分类号：O157.2　　单位代码：10335

学　　号：11106053

浙江大学

博士学位论文

中文论文题目：源于几类信息科学问题的极值组合构型

英文论文题目：**Extremal combinatorial configurations related to several problems of information science**

申请人姓名：张一炜

指导教师：葛根年　教授

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　2016年4月8日

源于几类信息科学问题的极值组合构型

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：冯克勤　教授　清华大学

委员1：冯克勤　教授　清华大学

委员2：宗传明　教授　北京大学

委员3：林东岱　研究员　中国科学院信息工程研究所

委员4：胡磊　研究员　中国科学院信息工程研究所

委员5：葛根年　教授　浙江大学

答辩日期：2016年5月14日

Extremal combinatorial configurations related to several problems of information science

Author's signature: _____

Supervisor's signature: _____

External Reviewers: _____

_____

_____

_____

_____

Examining Committee Chairperson:

Prof. Keqin Feng, Tsinghua University

Examining Committee Members:

Prof. Keqin Feng, Tsinghua University

Prof. Chuanming Zong, Peking University

Prof. Dongdai Lin, IIE CAS

Prof. Lei Hu, IIE CAS

Prof. Gennian Ge, Zhejiang University

Date of oral defence: May 14th, 2016

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： 2016 年 5 月 14 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： 2016 年 5 月 14 日　　签字日期： 2016 年 5 月 14 日

致　　谢

首先我要感谢我的导师葛根年教授。在这五年的博士生生涯中，葛老师在学习、科研、生活与为人处世等诸多方面给予了我很多的教导和建议。尤其在我科研进展处于低谷的那最为彷徨的阶段中，葛老师的指导与帮助使得我重拾信心，调整心态，才得以顺利完成这五年学业。葛老师高瞻远瞩的学术视野和严谨认真的学术作风将使学生终身受益。

我还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，特别是同济大学的杨亦挺老师，以色列理工学院 Tuvi Etzion 教授，浙江大学冯涛研究员，日本筑波大学缪莹教授等。在与他们的交流中，我得以开拓研究视野，体会到科研的乐趣。也尤其感谢他们对我的种种建议与鼓励。

感谢在一起学习与科研的同门：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、汪馨、上官冲、张韬、顾玉杰、马景学、丁报昆、钱昺辰、孔祥梁等。在这共同学习和生活的岁月中我们一起留下了许多美好的回忆。尤其是同门中最大的榜样胡思煌师兄与李抒行师兄的关心指导与督促，是指引我度过低谷的重要因素。

还要感谢我亲爱的朋友们：王雪、杜宇辉、冷正阳、张晓昱、邓一维、杨彬等。感谢你们的关怀与鼓励。也同时感谢这几年中陪伴我的一些精神支柱：缘宝，Liudmila Loglisci，曼彻斯特联俱乐部。

最后，我要感谢我的父母与家人。不让你们失望，才是一切动力的源泉。

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

信息科学与组合数学的交叉历来已久。信息科学在具体应用层面刺激着组合数学的发展，组合数学的体系的日臻成熟为信息科学的研究提供了理论支撑。信息科学中的若干问题，本质上都可以转化为一些组合数学中的极值构型问题。本学位论文将从组合数学的观点出发，融汇应用了图论、概率方法、极值组合等相关工具，对若干信息科学中的问题进行了一定的思考与推进。

在第 1 章绪论部分，我们将简要介绍本文所涉及的各信息科学问题的相关背景，并概述本文对此问题所做的推进工作。

在第 2 章中，我们的研究对象为置换群上的置换码与蛇形码，它们在电力线技术、分组密码、闪存中的排序调制等领域有着广泛应用。我们将对码字数目的研究转化为图论上的问题，通过构造合适的染色方案给出了图的独立数，进而分别改进了汉明距离和 Kendall's τ-距离下的置换码的下界。 Kendall's τ-距离下的蛇形码问题在奇数阶置换群和偶数阶置换群上有明显的区别。在 S_{2n+1} 上我们严格证明了“Horovitz-Etzion 构造”的可行性，并在其基础上进行微调得到了更优的蛇形码。在 S_{2n+2} 上我们利用之前 S_{2n+1} 中的蛇形码为基础进行复制与拼接，得到了非平凡的蛇形码构造，在渐进意义下达到最优。

在第 3 章中，我们的研究对象为源于数字产品版权保护背景的合谋-安全码及相关哈希函数族。我们将对码字数目的研究转化为超图上的问题，进而借助超图的独立数的相关结论，改进了特定参数条件下完全哈希函数族、防诬陷码、可分离码的下界。这种利用超图模型的分析方法尚属首次。

在第 4 章中，我们研究的问题是怎样的一个可逆二元矩阵中拥有最大比例的 2×2 可逆子矩阵。这个纯粹的组合问题的研究背景可追溯于图灵奖得主 Ron Rivest 为进一步加强分组密码的安全性所提出的一种预处理步骤 —— AONT 变换。我们通过建立问题的整数规划，结合概率方法的分析，完全确定了此问题的最优解，并以分圆构造为基础给出了近似最优的矩阵构造方法。

在第 5 章中，我们研究的问题为多部希尔伯特空间中的不可扩展乘积基的最小规模问题。此问题是量子信息学中的最基本问题之一，在量子信息的诸多领域有着广泛的应用。

我们综合利用图的正交表示、循环图的连通性、图的 1-因子分解等若干图论工具，决定了一系列参数下的最小规模 UPB 的大小的准确值。

在第 6 章中对其它在研问题做了简要汇报。

关键词： 置换码，蛇形码，独立集，分离哈希函数族，合谋-安全码，AONT 变换，不可扩展乘积基

Abstract

There is a long history of the interactions between information science and combinatorics. Information science provides problems and stimulates the development of combinatorics in a concrete applicational level while maturity of various fields of combinatorics offers theoretical supports to information scientific researches. Essentially, problems arising from information science may be turned into extremal configuration problems in combinatorics. This dissertation aims to investigate several problems arising from information science via a combinatorial perspective, with applications of tools from graph theory, probabilistic methods and extremal combinatorics.

In Section 1, we will briefly introduce the backgrounds of several problems arising from information science and summarize our main contributions towards these problems.

In Section 2, we will focus on permutation codes and snake-in-the-box codes in permutation groups. These are widely used in areas such as power line communications, block ciphers and rank modulation schemes for flash memories. We turn the problem of analyzing the number of codewords into a graph theoretic problem and construct proper colorings of certain graphs to analyze the independence number. In this way we can improve the lower bound on the number of codewords for permutation codes under Hamming metric or Kendall's τ-metric. The problem of snake-in-the-box codes under Kendall's τ-metric differs significantly in permutation groups of odd or even order. In S_{2n+1} we give a rigourous proof of a construction given by Horovitz and Etzion, and propose a better construction with a slight modification. In S_{2n+2} we get a nontrivial construction by merging several replicas of a snake in S_{2n+1}, which is asymptotically optimal.

In Section 3, we focus on collusion-secure codes and related hash families, arising from digital fingerprints. We turn the problem of deciding the number of codewords into a hypergraph theoretic problem and make use of results concerning the independence number of certain hypergraphs. In this way we improve the lower bounds of perfect hash families, frame-proof codes and separable codes with certain parameters. Our work is known to be the first application of this hypergraph approach.

In Section 4, we analyze when an invertible binary matrix contains the largest ratio of 2×2 invertible submatrices. The original motivation of this purely combinatorial problem can be traced to the Turing Award winner Ron Rivest, who proposes all-or-nothing transforms, a preprocessing to add additional securities for block ciphers. Via integer programming and probabilistic analyses, we completely solve this problem and offer explicit constructions via cyclotomies.

In Section 5, we focus on minimal size of unextendible product bases in a given multipartite Hilbert space, which is one of the most fundamental problems in quantum information theory and has wide applications in various areas of quantum information theory. We determine the precise value of the minimal size of unextendible product bases for some parameters, by applying several graph-theoretic tools including orthogonal representations of graphs, connectivity of circulant graphs and 1-factorizations of graphs.

In Section 6, we briefly introduce some other topics still under investigation.

Keywords: permutation codes, snake-in-the-box codes, independent set, separating hash families, collusion-secure codes, all-or-nothing transforms, unextendible product bases

插　　图

表　格

目　　次

1 绪论

信息科学与组合数学的发展相辅相成。信息科学所研究的对象大都具有很强的离散性质，通过一定的转化与抽象可以产生出新的组合问题，从具体应用的层面刺激了组合数学的发展。尤其在 21 世纪信息产业飞速发展的全新时代中，信息科学中的编码密码技术已越过军事和外交的需要，被更广泛应用到经济领域和日常生活中。同时，随着工程技术的进步而产生的新的信息存储设备与信息传播介质，也都为组合数学带来了崭新的丰富多彩的研究课题。组合数学的发展所提供的一系列工具为信息科学的研究提供了强大的理论支撑，尤其是近年来的概率方法、极值组合、代数组合、加法组合等，在各自逐步发展完善成为一个成熟的学科方向的同时也越来越频繁地被应用于编码密码等信息科学问题的研究中，带来令人欣喜的结果。

信息科学中的若干问题，本质上都可以转化为一些组合数学中的极值构型问题。本学位论文将从组合数学的观点出发，融汇应用了图论、概率方法、极值组合等相关工具，对下列信息科学中的问题进行了一定的思考与推进。具体包括：置换群上的置换码、源于闪存的排序调制中的蛇形码、针对数字产品版权保护的合谋-安全码及相关哈希函数族、源于密码背景的 AONT 变换、量子信息中的不可扩展乘积基等问题。下面将简要介绍各研究子课题的背景，并概述本文在各研究课题上所做的工作。

1.1 置换码与蛇形码

令 S_n 为 n 个元素上的置换群。一个置换码本质上是置换群 S_n 中的在给定的某种距离下满足一定的限制条件的一个子集。依据具体应用背景的不同，各种各样的距离意义下的置换码[46]多年来被广泛研究。本文主要考虑的是汉明距离和 Kendall's τ-距离。前者与电力线技术、分组密码等密切相关，后者则是闪存中的排序调制体系[76] 中的必需要求。

对置换码的研究的核心问题，是在给定的置换群 S_n 和给定的极小距离 d 下，寻找最大的码字数目并构造相应的最优码。汉明距离下的最大码字数目仅仅在零星一些参数下有精确的结论，而一般而言，不仅 $A_H(n,d)$ 的精确值很难估计，甚至其下界一直以来也仅仅

有 Gilbert-Varshamov 型的平凡下界。对此界的改进一直没有什么很有效的处理方法。本文中，我们将研究码字数目的问题转化到研究图的独立集的问题，这是图论方面最基本的极值问题之一。以 S_n 中的所有置换为点，两点之间连线当且仅当其汉明距离小于 d. 则此图的独立数即为 $A_H(n,d)$. 我们构造了图的一个正常染色，利用了图的独立数与染色数之间的一个基本的关系，从而得到了在 d 取定且 n 趋于无穷的意义下 $A_H(n,d)$ 的新的下界，比 Gilbert-Varshamov 型的平凡下界提高了近 n 倍。对于 Kendall's τ-距离下的最大码字数目 $A_K(n,d)$，我们也是利用类似的构造染色以分析独立数的方法，得到了 $A_K(n,d)$ 的新的下界。在之前的研究结果中，已经将 $A_K(n,d)$ 的下界控制在了球填充上界的常数比例内，我们的推进则是进一步缩小了上下界之间的常数差距。本工作已投稿至《IEEE Transactions on Information Theory》.

蛇形码的研究动机是在闪存上设置合适的编码方案，以有效针对电荷溢出或泄漏等带来的错误。闪存是一种非易失性存储器，可以进行电子写入与电子擦除。由于它使用寿命长，物理抗性好，存储密度高且有相对较高的性价比，因而当前越来越被广泛应用于日常生活之中，如 U 盘，相机中的记忆棒，手机中的存储卡等诸多存储介质中。简而言之，闪存是以其各个存储单元上的电荷来表示与存储信息的，其固有的电荷写入与电荷擦除这两个过程的不对称性是闪存的一大缺陷。写入电荷的过程，可以在单个存储单元上进行，但是如果想擦除一个存储单元上的电荷的话，需要对其所在的整个区块进行电荷擦除才行，亦即需要先对整个区块的信息进行备份，擦除整个区块的电荷，再将其它本应存储的信息重新写入。这样的过程既消耗大量时间，又对闪存的使用寿命有极大限制。因此，如果以各存储单元上的电荷的绝对数值作为信息存储的方式的话，在电荷写入过程中潜在的电荷溢出现象将是一个非常棘手的问题。这又使得现实中的数据写入经常要采取缓慢的一步步的操作，逐渐将电荷调整为所要写入的目标值。另外，闪存中还同时面临着电荷的泄漏与读取的干扰等问题。闪存的排序调制模式，不再以电荷的绝对数值作为存储信息的方法，而是以一组电荷之间的相对排序作为信息存储方式，这种模式将有效解决上述问题。另外，为减少写入电荷时的溢出所带来的困扰，电荷写入的过程被进一步要求为“推至顶端”操作，即把一个存储单元上的电荷调整为最大这样一个操作。在以上背景下，研究的核心问题即为如何将一组满足特定距离限制条件的码字，按照“推至顶端”操作的要求，排列成一组格雷码。可以检测一个 Kendall's τ-错误的这样的格雷码被称为 Kendall's τ-距离下的蛇形码。

对于如何构造一组码字数目尽量多的蛇形码这一问题，构造思路在奇数阶与偶数阶置换群上有着显著的区别。本文延续了 Yehezkeally 与 Schwartz 的工作[131] 和 Horovitz 与 Etzion 的工作[73]，在奇数阶偶数阶上分别做了一定推进，对 Horovitz 与 Etzion 所留下的

三个公开问题做出了回答。具体来说，在奇数阶上，本文的贡献是对 Horovitz-Etzion 所提出的构造方法给出了一个严谨的证明，并依据于他们的构造进行微调，在 S_7 上得到了更好的构造；在偶数阶上，我们利用奇数阶上已由我们证明成立的 Horovitz-Etzion 型蛇形码为基础，对其做一定的复制与拼接过程，得到了偶数阶上非平凡的蛇形码，在近似意义下也已是最优的构造。本工作的第一篇文章已发表于《IEEE Transactions on Information Theory》，另一篇已投稿至《IEEE Transactions on Information Theory》.

1.2 数字指纹：合谋-安全码与哈希函数族

在当今的大数据时代中，数字产品的版权保护问题越来越受关注，打击盗版行为刻不容缓。数字产品的发布者可以在数字产品中附加一些码字作为数字指纹。这将使得发布者在发现盗版产品时，可以通过调查所嵌入的数字指纹而追查到盗版的源头。然而，多个盗版者可进行协助、合谋攻击，通过对各自数字产品的组合而产出盗版产品，这也同时将各自的数字指纹做了整合，加大了追查盗版源头的难度。为了抵抗这种合谋攻击，近年来设计出很多合谋-安全码，比如防诬陷码、可确定性父元码、追踪码、可分离码等等。分离哈希函数族[112] 是一类重要的组合结构，除却其本身在密码学中的应用之外，也在近年来各种安全码的研究中有着重要的应用。通常来说，各种合谋-安全码或者是一类特殊参数下的分离哈希函数族，或者可与相关的分离哈希函数族所互相导出。对于安全码及其相关哈希函数族的研究的主要目标是在给定的参数下构造一个码字数目尽量多的码，或者是通过直接的确定性构造，或者是用概率方法说明其存在性。

与处理置换码的问题一样，我们也将对这些组合结构的界的研究转化为图论中的极值问题，但又有本质的区别。在已有的各种研究以及本文对于置换码的研究中，码上的限制条件都是两个码字之间的，这种问题可自然转化为图的模型来处理。而对于合谋-安全码与相关哈希函数族的研究问题中，码上的限制条件往往是针对一组多个码字之间的，则需要转化为超图的模型来处理。本文建立了这些组合结构与超图之间的关联，以所有备选码字为点，以一组违背码的要求的码字为边，则此超图的一个独立集即对应于一个合适的码。我们进而利用超图独立集的相关研究结论[53]，对这些组合结构的下界进行了分析。特别地，这样的一般方法分别应用于改进了特定参数下的完美哈希函数族、防诬陷码和可分离码的下界，改进了各自问题先前的由 Stinson 等人[113] 和 Gao 与 Ge 等人[65] 所得到的下界。同时，据我们所了解，这种利用超图模型的方法尚属首次。本工作已投稿至《IEEE Transactions on Information Theory》.

