MDS 存储码需要下载整个的原始数据。换句话说，MDS存储码的平均修复带宽，γ_{MDS}，等于1。

2010年，Dimakis等人[55]引入了再生码以降低分布式存储系统的修复带宽，它通过从每一个存活的节点下载相同数量的数据来修复损坏的系统节点。MSR码是最重要的再生码之一。它保持了MDS属性，且平均修复带宽率为$\gamma_{MSR} = \frac{k+r-1}{rk}$，这使当$r \ll k$时，有$\gamma_{MSR} \approx \frac{1}{r}$。当$r$逐渐增大时，$\gamma_{MSR}$ 比γ_{MDS}要小多了。然而，MSR码的一个缺点是，为了修复损坏的的系统节点，它的修复算法涉及到矩阵的乘法，其计算复杂度对现有的存储系统来说可能太高了。

构造具有以下特点的存储码是非常有意义的：满足MDS性质，低计算复杂性和低修复带宽。出于这些期望，开创性的论文[114,115]了提出一种piggybacking框架，它结合了MDS码和MSR码的优点。Piggybacking的想法是取多个现有码的实例，并从一例到另一例添加被精心设计过的piggyback函数。结果，文献[114]中定义的piggyback码（见文献[114]的第四节）不仅保持了MDS码的低计算复杂度，且有平均修复带宽率$\gamma_{RSR} = \frac{r-1}{2r-3} \approx \frac{1}{2} < \gamma_{MDS}$。从那时起，这个新想法已经被几个研究人员成功地应用了。在2013 年，它被Facebook[113]的新存储系统所采用了。2015年，Yang等人杨[149] 利用了piggybacking的策略来设计新的MSR码，它的校验节点也有几乎最优的修复带宽。Kumar等人[98]也使用这种技术，以降低容错性为代价，来构造具有低修复带宽和低修复复杂度的存储码。

不难看出，piggyback码的性能介于MDS码和MSR码之间。本文的主要目的是设计一个新的piggybacking框架，以进一步减少存储码的系统节点的修复带宽。我们的设计可以产生一个新的系统MDS存储码，其平均修复带宽率可以低至$\gamma_{NEW} = \frac{\sqrt{2r-1}}{r}$。显然，我们的结果对几乎所有的$r$都显著地改进了$\gamma_{RSR}$。此外，相比与MSR编码的高计算复杂度，修复新代码损坏的存储节点只涉及有限域中加法和乘法的运算。

7.2 Piggybacking框架

我们将介绍文献[114]所定义的一些概念。记$\mathbb{F} := \mathbb{F}_q$，这里$q$是一个素数幂。Piggybacking框架可以运行于任何一个已存在的码上，这个码被称之为基本码。不失一般性，我们可以假设基本码是由n个编码函数$\{f_i\}_{i=1}^n$所决定的，它被存储于n个存储节点中。考虑m个基本码的实例，则最初的编码体系如表7-1所示。

其中，$a_1, \ldots, a_m$表示m份基本码下被编码的信息。对每个$1 \le i \le n$ 与$2 \le j \le m$，我们可以为$f_i(a_j)$添加任意一个值$g_{i,j}(a_1, \ldots, a_{j-1})$。这些函数$g_{i,j} : \mathbb{F}^k \longrightarrow \mathbb{F},\ 1 \le i \le$

Node 1	$f_1(a_1)$	$f_1(a_2)$	$\cdots$	$f_1(a_m)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\cdots$
Node n	$f_n(a_1)$	$f_n(a_2)$	$\cdots$	$f_n(a_m)$

表 7-1 最初的编码系统

$n,\ 2 \leq j \leq m$就被称为是piggyback函数，它们是可以任意选取的。被添加的数值则被称为是piggybacks。因此，存储在第i个节点（行）和第j个实例（列）中的元素就是$f_i(a_j) + g_{i,j}(a_1, \ldots, a_{j-1})$。最后得到的piggyback码被描述在表7-2中。第一个实例中不含有piggybacks，这是因为这种安排可以让我们直接用基本码的译码算法来修复a_1。

Node 1	$f_1(a_1)$	$f_1(a_2) + g_{1,2}(a_1)$	$\cdots$	$f_1(a_m) + g_{1,m}(a_1, \ldots, a_{m-1})$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\cdots$
Node n	$f_n(a_1)$	$f_n(a_2) + g_{n,2}(a_1)$	$\cdots$	$f_n(a_m) + g_{n,m}(a_1, \ldots, a_{m-1})$

表 7-2 Piggyback码

在本文中，我们取基本码为一个系统的$(k+r, k)$MDS码，它的结构被表示在表7-3中，

Node 1	$a_{1,1}$	$a_{1,2}$	$\cdots$	$a_{1,m}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\ddots$
Node k	$a_{k,1}$	$a_{k,2}$	$\cdots$	$a_{k,m}$
Node $k+1$	$f_1(a_1)$	$f_1(a_2)$	$\cdots$	$f_1(a_m)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
Node $k+r$	$f_r(a_1)$	$f_r(a_2)$	$\cdots$	$f_r(a_m)$

表 7-3 系统的$(k+r, k)$ MDS码

其中，我们仍然取m份基本码的实例，并记$a_i = (a_{1,i}, a_{2,i}, \ldots, a_{k,i})^T$，$1 \leq i \leq m$。函数$\{f_i : 1 \leq i \leq r\}$被称为是校验函数，它们被选取以满足码的MDS性质。原始数据$\{a_1, a_2, \ldots, a_m\}$以不加编码的形式被存储在$k$个系统节点里。假设阵列中的每一个元素都存储了单位数量的数据。根据表7-2所介绍的piggybacking框架，表7-3 中的系统MDS码具有表7-4所描述的piggyback形式。

在piggyback的添加中，一个关键点是函数$g_{i,j}$仅仅能作用在它之前的实例上，即，$\{a_1, \ldots, a_{j-1}\}$。在下文中，我们将把这个限制条件称为“piggybacking条件”。已经被证明了，这个条件使得piggyback码保持了MDS性质（见文献[114]的定理1与引理2）。在文献[114] 中，作者提供了若干个码的构造。就修复带宽来说，第二个构造是最有效率的，

Node 1	$a_{1,1}$	$a_{1,2}$	$\cdots$	$a_{1,m}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\ddots$
Node k	$a_{k,1}$	$a_{k,2}$	$\cdots$	$a_{k,m}$
Node $k+1$	$f_1(a_1)$	$f_1(a_2)+g_{1,2}(a_1)$	$\cdots$	$f_1(a_m)+g_{1,m}(a_1,\ldots,a_{m-1})$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
Node $k+r$	$f_r(a_1)$	$f_r(a_2)+g_{r,2}(a_1)$	$\cdots$	$f_r(a_m)+g_{r,m}(a_1,\ldots,a_{m-1})$

表 7-4　系统的$(k+r,k)$ MDS piggyback码

它的最小平均带宽比为$\gamma_{RSR} \geq \frac{r-1}{2r-3}$，等号当$r-1 \mid k$时成立。在他们的构造中，共选取了基本码的$m := 2r-3$个实例。函数$f_i$为定义为$f_i(x) =< p_i, x >$，$1 \leq i \leq r$，其中$p_i \in \mathbb{F}^k$且$< \cdot,\cdot >$表示$\mathbb{F}$上传统的内积。表7-5简要的描述了存储在校验节点$k+i$中的元素，这里$i \in \{2,\ldots,r\}$。Piggybacks 的计算中涉及到的变量$v_i$，$q_{i,j}$，$i \in \{2,\ldots,r-2\}$，$j \in \{1,\ldots,r-1\}$全部属于$\mathbb{F}^k$。为了节约空间起见，这里我们并不给出其精确的表达。但我们可以一眼看出这个构造是有点复杂的，且难以理解。在下一节中，我们会给出一个简洁得多的piggybacking设计，然而，它可以得出低至$\gamma_{NEW} = \frac{\sqrt{2r-1}}{r}$的平均修复带宽率。

文献[98]中介绍了另一类piggyback码。它依据于两类校验元素，其中第一类被用于满足好的容错性，第二类被用于降低修复带宽和复杂性。然而，这样的构造并不能满足MDS性质。在第四小节，我们会比较这些构造的优劣性。

$p_i^T a_1$	$\cdots$	$p_i^T a_{r-2}$	$q_{i,i-1}^T a_{r-1} - \sum_{j=r}^{2r-3} p_i^T a_j$	$p_i^T a_r + q_{i,1}^T v_i$
$\cdots$	$p_i^T a_{r+i-3} + q_{i,i-2}^T v_i$	$p_i^T a_r + q_{i,i}^T v_i$	$\cdots$	$p_i^T a_{2r-3} + q_{i,r-1}^T v_i$

表 7-5　RSR piggyback码

7.3　新的piggybacking设计

在本节中，我们将介绍我们的piggybacking设计和相应的修复算法。我们的主要贡献在于减少系统节点的修复带宽，这是许多现有的存储码所主要关心的问题。我们的设计是基于对piggyback函数的仔细的选择和放置。我们首先从一个例子开始，用它来说明我们的想法。

7.3.1　Piggybacked (11,6) MDS码

我们将仔细描述一个(11,6)系统MDS码的piggybacking设计。取基本码的五份（我们是

有意识的去取五分）实例。构造被表示为如下表7-6。

$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$
$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$
$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$
$a_{4,1}$	$a_{4,2}$	$a_{4,3}$	$a_{4,4}$	$a_{4,5}$
$a_{5,1}$	$a_{5,2}$	$a_{5,3}$	$a_{5,4}$	$a_{5,5}$
$a_{6,1}$	$a_{6,2}$	$a_{6,3}$	$a_{6,4}$	$a_{6,5}$
$f_1(a_1)$	$f_1(a_2)$	$f_1(a_3)$	$f_1(a_4)$	$f_1(a_5)$
$f_2(a_1)$	$f_2(a_2)$	$f_2(a_3)+a_{5,1}+a_{6,1}$	$f_2(a_4)+a_{3,1}+a_{4,1}$	$f_2(a_5)+a_{1,1}+a_{2,1}$
$f_3(a_1)$	$f_3(a_2)$	$f_3(a_3)+a_{5,2}+a_{6,2}$	$f_3(a_4)+a_{3,2}+a_{4,2}$	$f_3(a_5)+a_{1,2}+a_{2,2}$
$f_4(a_1)$	$f_4(a_2)$	$f_4(a_3)$	$f_4(a_4)+a_{3,3}+a_{4,3}$	$f_4(a_5)+a_{1,3}+a_{2,3}$
$f_5(a_1)$	$f_5(a_2)$	$f_5(a_3)$	$f_5(a_4)$	$f_5(a_5)+a_{1,4}+a_{2,4}$