1.3 分组密码的预处理——AONT 变换

AONT 变换最早由图灵奖得主 Ron Rivest 提出[101]，以作为使用分组密码之前的预处理步骤，为分组密码提供了一层额外的安全性。1-AONT 可以在分组密码的使用之前提供一个被称为“包变换（package transform）”的预处理过程。假设我们想要加密的明文是 $(x_1, \ldots, x_s)$. 首先借由一个 1-AONT，将其转化为 $(y_1, \ldots, y_s) = \phi(x_1, \ldots, x_s)$. 要注明的是 ϕ 这个变换本身并不需要是秘密的。接下来用一个分组密码对 $(y_1, \ldots, y_s)$ 进行加密，将其转化成密文 $z_i = e_K(y_i)$，$1 \leq i \leq s$，其中 e_K 代表加密所使用的函数。密文的接收者可以对密文进行解密，再利用原 1-AONT 的逆变换 ϕ^{-1} 得到原始的明文。但是，对于任何一个窃听者而言，想得到明文中的任意一位信息，都必须对密文解密（比如穷尽搜索的方法）得到整体的 $(y_1, \ldots, y_s)$ 的信息才可以。换言之，由于 1-AONT 的性质，仅仅部分的破译对于得到明文中的任意一位信息没有任何帮助。在这种意义上，1-AONT 的应用为分组密码提供了一层额外的安全保护。

然而，问题搬移到二元域上时，完全符合 AONT 变换要求的矩阵并不存在。如何构造一个尽量接近 AONT 变换要求的二元矩阵? Stinson 等人[43] 将此问题转化为下面的等价问题：怎样的一个可逆的二元矩阵中有最大比例的可逆 2×2 子矩阵，这个最大的比例值为多少? 对于这样一个纯粹的组合问题，Stinson 等人的研究猜想这个最大的比例值的极限存在，给出了其下界上界分别为 0.492 和 0.625，并通过诸如组合设计等方法得到了一定的矩阵构造方式。

本文完整解决了此问题，证明此最大的比例值即为 0.5. 具体而言，首先我们建立了严格刻画此问题最优解的整数规划，并通过对其松弛线性规划的近似求解，得到了此比例的上界 0.5. 进而，通过矩阵的随机构造，辅以二阶矩方法的分析，我们证明了此比例的下界为 0.5. 两方面结合得到了我们的最终结论。同时，我们也提出了具体构作矩阵的方案，主要构造步骤利用了合适参数下的分圆类，辅以调整步骤以保证构造的矩阵本身可逆。本工作已投稿至《Discrete Mathematics》.

1.4 量子信息中的不可扩展乘积基

不可扩展乘积基（Unextendible Product Bases）[15,51] 是量子信息中的最基本问题之一，它在量子信息的诸多领域有着广泛的应用，如对 Bound 纠缠态的构造，构造不可约正算子，构造低维度的局部不可区分子空间，证明无纠缠态下的量子非局域性的现象的存在性等等。这些应用要求我们去研究在给定的多部希尔伯特空间中的不可扩展乘积

基的最小规模问题。令 $f_m(k_1,\ldots,k_m)$ 代表 $\bigotimes_{i=1}^{m}\mathbb{C}^{k_i}$ 中的规模最小的 UPB 的大小，Alon 与 Lovász[5] 率先发现了此问题本质的组合特性，利用图的正交表示这一工具，刻画了 $f_m(k_1,\ldots,k_m)=\sum_{i=1}^{m}(k_i-1)+1$ 这一最平凡下界可达到的充分必要条件。自此之后，仅有 Feng，Chen，Johnston 等人在此问题上有其它零星的工作[61,80,81]。

本文综合利用图的正交表示、循环图的连通性、图的 1-因子分解等若干图论工具，决定了一系列参数下的最小规模不可扩展乘积基的大小的准确值。其中包括了对于 $f(2,2,4k-1)=4k+2$ 这一公开问题的解决。其它所解决的一类参数，也有望对于量子信息中与不可扩展乘积基密切相关的诸多研究课题有物理意义下的贡献。本工作已投稿至《Physical Review A》.

2 置换码与蛇形码

2.1 介绍

本章的研究主题是置换群上的置换码与蛇形码。由于在电力线技术、分组密码、闪存中的排序调制等领域的应用，置换码与蛇形码长期以来得到了广泛关注与深入研究。

令 S_n 为 n 个元素上的置换群。一个置换码本质上是置换群 S_n 的一个子集，且在给定的某种距离下满足一定的限制条件。对于置换码最早的研究可以追溯于[47,63]。从此，依据具体应用背景的不同，人们开始研究各种各样距离意义下的置换码。关于置换码中大部分的重要的距离，可参见综述[46]。本章中，我们主要考虑的是汉明距离和 Kendall's τ-距离。

汉明距离下的置换码的研究的兴起，源于其在电力线上的数据传输[97] 以及在分组密码[44] 中的应用。我们简要介绍其在电力线传输领域的应用背景。电力线数据传输中的主要的三种噪声为：对频率有影响的永久性窄带噪声（如来自电子设备的噪声）、短时间脉冲噪声、高斯白噪声（背景噪声）。在众多传统的数据传输媒介之中（比如电话线传输与卫星传输等），高斯白噪声是对系统影响最大的噪声。然而，在电力线传输中却是另外两种噪声更为显著。在[62] 和[125] 中具体提出了用汉明距离下的置换码对这种噪声进行纠错的方案。汉明距离下的置换码的研究的核心问题，是讨论在给定的 S_n 和给定的极小距离 d 下，最大的码字数目 $A_H(n,d)$，以及达到或接近此最优值的码的具体构造。

Kendall's τ-距离下的置换码的研究的兴起，源于近年来闪存技术的发展。闪存是一种非易失性存储器，可以进行电子写入与电子擦除。由于它使用寿命长，物理抗性好，存储密度高且有相对较高的性价比，因而当前越来越被广泛应用于日常生活之中，如 U 盘、相机中的记忆棒、手机中的存储卡等诸多存储介质。简而言之，闪存是以其各个存储单元上的电荷来表示与存储信息的，其固有的电荷写入与电荷擦除这两个过程的不对称性是闪存的一大缺陷。写入电荷的过程，可以在单个存储单元上进行，但是如果想擦除一个存储单元上的电荷的话，却不得不对其所在的整个区块进行电荷擦除。完整的步骤是需要先对整个区块的信息进行备份，再擦除掉整个区块的电荷，最后将除去要擦除的单元之外的其它本应存储的信息重新写入。这样的过程既消耗大量时间，又对闪存的使用寿命有极大限

制。因此，如果以各存储单元上的电荷的绝对数值作为信息存储的方式的话，在电荷写入过程中潜在的电荷溢出现象将是一个非常棘手的问题。这又使得现实中的数据写入经常要采取缓慢的一步一步的操作，逐渐将电荷调整为所要写入的目标值。另外，闪存中还同时面临着电荷的泄漏与读取的干扰等问题。为了解决上述困难，[76] 中提出了创新性的“排序调制”模式。信息的存储将不再基于各存储单元上的电荷的绝对数值，而是基于一个区块上各个存储单元之间的电荷数值大小的排序。即，如果我们有 n 个存储单元，其上的电荷量分别为 $c_1, c_2, \ldots, c_n \in \mathbb{R}$，则称这个区块存储了 $\sigma \in S_n$，$c_{\sigma(1)} > c_{\sigma(2)} > \cdots > c_{\sigma(n)}$ 这样一个置换。在这种架构下，如果电荷之间仅仅有微小的错误，微小到并不会带来排序上的影响的话，那么我们就省下了去解决这个问题的麻烦。当然，当错误足够大，会带来排序上的错乱的话，这种错误仍是需要处理的。为了检验或纠正这种错误，需要定义一些合适的距离。置换群上的若干种距离都可以用来针对这种错误，除 Kendall's τ-距离[10,27,77,95] 之外，还有 Ulam 距离[60] 和 l_∞- 距离[84,118]。Kendall's τ-距离下的置换码的研究的核心问题之一，是讨论在给定的 S_n 和给定的极小距离 d 下，最大的码字数目 $A_K(n, d)$，以及达到或接近此最优值的码的具体构造。

出于上述同样的原因，文献[76] 以及之后的[56] 和[129] 进一步提出，在闪存的排序调制模式中唯一允许的电荷写入操作是把一个存储单元的电量调整到最高，这称为一个“推至顶端”操作。这进一步避免了在电荷写入过程中潜在的电荷溢出的风险。将 Kendall's τ-距离下的置换码依照“推至顶端”操作来排列成一组格雷码是闪存调制模式中另一个核心问题。格雷码最早在[69] 中被系统提出，[103] 是此研究课题的一篇很好的综述。在给定距离下可以检测一个错误的格雷码被称为蛇形码。我们的目标是在 Kendall's τ-距离下构造码字数目尽量多的蛇形码。

本章的结构如下。第 2.2 小节将详细介绍本章所涉及的定义符号，以及已知的关于汉明距离下的置换码、Kendall's τ-距离下的置换码、Kendall's τ-距离下的蛇形码等相关研究结果。第 2.3 小节将讨论汉明距离下的置换码，通过利用图的染色数来分析独立数大小的方法，给出汉明距离下的置换码码字数目 $A_H(n, d)$ 的新的下界。第 2.4 小节讨论 Kendall's τ- 距离下的置换码，也是用类似的方法给出 $A_K(n, d)$ 新的下界，并给出了其它几个零星结果。之后两小节将对于 Kendall's τ-距离下的蛇形码展开研究，其中第 2.5 小节讨论 S_{2n+1} 上的情形，包括了对于“ Horovitz-Etzion 构造”的可行性的严格证明，并辅以某些调整得到了潜在的更好的蛇形码的构造方案；第 2.6 小节讨论了 S_{2n+2} 上的情形，利用之前 S_{2n+1} 的蛇形码为基础进行复制与拼接，得到了非平凡的蛇形码构造，在渐进意义下达到最优。最后，第 2.7 小节对本章进行总结。

2.2　预备工作

本小节中我们给出置换码与蛇形码的相关定义，并简要综述相关的一系列已知结果。

记 $[n]$ 为集合 $\{1,2,\ldots,n\}$. 令 $\pi=[\pi_1,\pi_2,\ldots,\pi_n]$ 为 $[n]$ 上的一个**置换**，将每个 $i\in[n]$ 映射为 $\pi(i)=\pi_i$. 置换的这种表示方法称为其**向量表示**。对于任意 $x\in[n]$，$\pi^{-1}(x)$ 代表着 x 在 π 中的位置指标。另一个有用的表示置换的方法为其**循环表示**，即把一个置换依据其轨道表示成若干个不相交循环轨道的乘积，例如向量表示 $[3,4,5,2,1,6]$ 等价于循环表示 $(1,3,5)(2,4)(6)$. 对于两个置换 σ 和 π，它们的复合，记为 $\sigma\pi$，是对任意 $i\in[n]$ 满足 $\sigma\pi(i)=\sigma(\pi(i))$ 的这一置换。所有置换在这种复合运算下构成非交换群 S_n，$|S_n|=n!$，称为 $[n]$ 上的**置换群**。记 $\varepsilon\triangleq[1,2,\ldots,n]$ 为这个群中的幺元。对于一个无序的整数序对 $1\le x<y\le n$，如果 $\pi^{-1}(x)>\pi^{-1}(y)$，则称这一对数构成 π 中的一组**逆序**。令 $I(\pi)$ 为整个 π 中的逆序数之和。π 称为一个奇置换或偶置换，取决于 $I(\pi)$ 的奇偶性。

2.2.1　汉明距离下的置换码

对于两个置换 σ 和 π，定义它们的**汉明距离**为它们的向量表示中不相同的位置的数目，即

$$d_H(\sigma,\pi)=|\{i\in[n]:\sigma_i\neq\pi_i\}|.$$

对于 $1\le d\le n$，若 $\mathcal{C}\subset S_n$ 中的任何两个置换 $\sigma,\pi\in\mathcal{C}$ 之间的汉明距离满足 $d_H(\sigma,\pi)\ge d$，则称 $\mathcal{C}$ 为一个汉明距离下的 (n,d)**- 置换码**。记 $A_H(n,d)$ 为最大的汉明距离下的 (n,d)-置换码的码字数目，达到此最大值的码被称为最优的。$A_H(n,d)$ 的值及对应的最优码的构造是主要的研究目标。利用基本的组合技巧，有以下结论成立。

定理1.

- $A_H(n,2)=n!$;
- $A_H(n,3)=n!/2$;
- $A_H(n,n)=n$;
- $A_H(n,d)\le nA_H(n-1,d)$;
- $A_H(n,d)\le n!/(d-1)!$.

然而，对于 $4\le d\le n-1$，决定 $A_H(n,d)$ 的值是困难的。下面总结一些关于 $A_H(n,d)$ 的上下界的重要的已知结果。如同研究其它各式各样的码一样，最先要考虑的是球填充型

的上界和 Gilbert-Varshamov 型的下界。

令 $D(n,k)$ （$k=0,1,\ldots,n$）代表 S_n 中与幺元 ε 的汉明距离恰为 k 的所有置换的集合：

$$D(n,k)=\{\pi\in S_n : d_H(\pi,\varepsilon)=k\}.$$

$D(n,k)$ 的大小为

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

其中 D_k 为 k 阶错排数。

对于任何一个置换 $\pi\in S_n$，以 $B_H(\pi,r)$ 来表示以 π 为球心的半径为 r 的**汉明球**，定义为 $B_H(\pi,r)\triangleq\{\sigma\in S_n : d_H(\sigma,\pi)\le r\}$. 显然，半径为 r 的汉明球的大小并不依赖于球心的位置，我们记其大小为 $B_H(r)$：

$$B_H(r)=\sum_{k=0}^{r}|D(n,k)|.$$

对于汉明距离下的置换码，其 Gilbert-Varshamov 型下界[67,123] 和球填充型的上界[94] 如下。

定理2.

$$\frac{n!}{B_H(d-1)}\le A_H(n,d)\le\frac{n!}{B_H(\lfloor\frac{d-1}{2}\rfloor)}.$$

当取定 d，$n\to\infty$ 时，[66] 中对下界做出了改进。

定理3. [66] 令 d 取定，$n\to\infty$，则

$$A_H(n,d)\ge\Omega(\log n\ \frac{n!}{B_H(d-1)}).$$

之后，Tait，Vardy 和 Verstraëte 在[117] 中考虑了 d/n 取定时的情况，同样改进了 Gilbert-Varshamov 型下界。

定理4. [117] 令 d/n 为一个取定的比例，$0<d/n<0.5$，则当 $n\to\infty$ 时有

$$A_H(n,d)\ge\Omega(n\ \frac{n!}{B_H(d-1)}).$$

与汉明距离下的置换码相关的其它研究工作包括：基于纠错码[49,64,74] 和组合设计[38,41] 的一些构造置换码的方式，对带有给定自同构的置换码的算法搜索策略[22,75,106]，基于线性规划和半正定规划的上界[23,24,54,119]，用概率方法研究置换码的界[82]，以及从覆盖半径角度的相关分析[29,107]。

2.2.2 Kendall's τ-距离下的置换码

对于一个置换 $\pi = [\pi_1, \pi_2, \ldots, \pi_n] \in S_n$，一个“**相邻调换**”操作指的是对相邻两个位置 π_i 与 π_{i+1} 之间的交换，$1 \le i \le n-1$，从而得到 $[\pi_1, \ldots, \pi_{i-1}, \pi_{i+1}, \pi_i, \pi_{i+2}, \ldots, \pi_n]$ 这个新的置换。两个置换 σ 和 π 之间的 **Kendall's τ-距离**[83]，记为 $d_K(\sigma, \pi)$，是把其中一个转化为另一个时所需要的最少的相邻调换操作的数目。例如，$\pi_1 = [1,2,3,4,5]$ 和 $\pi_2 = [2,3,1,5,4]$ 之间的 Kendall's τ-距离为 3，具体的变换过程可以为：$[1,2,3,4,5] \to [2,1,3,4,5] \to [2,3,1,4,5] \to [2,3,1,5,4]$. Kendall's τ-距离的一个简明的数学表达式如下[77]：

$$d_K(\sigma, \pi) = |\{(i,j) : \sigma^{-1}(i) < \sigma^{-1}(j) \wedge \pi^{-1}(i) > \pi^{-1}(j)\}|.$$

对于 $1 \le d \le \binom{n}{2}$，若 $\mathcal{C} \subset S_n$ 中的任何两个置换 $\sigma, \pi \in \mathcal{C}$ 之间的 Kendall's τ-距离满足 $d_K(\sigma, \pi) \ge d$，则称 $\mathcal{C}$ 为一个 Kendall's τ-距离下的 (n,d)-置换码。记 $A_K(n,d)$ 为最大的 Kendall's τ-距离下的 (n,d)-置换码的码字数目，达到此最大值的码被称为最优的。$A_K(n,d)$ 的值及对应的最优码的构造是主要的研究目标。平凡的结论包括：$A_K(n,2) = \frac{n!}{2}$，对应最优码字为全体奇置换或全体偶置换；对于 $d \ge \frac{2}{3}\binom{n}{2}$，有 $A_K(n,d) = 2$ 这一平凡结论[27]。其它情况下，对于 $3 \le d \le \frac{2}{3}\binom{n}{2}$，决定 $A_K(n,d)$ 的值是困难的。下面总结一些关于 $A_K(n,d)$ 的上下界的重要的已知结果。

与上文类似，也首先考虑球填充型的上界和 Gilbert-Varshamov 型的下界。对于任何一个置换 $\pi \in S_n$，以 $B_K(\pi, r)$ 来表示以 π 为球心的半径为 r 的 **Kendall's τ-球**，定义为 $B_K(\pi, r) \triangleq \{\sigma \in S_n : d_K(\sigma, \pi) \le r\}$. 显然，半径为 r 的 Kendall's τ-球的大小并不依赖于球心的位置，我们记其大小为 $B_K(r)$. 球填充型的上界和 Gilbert-Varshamov 型的下界如下：

定理5. [77]

$$\frac{n!}{B_K(d-1)} \le A_k(n,d) \le \frac{n!}{B_K(\lfloor \frac{d-1}{2} \rfloor)}.$$

对于距离为 $d_K(\sigma, \pi) = 1$ 的两个置换 σ 和 π，以二者为球心的半径为 r 的 **Kendall's τ-双球**，定义为 $DB(\sigma, \pi, r) \triangleq B(\sigma, r) \cup B(\pi, r)$. 记 $DB_{n,r}$ 为 S_n 中球心在幺元和置换 $(1,2)$ 的半径为 r 的双球。在 d 为偶数时，[27] 中利用“码-反码”方法给出了对于下界的改进。

定理6. [27] *如果一个码 $\mathcal{C} \subset S_n$ 有极小 Kendall's τ-距离 d，一个反码 $\mathcal{A} \subset S_n$ 有极大 Kendall's τ-距离 $d-1$，则有 $|\mathcal{C}| \cdot |\mathcal{A}| \le n!$. 特别地，因为 $DB_{n,r}$ 是一个极大距离为 $2r+1$ 的反码，则*

有

$$A_K(n, 2(r+1)) \leq \frac{n!}{|DB_{n,r}|}.$$

补充说明一点。除了上述对置换码的上界有所参照之外，寻找 S_n 中在 Kendall's τ-距离下最优的反码本身也是很有趣的问题。直观上，半径为 r 的球很可能是极大距离为 $2r$ 的最优的反码，半径为 r 的双球很可能是极大距离为 $2r+1$ 的最优的反码。然而这个直观上符合想象的命题也仅仅在 $r=1$ 时得以证明，在 $r \geq 2$ 时是否成立是一个公开问题[27]。

下界方面，首先说明我们可以只着重考虑奇数 d 下的 $A_K(n,d)$，因为有下面这个简单却有用的事实[77]：

引理7. [77] *对任意正整数 n 和 $t \geq 1$，有 $A_K(n,2t) \geq \frac{1}{2}A_K(n,2t-1)$.*

在[10] 中对于下界有一个重要的改进，其方法是对于文献[77] 中利用 Lee 距离下的码构造 Kendall's τ-距离下的 $(n,3)$-置换码的方法的一般推广。对于固定的 t，这个推广可以构造出码字数目达到 Kendall's τ-距离下最优的 $(n,2t+1)$-置换码码字数目的常数比例级别的码。

定理8. [10] *令 $m = ((n-2)^{t+1}-3)/(n-3)$，其中 $n-2$ 为素数幂。则有*

$$A_K(n,2t+1) \geq \begin{cases} n!/(t(t+1)m), & \text{t 为奇数;} \\ n!/(t(t+2)m), & \text{t 为偶数。} \end{cases}$$

文献[10]中在渐进意义下考虑 $A_K(n,d)$：

定理9. [10] *令 $\mathfrak{C}(d) = \lim_{n\to\infty} \frac{\ln A_K(n,d)}{\ln n!}$ 为 Kendall's τ-距离下极小距离为 d 的码字的码率。则有*

$$\mathfrak{C}(d) = \begin{cases} 1, & \text{如果 } d = O(n); \\ 1-\epsilon, & \text{如果 } d = \Theta(n^{1+\epsilon}),\ 0<\epsilon<1; \\ 0, & \text{如果 } d = \Theta(n^2). \end{cases}$$

与 Kendall's τ-距离下的置换码相关的其它研究工作，大致以时间顺序，包括：基于码字的缩短截取或延长等技巧的一些递归性的界与构造[77]，基于传统纠错码的一些置换码的构造及简单的译码算法[95]，线性规划与半正定规划界[90]，系统置换码[28,132]，以及某些参数下纠正单个错误的完美码的不存在性[27].

2.2.3　Kendall's τ-距离下的蛇形码

下面沿用[131]与[73]的定义与符号介绍闪存排序调制中的蛇形码。

给定集合 $\mathcal{S}$ 与一个 $\mathcal{S}$ 自身上的变换集 $\mathcal{T} \subset \{f|f:\mathcal{S}\to\mathcal{S}\}$，定义 $\mathcal{S}$ 上依赖于变换集 $\mathcal{T}$ 的码字数目为 M 的**格雷码**为如下序列：$C=(c_0,c_1,\ldots,c_{M-1})$，由 $\mathcal{S}$ 中 M 个不同的元素（称为码字）所组成，且对于每个 $j\in[M-1]$ 存在变换 $t_j\in\mathcal{T}$ 使得 $c_j=t_j(c_{j-1})$. 如果额外要求存在变换 $t\in\mathcal{T}$ 使得 $c_0=t(c_{M-1})$，则称这样的格雷码称为循环的。这里我们仅考虑循环的格雷码。

在闪存的排序调制中，取 $\mathcal{S}=S_n$，变换集 $\mathcal{T}$ 由所谓的“**推至顶端**”操作所构成，即 $\mathcal{T}=\{t_2,t_3,\ldots,t_n\}$，其中 t_i 的定义为

$$t_i([a_1,\ldots,a_{i-1},a_i,a_{i+1},\ldots,a_n])=[a_i,a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n].$$

一个由如上定义的“推至顶端”操作所构成的序列称为**转换序列**。一个初始的置换 π_0 和一个转换序列 $t_{x_1},t_{x_2},\ldots,t_{x_l}$，$x_i\in\{2,3,\ldots,n\}$，$1\le i\le l$ 共同定义了一列置换 $\pi_0,\pi_1,\ldots,\pi_{l-1},\pi_l$，其中 $\pi_i=t_{x_i}(\pi_{i-1})$，$1\le i\le l$. 若 $\pi_l=\pi_0$ 且对于 $0\le i<j\le l-1$ 有 $\pi_i\neq\pi_j$，则这个序列是一个循环的格雷码。如果我们不考虑距离限制的话，那么在[76]中提出了将所有 S_n 中的置换排列成循环的格雷码的方法。引入距离限制的话，在给定距离下可以检测一个错误的格雷码被称为**蛇形码（Snake-in-the-box codes）**。置换上的蛇形码主要在 Kendall's τ-距离和 l_∞-距离下展开研究，也分别简记为 $\mathcal{K}$-蛇和 l_∞-蛇。研究目标是在给定的距离下构造码字数目尽量多的蛇形码。对于 l_∞-蛇的研究工作主要包括[131]和[128]，本文将并不涉及对 l_∞-蛇的讨论，而是只涉及有关 $\mathcal{K}$-蛇的改进工作。

对于 $\mathcal{K}$-蛇，Yehezkeally 和 Schwartz 在[131]中提出，仅仅在奇数位指标上做“推至顶端”操作，可以固定置换的奇偶性（如全是交错群 A_n 中的置换）。这些同种奇偶性的置换彼此之间 Kendall's τ-距离至少为 2。于是，虽然要付出只能局限于同种奇偶性的置换这样的代价，但我们得以省去了在构造之后再行对距离进行验证的麻烦。而且，在[131]中同样说明了，这种代价并不要紧，因为：

- 若 C 是 $(n,M,\mathcal{K})$-蛇形码，则有 $M\le\frac{|S_n|}{2}$；
- 若 C 是 $(n,M,\mathcal{K})$-蛇形码，且其转换序列中包含至少一个偶数位指标上的“推至顶端”操作，则有 $M\le\frac{|S_n|}{2}-\frac{1}{n-1}\binom{\lfloor n/2\rfloor-1}{2}$.

这就启示我们，对于奇数阶的置换群 S_{2n+1}，可以不考虑在偶数位指标上做“推至顶端”操作。基于此，Yehezkeally 和 Schwartz 在[131]中首先给出了一种递归构造方式，可以通过 Kendall's τ-距离下的 S_{2n-1} 中码字数目为 M_{2n-1} 的蛇形码得到 S_{2n+1} 中码字数目

为 $M_{2n+1} = (2n+1)(2n-1)M_{2n-1}$ 的蛇形码。之后，Horovitz 与 Etzion[73] 改进了前者的递归构造，得到 $M_{2n+1} = ((2n+1)2n-1)M_{2n-1}$，递归的起点是 S_5 中码字数目为 57 的蛇形码。他们同时提出了一个不依赖于递归的直接构造方式，目标为 S_{2n+1} 中码字数目为 $\frac{(2n+1)!}{2} - 2n + 1$ 的蛇形码，但并没有严格证明这个思路的正确性，而仅仅是对于 S_7 与 S_9 借助计算机搜索得到了理想的码。Horovitz 与 Etzion 猜想他们的构造方式对于一般的奇数阶置换群 S_{2n+1} 都是正确的，并将此列为了一个公开问题。同时，他们提出的另一公开问题是是否有更好的构造方式。

在偶数阶的置换群 S_{2n+2} 上，如果仍然坚持上述原则，则最后一个位置保持不动，本质上仍只是一个 S_{2n+1} 上的蛇而已，码长约为 $\frac{1}{4n+4}|S_{2n+2}|$，我们称这样一个非常粗糙的结果是平凡的。那么，如果想在 S_{2n+2} 上做得更好，就必须有偶数位指标上的“推至顶端”操作，进而整个蛇中既有奇置换，也有偶置换，在距离的检测上又会带来麻烦。证明或否认 S_{2n+2} 上有比 S_{2n+1} 上更长的蛇形码是[73] 中所提出的又一公开问题。

2.3 汉明距离下的置换码码字数目的下界

本小节中，我们利用图论的思想改进 $A_H(n,d)$ 的下界。令图 G 中的点集为 $V(G)$，边集为 $E(G)$，若有边 $\{u,v\} \in E(G)$ 则称两个顶点 u 和 v 是相邻的。图的一个**独立集**是点集的一个子集，其内任意两点不相邻。图的最大独立集的大小称为图的**独立数**，记为 $\alpha(G)$. 研究码字数目和研究相应的图的独立数之间有自然的关联。以本小节考虑的 $A_H(n,d)$ 为例，令图 G_H 的点集对应于置换群 S_n，两个顶点相连当且仅当它们对应的码字的汉明距离至多为 $d-1$. 于是，一个汉明距离下的 (n,d)-置换码即对应于此图中的一个独立集。通过这样的联系，就把围绕码字数目的问题转换为对应的图的独立集大小的问题，进而有诸多图论工具可利用。这种方法最早出现在 Jiang 和 Vardy 的工作中[78]，他们利用这种方法改进了二元纠错码的 Gilbert-Varshamov 型下界。前文所述的汉明距离下的置换码的已知结果定理 3 和 4 也是通过这种思想所得到。

我们这里考虑图的独立数与图的染色数之间的一个简单的关联。图的一个**正常（点）染色**，是指对每个顶点赋予一种颜色，使得任意相邻的点不同色。图的**染色数** $\chi(G)$ 是最小的正整数 k，使得用 k 种颜色可以对图做正常染色。给定一个正常染色，由定义可知，染同一种颜色的点所组成的集合是图的一个独立集。则我们有

引理10. $\alpha(G) \geq |V(G)|/\chi(G)$.