表 7-6 Piggybacked (11,6) MDS码

可以观察到所有系统节点被划分为三个子集$S_1=\{1,2\}$，$S_2=\{3,4\}$与$S_3=\{5,6\}$。S_1, S_2, S_3的部分元素被分别放入实例5，4，3作为piggybacks。更准确地说，S_1的前四个实例的元素被放入实例5作为piggybacks，S_2的前三个实例的元素被放入实例4作为piggybacks，S_3的前两个实例的元素被放入实例3作为piggybacks。因此，不同S_i的节点有不同的修复算法，每个S_i我们都取一个节点为例：

(a) 考虑节点1的修复。首先，下载$\{a_{i,5}:2\le i\le 6\}$与$f_1(a_5)$，利用MDS性质解码整个向量a_5。那么，可以分别从实例（列）5与节点2中下载$\{f_{j+1}(a_5)+a_{1,j}+a_{2,j}:1\le j\le 4\}$与$\{a_{2,j}:1\le j\le 4\}$。因为$a_5$是完全已知的，可以计算出$\{f_{j+1}(a_5):1\le j\le 4\}$。那么对$1\le j\le 4$，$a_{1,j}$可以由从$f_{j+1}(a_5)+a_{1,j}+a_{2,j}$中减去$a_{2,j}$与$f_{j+1}(a_5)$得到。在修复节点1时下载的所有数据量是$6+4\times 2=14$。节点2的修复策略是类似的。

(b) 考虑节点3的修复。首先，$a_{3,5}$可以由下载$\{a_{i,5}:1\le i\le 6,\ i\ne 3\}$与$f_1(a_5)$所恢复（利用MDS性质）。那么，$a_{3,4}$可以由下载$\{a_{i,4}:1\le i\le 6,\ i\ne 3\}$与$f_1(a_4)$所恢复。现在只需修复$\{a_{3,j}:1\le j\le 3\}$。我们将使用实例（列）4中添加的piggybacks。分别从实例4与节点4中下载$\{f_{j+1}(a_4)+a_{3,j}+a_{4,j}:1\le j\le 3\}$与$\{a_{4,j}:1\le j\le 3\}$。由于$a_4$是完全已知的，可以计算出$\{f_{j+1}(a_4):1\le j\le 3\}$。因此，对$1\le j\le 3$，$a_{3,j}$可以通过从$f_{j+1}(a_4)+a_{3,j}+a_{4,j}$中减去$a_{4,j}$与$f_{j+1}(a_4)$所恢复。修复节点3所需下载的数据量为$6\times 2+3\times 2=18$。节点4的修复策略是类似的。

(c) 考虑节点5的修复。首先，$\{a_{5,j} : 3 \le j \le 5\}$可以通过下载$\{a_{i,j} : 1 \le i \le 6,\ i \ne 5,\ 3 \le j \le 5\}$与$\{f_1(a_j) : 3 \le j \le 5\}$所恢复（利用MDS性质）。现在只需恢复$a_{5,1}$与$a_{5,2}$，它们可以通过利用添加到$f_2(a_3)$与$f_3(a_3)$的piggybacks来恢复。可以计算出修复节点5所需下载的数据量为$6 \times 3 + 2 \times 2 = 22$。节点6的修复策略是类似的。

很容易看到，该码的平均修复带宽为$\frac{14+18+22}{3} = 18$，平均修复带宽率为$\gamma = \frac{18}{30} = \frac{3}{5}$。修复属于不同集合的节点所需的数据量是属于不同层级的。它的原因是第二小节中介绍的piggybacking条件，即，后面的实例中存储的元素不能作为piggybacks被添加到前面的实例中去。因此，我们只能通过MDS性质而不是piggybacking来获取更多的信息。例如，在节点1的修复时，我们只利用了一次MDS 属性，（恢复a_5），但是为了恢复节点3，我们必须用MDS性质两次（一次恢复a_4，另一次恢复a_5，a_5中的信息只能通过使用MDS性质从实例5中得知）。这个观察实际上揭露了我们的构造的关键点：把系统节点分成不同的子集，把相同子集里的元素作为piggybacks添加到同一个实例上。

7.3.2 一般的piggybacking框架

我们将介绍关于修复MDS码系统节点的一般的piggybacking框架。任取一个系统$(k + r, k)$ MDS码作为基本码。一般地说，为了构造一个piggyback码$\mathcal{C}$，我们将取基本码的r份实例。令$\mathcal{S} = \{s_i : 1 \le i \le t\}$是$t$个正整数的集合，使得$\sum_{i=1}^{t} s_i = k$。如上面的例子所示，$\mathcal{C}$的$k$个系统节点被划分为$t$个组，$\mathcal{S}_1, \ldots, \mathcal{S}_t$，使得$|\mathcal{S}_i| = s_i$，$1 \le i \le t$。不失一般性，假设$\mathcal{S}_1 = \{1, 2, \ldots, s_1\}$和$\mathcal{S}_i = \{\sum_{j=1}^{i-1} s_j + 1, \ldots, \sum_{j=1}^{i} s_j\}$对$2 \le i \le t$成立。对一个$\mathbb{F}$上$k$长向量$\Lambda = (\lambda_1, \ldots, \lambda_k)$，$t$个piggyback函数$\{g_i : 1 \le i \le t\}$被定义为是$g_i(\Lambda) = \sum_{j \in \mathcal{S}_i} \lambda_j$。我们一般的piggybcking框架如下所示。

Node 1	$a_{1,1}$	$\cdots$	$a_{1,r-t}$	$a_{1,r-t+1}$	$\cdots$	$a_{1,r-1}$	$a_{1,r}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Node k	$a_{k,1}$	$\cdots$	$a_{k,r-t}$	$a_{k,r-t+1}$	$\cdots$	$a_{k,r-1}$	$a_{k,r}$
Node $k+1$	$f_1(a_1)$	$\cdots$	$f_1(a_{r-t})$	$f_1(a_{r-t+1})$	$\cdots$	$f_1(a_{r-1})$	$f_1(a_r)$
Node $k+2$	$\vdots$	$\ddots$	$\vdots$	$f_2(a_{r-t+1}) + g_t(a_1)$	$\cdots$	$f_2(a_{r-1}) + g_2(a_1)$	$f_2(a_r) + g_1(a_1)$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Node $k+r-t+1$	$\vdots$	$\ddots$	$\vdots$	$f_{r-t+1}(a_{r-t+1}) + g_t(a_{r-t})$	$\ddots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Node $k+r-1$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\ddots$	$f_{r-1}(a_{r-1}) + g_2(a_{r-2})$	$\vdots$
Node $k+r$	$f_r(a_1)$	$\cdots$	$f_r(a_{r-t})$	$f_r(a_{r-t+1})$	$\cdots$	$f_r(a_{r-1})$	$f_r(a_r) + g_1(a_{r-1})$

表 7-7 一般的piggybacking框架

注意到在上述表格中，前$k+1$个节点是保持不变的。我们的构造可以被总结如下：

(a) a_r中没有任何元素被当做piggybacks。

(b) 对$r-t+1 \le j \le r-1$，a_j的元素中属于$\cup_{l=1}^{r-j}\mathcal{S}_l$的被当做了piggybacks。更精确地说，对$1 \le l \le r-j$，$a_j$中被限制于$\mathcal{S}_l$的元素被放入第$r-l+1$个实例的第$(j+1)$个校验节点中作为piggybacks。

(c) 对$1 \le j \le r-t$，a_j中的所有元素被作为piggybacks。更精确地，对$1 \le l \le t$，a_j中被限制于$\mathcal{S}_l$的元素被入第$r-l+1$个实例的第$(j+1)$个校验节点中作为piggybacks。

因此，修复属于不同组的系统节点所需的数据量属于不同的层级。例如，假设我们希望恢复$\mathcal{S}_l$中某个被损坏的节点i，即元素$\{a_{i,j} : 1 \le j \le r\}$。注意到对$1 \le j \le r-l$，元素$a_{i,j}$被以形式$f_{j+1}(a_{r-l+1}) + g_l(a_j)$添加为第$r-l+1$个实例的第$j+1$个校验节点作为piggyback。为了更好地理解，我们可以回忆表7-7的第i行和第$(r-l+1)$列：

			$\vdots$			
$a_{i,1}$	$\cdots$	$a_{i,r-l}$	$a_{i,r-l+1}$	$a_{i,r-l+2}$	$\cdots$	$a_{i,r}$
			$f_1(a_{r-l+1})$			
			$f_2(a_{r-l+1}) + g_l(a_1)$			
			$\vdots$			
			$f_{r-l+1}(a_{r-l+1}) + g_l(a_{r-l})$			
			$f_{r-l+2}(a_{r-l+1})$			
			$\vdots$			
			$f_r(a_{r-l+1})$			

为了修复$\{a_{i,j} : 1 \le j \le r\}$，首先，每个$a_{i,j}$, $r-l+1 \le j \le r$只能用MDS性质来恢复，因此我们需要下载的数据量是kl。其次，每个$a_{i,j}$，$1 \le j \le r-l$可以由下载$f_{j+1}(a_{r-l+1}) + g_l(a_j)$与$\{a_{i',j} : i' \in \mathcal{S}_l,\ i' \ne i\}$所恢复，因此所需下载的数据量为$(r-l)|\mathcal{S}_l|$。因为我们可知$f_{j+1}(a_{r-l+1})$，如果$a_{r-l+1}$被恢复了，$a_{i,j}$可以由从$f_{j+1}(a_{r-l+1}) + g_l(a_j)$中减去$f_{j+1}(a_{r-l+1})$与$\sum_{i':i' \in \mathcal{S}_l, i' \ne i} a_{i',j}$所恢复。因此，恢复节点$i \in \mathcal{S}_l$所需下载的数据量是$kl + (r-l)s_l$。我们可以得出修复所有系统点时所需下载的数据量为：

$$\sum_{l=1}^{t}(kl + (r-l)s_l)s_l.$$

现在只需找出(7-1)的最小值：

$$\begin{aligned} &\min \sum_{l=1}^{t}(kl+(r-l)s_l)s_l, \\ &s.t.\ \sum_{l=1}^{t} s_l = k\ and\ s_1,\ldots,s_t,t \in \mathbb{Z}^+. \end{aligned} \tag{7-1}$$

遗憾地是，我们不能精确地计算出(7-1)的最小值。无论如何，我们总可以令s_i为某些特殊值，使得目标函数足够小。例如，我们令$s_1 = \cdots = s_t = \frac{k}{t}$，这导出了如下的平均修复带宽率：

$$\begin{aligned} \gamma &= \frac{1}{rk^2}\sum_{l=1}^{t}\frac{k}{t}(kl+(r-l)\frac{k}{t}) \\ &= \frac{1}{2}(\frac{t}{r}+\frac{1}{t}(2-\frac{1}{r})). \end{aligned} \tag{7-2}$$

由平均值不等式，(7-2)在$t=\sqrt{2r-1}$时达到最小值$\gamma = \frac{\sqrt{2r-1}}{r}$。.