于是，对独立数 $\alpha(G)$ 的下界的分析可以由对染色数 $\chi(G)$ 上界的分析得到。下面我们具体展开对 $A_H(n,d)$ 的下界的分析。

定理11. 对给定的整数 n，d，和一个不小于 n 的素数 p，有

$$A_H(n,d) \geq \frac{n!}{p^{d-2}}.$$

证明. 如上构造图 G_H .令 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ 为模 p 的剩余类环。将置换的向量表示视为一个 $n \times 1$ 的列向量。考虑映射

$$f : S_n \to \mathbb{Z}_p^{d-1},$$

将每个置换 $\sigma \in S_n$ 映射为

$$f(\sigma) = A\sigma \pmod{p},$$

其中 A 是如下一个 $(d-1) \times n$ 的范德蒙矩阵（$x_1, x_2, \ldots, x_n$ 为 $\{0, 1, \ldots, p-1\}$ 中互不相同的整数）：

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{d-2} & x_2^{d-2} & \cdots & x_n^{d-2} \end{pmatrix}.$$

我们声称这样的一个映射是一个正常染色。对于任意两个染为同样颜色 $v \in \mathbb{Z}_p^{d-1}$ 的置换 σ 和 π，我们有 $A\sigma \equiv A\pi \equiv v \pmod{p}$. 于是 $A(\sigma - \pi) \equiv 0 \pmod{p}$. 假设 σ 和 π 之间的汉明距离小于 d，则在 $\sigma - \pi$ 这个向量的差中至多有 $d-1$ 个坐标非零。则 A 中存在着 $\mathbb{Z}_p$-线性相关的 $d-1$ 列。而出于范德蒙矩阵 A 的性质，易知其任意 $d-1$ 列是 $\mathbb{Z}_p$-线性无关的，矛盾。综上，相同着色的两点并不相邻，于是我们构造的染色是图 G_H 的一个正常染色。

下面计数一下所用的颜色数目 T. 映射的象集为 $\mathbb{Z}_p^{d-1}$ 且实际上向量的第一位是常数 $1 + 2 + \cdots + n \pmod{p}$. 于是 $T \leq p^{d-2}$. 则由引理 10 可得

$$|A_H(n,d)| \geq \frac{n!}{p^{d-2}}.$$

□

当 d 取定，令 n 趋于无穷时，考虑我们得到的下界的渐进性质。使用以下符号来简化之后的叙述与对比。在本小节余下的部分，记 $A_H(n,d)$ 为定理 11 中我们所得到的下界，

$A_H^{GV}(n,d)$ 为经典的 Gilbert-Varshamov 型下界，$\widetilde{A}_H(n,d)$ 为在文献[66] 中所得到的下界（也是通过独立集的分析方法所得）。

推论12. *当 d 取定，令 n 趋于无穷时，有*

$$\frac{A_H(n,d)}{A_H^{GV}(n,d)} = \Omega(n).$$

证明. 由于错排数 $D_k = \lfloor \frac{k!}{e} + \frac{1}{2} \rfloor$，则

$$B_H(d-1) = \sum_{k=0}^{d-1} |D(n,k)| = \sum_{k=0}^{d-1} \binom{n}{k} D_k = \Theta(n^{d-1}).$$

众所周知[33] 对任意正整数 n 存在素数 p 满足 $n \leq p \leq 2n$，

$$A_H(n,d) \geq \frac{n!}{p^{d-2}} \geq \frac{n!}{(2n)^{d-2}}.$$

于是

$$\frac{A_H(n,d)}{A_H^{GV}(n,d)} \geq \frac{B_H(d-1)}{(2n)^{d-2}} = \Omega(n).$$

□

事实上，在较小的参数 n 上我们得到的界也表现出很好的结果。例如对于 $d = 5$ 和 $8 \leq n \leq 20$，表 2-1 列出了我们的结果 $A_H(n,d)$ 与之前最好的结果 $\widetilde{A}_H(n,d)$ 的对比。相对更好的结果以加粗字体表示。

综上所述，我们对于汉明距离下置换码的下界的改进为:

定理13. *当 d 取定，令 n 趋于无穷时，有*

$$A_H(n,d) \geq \Omega(n \frac{n!}{B_H(d-1)}).$$

最后要补充说明两点。首先，最近另一份独立的研究[79] 中也得到了与本节相同的结果，相比较而言我们的方法更为简单明了。另外，要说明我们的结果与之前 Tait，Vardy 和 Verstraëte[117] 的定理 4 的对比。他们针对的情形是在 d/n 为固定的比例且 $0 < d/n < 0.5$ 时，考虑 $A_H(n,d)$ 的渐进表现。我们的结果针对当 d 取定，令 n 趋于无穷时的情形，则比例 d/n 是趋于零的。所以说，某种意义上，我们的结果是与他们的结果是互为补充的。

表 2-1　对于 $8 \le n \le 20$，$A_H(n,5)$ 与 $\widetilde{A}_H(n,5)$ 之间的比较

n	$A_H(n,5)$	$\widetilde{A}_H(n,5)$
8	30	**90**
9	272	**509**
10	2726	**3386**
11	**29990**	25885
12	218025	**223378**
13	**2834328**	2147724
14	17744410	**22767826**
15	**266166164**	263832788
16	**4258658637**	3317928906
17	**72397196844**	45006297715
18	**933426695688**	655021291542
19	**17735107218083**	10181693092799
20	**199959070286565**	168351610362186

2.4　Kendall's τ-距离下的置换码码字数目的界

本小节起我们将注意力转移到 Kendall's τ-距离上。首先是同样利用图论的思想改进 $A_K(n,d)$ 的下界，具体过程也是通过构造图的染色方案来对独立数进行分析。接下来是其它一些零星的结果。

2.4.1　$A_K(n,d)$ 的下界

在定理 8 中已经得到，$A_K(n,d)$ 的下界与球填充上界在渐进意义下是吻合的，双方仅有常数级别的差距[10]。我们对 $A_K(n,d)$ 的下界的改进就是要缩小它们之间的差距这个常数。事实上，我们的手法本质上与[10] 相仿，改进是基于一个微小而简单的修改。

对于一个置换 $\pi \in S_n$，定义它的**逆序向量**为 $x_\pi = (x_\pi(1), x_\pi(2), \ldots, x_\pi(n-1)) \in \mathbb{Z}_n! \triangleq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \cdots \times \mathbb{Z}_n$，其表达式为:

$$x_\pi(i) = |\{j : j < i+1, \pi^{-1}(j) > \pi^{-1}(i+1)\}|, 1 \le i \le n-1.$$

即，$x_\pi(i) \in \mathbb{Z}_{i+1}$ 计数了“$i+1$”与“y”所组成的逆序的数目，$1 \le y \le i$. 逆序向量的所有元的加和即置换的逆序数 $I(\pi)$. 显然，一个相邻调换对于 x_π 会引入一个汉明重量为“1”

的错误。具体而言，如果置换的向量表示中有连续两个相邻元素 a 和 b，$a<b$，则交换它们位置的相邻调换将会为 x_π 引入错误 $\mathbf{e}_{\mathbf{b}}^{+}$，即在第 $b-1$ 位上取 $+1$，其余位置为 0 的向量。反之，如果有连续两个相邻元素 b 和 a，$a<b$，则交换它们位置的相邻调换将会为 x_π 引入错误 $\mathbf{e}_{\mathbf{b}}^{-}$，即在 $b-1$ 位上取 -1，其余位置为 0 的向量。t 个相邻变换结合在一起引入了错误向量 $\mathbf{e}$，由每个错误分别引进的错误向量累加所形成。令 $\omega(\mathbf{e})$ 为向量 $\mathbf{e}$ 的各元的绝对值的加和，注意到在 $\mathbf{e}$ 的组合过程中有潜在的正负抵消，所以 $\omega(\mathbf{e})$ 是一个绝对值不超过 t 的整数。

最核心的工具是下述著名的由 Bose 与 Chowla 提出的引理[26]:

引理14. [26] *令 q 为素数幂，$m=\frac{q^{t+1}-1}{q-1}$. 则存在 $q+1$ 个取自于 $\mathbb{Z}_m$ 的整数 $j_1=0, j_2, \ldots, j_{q+1}$，使得它们中任何 t 个（可重复选取）的加和*

$$j_{i_1}+j_{i_2}+\cdots+j_{i_t} \qquad (1\le i_1\le i_2\le\cdots\le i_t\le q+1)$$

在模 m 之下皆不同。

取 $q+1=n-1$. 我们开始分析 $A_K(n,2t+1)$. 令图 G_K 的点集对应于置换群 S_n. 两个顶点相连当且仅当它们对应的码字的 Kendall's τ-距离至多为 $d-1$. 于是，一个 Kendall's τ-距离下的 (n,d)-置换码即对应于此图中的一个独立集。现在对每个点做染色，颜色为 $(c_1,c_2)\in\mathbb{Z}_{2t+1}\times\mathbb{Z}_m$.

定理15. *在上述参数下，对每个顶点所代表的置换 $\pi\in S_n$，令 $c_1(\pi)\equiv I(\pi)\pmod{2t+1}$，$c_2(\pi)\equiv\sum_{i=1}^{n-1} j_i x_\pi(i)\pmod m$. 则对于任何两个距离为 $d_K(\pi,\sigma)<2t+1$ 的置换 π 和 σ，有 $(c_1(\pi),c_2(\pi))\neq(c_1(\sigma),c_2(\sigma))$.*

证明. 令向量 $\mathbf{e}=x_\pi-x_\sigma$ 为两个置换的逆序向量之间的差。因为 $d_K(\pi,\sigma)<2t+1$，则 $|\omega(\mathbf{e})|\le 2t$. 如果 $|\omega(\mathbf{e})|\neq 0$，则显然 $c_1(\pi)\neq c_1(\sigma)$. 否则，$|\omega(\mathbf{e})|=0$，那么 $c_2(\pi)-c_2(\sigma)$ 模 m 的值为两段加和的差，每段加和分别为 $\{j_1,\ldots,j_{q+1}\}$ 中的 s 个整数的和，$s\le t$，两段之间没有重复。由 Bose-Chowla 定理可知，这个差是非零的，所以 $c_2(\pi)\neq c_2(\sigma)$. □

于是上述染色是对图 G_K 的一个正常染色。要说明的是，在 Barg 和 Mazumdar[10] 的证明中本质上也是构造了一个染色方案，他们所用的染色是想能同时区分所有的相邻置换所带来的错误向量，然而这种同时性也限制了他们的染色数，不得不达到了 $t(t+1)m$（当 t 为奇数时）或者 $t(t+2)m$（当 t 为偶数时），这比我们的方法中的颜色数目 $(2t+1)m$ 更多。我们所做的微小的修改，本质上是把染色方式变成一个颜色序对，来分别用以区分不

同的错误向量，取决于 $|\omega(\mathbf{e})|$ 是否为零。这个小的修改收到了很好的效果。综上，我们的染色方案给出了

定理16. 令 $m=((n-2)^{t+1}-1)/(n-3)$，其中 $n-2$ 为素数幂。则 $A_K(n,2t+1)\geq \frac{n!}{(2t+1)m}$.

而对于 $A_K(n,2t)$，由上述结果和引理 7 可自然得到:

定理17. 令 $m=((n-2)^{t}-1)/(n-3)$，其中 $n-2$ 为素数幂。则 $A_K(n,2t)\geq \frac{n!}{2(2t-1)m}$.

最后我们提及，上述仍有一定改进空间。在我们的框架下，我们处理 $|\omega(\mathbf{e})|\neq 0$ 的错误时，方式是计算一个置换的逆序数模 $2t+1$ 的值。这个数目可以进一步缩小么? 我们进一步用 Bose 与 Chowla 在[26] 中提出的另一个引理。实际上两个引理使用起来的效果是类似的，前者的效果相对更好一些，不过接下来要提及的后者对于之后的分析更为便利。

引理18. [26] 令 $q=p^n$ 为一个素数幂，则我们可以找到 q 个非零正整数（小于 q^t）$d_1=1,d_2,\ldots,d_q$ 使得下列加和

$$d_{i_1}+d_{i_2}+\cdots+d_{i_t}\qquad (1\leq i_1\leq i_2\leq\cdots\leq i_t\leq q)$$

在模 q^t-1 之下皆不同。

此引理中的整数 $d_1=1,d_2,\ldots,d_q$ 的构造如下。令 $\alpha_1=0,\alpha_2,\ldots,\alpha_q$ 代表 $\mathbb{F}_{p^n}$ 中的所有元素。令 y 为扩域 $\mathbb{F}_{p^{nr}}$ 中的一个本原元。取 $y^{d_i}=y+\alpha_i$，$i=1,2\ldots,q$，其中 $d_i<p^{nr}$. 则整数集 $\{d_i\}_{1\leq i\leq q}$ 即引理所需要的整数。它由本原元 y 的选取，或者等价的说由以 $\mathbb{F}_{p^n}$ 为系数的 r 次不可约多项式的选取所唯一决定。我们现在期望这个不可约多项式有些许更好的性质。

以 $A_K(n,5)$ 为例。需要以 $\mathbb{F}_{p^n}$ 为系数的 2 次不可约多项式，记为 $y^2=ay+b$，$a,b\in\mathbb{F}_{p^n}$. 现在我们进一步要求对应的整数集 $\{d_i\}_{1\leq i\leq q}$ 满足，其中任意三个的加和模 $p^{2n}-1$ 非零。亦即，对任意 $i,j,k\in\mathbb{F}_{p^n}$ 有 $(y+i)(y+j)(y+k)\neq 1$. 可以检验这等价于下面的问题:

Problem: 对任何素数幂 p^n，是否存在 $a,b\in\mathbb{F}_{p^n}$ 使得

- $y^2=ay+b$ 为 $\mathbb{F}_{p^n}$ 上的不可约多项式，

- 下面以 i,j,k 为未知数的方程在 $\mathbb{F}_{p^n}^3$ 中无解。

$$\begin{cases} a^2+b+ai+aj+ak+ij+ik+jk=0 \\ ab+ib+jb+kb+ijk=1 \end{cases}$$

通过计算机搜索，虽然期望的 a 与 b 在 $\mathbb{F}_5$ 和 $\mathbb{F}_7$ 上并不存在，但对于 11，13，17，19，23 确实找到了期望的值。我们猜想对于无穷多的素数，期望的 a 与 b 是存在的。

对于素数 n，在 a 与 b 存在的时候，可以对我们的染色方案做些许调整。令 $\widetilde{c}_1(\pi) \equiv I(\pi) \pmod 3$，而不再是模 5. 对于任意两个距离 $d_K(\sigma,\pi) < 2t+1$ 的置换 σ 和 τ，$\widetilde{c}_1(\sigma) = \widetilde{c}_1(\pi)$ 且 $\omega(x_\pi - x_\sigma) = 0$ 同时成立的唯一的可能性是，它们的逆序向量 x_σ 和 x_π 之差恰有三位为“1”，其余为“0”。但由 a 与 b 选取时附加的性质，得以保证 $c_2(\sigma) \neq c_2(\pi)$. 于是通过这样的微调，我们可以把下界与球填充上界之间的常数差距进一步缩小。

2.4.2 其它关于 $A_K(n,d)$ 的零星结果

依然是将 $A_K(n,d)$ 的问题转化为图上的独立集问题来看待。这里需要关于图的独立数的另外一个结论。图 G 的一个**自同构**是 $f: V(G) \to V(G)$ 这样一个双射，使得对任意两点 $u,v \in V(G)$，$(f(u),f(v)) \in E(G)$ 当且仅当 $(u,v) \in E(G)$. 若对于图中任何两点 u 和 v，存在一个自同构 $f: V(G) \to V(G)$ 使得 $f(u) = v$，则称 G 为**点传递**的。对于点传递图有以下结论[68]：

引理19. *如果 G 是点传递的，G' 是 G 的一个诱导子图。则我们有*

$$\frac{\alpha(G)}{|V(G)|} \leq \frac{\alpha(G')}{|V(G')|}.$$

在引理 19 中，[27] 中使用的“码-反码”方法对应于寻找一个诱导子图 G'，满足 $\alpha(G') = 1$，且目标是使 $|G'|$ 尽量大。一个自然的推广是跳出 $\alpha(G') = 1$ 这一限制。即，正如引理 19 所指出的，我们本质上是要搜索诱导子图 G'，使得 $\alpha(G')/|G'|$ 这个比例尽量小。作为一个启发性的例子，我们可以精确决定 $A_K(5,3)$ 的值。在[27] 中已经证明了 $20 \leq A_K(5,3) \leq 23$. 下面说明，20 是准确的值。

定理20.

$$A_K(5,3) = 20.$$

证明. 对于 $A_K(5,3)$ 所对应的图，取 $G' = \{[1,2,3,4,5]$，$[1,2,3,5,4]$，$[1,2,4,3,5]$，$[1,2,4,5,3]$，$[1,2,5,3,4]$，$[1,2,5,4,3]$，$[2,1,3,4,5]$，$[2,1,3,5,4]$，$[2,1,4,3,5]$，$[2,1,4,5,3]$，$[2,1,5,3,4]$，$[2,1,5,4,3]\}$. 可以验证这些点生成的诱导子图满足 $\alpha(G') = 2$，于是 $\frac{A_K(5,3)}{5!} \leq \frac{\alpha(G')}{|G'|} = \frac{2}{12}$，推出 $A_K(5,3) \leq 20$，进而完全决定了 $A_K(5,3) = 20$. □

虽然这仅仅是一个简单的例子，但是这种对“码-反码”方法的扩展或许在其它参数下，甚至在其它各种码字的研究中也会有潜在的应用。

另有一些在 $n = 5$ 和 $n = 6$ 下的零星结果，借由搜索图的最大独立集的算法所给出。我们利用 Ashay Dharwadker[48] 所研制的算法，搜索出了部分结果，比之前已知的下界[27]更好。这些值列在下面的结论中，并附对应的码的例子。由算法所暗示，这些值或许是精确的，但缺乏严格的数学证明。

定理21.

$$A_K(5,4) \geq 12,$$
$$A_K(6,3) \geq 101, A_K(6,4) \geq 64, A_K(6,5) \geq 25,$$
$$A_K(6,6) \geq 20, A_K(6,7) \geq 11, A_K(6,8) \geq 7.$$

Kendall's τ-距离下码字数目为 12 的 (5,4)-置换码：

$$[1,2,3,4,5], [1,3,5,4,2], [1,4,5,2,3], [2,1,5,4,3], [2,4,3,1,5], [3,4,5,1,2],$$
$$[3,5,2,1,4], [4,1,3,2,5], [4,2,5,1,3], [5,1,2,3,4], [5,2,4,3,1], [5,4,1,3,2].$$

Kendall's τ-距离下码字数目为 101 的 (6,3)-置换码：

$$[1,2,3,4,6,5], [1,2,5,4,3,6], [1,2,6,4,3,5], [1,2,6,5,3,4], [1,3,2,6,5,4], [1,3,4,6,2,5],$$
$$[1,3,5,2,4,6], [1,3,6,5,4,2], [1,4,2,5,6,3], [1,4,3,2,5,6], [1,4,5,6,3,2], [1,4,6,2,3,5],$$
$$[1,5,2,3,6,4], [1,5,3,4,6,2], [1,5,6,4,2,3], [1,6,4,3,5,2], [1,6,5,3,2,4], [2,1,3,5,6,4],$$
$$[2,1,4,3,5,6], [2,1,4,6,5,3], [2,3,1,6,4,5], [2,3,4,1,5,6], [2,3,6,4,5,1], [2,4,3,5,6,1],$$
$$[2,4,5,1,6,3], [2,4,6,1,3,5], [2,5,1,6,4,3], [2,5,3,1,6,4], [2,5,4,3,1,6], [2,5,6,3,4,1],$$
$$[2,6,1,3,4,5], [2,6,1,5,4,3], [2,6,3,5,1,4], [2,6,4,5,1,3], [3,1,2,4,5,6], [3,1,4,5,6,2],$$

$[3,1,5,6,2,4],[3,1,6,2,4,5],[3,2,4,6,1,5],[3,2,5,1,4,6],[3,2,5,6,4,1],[3,2,6,1,5,4],$

$[3,4,1,2,6,5],[3,4,2,5,6,1],[3,4,5,1,2,6],[3,4,6,5,1,2],[3,5,6,4,2,1],[3,6,1,4,5,2],$

$[3,6,4,2,1,5],[3,6,5,2,1,4],[4,1,2,3,6,5],[4,1,3,6,5,2],[4,1,5,3,2,6],[4,1,6,5,2,3],$

$[4,2,1,5,3,6],[4,2,3,6,1,5],[4,2,6,5,3,1],[4,3,2,1,5,6],[4,3,5,6,2,1],[4,3,6,1,2,5],$

$[4,5,1,2,6,3],[4,5,2,3,6,1],[4,5,3,1,6,2],[4,5,6,2,1,3],[4,6,2,1,5,3],[4,6,3,2,5,1],$

$[4,6,5,1,3,2],[5,1,2,4,6,3],[5,1,4,3,2,6],[5,1,6,2,3,4],[5,2,1,3,4,6],[5,2,3,4,6,1],$

$[5,2,4,6,1,3],[5,2,6,1,3,4],[5,3,1,2,4,6],[5,3,1,6,4,2],[5,3,2,6,1,4],[5,3,4,2,1,6],$

$[5,3,4,6,1,2],[5,4,1,6,3,2],[5,4,2,1,3,6],[5,4,6,3,2,1],[5,6,1,3,4,2],[5,6,3,2,4,1],$

$[5,6,4,1,2,3],[6,1,2,3,5,4],[6,1,2,4,5,3],[6,1,3,4,2,5],[6,1,5,4,3,2],[6,2,4,3,1,5],$

$[6,2,5,1,3,4],[6,2,5,4,3,1],[6,3,1,5,2,4],[6,3,2,1,4,5],[6,3,2,5,4,1],[6,3,4,5,2,1],$

$[6,4,1,2,3,5],[6,4,3,1,5,2],[6,4,5,2,3,1],[6,5,1,2,4,3],[6,5,4,3,1,2].$

Kendall's τ-距离下码字数目为 64 的 (6,4)-置换码：

$[1,2,3,5,6,4],[1,2,4,6,5,3],[1,3,2,4,6,5],[1,3,4,5,6,2],[1,4,2,3,5,6],[1,5,2,6,4,3],$

$[1,5,4,3,2,6],[1,5,6,3,4,2],[1,6,2,5,3,4],[1,6,3,4,2,5],[1,6,4,5,2,3],[2,1,5,4,3,6],$

$[2,1,6,3,4,5],[2,3,1,4,5,6],[2,3,5,6,1,4],[2,3,6,4,1,5],[2,4,1,3,6,5],[2,4,6,5,1,3],$

$[2,5,1,6,3,4],[2,5,4,3,6,1],[2,6,1,5,4,3],[2,6,5,3,4,1],[3,1,5,2,4,6],[3,1,6,5,4,2],$

$[3,2,1,6,5,4],[3,2,5,4,1,6],[3,4,2,1,6,5],[3,4,5,1,2,6],[3,5,4,6,2,1],[3,5,6,1,2,4],$

$[3,6,1,2,4,5],[3,6,2,5,4,1],[3,6,4,5,1,2],[4,1,5,6,3,2],[4,1,6,2,3,5],[4,2,1,5,6,3],$

$[4,2,3,5,1,6],[4,2,6,3,1,5],[4,3,1,6,5,2],[4,3,6,2,5,1],[4,5,1,2,3,6],[4,5,2,6,3,1],$

$[4,5,3,6,1,2],[4,6,5,1,2,3],[5,1,3,2,6,4],[5,1,4,6,2,3],[5,2,3,1,4,6],[5,2,4,1,6,3],$

$[5,3,1,4,6,2],[5,3,2,6,4,1],[5,4,3,2,1,6],[5,6,1,2,3,4],[5,6,3,4,1,2],[5,6,4,2,1,3],$

$[6,1,2,4,3,5],[6,1,3,5,2,4],[6,2,3,1,5,4],[6,2,4,3,5,1],[6,3,4,2,1,5],[6,4,1,3,5,2],$

$[6,4,2,1,5,3],[6,4,5,3,2,1],[6,5,1,4,3,2],[6,5,3,2,1,4].$

Kendall's τ-距离下码字数目为 25 的 (6,5)-置换码：

$[1,2,3,4,6,5],[1,3,5,4,2,6],[1,5,4,6,2,3],[1,6,3,5,2,4],[2,1,4,5,6,3],[2,3,6,4,5,1],$
$[2,5,4,3,6,1],[2,6,1,5,3,4],[3,1,6,4,2,5],[3,2,1,5,6,4],[3,5,4,2,6,1],[4,1,3,6,5,2],$
$[4,2,3,1,5,6],[4,2,6,5,1,3],[4,3,6,2,5,1],[4,5,1,2,3,6],[5,2,1,3,4,6],[5,3,1,6,4,2],$
$[5,4,6,3,1,2],[5,6,1,2,3,4],[6,1,4,5,3,2],[6,2,4,1,3,5],[6,3,2,5,1,4],[6,3,4,5,1,2],$
$[6,5,2,4,3,1].$

Kendall's τ-距离下码字数目为 20 的 (6,6)-置换码：

$[1,2,3,4,6,5],[1,5,4,3,6,2],[1,6,3,5,2,4],[1,6,4,2,5,3],[2,1,5,4,6,3],[2,3,4,5,6,1],$
$[2,6,4,1,3,5],[2,6,5,3,1,4],[3,2,1,5,6,4],[3,4,5,1,6,2],[3,6,1,4,2,5],[3,6,5,2,4,1],$
$[4,3,2,1,6,5],[4,5,1,2,6,3],[4,6,1,3,5,2],[4,6,2,5,3,1],[5,1,2,3,6,4],[5,4,3,2,6,1],$
$[5,6,2,4,1,3],[5,6,3,1,4,2].$

Kendall's τ-距离下码字数目为 11 的 (6,7)-置换码：

$[1,2,3,4,5,6],[1,5,4,3,6,2],[2,1,6,5,4,3],[2,6,3,4,5,1],[3,4,5,6,1,2],[3,5,2,1,6,4],$
$[4,3,2,1,6,5],[4,5,2,1,6,3],[5,6,1,2,3,4],[6,1,3,4,2,5],[6,5,4,3,2,1].$

Kendall's τ-距离下码字数目为 7 的 (6,8)-置换码：

$$[1,2,3,6,4,5],[1,4,5,6,2,3],[2,4,5,3,1,6],[3,4,6,2,1,5],$$
$$[3,5,1,4,2,6],[5,2,6,1,3,4],[6,5,4,3,1,2].$$

2.5　Kendall's τ-距离下 S_{2n+1} 中的蛇形码

本小节将讨论在 Kendall's τ-距离下奇数阶置换群 S_{2n+1} 中的蛇形码的相关问题。具体分为三个部分。一是对于 Horovitz-Etzion 蛇形码构造过程的详细回顾，二是对他们的方案的可行性给出了严格的证明，三是基于他们的方案进行微调，得到了潜在的更优方案。

2.5.1　Horovitz-Etzion 蛇形码的构造

Horovitz 与 Etzion 在[73]中给出的直接构造的目标是 S_{2n+1} 中码字数目达到 $M_{2n+1}=\frac{(2n+1)!}{2}-2n+1$ 的蛇形码。他们猜想这个方案对于一般的奇数 $2n+1\geq 5$ 皆可行，并通过计算机搜索对 S_5，S_7 与 S_9 做出了证实。

前文已说明，我们将“推至顶端”操作只作用于奇数位指标上，整个过程不改变置换的奇偶性。即可以只考虑交错群 A_{2n+1} 中的置换如何排列成尽量长的蛇形码。首先，将交错群 A_{2n+1} 依据最后两位有序对而分拆成为不交的**类**。即，一个标记为 $[x,y]$ 的类包含了所有倒数第二位为 $a_{2n}=x$ 且末位为 $a_{2n+1}=y$ 的置换 $\pi=[a_1,a_2,\ldots,a_{2n+1}]\in A_{2n+1}$. 总计有 $2n(2n+1)$ 个类，每个类中有 $\frac{(2n-1)!}{2}$ 个偶置换。进一步将每个类分拆成为 $\frac{(2n-2)!}{2}$ 个**子类**，分拆依据为：置换中的前 $2n-1$ 个元素按其循环关系构成一个子类。记 $[x,y]$ 类中的每个子类为 $[\alpha]-[x,y]$，其中 α 是前 $2n-1$ 个元素的一个循环排序。（下文中每当置换的向量表示中出现希腊字母 $\alpha,\beta,\gamma\ldots$ 时，它代表了一列数，当然也可能是单个的数字，其大小和具体包含哪些数字可从上下文推断得到）。例如，S_7 中的一个类 $[1,2]$ 包含了所有以 $a_6=1$ 和 $a_7=2$ 收尾的置换 $\pi=[a_1,a_2,\ldots,a_7]$，它其中的一个子类 $[3,4,5,6,7]-[1,2]$ 包含了下面 5 个置换：$[3,4,5,6,7,1,2]$，$[7,3,4,5,6,1,2]$，$[6,7,3,4,5,1,2]$，$[5,6,7,3,4,1,2]$ 和 $[4,5,6,7,3,1,2]$. 显然，这样一个子类本身是一个蛇形码，所有的“推至顶端”操作均作用于第 $2n-1$ 个位置上。我们将这种初始结构称为一个**项链**。

下一步是将若干项链组合在一起形成一个更长的蛇形码。为达到这个目标，我们需要一些将项链进行组合的方法，这些方法由下面的 3-超图给出。此部分是本构造的核心。

如下定义一张 3-超图 $H_{2n+1}=(V_{2n+1},E_{2n+1})$. 图的点集对应于 S_{2n+1} 中的所有类 $[x,y]$. 对于不同的 $x,y,z\in[2n+1]$，一条名为 $\langle x,y,z\rangle$ 的边包含了三个顶点 $[x,y]$，$[y,z]$ 和 $[z,x]$. 此图上的一个近似生成树 T_{2n+1} 是一个包含除却 $[2,1]$ 之外所有顶点的树。例如，我们可以取 T_5 包含如下九条边：$\langle1,2,3\rangle$，$\langle1,2,4\rangle$，$\langle1,2,5\rangle$，$\langle1,5,3\rangle$，$\langle2,3,5\rangle$，$\langle1,3,4\rangle$，$\langle2,4,3\rangle$，$\langle1,4,5\rangle$，$\langle2,5,4\rangle$. T_{2n+1} 可以在 T_{2n-1} 的基础上递归定义得到，所额外添加的边为：对于 $2\le x\le 2n-2$ 时的 $\langle x,x+1,2n\rangle$，对于 $2\le x\le 2n-2$ 时的 $\langle x,x+1,2n+1\rangle$，以及另外的边 $\langle1,2,2n\rangle$，$\langle1,2n,2n-1\rangle$，$\langle1,2n+1,2n-1\rangle$，$\langle1,2n,2n+1\rangle$，$\langle2,2n+1,2n\rangle$. 在[73] 中出现的图 2-1 示意了通过 T_5 得到 T_7 的过程。图中的实线矩形和圆圈代表了 T_5 中的边和点，虚线矩形和双圆圈代表了为得到 T_7 所添加的边和点。

在定义了近似生成树 T_{2n+1} 之后，我们开始叙述由这个树所指示的将若干项链结合成更长的 $\mathcal{K}$-蛇的方法。初始的项链选取为任何的 $[\alpha]-[1,2]$. 按顺序考虑 T_{2n+1} 中的边。注意到如[73] 中所提及，不同的取边的顺序将对应了不同的结合顺序，致使得到的最终的 $\mathcal{K}$-蛇也不同。我们这里取边的顺序遵从上文递归定义过程中的顺序。当取到一条边 $\langle x,y,z\rangle$ 时，已构造的 $\mathcal{K}$-蛇中将恰恰包含 $[x,y]$，$[y,z]$，$[z,x]$ 这三个类中的唯一一个类中的一条项链。不失一般性假设已构造的 $\mathcal{K}$-蛇中已融入了一段 $[x,y]$-项链。现在要将一段 $[y,z]$-项链和一段 $[z,x]$-项链镶嵌进去。将已构造的 $\mathcal{K}$-蛇在某个 $[\beta,z,x,y]$ 之后的位置断开，其中 β 代表了置换中的前 $2n-2$ 个元素。这样的位置必然存在，因为已融入 $\mathcal{K}$-蛇中的 $[x,y]$-项链自