我们把具有以上参数的码记为$\mathcal{C}_{NEW}$。若我们通过下载所有的数据来修复损坏的校验节点，则当$r \ll k$时，所有节点的平均修复带宽率为

$$\gamma_{NEW} = \frac{\frac{\sqrt{2r-1}}{r}k+r}{k+r} \approx \frac{\sqrt{2r-1}}{r} = \mathcal{O}(\frac{1}{\sqrt{r}}).$$

7.4 一些现存的码的比较

在本节中，我们比较一些现存的存储码的表现，即，MDS码，文献[98]与文献[114]提出的piggyback码，以及我们新构造的piggyback码。为了衡量这些码类的修复复杂度和编码复杂度，我们首先考虑有限域$\mathbb{F}_q$上基本运算的复杂性。记$e = \lceil \log_2 q \rceil$，那么一次加法需要$e$次初等的二元加法，一次乘法则需要$e^2$次。对$1 \le i \le r$，我们定义校验函数$f_i$为$f_i(a) =< p_i, a >$，其中$p_i \in \mathbb{F}_q^k$是经仔细选择过的向量。那么MDS码的单个节点的修复复杂度为$ke^2+(k-1)e$。令$x := ke^2+(k-1)e$。考虑新构造的piggyback码，对$1 \le l \le t$，一个系统节点$i \in \mathcal{S}_l$ 的修复复杂度为

$$lx+(r-l)(x+s_le) = rx+(r-l)s_le,$$

其中求和的第一部分对应修复节点i中最后l个元素的计算量，第二部分则对应于修复节点i中前$r-l$个元素所需的计算量。修复所有系统节点的总计算量为$\sum_{l=1}^{t} s_l(rx+(r-l)s_le)$。

另一方面修复所有r个校验节点的总计算量为$r^2x+\sum_{l=1}^{t}(r-l)s_le$。所以，全部$k+r$个节点的平均修复复杂度最多为

$$\frac{\sum_{l=1}^{t}s_l(rx+(r-l)s_le)+r^2x+\sum_{l=1}^{t}(r-l)s_le}{k+r}=rx+\frac{\sum_{l=1}^{t}(r-l)s_l(s_l+1)e}{k+r}.$$

我们也能计算出MDS码（仅有一个实例时）与新码的编码复杂度，它们分别是rx与$r^2x+\sum_{l=1}^{t}s_l(r-l)e$。容易看出，在都有$r$个实例时，MDS码与新码的修复复杂度与编码复杂度都是非常接近的。对文献[98,114]中的piggyback码，也能计算出类似的参数。我们总结如下：

	Number of Instances	Fault Tolerance	Average Repair Bandwidth Rate	Average Repair Complexity	Encoding Complexity
MDS	1	r	1	x	rx
RSR[114]	$2r-3$	r	$\frac{r-1}{2r-3}$	$\mathcal{O}((2r-3)x)$	$\leq(2r-3)rx+kre^2+kre$
KAAB[98]	k	$\geq n_A-k-\tau+1$	$<\frac{k+\tau+(k-\tau-1)^2}{k^2}$	$\frac{C_R}{k}$	C_E
New code	r	r	$\approx\frac{\sqrt{2r-1}}{r}$	$\leq rx+\sqrt{r}x$	$\leq r^2x+kre$

表 7-8 一些$(k+r,k)$ piggyback码的比较

其中，$n_A\leq\min\{k+r,2k\}$，$\tau\geq1$，C_R, C_E被定义在文献[98]中，我们记新码为$\mathcal{C}_{NEW}$。

结合实例的数量考虑，我们发现MSR码，RSR码和新码的容错能力，平均修复复杂性和编码复杂性都是非常相近的。对平均修复带宽率来说，我们有$\gamma_{NEW}\ll\gamma_{RSR}<\gamma_{MDS}$。对KAAB 码来说，文献[98]提到它的平均修复复杂度与编码复杂度甚至可以比MDS 码还要低。然而，如果我们令$\gamma_{KAAB}=\Theta(\frac{1}{\sqrt{r}})$，则有$\tau=\Theta(k(1-\frac{1}{r^{1/4}})$，这导致容错能力损失非常大。我们构造的另一个优点是，所需实例的个数比RSR要少，且在$r\ll k$时比KAAB码要少得多。

如同文献[114]中所提到的，实际应用中的数据中心希望存储码是MDS，高码率的且仅有少部分的实例，此外，它们还需有低修复带宽和复杂性。不难看出，我们新构造的码比其它码要更能符合这些条件。

7.5 结语

本章的主要目的是优化修复分布式存储系统中的系统节点时所需的带宽和复杂性。遗憾地是，我们很难构造出满足以下三个条件的好码：

(a) MDS性质，

(b) 修复复杂性相近于MDS码，

(c) 平均修复带宽率相近于MSR码，即可以低至c/r，c为某个常数。

我们新构造的码仅满足前两个条件，且有平均修复带宽率$\gamma_{NEW} = \Theta(\frac{1}{\sqrt{r}})$。因此，为了以后的研究，我们可以提出如下两个公开问题。

问题1：给出一个等式或不等式，使得修复复杂性和修复带宽之间的权衡可以用数学公式表达出来。

问题2：在条件(a)和(b)下，决定修复一个损坏节点的最小修复带宽率。

8 有限域上的直角

8.1 简介

8.1.1 多项式方法

Croot，Lev和Pach[53]以及Ellenberg和Gijswijt[64]最近的突破性文章分别证明了$\mathbb{Z}_4^n$与$\mathbb{F}_3^n$上不含三长等差数列的子集都是指数小的。他们证明里核心的思想是一种新颖的多项式方法的应用。随后，陶哲轩[138]在他的博客中总结了这种方法，把它归于一个计算某些函数和超矩阵的秩的一种准则。

这个问题也可以被看做是一个有限域上的极值问题，它禁止了某些给定结构的存在。为了使用多项式方法来处理这个问题，基本的思路是用一个合适的多项式来刻画这个被禁止的结构。例如，令A是$\mathbb{F}_3^n$的一个子集，且不含有三长的等差数列。这等价于说对三个元素$x,y,z\in A$，$x+y+z=0^n$当且仅当$x=y=z$。在文献[138]里，这个观察被看做是定义在$A\times A\times A$到$\mathbb{F}_3$上的两个多项式之间的等式：

$$\delta_{0^n}(x+y+z)=\sum_{a\in A}\delta_a(x)\delta_a(y)\delta_a(z), \tag{8-1}$$

这里$\delta_a(x)$是Kronecker函数，使得$x=a$时，$\delta_a(x)=1$，其它情况下，$\delta_a(x)=0$。因此，如果我们可以对$\mathbb{F}_3^n$ 上的多值函数定义一个合适的秩，那么我们或许可以通过用两种方式计算(8-1)中函数的秩，给A的大小一个上界。

我们把这类极值问题称为是“对称的”，因为目标集合中的一些元素形成禁止结构当且仅当它们是全部相等的。例如，对任意$a,b,c\in\mathbb{F}_q$满足$a+b+c=0$，决定$\mathbb{F}_q^n$的最大子集使得其不含方程$ax+by+cz=0$的非平凡解（一个解是平凡的当且仅当$x=y=z$）是对称的。文献[95]中研究的tri-colored sum-free集与文献[105]中研究的sunflower-free集也都是对称的。所有这些对称的极值问题都可以用一个类似于(8-1)的秩的计算方式来处理。然而，在研究中有很多“非对称”的极值问题也是非常有趣的。例如，一个集族$\mathcal{F}\subseteq 2^{[n]}$被称为是2-cover-free[66]的，如果对任意的$A,B,C\in\mathcal{F}$，$A\subseteq B\cup C$当且仅当$A=B$或$A=C$。显

然，由我们的定义这是一个非对称的问题。文献[131]中提到的$\{1,2\}$-可分哈希族也是一类非对称的极值问题。

本文的目的就是拓展之前研究者们的多项式方法来处理一个非对称的极值问题。我们采用了陶哲轩的计数引理的一个变形（见引理8.2.2）。我们的新引理也是可以写成一族Kronecker函数的和，这让我们可以用一个类似于[138]中的方法来得到一个极值问题的上界，我们将在下一节详细介绍。

8.1.2 $\mathbb{F}_q^n$上的直角

设q为一个素数幂，$V := \mathbb{F}_q^n$ 是有限域$\mathbb{F}_q$上的n维向量空间。我们将考察V的一个极值性质。我们感兴趣的是V的最大子集的大小，使得其不包含任何直角。一个集合$A \subseteq V$包含一个直角如果存在三个不同的元素$x, y, z \in A$使得$< z-x, y-x >= 0$，这里$< \cdot, \cdot >$表示$\mathbb{F}_q$上的内积。这个问题是Erdős-Flaconer型问题的有限域版本。它是该问题在欧式空间[69,72,83]下的自然推广。在欧式空间里，人们关心对给定的n和α，最小的d使得对任何紧集$A \subseteq \mathbb{R}^n$，其Hausdorff维数大于d时就包含三个点形成角α。文献[84]介绍了更多欧式空间问题的有限域版本。