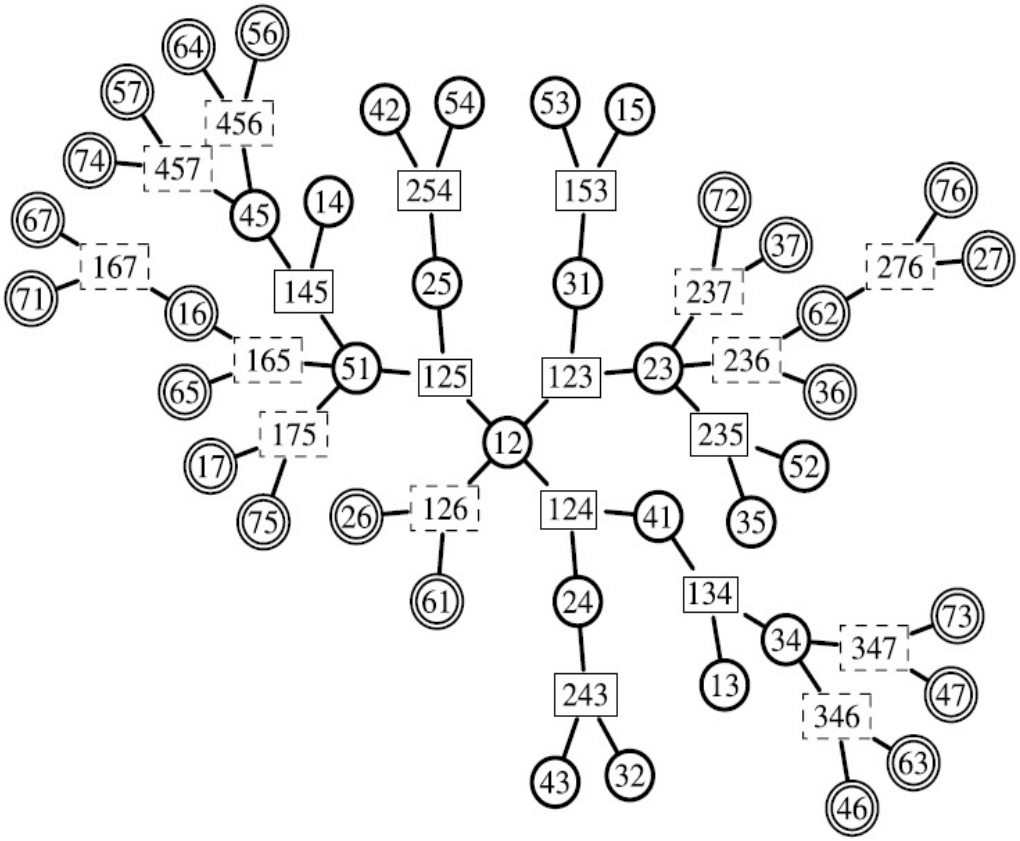

图 2-1　由 T_5 得到 T_7

身是一个在前 $2n-1$ 个位置上循环的结构。我们按如下操作镶嵌进一段 $[y,z]$-项链和一段 $[z,x]$-项链。在断点处，做一个“推至顶端”操作 t_{2n+1}，得到置换 $[y,\beta,z,x]$. 进而将整个以 $[y,\beta,z,x]$ 开头至 $[\beta,y,z,x]$ 的 $[z,x]$-项链写入。再做一次操作 t_{2n+1} 得到 $[x,\beta,y,z]$，续上它所在的整个 $[y,z]$-项链，以 $[\beta,x,y,z]$ 收尾。最后再做一次操作 t_{2n+1} 回到 $[z,\beta,x,y]$，这恰恰是原先断点之后紧接的置换。作为示例，图 2-2 中给出了 S_5 中按此方法所构造的一个长为 57 的 $\mathcal{K}$-蛇的过程。在遍历完近似生成树的所有边之后，可以得到一个 $\mathcal{K}$-蛇，包含了除却 $[2,1]$ 之外的每个类中恰好一条项链。当前的结构，我们称之为一条**锁链**。对于上述固定的近似生成树的边的遍历顺序，可以从任何一条初始项链 $[\alpha]-[1,2]$ 开始得到一条锁链，则我们以下在不引起混淆的前提下，用同样的记号 $[\alpha]-[1,2]$ 来表示这条锁链。有时也直接称这条锁链为 $c[\alpha]$. 在[73] 中证明，按上述方式，除却 $[2,1]$ 类之外的所有置换可以分拆到彼此不交的锁链之中。

截至目前我们共有 $\frac{(2n-2)!}{2}$ 条锁链，涵盖了除却 $[2,1]$ 类之外的所有置换。下一步则是如何利用余下的 $[2,1]$ 类中的置换，来把各锁链串联起来得到更长的 $\mathcal{K}$-蛇。[73] 中证明了下面的引理。

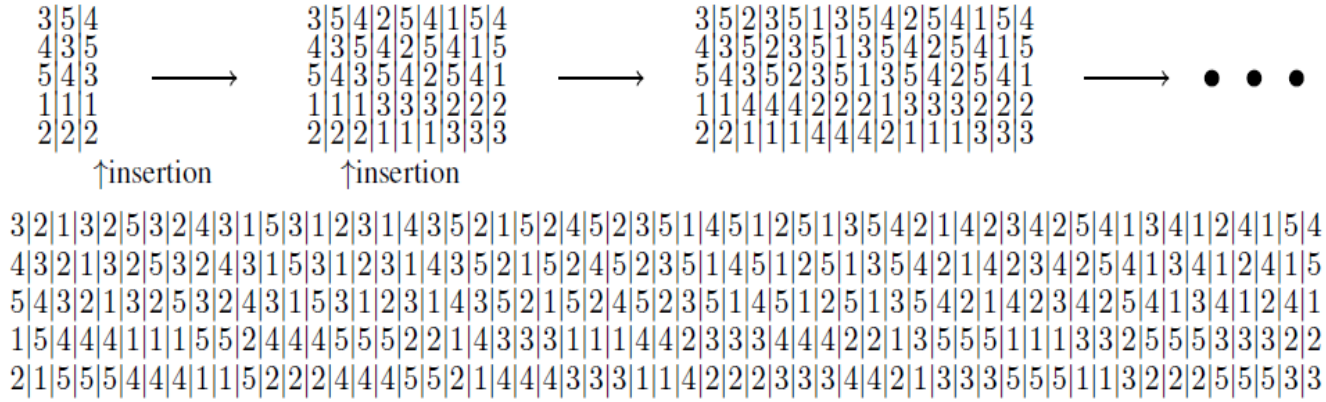

图 2-2　将项链结合成锁链，$M_5 = 57$

引理22. *对于整数 $3 \le x \le 2n+1$，令 α 为 $[2n+1]\backslash\{x,1,2\}$ 这些元素上的一个置换。若 $[\alpha,1,x,2]$ 和 $[\alpha,2,1,x]$ 包含于不同的锁链之中，则可以通过项链 $[\alpha,x]-[2,1]$ 来融合这两条锁链。*

上述融合过程称为一个 $M[x]$-**链接**。把项链 $[\beta]-[2,1]$ 称为**链接介质**，其中 β 等同于 $[\alpha,x]$ 的一个循环排序。链接过程如图 2-3 所示。

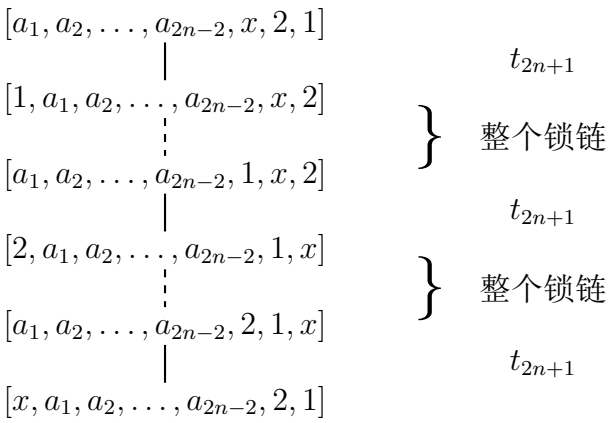

图 2-3　$M[x]$-链接

在[73]中，作者不加证明地提出，如果 $x \in \{3,4,5\}$ 则置换 $[\alpha,1,x,2]$ 和 $[\alpha,2,1,x]$ 包含于同一条锁链之中，于是并没有 $M[3]$-链接，$M[4]$-链接或者 $M[5]$-链接。这其实是由之前选定的生成树的结构和边的遍历顺序所决定的。我们下面详细证明这一点，并阐述在 $x > 5$ 时一些关于 $M[x]$-链接的性质。

定理23. *对于 $x = 3,4,5$ 不存在 $M[x]$-链接。对于 $x \in \{2t, 2t+1\}$，$t \ge 3$，经由链接介质 $[\pi]-[2,1]$ 的 $M[x]$-链接将 $[(3,x)\pi]-[1,2]$ 和 $[\sigma\pi]-[1,2]$ 这两条锁链融合，其中 σ 是一个*

置换，它的循环表示形如 $\sigma=(5,6,\ldots,2t-1,x)$.

证明. 由近似生成树所指示的融合的规则，意味着对于 T_{2n+1} 中的任何一条边 $\langle x,y,z\rangle$，项链 $[\beta,x]-[y,z]$，$[\beta,y]-[z,x]$，$[\beta,z]-[x,y]$ 三者被融合在同一条锁链之中。于是可以通过锁链中的一条项链甚至一个置换去逐步反推锁链的名字。

例如，对于 $x=3$. 我们特别地强调出数字“4”的位置，将置换 $[\alpha,1,3,2]$ 写成 $\pi_1=[\beta,4,\gamma,1,3,2]$. π_1 与 $\pi_2=[\gamma,1,\beta,4,3,2]$ 隶属于同一条项链之中。由近似生成树中的边 $\langle 2,4,3\rangle$ 可知，此项链与包含 $\pi_3=[\gamma,1,\beta,3,2,4]$ 的项链在同一条锁链中。进而，π_3 与 $\pi_4=[\beta,3,\gamma,1,2,4]$ 隶属于同一条项链之中。最后由近似生成树中的边 $\langle 1,2,4\rangle$ 可知，此锁链中含有 $[\beta,3,\gamma,4,1,2]$. 如此我们反推出来，置换 $[\alpha,1,3,2]$ 被包含在 $c[\beta,3,\gamma,4]$ 这个锁链之中。

类似地，将置换 $[\alpha,2,1,3]$ 写成 $\sigma_1=[\beta,4,\gamma,2,1,3]$. σ_1 与 $\sigma_2=[\gamma,2,\beta,4,1,3]$ 隶属于同一条项链之中。由近似生成树中的边 $\langle 1,3,4\rangle$ 可知，此项链与包含 $\sigma_3=[\gamma,2,\beta,3,4,1]$ 的项链在同一条锁链中。进而，σ_3 与 $\sigma_4=[\beta,3,\gamma,2,4,1]$ 隶属于同一条项链之中。最后由近似生成树中的边 $\langle 1,2,4\rangle$ 可知，此锁链中含有 $[\beta,3,\gamma,4,1,2]$. 如此我们反推出来，置换 $[\alpha,2,1,3]$ 被包含在 $c[\beta,3,\gamma,4]$ 这个锁链之中。综上我们得到，置换 $[\alpha,1,3,2]$ 与 $[\alpha,2,1,3]$ 在同一条锁链之中。

对于 $x=4,5$ 有类似的分析过程。置换 $[\alpha,1,4,2]=[\beta,5,\gamma,1,4,2]$ 和 $[\alpha,2,1,4]=[\beta,5,\gamma,2,1,4]$ 都在同一条锁链 $c[\beta,4,\gamma,5]$ 之中。置换 $[\alpha,1,5,2]=[\beta,3,\gamma,1,5,2]$ 和 $[\alpha,2,1,5]=[\beta,3,\gamma,2,1,5]$ 都在同一条锁链 $c[\beta,5,\gamma,3]$ 之中。于是对于 $x=3,4,5$，并不存在 $M[x]$-链接。

余下的分析也是类似的。对于 $x\in\{2t,2t+1\}$，$t\geq 3$，链接介质 $[\pi]-[2,1]=[\alpha,x]-[2,1]$，强调出数字“3”的位置，记 $[\alpha,1,x,2]$ 为 $[\beta,3,\gamma,1,x,2]$. 则我们可以在它所在的锁链中依次找到如下置换：$[\gamma,1,\beta,3,x,2]$，$[\gamma,1,\beta,x,2,3]$，$[\beta,x,\gamma,1,2,3]$，$[\beta,x,\gamma,3,1,2]$. 由于 $[\pi]=[\alpha,x]=[\beta,3,\gamma,x]$，则可知它所在的锁链为 $[(3,x)\pi]-[1,2]$.

反推置换 $[\alpha,2,1,x]$ 所在的锁链的名字相对而言比较复杂，我们用一个归纳的方式进行说明。首先考虑归纳的初始情形 $x\in\{6,7\}$. 强调出数字“5”的位置，记 $[\alpha,2,1,x]$ 为 $[\beta',5,\gamma',2,1,x]$，则我们可以在它所在的锁链中依次找到如下置换：$[\gamma',2,\beta',5,1,x]$，$[\gamma',2,\beta',x,5,1]$，$[\beta',x,\gamma',2,5,1]$，$[\beta',x,\gamma',5,1,2]$. 由于 $[\pi]=[\alpha,x]=[\beta',5,\gamma',x]$，则可知它所在的项链为 $[(5,x)\pi]-[1,2]$. 假设已经对所有整数 $5<x<2t$ 得证，考虑 $x\in\{2t,2t+1\}$. 强调出数字“$2t-1$”和“$2t-2$”的位置，记 $[\alpha,2,1,x]$ 为 $[\beta',2t-1,\omega',2t-2,\gamma',2,1,x]$（当然也可能是另外一种形式，交换前式中的 $2t-1$ 和 $2t-2$ 的位置，证明是相似

的，略去），则可以在它所在的锁链中依次找到如下置换：$[\omega', 2t-2, \gamma', 2, \beta', 2t-1, 1, x]$，$[\omega', 2t-2, \gamma', 2, \beta', x, 2t-1, 1]$，$[\gamma', 2, \beta', x, \omega', 2t-2, 2t-1, 1]$，$[\gamma', 2, \beta', x, \omega', 2t-1, 1, 2t-2]$，$[\beta', x, \omega', 2t-1, \gamma', 2, 1, 2t-2]$. 由归纳可知，最后一个置换所在的锁链为 $c[(5, 6, \ldots, 2t-3, 2t-2)[\beta', x, \omega', 2t-1, \gamma', 2t-2]]$，等价于 $c[(5, 6, \ldots, 2t-3, 2t-2)(2t-2, 2t-1, x)\pi] = c[(5, 6, \ldots, 2t-1, x)\pi]$. □

定义一张图 $\mathcal{G}_{2n+1} = (\mathcal{V}_{2n+1}, \mathcal{E}_{2n+1})$，其中点集对应着所有锁链。两个顶点相连当且仅当它们代表的锁链之间可以如引理 22 那样被融合。这条边上有一个**符号** $M[x]$（表示这两个锁链由一个 $M[x]$-链接所融合）和一个**标记** $[\alpha, x] - [2, 1]$（指出链接介质的名称）。将所有项链融合到一个 $\mathcal{K}$-蛇的问题，即转化为在图 $\mathcal{G}_{2n+1}$ 中寻找一个各边的标记不同的生成树 $\mathcal{T}_{2n+1}$ 的问题。各边的标记不同这一要求，是为了同时尽量融合最多的（只剩余一个） $[2, 1]$-项链。一旦这种符合条件的生成树确实存在，则可以通过做这个树上的边所指代的融合过程，将所有锁链和只排除一个的所有 $[2, 1]$-项链融合成一个 $\mathcal{K}$-蛇，长度达到 $M_{2n+1} = \frac{(2n+1)!}{2} - 2n + 1$. Horovitz 与 Etzion[73] 猜想这种生成树确实存在，但只对 S_7 和 S_9 完成了计算机搜索。下面我们的主要贡献即是明确构造出来这样的生成树，从而将 Horovitz 与 Etzion 的构造方案彻底补充完整。要注意的是，也如在[73] 中所提及的，此生成树的每条边决定了一个唯一的融合操作，但是遍历此生成树的边的顺序是没有限制的，我们可以任意安排这些边的顺序，进而按顺序进行融合操作，最终也会得到不同的 $\mathcal{K}$-蛇。所以，即便给定了生成树，对于详细的融合过程的讨论既繁琐又没有必要。唯一要紧的事情仅仅是这样一个各边标记不同的生成树的存在性。

另外需要预先评论的一点是， Horovitz 与 Etzion 如此构造的 $\mathcal{K}$-蛇有一个有用的性质：它的转换序列中仅存在倒数第三位和末位上的“推至顶端”操作，t_{2n-1} 与 t_{2n+1}.