注意到，若A不含直角，则对任何三个元素（不一定互不相同）$x, y, z \in A$，$< z-x, y-x >= 0$当且仅当$z = x$或$y = x$，或$z = y$且$< y-x, y-x >= 0$。容易看出，这是一个非对称的问题。公式(8-1)并不能用来直接解决这个问题。

记$R(n,q)$为$\mathbb{F}_q^n$的最大的不含直角的子集。在文献[22]中，Bennett证明了$R(n,q) \leq \mathcal{O}(q^{\frac{n+2}{3}})$。在这篇文章里，对奇的素数幂$q$，我们证明了$R(n,q) \leq \binom{n+q}{q-1} + 3$（见定理8.3.1）。当$q$固定时，我们的结果显著地改进了之前的结果。例如，当$q = 3$时，$R(n,3)$被从$\mathcal{O}(3^{\frac{n+2}{3}})$改进到$(n+3)^2+3$。我们的新上界实际上是$n$ 的一个多项式函数。这是非常有意思的，因为之前使用类似的多项式方法得到的结果都是n的指数函数。

8.2 Tao的计数公式的变形

我们从[138]中引入的一些必要的几号开始。令$\mathbb{F}$是一个域，A是一个有限集合。一个定义在k个变量$x_1, \ldots, x_k$上的函数被称为是秩一的，如果它是非零的，且有形式$T(x_1, \ldots, x_k) = f(x_i)g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$，其中$1 \leq i \leq k$，$f : A \longrightarrow \mathbb{F}$与$g : A^{k-1} \longrightarrow \mathbb{F}$。一个一般的函数$T : A^k \longrightarrow \mathbb{F}$的秩被定义为所需的最少的秩一函数以把$T$表示成它们的线性组合。例如，当$k = 2$时，一个秩一函数有形式$T(x,y) = f(x)g(y)$，其中$f, g : A \longrightarrow \mathbb{F}$。当$k = 3$时，秩一函数有形式$T_1(x,y,z) = f_1(x)g_1(y,z)$或$T_2(x,y,z) =$

$f_2(y)g_2(x,z)$或$T_3(x,y,z)=f_3(z)g_3(x,y)$，其中$f_i:A\longrightarrow\mathbb{F}$，$g_i:A^2\longrightarrow\mathbb{F}$，$1\leq i\leq 3$。注意到$r$个秩一函数的线性组合将给出一个秩最多为$r$的函数。

在[138]中，作者说明了$\sum_{a\in A}\delta_a(x)\delta_a(y)\delta_a(z)$ 的秩是$|A|$。本节的主要目的是证明一个类似的结果，它说明了$\sum_{a\in A}(\delta_a(y)\delta_a(z)+(1-\delta_a(y))(1-\delta_a(z)))\delta_a(x)$的秩至少为$|A|-2$。

引理8.2.1. 令$A=\{a_1,\ldots,a_m\}$是一个大小为m的有限集合，$\mathbb{F}$是一个奇特征的有限域。对每个$a\in A$，令$c_a\in\mathbb{F}$为一个非零常数。那么，函数$T(y,z):A\times A\longrightarrow\mathbb{F}$

$$T(y,z)=\sum_{a\in A}c_a\cdot(\delta_a(y)\delta_a(z)+(1-\delta_a(y))(1-\delta_a(z))) \tag{8-2}$$

的秩至少是$m-2$。

证明. 假设$r(T(y,z))=s$，即，我们有表示$T(y,z)=\sum_{i=1}^{s}f_i(y)g_i(z)$，$f_i$与$g_i$为某些函数。我们的目标是证明$s\geq m-2$。记$\sum_{a\in A}c_a=\tau$，容易计算并得出

$$T(y,z)=\begin{cases}\tau, & y=z,\\ \tau-c_y-c_z, & y\neq z.\end{cases}$$

考虑$m\times m$的矩阵$\mathcal{P}$，

$$\mathcal{P}=\sum_{i=1}^{s}\begin{pmatrix}f_i(a_1)\\ f_i(a_2)\\ \vdots\\ f_i(a_m)\end{pmatrix}\begin{pmatrix}g_i(a_1), & g_i(a_2), & \cdots, & g_i(a_m)\end{pmatrix}.$$

$\mathcal{P}$在$\mathbb{F}$上的传统的矩阵秩最多为s。此时，为了证明引理，只需说明矩阵$\mathcal{P}$的秩最少是$m-2$。考察$\mathcal{P}$的第j行第k列的元素p_{jk}，容易看出

$$p_{jk}=\sum_{i=1}^{s}f_i(a_j)g_i(a_k)=T(a_j,a_k)=\begin{cases}\tau, & j=k,\\ \tau-c_j-c_k, & j\neq k,\end{cases}$$

此处我们记$c_j=c_{a_j}$，$1\leq j\leq m$。所以$\mathcal{P}$有如下的表示形式

$$\mathcal{P} = \begin{pmatrix} \tau & & & & \\ & \tau & & \tau - c_k - c_j & \\ & & \ddots & & \\ & \tau - c_j - c_k & & \ddots & \\ & & & & \tau \end{pmatrix}.$$

通过简单的高斯消去法（先利用$\mathcal{P}$的第一列做消除，再利用新矩阵的第二行做消除），$\mathcal{P}$可以被转化为下面的矩阵

$$\begin{pmatrix} \tau & -c_1 - c_2 & -c_1 - c_3 & \cdots & \cdots & -c_1 - c_m \\ \tau - c_1 - c_2 & c_1 + c_2 & c_1 - c_3 & \cdots & \cdots & c_1 - c_m \\ c_2 - c_3 & -2c_2 & 2c_3 & 0 & \cdots & 0 \\ \vdots & \vdots & 0 & \ddots & & \vdots \\ \vdots & \vdots & \vdots & & \ddots & 0 \\ c_2 - c_m & -2c_2 & 0 & \cdots & 0 & 2c_m \end{pmatrix}.$$

因此，$\mathcal{P}$的矩阵秩最少为$m-2$，因为上面的矩阵包含一个$(m-2)\times(m-2)$的对角矩阵，其对角元素$2c_3, \ldots, 2c_m$都是$\mathbb{F}$的非零元素。引理可由不等式$s \geq m-2$推出。 □

一个很重要的观察是，如果我们把$\delta_a(x)$加到(8-2)右边的求和项中，新函数$T(x,y,z)$的秩保持不变。

引理8.2.2. 令$A = \{a_1, \ldots, a_m\}$是一个大小为m的有限集，$\mathbb{F}$为奇特征的有限域。对每个$a \in A$，令$c_a \in \mathbb{F}$为一个非零系数。则函数$T(x,y,z) : A \times A \times A \longrightarrow \mathbb{F}$

$$T(x,y,z) = \sum_{a \in A} c_a(\delta_a(y)\delta_a(z) + (1-\delta_a(y))(1-\delta_a(z)))\delta_a(x)$$

的秩至少为$m-2$。

证明. 假设$r(T(x,y,z)) \leq m-3$。换句话说，我们有

$$T(x,y,z) = \sum_{\alpha \in I_1} f_\alpha(x) g_\alpha(y,z) + \sum_{\beta \in I_2} f_\beta(y) g_\beta(x,z) + \sum_{\gamma \in I_3} f_\gamma(z) g_\gamma(x,y) \tag{8-3}$$

对某些集合I_1, I_2, I_3，$|I_1| + |I_2| + |I_3| \leq m-3$成立。

考察$\mathbb{F}$上的线性空间，它含有正交于所有$f_\alpha(x), \alpha \in I_1$的函数，也就是被定义为

$$H = \{h : A \longrightarrow \mathbb{F} \mid \sum_{x\in A} f_\alpha(x)h(x) = 0 \text{ for all } \alpha \in \mathrm{I}_1\}$$

的空间。那么，我们有$d := \dim_{\mathbb{F}}(H) \geq |A| - |I_1| = m - |I_1|$。设$\{h_1, \ldots, h_d\}$为$H$的一组基。$h_i(a_j), 1 \leq i \leq d, 1 \leq j \leq m$生成的$d \times m$矩阵是行满秩的，包含一个非奇异的$d \times d$子矩阵，该子矩阵的边集对应于某个$A' \subseteq A$，$|A'| = d$。由$A'$标记的那些列的非奇异性，不难得出存在一个函数$h \in H$在$A'$的每个元素都取零值。

如果我们把(8-3)的两边都乘以$h(x)$，并对x求和，则有

$$\begin{aligned}
&\sum_{x\in A}\sum_{a\in A} c_a(\delta_a(y)\delta_a(z) + (1-\delta_a(y))(1-\delta_a(z)))\delta_a(x)h(x) \\
=&\sum_{a\in A} c_a h(a)(\delta_a(y)\delta_a(z) + (1-\delta_a(y))(1-\delta_a(z))) \\
:=&T_1(y,z)
\end{aligned} \tag{8-4}$$

与

$$\begin{aligned}
&\sum_{x\in A}(\sum_{\alpha\in I_1} f_\alpha(x)g_\alpha(y,z) + \sum_{\beta\in I_2} f_\beta(y)g_\beta(x,z) + \sum_{\gamma\in I_3} f_\gamma(z)g_\gamma(x,y))h(x) \\
=&\sum_{\alpha\in I_1} g_\alpha(y,z)\sum_{x\in A} f_\alpha(x)h(x) + \sum_{\beta\in I_2} f_\beta(y)\sum_{x\in A} g_\beta(x,z)h(x) \\
+&\sum_{\gamma\in I_3}\sum_{x\in A} f_\gamma(z)g_\gamma(x,y)h(x) \\
=&\sum_{\beta\in I_2} f_\beta(y)\sum_{x\in A} g_\beta(x,z)h(x) + \sum_{\gamma\in I_3} f_\gamma(z)\sum_{x\in A} g_\gamma(x,y)h(x) \\
:=&T_2(x,y,z),
\end{aligned} \tag{8-5}$$

这里(8-5)的第二个等式来自于事实$h \in H$。注意到，$c_a \neq 0$对所有$a \in A$都成立，且$h(x)$在A的至少$m - |I_1|$个元素上非零。那么$\{c_a h(a) : a \in A\}$的非零元素至少有$m - |I_1|$个。由引理8.2.1可知，$r(T_1(y,z)) \geq m - |I_1| - 2$。另一方面，显然有$r(T_2(x,y,z)) \leq |I_2| + |I_3| \leq m - 3 - |I_1|$。由于$T_1(y,z) = \sum_{x\in A} T(x,y,z)h(x) = T_2(x,y,z)$，则$m - |I_1| - 2 \leq r(\sum_{x\in A} T(x,y,z)h(x)) \leq m - 3 - |I_1|$，这是一个矛盾。因此，我们有$r(T(x,y,z)) \geq m - 2$。

□

注记8.2.3. *引理8.2.1与引理8.2.2是文献[138]中引理1的非对称形式，它可以被用来处理第一节中定理的非对称极值问题。引理8.2.1仅对有限域有奇特征成立。这是因为在我们的问*

题里，$< z-x, y-x >$可能在$z=y$且$< y-x, y-x >= 0$时取零值。对一些其它的应用，例如x, y, z满足某个性质“*P*”当且仅$x=y$或$x=z$（但不是$y=z$），我们可以移除奇特征的限制，则这种情况下*(8-2)* 的右端应该为$\sum_{a\in A} c_a \cdot (1-\delta_a(y))(1-\delta_a(z))$。这种方法也能被拓展到更一般的情形，即，若某些元素$x_0, x_1, \ldots, x_k$满足性质*P*当且仅当$x_0 = x_i$对某个$1 \le i \le k$成立。这个证明非常类似于引理*8.2.1*与引理*8.2.2*的证明。

8.3 $\mathbb{F}_q^n$上不包含直角的子集

在本节中，我们用之前章节里建立的秩的计算方法来证明这篇文章的主要结论。

定理8.3.1. 令q是一个奇素数幂，A是$\mathbb{F}_q^n$的一个子集，使得不存在三个不同元素$x, y, z \in A$满足$< z-x, y-x >= 0$，那么，$|A| \le \binom{n+q}{q-1} + 3$。

证明. 定义函数$f : A \times A \times A \longrightarrow \mathbb{F}_q$ 为

$$f(x,y,z) = \sum_{a\in A} \delta_a(y)\delta_a(z) + (1 - \sum_{a\in A} \delta_a(y)\delta_a(z)) < z-x, y-x >^{q-1}. \tag{8-6}$$

由于A不含直角，则$< y-x, z-x >\neq 0$对$x, y, z \in A$都成立。因此，若x, y, z是A的不同元素，$< y-x, z-x >^{q-1}= 1$。容易验证

$$f(x,y,z) = \begin{cases} 0, & y \neq z \; and \; x = y \; or \; x = z, \\ 1, & otherwise. \end{cases} \tag{8-7}$$

不妨回忆引理8.2.2中定义的函数$T(x, y, z)$。如果我们把所有系数c_a都取为1，更新$T(x, y, z)$为

$$T(x,y,z) = \sum_{a\in A} (\delta_a(y)\delta_a(z) + (1-\delta_a(y))(1-\delta_a(z)))\delta_a(x),$$

那么也不难证明

$$T(x,y,z) = \begin{cases} 0, & y \neq z \; and \; x = y \; or \; x = z, \\ 1, & otherwise. \end{cases} \tag{8-8}$$

因此，式(7)和式(8)说明作为定义在$A \times A \times A \longrightarrow \mathbb{F}_q$的函数，我们有$T(x, y, z) = f(x, y, z)$。一方面，引理8.2.2说明$r(f(x, y, z)) = r(T(x, y, z)) \ge |A| - 2$。另一方面，通过式(8-6)我们可以把$f(x, y, z)$表示为

$$\begin{aligned}f(x,y,z) =& \sum_{a\in A}\delta_a(y)\delta_a(z) + (1-\sum_{a\in A}\delta_a(y)\delta_a(z))\cdot \\ & (\sum_{i=1}^{n} y_i z_i + \sum_{i=1}^{n} x_i^2 - x_1(y_1+z_1) - \cdots - x_n(y_n+z_n))^{q-1} \\ =& H_1(y,z) + H_2(y,z)(F_1(y,z)+F_2(x)-x_1(y_1+z_1)-\cdots-x_n(y_n+z_n))^{q-1},\end{aligned}$$

这里$H_1(y,z) = \sum_{a\in A}\delta_a(y)\delta_a(z)$，$H_2(y,z) = 1-\sum_{a\in A}\delta_a(y)\delta_a(z)$，$F_1(y,z) = \sum_{i=1}^{n} y_i z_i$，$F_2(x) = \sum_{i=1}^{n} x_i^2$。可以验证，在$f(x,y,z)$上面的表达式中，每个单项式都有形式$H_1(y,z)$或者

$$H_2(y,z)(F_1(y,z))^i(F_2(x))^j(x_1(y_1+z_1))^{k_1}\cdots(x_n(y_n+z_n))^{k_n},$$

这里$i,j,k_1,\cdots,k_n$是加和为$q-1$的非负整数。所以，所有单项式可以被写成秩一函数$H_1(y,z)$或者

$$(F_2(x)^j x_1^{k_1}\cdots x_n^{k_n})(H_2(y,z)F_1(y,z)^i(y_1+z_1)^{k_1}\cdots(y_n+z_n)^{k_n}).$$

因此，$f(x,y,z)-H_1(y,z)$的秩的上界被$(X_1+\cdots+X_{n+2})^{q-1}$的表达式中出现的不同单项式的数量所限制了，这个值即为$\binom{n+q}{q-1}$。我们的定理可以由不等式$|A|-2 \le r(T(x,y,z)) = r(f(x,y,z)) \le \binom{n+q}{q-1}+1$推得。 □

8.4 结语

在本文中，我们先提出了一种新的计数方式，然后用它来得到一个有限域上的极值问题的新上界。我们认为我们的方法是很有趣的，也许会有一些新的应用或拓展。如果能对某几个q确定$R(n,q)$的值，那也会是很有趣的。我们自然有如下问题：

问题： 当q为偶素数幂时，给出$R(n,q)$的上界。

9 其它在研问题

9.1 多重常重码

现代密码体系主要依赖于单向函数的应用，但是通常的单向函数总是基于还未被证明的猜想来保证它的安全性。由Pappu等人[111]中提出的物理不可克隆函数（PUF）提供了一种认证消耗低和抵抗物理攻击的新选择。近年来，物理不可克隆函数的研究已经成为在无线电频率识别和智能卡领域[48,79,111,133]的一种潮流。在文献[49]中，Chee等人提出了多重常重码（MCWC），从而为设计环形物理不可克隆函数和编码理论建立起了桥梁。在一个多重常重码中，每一个码字是一个长为mn的二元向量，它可以被划分成m个相同大小的部分，且每部分的重量都恰好是w。这个定义事实上是常重码（CWC）（$m=1$）和双重常重码（$m=2$）的自然推广[91,99]。

作者在多重常重码的领域内的贡献如下，首先，我们推广了Agrell等人[6]的方法，改进了文献[43]中的第三型Johnson界。同时我们得到了多重常重码的Gilbert-Varshamov界，并且证明了在渐近意义下可以改进文献[43]中通过级联的方法得到的下界。其次，我们得到了两类最优多重常重码的渐近存在性，第一类推广了文献[44]中的结果，第二类说明了极小距离为$2mw-2w$的多重常重码的Johnson界是紧的。

在该主题上，作者已与合作者共同完成了一篇论文（见主要研究成果中的文献2），发表于发表于《IEEE Transactions on Information Theory》。

9.2 可分哈希族

我们已经在第五章中介绍了可分哈希族。最近，我们又得到了一些可分哈希族的渐进界。我们的研究对象主要是$SHF(u;n,q,\{w_1,\ldots,w_t\})$，这里$u=\sum_{i=1}^{t}w_i$。记当$u,q,\{w_1,\ldots,w_t\}$给定后，可分哈希族的最大元素个数为$C(u,q,\{w_1,\ldots,w_t\})$。利用Johnson型上界与移除引理，我们证明当$q$充分大时，只有当$\{w_1,\ldots,w_t\}=\{1,w\}$时才有$C(u,q,\{w_1,\ldots,w_t\})=C(w+1,q,\{1,w\})=\Theta(q^2)$，其它情况下都有$C(u,q,\{w_1,\ldots,w_t\})=o(q^2)$。我们的结果是该研究方向的一个突破性成果，因为前人的工作都集中于改

进$C(u,q,\{w_1,\ldots,w_t\}) \le c_1q^2+c_2q$中的常数$c_1$或$c_2$，而实际上大多数情况下可分哈希族的阶应该是$o(q^2)$。另一方面，关于构造性结果，我们利用加法数论的技巧证明，当q充分大时有$C(3,q,\{1,1,1\}) > q^{2-o(1)}$，$C(4,q,\{2,2\}) \ge C(4,q,\{1,1,2\}) \ge C(4,q,\{1,1,1,1\}) > q^{2-o(1)}$。

在该主题上，作者已与合作者共同完成了一篇论文（见主要研究成果中的文献10）。

9.3 $\{0,1\}^n$中的锐角集

1950年左右，Erdős猜测任给$\mathbb{R}^n$上2^n+1个点，则一定存在三个点可以形成一个钝角三角形。注意到$\{0,1\}^n$中所有2^n个点只构成锐角或直角三角形。1962年，Danzer和Grünbaum[7]证明了这个猜想。之后人们开始考虑$\{0,1\}^n$只含锐角的最大子集大小，不妨用$\kappa(n)$来表示这个值。1983年，Erdős和Füredi[65]给出了下界$\kappa(n) > \frac{1}{2}(\frac{2}{\sqrt{3}})^n$，这个界后来被Ackerman和Ben-Zwi[5]改进为$\kappa(n) > c\sqrt{n}(\frac{2}{\sqrt{3}})^n$。关于$\kappa(n)$的上界，目前已知的最优结果是Harangi[82]于2011年给出的$\kappa(n) \le 2(\sqrt{2})^n$，$n$为偶数；$\kappa(n) \le \frac{3}{\sqrt{2}}(\sqrt{n})^n$，$n$为奇数。通过一系列组合计数的手法，我们把上界改进为$\kappa(n) \le \frac{4}{3}(\sqrt{2})^n$，$n$为偶数；$\kappa(n) \le 2(\sqrt{n})^n$，$n$为奇数。

在该主题上，作者已与合作者共同完成了一篇论文（见主要研究成果中的文献11）。

参考文献

[1] *Cisco visual networking index: Global mobile data traffic forecast update, 2015-2020.*, [Online]. Available: http://goo.gl/1XYhqY.