2.5.2 Horovitz-Etzion 蛇形码的严格证明

先从 S_7 这个例子入手来看一下整个证明的思路。图 $\mathcal{G}_7$ 包含如下 12 个点，对应于 12 条锁链（$C_{i,j}$ 这种形式的符号的命名将在后文解释）：

$$c_1=[5,6,7,3,4]-[1,2]\triangleq C_{2,3},\qquad c_2=[6,7,5,3,4]-[1,2]\triangleq C_{1,2},$$
$$c_3=[7,5,6,3,4]-[1,2]\triangleq C_{3,1},\qquad c_4=[7,6,3,5,4]-[1,2]\triangleq C_{2,1},$$
$$c_5=[7,3,5,6,4]-[1,2]\triangleq C_{4,1},\qquad c_6=[3,5,7,6,4]-[1,2]\triangleq C_{4,3},$$
$$c_7=[5,7,3,6,4]-[1,2]\triangleq C_{4,2},\qquad c_8=[3,6,5,7,4]-[1,2]\triangleq C_{2,4},$$
$$c_9=[5,3,6,7,4]-[1,2]\triangleq C_{3,4},\qquad c_{10}=[6,5,3,7,4]-[1,2]\triangleq C_{1,4},$$
$$c_{11}=[6,3,7,5,4]-[1,2]\triangleq C_{1,3},\qquad c_{12}=[3,7,6,5,4]-[1,2]\triangleq C_{3,2}.$$

12 个链接介质（$[2,1]$-项链）如下（$L_{i,j}$ 这种形式的符号的命名将在后文解释）：

$$\eta_1=[5,7,6,3,4]-[2,1]\triangleq L_{3,2},\qquad \eta_2=[6,5,7,3,4]-[2,1]\triangleq L_{1,3},$$
$$\eta_3=[7,6,5,3,4]-[2,1]\triangleq L_{2,1},\qquad \eta_4=[6,7,3,5,4]-[2,1]\triangleq L_{1,2},$$
$$\eta_5=[3,5,6,7,4]-[2,1]\triangleq L_{3,4},\qquad \eta_6=[6,3,5,7,4]-[2,1]\triangleq L_{1,4},$$
$$\eta_7=[7,5,3,6,4]-[2,1]\triangleq L_{4,1},\qquad \eta_8=[7,3,6,5,4]-[2,1]\triangleq L_{3,1},$$
$$\eta_9=[3,6,7,5,4]-[2,1]\triangleq L_{2,3},\qquad \eta_{10}=[5,6,3,7,4]-[2,1]\triangleq L_{2,4},$$
$$\eta_{11}=[3,7,5,6,4]-[2,1]\triangleq L_{4,2},\qquad \eta_{12}=[5,3,7,6,4]-[2,1]\triangleq L_{4,3}.$$

由定理 23，$\mathcal{G}_7$ 中的边上的符号仅有 $M[6]$ 和 $M[7]$. 经由一个 $M[6]$-链接，链接介质 $[\alpha]-[2,1]$ 将融合 $[(36)\alpha]-[1,2]$ 和 $[(56)\alpha]-[1,2]$ 这两条锁链。类似地，经由一个 $M[7]$-链接，链接介质 $[\alpha]-[2,1]$ 将融合 $[(37)\alpha]-[1,2]$ 和 $[(57)\alpha]-[1,2]$ 这两条锁链。上面列出锁链和链接介质的顺序其实与[73] 中是一样的，区别在于他们把每个锁链 $[\alpha]-[1,2]$ 或链接介质 $[\alpha]-[2,1]$ 中的 α 以“3”开头来写，而我们是以“4”作为结尾来写，这主要是为后文分析的便利。

现在要解释一下 $C_{i,j}$ 与 $L_{i,j}$ 符号的含义。这其实是基于“6”和“7”的位置对锁链和链接介质进行的重命名。对于每个锁链 $[\alpha]-[1,2]$ 或链接介质 $[\alpha]-[2,1]$，我们已经在 α 的写法中将“4”固定在了末位。假设“6”出现在第 i 位，“7”出现在第 j 位，则 α 被唯一决定（因为整个置换本身需要是偶置换，则“3”和“5”的位置唯一化），则这个锁链或链接介质分别被记为 $C_{i,j}$ 或 $L_{i,j}$，$1\leq i,\ j\leq 4$ 且 $i\neq j$. 接下来在本段中的加减法将在模 4 下进行。经由一个 $M[6]$-链接，链接介质 $L_{i,j}$ 所融合的两锁链为 $C_{k,j}$ 和 $C_{l,j}$，其中 k 和 l 为 $\{1,2,3,4\}\backslash\{i,j\}$ 中的那两个元。类似地，经由一个 $M[7]$-链接，链接介质 $L_{i,j}$ 所融

合的两锁链为 $C_{i,k}$ 和 $C_{i,l}$，其中 k 和 l 为 $\{1,2,3,4\}\backslash\{i,j\}$ 中的那两个元。由此画出 $\mathcal{G}_7$ 如图 2-4 所示。下一步目标是从中寻找一个各边标号不同的生成树 $\mathcal{T}_7$. 为此，我们做更强的要求，寻找图中一个各边标号不同的 Hamiltonian 圈 $\mathcal{C}_7$，进而删除这个圈的任何一条边都将得到想得到的生成树。这个强化的要求在后面的分析中更能体现出其意义。圈的取法如下：对于链接介质 $L_{i,j}$，$j \equiv i-1 \pmod 4$，选取利用它做 $M[6]$-链接所对应的边，即联系 $C_{i+1,i-1}$ 和 $C_{i+2,i-1}$ 的边；对于其它每个链接介质，选取利用它做 $M[7]$-链接所对应的边，即，链接介质 $L_{i,i+1}$ 经由 $M[7]$-链接所对应的是联系 $C_{i,i+2}$ 和 $C_{i,i+3}$ 的边，链接介质 $L_{i,i+2}$ 经由 $M[7]$-链接所对应的是联系 $C_{i,i+1}$ 和 $C_{i,i+3}$ 的边。所得到的 Hamiltonian 圈如图 2-4 所示。删除圈中任意一条边可得一个生成树，以此生成树的指示做融合操作即可得一个长度达到 $M_7 = 2515$ 的$\mathcal{K}$-蛇，包含了所有锁链以及除却一条之外的所有 $[2,1]$-项链。缺失的五个置换即是被删除的那条边的标记所对应的 $[2,1]$-项链中的那五个置换。

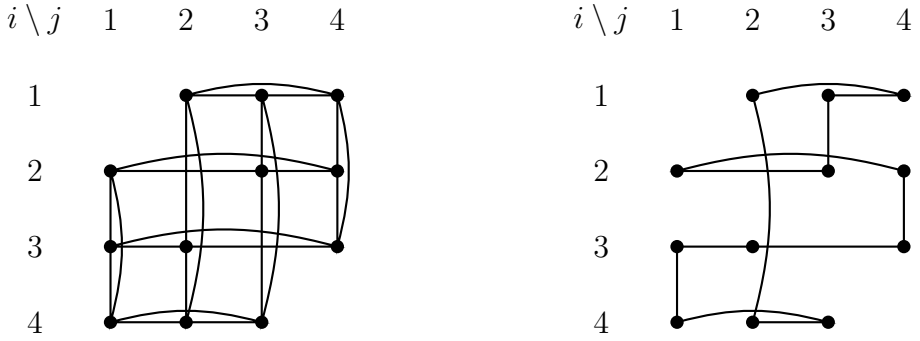

图 2-4　图 $\mathcal{G}_7$ 和对应的 Hamiltonian 圈 $\mathcal{C}_7$

在这个初始的例子之后，接下来对于 $\mathcal{T}_{2n+1}$ 的构造将通过递归构造的方式完成。递归的可行性依赖于[73] 中的发现。

引理24. *对任意 $n \geq 4$，图 $\mathcal{G}_{2n+1}$ 包含了 $(2n-3)(2n-2)$ 份不相交的与 $\mathcal{G}_{2n-1}$ 同构的子图，这每份子图称为一个“部”。在两个不同的部之间的边上的符号仅为 $M[2n]$ 和 $M[2n+1]$.*

仔细观察 $\mathcal{G}_{2n+1}$ 的结构。对于每个锁链 $[\alpha]-[1,2]$ 和链接介质 $[\alpha]-[2,1]$，将 α 写成把“4”放于第 $(2n-1)$ 个位置的形式。令 $C_{i,j}$ 或 $L_{i,j}$ 分别表示 α 中“$2n$”在第 i 位且“$2n+1$”在第 j 位所对应的所有锁链或所有链接介质的集合，$i,j \in \{1,2,\ldots,2n-2\}$, $i \neq j$. 由定理 23，$L_{i,j}$ 中任何一个链接介质经由 $M[x]$- 链接，$x \notin \{2n, 2n+1\}$，所对应的边是 $C_{i,j}$ 内部的一条边。另外，对于给定的一对 i 和 j，$C_{i,j}$ 中的所有锁链，加上 $L_{i,j}$ 中所有链接介质经由 $M[x]$-链接所对应的边，$x \notin \{2n, 2n+1\}$，这些点与边一同构成了与 $\mathcal{G}_{2n-1}$ 同构的一个子图。亦即，这就是上文引理 24 所说的一个“部”。

再定义一张新的图，$\hat{\mathcal{G}}_{2n+1}=(\hat{\mathcal{V}}_{2n+1},\hat{\mathcal{E}}_{2n+1})$，其中点对应于 $\{C_{i,j}:1\le i,j\le 2n-2,i\ne j\}$，即每个“部”。对于任意两个锁链 $c_1\in C_{i,j}$ 和 $c_2\in C_{i',j'}$，其中 $C_{i,j}$ 和 $C_{i',j'}$ 不相同，如果 c_1 与 c_2 在 $\mathcal{G}$ 中有边相连，则在 $\hat{\mathcal{G}}_{2n+1}$中将点 $C_{i,j}$ 和 $C_{i',j'}$ 连一条有着同样符号与标记的边。由引理 24，$\hat{\mathcal{G}}_{2n+1}$ 中的边仅有 $M[2n]$ 和 $M[2n+1]$ 这两种符号。

定理25. *$\hat{\mathcal{G}}_{2n+1}$ 中存在 Hamiltonian 圈 $\hat{\mathcal{C}}_{2n+1}$，其中任意两条边的标记来源于不同的 $L_{i,j}$.*

证明. 本证明中的加减法将在模 $2n-2$ 下进行。对于链接介质集合 $L_{i,j}$，$j\equiv i-1\pmod{2n-2}$，我们从中挑选一个“3”在第 $(i-2)$ 位，“$2n-1$”在第 $(i-3)$ 位的链接介质，它经由一个 $M[2n]$-链接，融合了 $C_{i-2,j}$ 和 $C_{i-3,j}$ 中的各自一个锁链。这在图 $\hat{\mathcal{G}}_{2n+1}$ 中对应于一条连结 $C_{i-2,i-1}$ 和 $C_{i-3,i-1}$ 的边。对于链接介质集合 $L_{i,j}$，$j\equiv i-2\pmod{2n-2}$，我们从中挑选一个“3”在第 $(i-1)$ 位，“$2n-1$”在第 $(i+1)$ 位的链接介质，它经由一个 $M[2n+1]$-链接，融合了 $C_{i,i-1}$ 和 $C_{i,i+1}$ 中的各自一个锁链。这在图 $\hat{\mathcal{G}}_{2n+1}$ 中对应于一条连结 $C_{i,i-1}$ 和 $C_{i,i+1}$ 的边。对于其它每个链接介质集合 $L_{i,j}$，我们从中挑选一个“3”在第 $(j+1)$ 位，“$2n-1$”在第 $(j+2)$ 位的链接介质，它经由一个 $M[2n+1]$-链接，融合了 $C_{i,j+1}$ 和 $C_{i,j+2}$ 中的各自一个锁链。这在图 $\hat{\mathcal{G}}_{2n+1}$ 中对应于一条连结 $C_{i,j+1}$ 和 $C_{i,j+2}$ 的边。可检验得知，上述的边构成了$\hat{\mathcal{G}}_{2n+1}$ 中的一个 Hamiltonian 圈 $\hat{\mathcal{C}}_{2n+1}$，其中任意两条边的标记来源于不同的 $L_{i,j}$. □

作为一个示例，$\hat{\mathcal{G}}_9$ 中的符合要求的 Hamiltonian 圈 如图 2-5 所示。

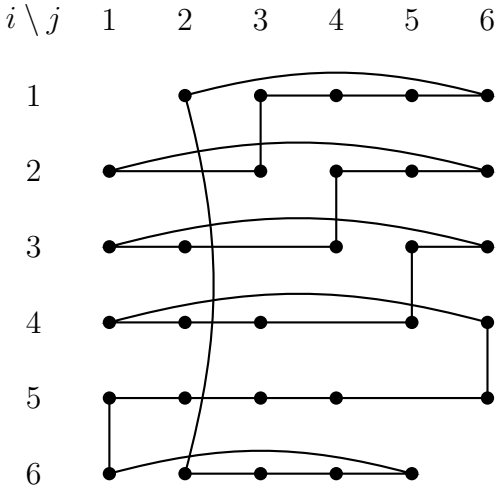

图 2-5　$\hat{\mathcal{G}}_9$ 中的 Hamiltonian 圈示例

在以上准备的基础上，我们可以通过归纳的方法说明图 $\mathcal{G}_{2n+1}$ 中必存在各边标记不同的生成树。归纳的步骤如下。删除 $\hat{\mathcal{C}}_{2n+1}$ 中的任何一条边，得到 $\hat{\mathcal{G}}_{2n+1}$ 中的一个任意两条

边的标记来源于不同的 $L_{i,j}$ 的生成树。则这棵树上占用了每个 $L_{i,j}$ 中至多一个链接介质。由归纳假设，$C_{i,j}$ 这个锁链集合自身作为与 $\mathcal{G}_{2n-1}$ 同构的一个“部”，其内部有生成树，各边的标号来自 $L_{i,j}$ 中所有不同的链接介质。通过做一定的 $[n]$ 自身上的双射，可调整得到一个生产树，各边的标号所对应的链接介质并不包含那个已经被 $\hat{\mathcal{C}}_{2n+1}$ 占用的链接介质。各局部 $C_{i,j}$ 的内部由这样的生成树连通，将各局部 $C_{i,j}$ 视为一个点的图 $\hat{\mathcal{G}}_{2n+1}$ 也由生成树连通，于是综上所述，我们对于图 $\mathcal{G}_{2n+1}$ 找到了各边标记不同的生成树。

以上，完成了对于长度可达到 $M_{2n+1} = \frac{(2n+1)!}{2} - 2n + 1$ 的 Horovitz-Etzion 蛇形码的严格证明。

2.5.3 对 Horovitz-Etzion 蛇形码的改进

延续 Horovitz-Etzion 蛇形码的构造思想并加以微调，我们将在接下来给出一个更优的构造，得到 S_7 中码字数目为 $M_7 = 2517$ 的 $\mathcal{K}$-蛇，比 $M_7 = 2515$ 的 Horovitz-Etzion 蛇形码增加了 2 个码字。先预备如下引理。

引理26. 对任意一个置换 $\pi \in S_{2n+1}$，有 $t_{2n-3}^{-1} t_{2n-1} t_{2n-3}^{-1}(\pi) = t_{2n-1}^{-1} t_{2n-3} t_{2n-1}^{-1}(\pi)$.