[2] *Google-gfs2 colossus, http://www.quora.com/colossus-google-gfs2, google, 2012.*

[3] *Hdfs-raid, http://wiki.apache.org/hadoop/hdfs-raid.*

[4] *Strong edge-colorings*, [Online]. http://www.math.illinois.edu/~dwest/openp/strongedge.html.

[5] E. ACKERMAN AND O. BEN-ZWI, *On sets of points that determine only acute angles*, European J. Combin., 30 (2009), pp. 908–910.

[6] E. AGRELL, A. VARDY, AND K. ZEGER, *Upper bounds for constant-weight codes*, IEEE Trans. Inform. Theory, 46 (2000), pp. 2373–2395.

[7] M. AIGNER AND G. ZIEGLER, *Proofs from The Book*, Springer-Verlag, Berlin, fifth ed., 2014. Including illustrations by Karl H. Hofmann.

[8] N. ALON, G. COHEN, M. KRIVELEVICH, AND S. LITSYN, *Generalized hashing and parent-identifying codes*, J. Combin. Theory Ser. A, 104 (2003), pp. 207–215.

[9] N. ALON, R. DUKE, H. LEFMANN, V. RÖDL, AND R. YUSTER, *The algorithmic aspects of the regularity lemma*, J. Algorithms, 16 (1994), pp. 80–109.

[10] N. ALON, E. FISCHER, AND M. SZEGEDY, *Parent-identifying codes*, J. Combin. Theory Ser. A, 95 (2001), pp. 349–359.

[11] ——, *Parent-identifying codes*, J. Combin. Theory Ser. A, 95 (2001), pp. 349–359.

[12] N. ALON, A. MOITRA, AND B. SUDAKOV, *Nearly complete graphs decomposable into large induced matchings and their applications*, J. Eur. Math. Soc. (JEMS), 15 (2013), pp. 1575–1596.

[13] N. ALON AND M. NAOR, *Derandomization, witnesses for Boolean matrix multiplication and construction of perfect hash functions*, Algorithmica, 16 (1996), pp. 434–449.

[14] N. ALON AND A. SHAPIRA, *On an extremal hypergraph problem of Brown, Erdős and Sós*, Combinatorica, 26 (2006), pp. 627–645.

[15] N. ALON AND U. STAV, *New bounds on parent-identifying codes: the case of multiple parents*, Combin. Probab. Comput., 13 (2004), pp. 795–807.

[16] ——, *New bounds on parent-identifying codes: the case of multiple parents*, Combin. Probab. Comput., 13 (2004), pp. 795–807.

[17] A. BARG, G. COHEN, S. ENCHEVA, G. KABATIANSKY, AND G. ZÉMOR, *A hypergraph approach to the identifying parent property: the case of multiple parents*, SIAM J. Discrete Math., 14 (2001), pp. 423–431 (electronic).

[18] A. BARG AND G. KABATIANSKY, *A class of I.P.P. codes with efficient identification*, J. Complexity, 20 (2004), pp. 137–147.

[19] M. BAZRAFSHAN AND T. TRUNG, *Bounds for separating hash families*, J. Combin. Theory Ser. A, 118 (2011), pp. 1129–1135.

[20] ——, *Improved bounds for separating hash families*, Des. Codes Cryptogr., 69 (2013), pp. 369–382.

[21] F. A. BEHREND, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci. U. S. A., 32 (1946), pp. 331–332.

[22] M. BENNETT, *Right angles in* $\mathbb{F}_q^d$, arXiv preprint arXiv:1511.08942, (2015).

[23] C. BERGE, *Hypergraphs*, in Selected topics in graph theory, 3, Academic Press, San Diego, CA, 1988, pp. 189–206.

[24] ——, *Hypergraphs*, vol. 45 of North-Holland Mathematical Library, North-Holland Publishing Co., Amsterdam, 1989. Combinatorics of finite sets, Translated from the French.

[25] T. BERGER, N. MEHRAVARI, D. TOWSLEY, AND J. WOLF, *Random multiple-access communication and group testing*, IEEE Trans. Commun., 32 (1984), pp. 769–779.

[26] R. BHAGWAN, K. TATI, Y. CHENG, S. SAVAGE, AND G. M. VOELKER, *Total recall: system support for automated availability management*, Nsdi, 1 (2004), pp. 337–350.

[27] S. BLACKBURN, *Perfect hash families with few functions.*, Unpublished manuscript, 2000; available online as IACR research report 2003/17; see http://eprint.iacr.org/2003/017.

[28] ——, *Perfect hash families: probabilistic methods and explicit constructions*, J. Combin. Theory Ser. A, 92 (2000), pp. 54–60.

[29] ——, *Combinatorial schemes for protecting digital content*, in Surveys in combinatorics, 2003 (Bangor), vol. 307 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 2003, pp. 43–78.

[30] ——, *An upper bound on the size of a code with the k-identifiable parent property*, J. Combin. Theory Ser. A, 102 (2003), pp. 179–185.

[31] S. BLACKBURN, M. BURMESTER, Y. DESMEDT, AND P. WILD, *Efficient multiplicative sharing schemes*, in Advances in cryptology—EUROCRYPT '96 (Saragossa, 1996), vol. 1070 of Lecture Notes in Comput. Sci., Springer, Berlin, 1996, pp. 107–118.

[32] S. BLACKBURN, T. ETZION, D. STINSON, AND G. ZAVERUCHA, *A bound on the size of separating hash families*, J. Combin. Theory Ser. A, 115 (2008), pp. 1246–1256.

[33] S. R. BLACKBURN, *Perfect hash families: probabilistic methods and explicit constructions*, J. Combin. Theory Ser. A, 92 (2000), pp. 54–60.

[34] ——, *Frameproof codes*, SIAM J. Discrete Math., 16 (2003), pp. 499–510 (electronic).

[35] ——, *An upper bound on the size of a code with the k-identifiable parent property*, J. Combin. Theory Ser. A, 102 (2003), pp. 179–185.

[36] S. R. BLACKBURN, T. ETZION, AND S. NG, *Traceability codes*, J. Combin. Theory Ser. A, 117 (2010), pp. 1049–1057.

[37] D. BONEH AND J. SHAW, *Collusion-secure fingerprinting for digital data*, IEEE Trans. Inform. Theory, 44 (1998), pp. 1897–1905.

[38] ——, *Collusion-secure fingerprinting for digital data*, IEEE Trans. Inform. Theory, 44 (1998), pp. 1897–1905.

[39] W. G. BROWN, P. ERDŐS, AND V. T. SÓS, *On the existence of triangulated spheres in* 3*-graphs, and related problems*, Period. Math. Hungar., 3 (1973), pp. 221–228.

[40] ——, *Some extremal problems on* r*-graphs*, in New directions in the theory of graphs (Proc. Third Ann Arbor Conf., Univ. Michigan, Ann Arbor, Mich, 1971), Academic Press, New York, 1973, pp. 53–63.

[41] F. BUEKENHOUT, ed., *Handbook of incidence geometry*, North-Holland, Amsterdam, 1995. Buildings and foundations.

[42] Y. CHEE, *Turán-type problems in group testing, coding theory and cryptography*, University of Waterloo, 1996.

[43] Y. CHEE, Z. CHERIF, J.-L. DANGER, S. GUILLEY, H. KIAH, J. KIM, P. SOLE, AND X. ZHANG, *Multiply constant-weight codes and the reliability of loop physically unclonable functions*, IEEE Trans. Inform. Theory, 60 (2014), pp. 7026–7034.

[44] Y. CHEE, F. GAO, H. KIAH, A. C. H. LING, H. ZHANG, AND X. ZHANG, *Decompositions of edge-colored digraphs: A new technique in the construction of constant-weight codes and related families*, arXiv preprint arXiv:1401.3925, (2014).

[45] C. CHEN AND F. HWANG, *Detecting and locating electrical shorts using group testing*, IEEE Trans. Circuits Syst., 36 (1989), pp. 1113–1116.

[46] H. CHEN AND F. HWANG, *Exploring the missing link among* d*-separable,* $\overline{d}$*-separable and* d*-disjunct matrices*, Discrete Appl. Math., 155 (2007), pp. 662–664.

[47] Y. CHENG AND D. DU, *New constructions of one- and two-stage pooling designs*, J. Comput. Biol., 15 (2008), pp. 195–205.

[48] Z. CHERIF, J.-L. DANGER, S. GUILLEY, AND L. BOSSUET, *An easy-to-design puf based on a single oscillator: The loop puf*, in Digital System Design (DSD), 2012 15th Euromicro Conference on, Sept 2012, pp. 156–162.

[49] Z. CHERIF, J.-L. DANGER, S. GUILLEY, J.-L. KIM, AND P. SOLE, *Multiply constant weight codes*, in Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, July 2013, pp. 306–310.

[50] B. CHOR, A. FIAT, AND M. NAOR, *Tracing traitors*, Advances in cryptology—CRYPTO' 94, (1994), pp. 257–270.

[51] B. CHOR, A. FIAT, M. NAOR, AND B. PINKAS, *Tracing traitors*, IEEE Trans. Inform. Theory, 46 (2000), pp. 893–910.

[52] D. CONLON AND J. FOX, *Graph removal lemmas*, in Surveys in combinatorics 2013, vol. 409 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 2013, pp. 1–49.

[53] E. CROOT, V. LEV, AND P. PACH, *Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small*, Ann. of Math., 185 (2017), pp. 331–337.

[54] D. DE CAEN, *The current status of Turán's problem on hypergraphs*, in Extremal problems for finite sets (Visegrád, 1991), vol. 3 of Bolyai Soc. Math. Stud., János Bolyai Math. Soc., Budapest, 1994, pp. 187–197.

[55] A. G. DIMAKIS, P. B. GODFREY, Y. WU, AND M. J. WAINWRIGHT, *Network coding for distributed storage systems*, IEEE Trans. Inform. Theory, 56 (2010), pp. 4539–4551.

[56] R. DORFMAN, *The detection of defective members of large populations*, Ann. Math. Stat., 14 (1943), pp. 436–440.

[57] D. DU AND F. HWANG, *Combinatorial group testing and its applications*, vol. 12 of Series on Applied Mathematics, World Scientific Publishing Co., Inc., River Edge, NJ, second ed., 2000.

[58] ——, *Pooling designs and nonadaptive group testing: important tools for DNA sequencing*, vol. 18, World Scientific Pub Co Inc, 2006.

[59] A. D'YACHKOV AND V. RYKOV, *Bounds on the length of disjunctive codes*, Problemy Peredachi Informatsii, 18 (1982), pp. 7–13.

[60] ——, *A survey of superimposed code theory*, Problems Control Inform. Theory, 12 (1983), pp. 229–242.

[61] A. D'YACHKOV, I. VOROBYEV, N. POLYANSKII, AND V. SHCHUKIN, *Bounds on the rate of superimposed codes*, in 2014 IEEE Int. Symposium on Information Theory (ISIT), IEEE, 2014, pp. 2341–2345.

[62] A. D'YACHKOV, I. VOROBYEV, N. POLYANSKY, AND V. SHCHUKIN, *Bounds on the rate of disjunctive codes*, Probl. Inf. Transm., 50 (2014), pp. 27–56.

[63] A. G. D'YACHKOV, I. V. VOROBYEV, N. A. POLYANSKII, AND V. Y. SHCHUKIN, *Cover-free codes and separating system codes*, Proc. IEEE Symp. Inform. Theory, (2015).

[64] J. S. ELLENBERG AND D. GIJSWIJT, *On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression*, Ann. of Math., 185 (2017), pp. 339–443.

[65] P. ERD˝OS AND Z. FÜREDI, *The greatest angle among n points in the d-dimensional Euclidean space*, in Combinatorial mathematics (Marseille-Luminy, 1981), vol. 75 of North-Holland Math. Stud., North-Holland, Amsterdam, 1983, pp. 275–283.

[66] P. ERDŐS, P. FRANKL, AND Z. FÜREDI, *Families of finite sets in which no set is covered by the union of two others*, J. Combin. Theory Ser. A, 33 (1982), pp. 158–166.

[67] ——, *Families of finite sets in which no set is covered by the union of r others*, Israel J. Math., 51 (1985), pp. 79–89.

[68] P. ERDŐS, P. FRANKL, AND V. RÖDL, *The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent*, Graphs Combin., 2 (1986), pp. 113–121.

[69] P. ERDŐS AND Z. FÜREDI, *The greatest angle among n points in the d-dimensional Euclidean space*, in Combinatorial mathematics (Marseille-Luminy, 1981), vol. 75 of North-Holland Math. Stud., North-Holland, Amsterdam, 1983, pp. 275–283.

[70] P. ERDŐS AND T. GALLAI, *On maximal paths and circuits of graphs*, Acta Math. Acad. Sci. Hungar, 10 (1959), pp. 337–356 (unbound insert).

[71] P. ERDŐS AND D. J. KLEITMAN, *On coloring graphs to maximize the proportion of multi-colored k-edges*, J. Combinatorial Theory, 5 (1968), pp. 164–169.

[72] K. J. FALCONER, *On a problem of erdős on fractal combinatorial geometry*, J. Combin. Theory Ser. A, 59 (1992), pp. 142–148.

[73] E. FISCHER, E. LEHMAN, I. NEWMAN, S. RASKHODNIKOVA, R. RUBINFELD, AND A. SAMORODNITSKY, *Monotonicity testing over general poset domains*, in Proceedings of the

Thirty-Fourth Annual ACM Symposium on Theory of Computing, ACM, New York, 2002, pp. 474–483.

[74] P. FRANKL, *Improved bounds for Erdős' matching conjecture*, J. Combin. Theory Ser. A, 120 (2013), pp. 1068–1072.

[75] R. FUJI-HARA, *Perfect hash families of strength three with three rows from varieties on finite projective geometries*, Des., Codes Cryptogr., (to appear. DOI: 10.1007/s10623-015-0052-z).

[76] Z. FÜREDI, *Turán type problems*, in Surveys in combinatorics, 1991 (Guildford, 1991), vol. 166 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1991, pp. 253–300.

[77] ——, *On r-cover-free families*, J. Combin. Theory Ser. A, 73 (1996), pp. 172–173.

[78] Z. FÜREDI AND M. RUSZINKÓ, *Uniform hypergraphs containing no grids*, Adv. Math., 240 (2013), pp. 302–324.

[79] B. GASSEND, D. CLARKE, M. VAN DIJK, AND S. DEVADAS, *Silicon physical random functions*, in Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS '02, New York, NY, USA, 2002, ACM, pp. 148–160.

[80] C. GUO, D. R. STINSON, AND T. VAN TRUNG, *On symmetric designs and binary frameproof codes*, Springer Proceedings in Mathematics and Statistics: Algebraic Design Theory and Hadamard Matrices.

[81] ——, *On tight bounds for binary frameproof codes*, Des. Codes Cryptogr., 77 (2015), pp. 301–319.

[82] V. HARANGI, *Acute sets in Euclidean spaces*, SIAM J. Discrete Math., 25 (2011), pp. 1212–1229.

[83] V. HARANGI, T. KELETI, G. KISS, P. MAGA, A. MÁTHÉ, P. MATTILA, AND B. STRENNER, *How large dimension guarantees a given angle?*, Monatsh. Math., 171 (2013), pp. 169–187.

[84] D. HART, A. IOSEVICH, D. KOH, AND M. RUDNEV, *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture*, Trans. Amer. Math. Soc., 363 (2011), pp. 3255–3275.

[85] D. L. HOLLMANN, J. H. VAN LINT, J.-P. LINNARTZ, AND L. M. G. M. TOLHUIZEN, *On codes with the identifiable parent property*, J. Combin. Theory Ser. A, 82 (1998), pp. 121–133.

[86] C. HUANG, H. SIMITCI, Y. XU, A. OGUS, B. CALDER, P. GOPALAN, J. LI, AND S. YEKHANIN, *Erasure coding in windows azure storage*, in Usenix Conference on Technical Conference, 2012, pp. 2–2.

[87] S. HUANG AND F. HWANG, *When is individual testing optimal for nonadaptive group testing?*, SIAM J. Discrete Math., 14 (2001), pp. 540–548.

[88] J. Q. JENNIFER AND T. B. ARTHUR, *Strong chromatic index of subset graphs*, Journal of Graph Theory, 24 (1997), pp. 267–273.

[89] M. JI, G. CAIRE, AND A. F. MOLISCH, *Fundamental limits of caching in wireless d2d networks*, IEEE Trans. Inform. Theory, 62 (2016), pp. 849–869.

[90] ——, *Wireless device-to-device caching networks: Basic principles and system performance*, IEEE J. Sel. Areas Commun., 34 (2016), pp. 176–189.

[91] S. JOHNSON, *Upper bounds for constant weight error correcting codes*, Discrete Mathematics, 3 (1972), pp. 109–124.

[92] N. KARAMCHANDANI, U. NIESEN, M. A. MADDAH-ALI, AND S. N. DIGGAVI, *Hierarchical coded caching*, IEEE Trans. Inform. Theory, 62 (2016), pp. 3212–3229.

[93] W. KAUTZ AND R. SINGLETON, *Nonrandom binary superimposed codes*, IEEE Trans. Inform. Theory, 10 (1964), pp. 363–377.

[94] P. KEEVASH, *Hypergraph Turán problems*, in Surveys in combinatorics 2011, vol. 392 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 2011, pp. 83–139.

[95] R. KLEINBERG, W. F. SAWIN, AND D. E. SPEYER, *The growth rate of tri-colored sum-free sets*, arXiv preprint arXiv:1607.00047v1.

[96] J. KÖRNER AND K. MARTON, *New bounds for perfect hashing via information theory*, European J. Combin., 9 (1988), pp. 523–530.

[97] J. KUBIATOWICZ, D. BINDEL, Y. CHEN, S. CZERWINSKI, P. EATON, D. GEELS, R. GUMMADI, S. RHEA, H. WEATHERSPOON, AND C. WELLS, *Oceanstore: an architecture for global-scale persistent storage*, ACM SIGPLAN Notices, 35 (2002), pp. 190–201.

[98] S. KUMAR, A. GRAELL I AMAT, I. ANDRIYANOVA, AND F. BRÄNNSTRÖM, *A family of erasure correcting codes with low repair bandwidth and low repair complexity*, in IEEE Global Commun. Conf., 2015, pp. 1–6.

[99] V. I. LEVENSHTEIN, *Upper-bound estimates for fixed-weight codes*, Probl.peredachi Inf, (1971), pp. 3–12.

[100] A. MACULA AND L. POPYACK, *A group testing method for finding patterns in data*, Discrete Appl. Math., 144 (2004), pp. 149–157.

[101] M. A. MADDAH-ALI AND U. NIESEN, *Fundamental limits of caching*, IEEE Trans. Inform. Theory, 60 (2014), pp. 2856–2867.

[102] ——, *Decentralized coded caching attains order-optimal memory-rate tradeoff*, IEEE/ACM Trans. Netw., 23 (2015), pp. 1029–1040.

[103] S. MARTIROSYAN AND T. TRUNG, *Explicit constructions for perfect hash families*, Des. Codes Cryptogr., 46 (2008), pp. 97–112.

[104] K. MEHLHORN, *Data structures and algorithms. 1*, EATCS Monographs on Theoretical Computer Science, Springer-Verlag, Berlin, 1984. Sorting and searching.

[105] E. NASLUND AND W. F. SAWIN, *Upper bounds for sunflower-free sets*, arXiv preprint arXiv:1606.09575v1.

[106] I. NEWMAN AND A. WIGDERSON, *Lower bounds on formula size of Boolean functions using hypergraph entropy*, SIAM J. Discrete Math., 8 (1995), pp. 536–542.

[107] U. NIESEN AND M. A. MADDAH-ALI, *Coded caching with nonuniform demands*, 2014.

[108] A. NILLI, *Perfect hashing and probability*, Combin. Probab. Comput., 3 (1994), pp. 407–409.

[109] S. OWEN AND S.-L. NG, *A note on an upper bound of traceability codes*, Australas. J. Combin., 62 (2015), pp. 140–146.

[110] G. P., H. C., S. H., AND Y. S., *On the locality of codeword symbols*, IEEE Trans. Inform. Theory, 58 (2012), pp. 6925–6934.

[111] R. PAPPU, B. RECHT, J. TAYLOR, AND N. GERSHENFELD, *Physical one-way functions*, Science, 297 (2002), pp. 2026–2030.

[112] R. PEDARSANI, M. A. MADDAH-ALI, AND U. NIESEN, *Online coded caching*, IEEE/ACM Trans. Netw., 24 (2016), pp. 836–845.

[113] K. V. RASHMI, N. B. SHAH, D. GU, H. KUANG, D. BORTHAKUR, AND K. RAMCHANDRAN, *A solution to the network challenges of data recovery in erasure-coded distributed storage systems: A study on the facebook warehouse cluster*, Usenix Hotstorage, (2013).

[114] K. V. RASHMI, N. B. SHAH, AND K. RAMCHANDRAN, *A piggybacking design framework for read-and download-efficient distributed storage codes*, 2013. [Online]. Available: http://arxiv.org/pdf/1302.5872.pdf.

[115] ——, *A piggybacking design framework for read-and download-efficient distributed storage codes*, in Proc. IEEE Int. Symp. Inf. Theory, 2013, pp. 331–335.

[116] M. RUSZINKÓ, *On the upper bound of the size of the r-cover-free families*, J. Combin. Theory Ser. A, 66 (1994), pp. 302–310.

[117] ——, *On the upper bound of the size of the r-cover-free families*, J. Combin. Theory Ser. A, 66 (1994), pp. 302–310.

[118] I. Z. RUZSA, *Solving a linear equation in a set of integers. I*, Acta Arith., 65 (1993), pp. 259–282.

[119] I. Z. RUZSA AND E. SZEMERÉDI, *Triple systems with no six points carrying three triangles*, in Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II, vol. 18 of Colloq. Math. Soc. János Bolyai, North-Holland, Amsterdam-New York, 1978, pp. 939–945.

[120] G. N. SÁRKÖZY AND S. SELKOW, *An extension of the Ruzsa-Szemerédi theorem*, Combinatorica, 25 (2005), pp. 77–84.

[121] ——, *On a Turán-type hypergraph problem of Brown, Erdős and T. Sós*, Discrete Math., 297 (2005), pp. 190–195.

[122] K. SHANMUGAM, M. JI, A. M. TULINO, J. LLORCA, AND A. G. DIMAKIS, *Finite-length analysis of caching-aided coded multicasting*, IEEE Trans. Inform. Theory, 62 (2016), pp. 5524–5537.

[123] K. SHANMUGAM, A. M. TULINO, AND A. G. DIMAKIS, *Coded caching with linear subpacketization is possible using ruzsa-szeméredi graphs*, arXiv preprint arXiv:1701.07115v1, (2017).

[124] A. SIDORENKO, *What we know and what we do not know about Turán numbers*, Graphs and Combinatorics, 11 (1995), pp. 179–199.

[125] A. SILVERBERG, J. STADDON, AND J. L. WALKER, *Applications of list decoding to tracing traitors*, IEEE Trans. Inform. Theory, 49 (2003), pp. 1312–1318.

[126] M. SOBEL AND P. GROLL, *Group testing to eliminate efficiently all defectives in a binomial sample*, Bell System Tech. J., 38 (1959), pp. 1179–1252.

[127] D. SOLYMOSI AND J. SOLYMOSI, *Small cores in 3-uniform hypergraphs*, J. Combin. Theory Ser. B, 122 (2017), pp. 897–910.

[128] J. N. STADDON, D. R. STINSON, AND R. WEI, *Combinatorial properties of frameproof and traceability codes*, IEEE Trans. Inform. Theory, 47 (2001), pp. 1042–1049.

[129] D. STINSON, T. TRUNG, AND R. WEI, *Secure frameproof codes, key distribution patterns, group testing algorithms and related structures*, J. Statist. Plann. Inference, 86 (2000), pp. 595–617. Special issue in honor of Professor Ralph Stanton.

[130] D. STINSON AND R. WEI, *Combinatorial properties and constructions of traceability schemes and frameproof codes*, SIAM J. Discrete Math., 11 (1998), pp. 41–53 (electronic).

[131] D. STINSON, R. WEI, AND K. CHEN, *On generalized separating hash families*, J. Combin. Theory Ser. A, 115 (2008), pp. 105–120.

[132] B. SUDAKOV, *Recent developments in extremal combinatorics: Ramsey and Turán type problems*, in Proceedings of the International Congress of Mathematicians. Volume IV, Hindustan Book Agency, New Delhi, 2010, pp. 2579–2606.

[133] G. SUH AND S. DEVADAS, *Physical unclonable functions for device authentication and secret key generation*, in Design Automation Conference, 2007. DAC '07. 44th ACM/IEEE, June 2007, pp. 9–14.

[134] I. TAMO AND A. BARG, *A family of optimal locally recoverable codes*, IEEE Trans. Inform. Theory, 60 (2013), pp. 4661–4676.

[135] I. TAMO, Z. WANG, AND J. BRUCK, *Zigzag codes: Mds array codes with optimal rebuilding*, IEEE Trans. Inform. Theory, 59 (2015), pp. 1597–1616.

[136] L. TANG AND A. RAMAMOORTHY, *Coded caching with low subpacketization levels*, arXiv preprint arXiv:1607.07920v1, (2016).

[137] T. TAO, *Notes on the slice rank of tensors*, [Online]:https://terrytao.wordpress.com/2016/08/24/notes-on-the-slice-rank-of-tensors/, (2016).

[138] ——, *A symmetric formulation of the croot-lev-pach-ellenberg-gijswijt capset bound*, [Online]:https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pach- ellenberg-gijswijt-capset-bound/, (2016).

[139] J. H. VAN LINT, *Introduction to coding theory*, vol. 86, Springer Science & Business Media, 2012.

[140] T. VAN TRUNG, *A tight bound for frameproof codes viewed in terms of separating hash families*, Des. Codes Cryptogr., 72 (2014), pp. 713–718.

[141] R. WALKER II AND C. COLBOURN, *Perfect Hash families: constructions and existence*, J. Math. Cryptol., 1 (2007), pp. 125–150.

[142] K. WAN, D. TUNINETTI, AND P. PIANTANIDA, *On the optimality of uncoded cache placement*, arXiv preprint arXiv:1511.02256v1, (2015).

[143] Z. WANG, I. TAMO, AND J. BRUCK, *Long mds codes for optimal repair bandwidth*, in In Proc. IEEE Int. Symp. Inf. Theory, 2012, pp. 1182–1186.

[144] I. M. WANLESS, *A partial latin squares problem posed by blackburn*, Bull. Inst. Combin. Appl., 42 (2004), pp. 76–80.

[145] J. WOLF, *Born again group testing: multiaccess communications*, IEEE Trans. Inform. Theory, 31 (1985), pp. 185–191.

[146] Y. XUAN, I. SHIN, M. THAI, AND T. ZNATI, *Detecting application denial-of-service attacks: A group-testing-based approach*, IEEE Trans. Parallel and Distributed Systems, 21 (2010), pp. 1203–1216.

[147] Q. YAN, M. CHENG, X. TANG, AND Q. CHEN, *On the placement delivery array design in centralized coded caching scheme*, arXiv preprint arXiv:1510.05064v3, (2015).

[148] ——, *Placement delivery array design through strong edge coloring of bipartite graphs*, arXiv preprint arXiv:1609.02985v1, (2016).

[149] B. YANG, X. TANG, AND J. LI, *A systematic piggybacking design for minimum storage regenerating codes*, IEEE Trans. Inform. Theory, 61 (2015), pp. 5779–5786.

[150] Q. YU, M. A. MADDAH-ALI, AND A. S. AVESTIMEHR, *The exact rate-memory tradeoff for caching with uncoded prefetching*, arXiv preprint arXiv:1609.07817v1, (2016).

攻读博士学位期间主要研究成果

1. Chong Shangguan and Gennian Ge, New bounds on the number of tests for disjunct matrices. IEEE Trans. Inform. Theory, 62(12):7518–7521, 2016. (**ZJU TOP100**)

2. Xin Wang, Hengjia Wei, Chong Shangguan, and Gennian Ge, New bounds and constructions for multiply constant-weight codes, IEEE Trans. Inform. Theory, 62(11):6315–6327, 2016. (**ZJU TOP100**)

3. Chong Shangguan and Gennian Ge, Separating Hash Families: A Johnson-type bound and new constructions. SIAM J. Discrete Math., 30(4):2243–2264, 2016.

4. Chong Shangguan, Xin Wang, Gennian Ge and Ying Miao (2014), New bounds for frameproof codes, submitted. (arXiv:1411.5782)

5. Chong Shangguan, Jingxue Ma and Gennian Ge (2016), New results for traitor tracing schemes, submitted. (arXiv:1610.07719)

6. Chong Shangguan, Yiwei Zhang and Gennian Ge (2016), Centralized coded caching schemes: A hypergraph theoretical approach, submitted. (arXiv:1610.07719)

7. Chong Shangguan and Gennian Ge (2016), A new piggybacking design for systematic MDS storage codes, submitted. (arXiv:1610.08223)

8. Gennian Ge and Chong Shangguan (2016), Rank counting and maximum subsets of $\mathbb{F}_q^n$ containing no right angles, submitted. (arXiv:1612.08255)

9. Chong Shangguan and Gennian Ge (2017), Sparse hypergraphs: new bounds and constructions, manuscript.

10. Chong Shangguan and Gennian Ge (2017), Some new asymptotically tight bounds for separating hash families, manuscript.

11. Gennian Ge, Xiangliang Kong and Chong Shangguan (2017), A new upper bound for cubic acute sets, manuscript.