证明. 设 $\pi = [a_1, a_2, \ldots, a_{2n+1}]$.

$$
\begin{aligned}
& t_{2n-3}^{-1} t_{2n-1} t_{2n-3}^{-1}(\pi) \\
&= t_{2n-3}^{-1} t_{2n-1} [a_2, a_3, \ldots, a_{2n-3}, a_1, a_{2n-2}, a_{2n-1}, a_{2n}, a_{2n+1}] \\
&= t_{2n-3}^{-1} [a_{2n-1}, a_2, a_3, \ldots, a_{2n-3}, a_1, a_{2n-2}, a_{2n}, a_{2n+1}] \\
&= [a_2, a_3, \ldots, a_{2n-3}, a_{2n-1}, a_1, a_{2n-2}, a_{2n}, a_{2n+1}].
\end{aligned}
$$

$$
\begin{aligned}
& t_{2n-1}^{-1} t_{2n-3} t_{2n-1}^{-1}(\pi) \\
&= t_{2n-1}^{-1} t_{2n-3} [a_2, a_3, \ldots, a_{2n-3}, a_{2n-2}, a_{2n-1}, a_1, a_{2n}, a_{2n+1}] \\
&= t_{2n-1}^{-1} [a_{2n-2}, a_2, a_3, \ldots, a_{2n-3}, a_{2n-1}, a_1, a_{2n}, a_{2n+1}] \\
&= [a_2, a_3, \ldots, a_{2n-3}, a_{2n-1}, a_1, a_{2n-2}, a_{2n}, a_{2n+1}].
\end{aligned}
$$

□

预备的步骤正如 Horovitz 与 Etzion 的构造相同。首先将除却 $[2, 1]$ 这个类之外的所有置换分拆得到 12 条锁链，所缺失的置换为 12 个来自类 $[2, 1]$ 中的项链，每个长度为 5.

图 2-6　S_7 中长度为 $M_7 = 2517$ 的 $\mathcal{K}$-蛇

Horovitz 和 Etzion 的做法是将这些项链作为链接介质来对锁链进行融合，这样无论如何操作总会余下一条项链没有使用。换一个思路，如果先将 $[2,1]$ 这个类之中的置换先行排列出一个 $\mathcal{K}$-蛇会怎样？这等价于做一个 S_5 中的 $\mathcal{K}$-蛇，前文图 2-2 中已经描述了 S_5 中长度为 57 的 $\mathcal{K}$-蛇。取一个一一映射 $f:\{1,2,3,4,5\}\to\{3,4,5,6,7\}$，再向尾巴上添加“2”和“1”，则将 S_5 中 $\mathcal{K}$-蛇转化为了 S_7 中由 $[2,1]$ 这个类之中的置换构成的 $\mathcal{K}$-蛇。额外要求映射 f 的选择要保证生成的 $\mathcal{K}$-蛇中皆为偶置换。

下一步是将这 12 条锁链嵌入这个 $\mathcal{K}$-蛇之中。由引理 22 所指出，如果此 $\mathcal{K}$-蛇之中有连续两个置换 $[\alpha,x,2,1]$ 和 $[x,\alpha,2,1]$，$x\in\{6,7\}$，则可以将包含 $[1,\alpha,x,2]$ 和包含 $[2,\alpha,1,x]$的锁链嵌入其中，称之为一个可行的嵌入。如果可以找到 $\mathcal{G}_7$ 的一个匹配，其中每条边对应的都是可行的嵌入，则将如愿得到长为 2517 的 $\mathcal{K}$-蛇。$\mathcal{G}_7$ 中不同的匹配的数目很多，然而每个匹配中的六条边是否都对应于可行的嵌入是需要检查的，这是由于当前构造的 $\mathcal{K}$-蛇中有很多的“推至顶端”操作 t_3 的存在。粗略地说，“推至顶端”操作 t_5 越多，则对应的可行嵌入越多，越有助于我们寻找到合适的匹配。我们可以利用引理 26，即对任意 $\pi\in S_7$ 有 $t_3^{-1}t_5t_3^{-1}(\pi)=t_5^{-1}t_3t_5^{-1}(\pi)$，来对当前构造的 $\mathcal{K}$-蛇做一些“缝补”。缝补的过程

是将从 $t_3(\pi)$ 到 $t_3^{-1}t_5(\pi)$ 这一段剪切下来，将断点两头的 π 与 $t_5(\pi)$ 缝合，再将裁下来的那段嵌入到 $t_5^{-1}t_3(\pi)$ 与 $t_3t_5^{-1}t_3(\pi)$ 之间。上述过程只要当 $t_5^{-1}t_3(\pi)$ 和 $t_3t_5^{-1}t_3(\pi)$ 不在所切下的片段内部的话皆可行。这样的缝补过程为 $\mathcal{K}$-蛇的转换序列之中引入了更多的 t_5，同时也没有改变原先存在的 t_5. 现在可以如图 2-6 所示成对地将 12 条锁链进行嵌入。

我们猜想这样的思路对于所有奇数阶置换群都可成立。它潜在的可行性强烈依赖于 Horovitz 与 Etzion 所构造的 $\mathcal{K}$-蛇的结构。前文已提及， Horovitz 与 Etzion 所构造的 S_{2n-1} 中的 $\mathcal{K}$-蛇的转换序列中只有 t_{2n-1} 与 t_{2n-3}. 从这样一个 $\mathcal{K}$-蛇出发，选取合适的一一映射 $f:\{1,2,\ldots,2n-1\}\to\{3,4,\ldots,2n+1\}$，再向尾巴上添加“2”和“1”，则得到了一个 S_{2n+1} 中的由 $[2,1]$ 这个类之中的置换构成的 $\mathcal{K}$-蛇，转换序列仅包含 t_{2n-1} 和 t_{2n-3}. 与上文类似，我们可以利用引理 26，即对任意 $\pi\in S_{2n+1}$ 有 $t_{2n-3}^{-1}t_{2n-1}t_{2n-3}^{-1}(\pi)=t_{2n-1}^{-1}t_{2n-3}t_{2n-1}^{-1}(\pi)$，来对当前构造的 $\mathcal{K}$-蛇做一些“缝补”。缝补的过程是将从 $t_{2n-3}(\pi)$ 到 $t_{2n-3}^{-1}t_{2n-1}(\pi)$ 这一段剪切下来，将断点两头的 π 与 $t_{2n-1}(\pi)$ 缝合，再将裁下来的那段嵌入到 $t_{2n-1}^{-1}t_{2n-3}(\pi)$ 与 $t_{2n-3}t_{2n-1}^{-1}t_{2n-3}(\pi)$ 之间。上述过程只要当 $t_{2n-1}^{-1}t_{2n-3}(\pi)$ 和 $t_{2n-3}t_{2n-1}^{-1}t_{2n-3}(\pi)$ 不在所切下的片段内部的话皆可行。这样的缝补过程为 $\mathcal{K}$-蛇的转换序列之中引入了更多的 t_{2n-1}，同时也没有改变原先存在的 t_{2n-1}. 经过充分多的调整之后，在相邻的两个置换$[\alpha,x,2,1]$ 和 $[x,\alpha,2,1]$ 之间即可进行某对锁链的嵌入，其中 $x>5$. 由于 $\mathcal{G}_{2n+1}$ 之中有许多匹配且上述调整有很强的机动性，则这些乐观的证据让我们有理由相信，可以找到一个匹配其所有边都对应于可行的置换。然而严格的数学证明有待分析。

综上所述，我们有如下猜想（并对 $2n+1=7$ 给出了证明）

猜想27. *对任意整数 $n\geq 3$，存在 S_{2n+1} 中的 $\mathcal{K}$-蛇，达到长度 $M_{2n+1}=\frac{(2n+1)!}{2}-2n+3$.*

2.6 Kendall's τ-距离下 S_{2n+2} 中的蛇形码

本小节将讨论在 Kendall's τ-距离下偶数阶置换群 S_{2n+2} 中的蛇形码的相关问题。在前文预备工作部分已提及了此问题在偶数阶和奇数阶上的不同之处。如果依然只在奇数位指标上做“推至顶端”操作，则置换的末位不动，那此时 S_{2n+2} 中的蛇形码本质上就是 S_{2n+1} 中的蛇形码，这是平凡的结果，码字数目也不尽人意。若想得到非平凡的 S_{2n+2} 中的蛇形码，就必须打破奇偶置换之间的壁障，即需要某些时候在偶数位指标上做“推至顶端”操作。

我们将基于 S_{2n+1} 中的 Horovitz-Etzion 型的 $\mathcal{K}$-蛇，构造 S_{2n+2} 中的蛇形码。首先再次强调重申一下 Horovitz-Etzion 型的 $\mathcal{K}$-蛇的一个重要性质。

引理28. [73] 对任意整数 $n \geq 2$，S_{2n+1} 中的 *Horovitz-Etzion* 型的 $\mathcal{K}$-蛇达到长度 $M_{2n+1} = \frac{(2n+1)!}{2} - 2n + 1$. 其转换序列中仅包含 t_{2n-1} 与 t_{2n+1}.

对于置换 $\pi \in S_{2n+2}$，记 $\pi_{\downarrow} \in S_{2n+1}$ 为将 π 中的元素“$2n+2$”删除之后所得到的置换。对于置换 $\pi \in S_{2n+1}$，记 $\pi_{\uparrow,i} \in S_{2n+2}$ 为向 π 中把元素“$2n+2$”插入到第 i 个位置上所得到的置换，$1 \leq i \leq 2n+2$.

将任意一条初始的 S_{2n+1} 中的 Horovitz-Etzion 型的 $\mathcal{K}$-蛇记为 $\pi^1, \pi^2, \ldots, \pi^{M_{2n+1}}$. 模糊地讲，我们接下来要构造的 S_{2n+2} 中的蛇是将 Horovitz-Etzion 型的 $\mathcal{K}$-蛇的一系列“复制品”串联起来所得到的。首先描述第一个复制品。

从置换 $\pi^1_{\uparrow,1}$ 出发。接下来的转换序列中每个操作的选取遵循以下两种规则。

• 规则1：只要当元素“$2n+2$”掉到第 $2n-2$ 位时，就立即做一次操作 t_{2n-2}，即把元素“$2n+2$”推到顶端。这种操作下连续的两个置换形如 $\pi_{\uparrow,2n-2}$ 和 $\pi_{\uparrow,1}$，其中 $\pi \in S_{2n+1}$.

• 规则2：否则，参照初始的 S_{2n+1} 中的 Horovitz-Etzion 型的 $\mathcal{K}$-蛇的转换序列。对于元素“$2n+2$”不在第 $2n-2$ 位上的置换 $\pi \in S_{2n+2}$，考虑它对应的置换 $\pi_{\downarrow} \in S_{2n+1}$. $\pi_{\downarrow}$ 在初始的 S_{2n+1} 中的 Horovitz-Etzion 型的 $\mathcal{K}$-蛇中出现，且在其中它的下一个置换是由将某个元素，比如说“x”，推到顶端所得到的。那么在将要构造的蛇中我们也推同样的元素。由于原 $\mathcal{K}$-蛇的转换序列中仅有 t_{2n-1} 和 t_{2n+1}，且现在“$2n+2$”是保持在前 $2n-2$ 个位置上的，所以新的转换序列中对应的操作实为 t_{2n} 和 t_{2n+2}. 另外，元素“$2n+2$”的位置指标也随这样一个操作而加一。于是这种操作下连续的两个置换形如 $\pi^s_{\uparrow,i}$ 和 $\pi^{s+1}_{\uparrow,i+1}$，其中 π^s 和 π^{s+1} 为初始的 S_{2n+1} 中的 Horovitz-Etzion 型的 $\mathcal{K}$-蛇中的两个连续的置换，$1 \leq i \leq 2n-3$.

于是第一个复制品由以下置换构成：

$$\pi^1_{\uparrow,1}, \pi^2_{\uparrow,2}, \pi^3_{\uparrow,3}, \ldots, \pi^{2n-2}_{\uparrow,2n-2}, \pi^{2n-2}_{\uparrow,1}, \pi^{2n-1}_{\uparrow,2}, \ldots, \pi^{M_{2n+1}}_{\uparrow,2n-5}.$$

上述最后一个置换为 $\pi^{M_{2n+1}}_{\uparrow,2n-5}$ 是容易由上述规则的周期性以及 M_{2n+1} 的值所推断得到的，即依据于 $M_{2n+1} \equiv -2 \pmod{2n-3}$. 现在我们继续沿用上述两条规则得到第二个复制品如下：

$$\pi^1_{\uparrow,2n-4}, \pi^2_{\uparrow,2n-3}, \ldots, \pi^{M_{2n+1}}_{\uparrow,2n-7},$$

同样，接下来的复制品依次为：

$$\pi^1_{\uparrow,2n-6}, \pi^2_{\uparrow,2n-5}, \ldots, \pi^{M_{2n+1}}_{\uparrow,2n-9},$$

$$\pi^1_{\uparrow,2n-8}, \pi^2_{\uparrow,2n-7}, \ldots, \pi^{M_{2n+1}}_{\uparrow,2n-11},$$

$$\cdots\cdots\cdots\cdots$$

$$\pi^1_{\uparrow,6}, \pi^2_{\uparrow,7}, \ldots, \pi^{M_{2n+1}}_{\uparrow,3},$$

$$\pi^1_{\uparrow,4}, \pi^2_{\uparrow,5}, \ldots, \pi^{M_{2n+1}}_{\uparrow,2n-2}.$$

此处暂停。到此为止我们已经有了 $n-2$ 段复制品。如果依然按上述规则的话接下来的置换应为 $\pi^{M_{2n+1}}_{\uparrow,1}$，但我们此时改变成下面的思路。现在无视掉第一条规则，而是严格遵循第二条规则来构造最后一段复制品。即，元素“$2n+2$”将不再被推至顶端。接下来的置换为 $\pi^1_{\uparrow,2n-1}$ 和 $\pi^2_{\uparrow,2n}$. 余下的部分为 $\pi^k_{\uparrow,p_k}$，其中 $\{p_k\}_{3\le k\le M_{2n+1}}$ 为单调不减的整数序列，取值于 $2n$ 到 $2n+2$. 因为初始的 $\mathcal{K}$-蛇的转换序列中有许多 t_{2n+1}，则很容易保证了 $p_{M_{2n+1}} = 2n+2$，即此时已经得到了 $\pi^{M_{2n+1}}_{\uparrow,2n+2}$. 最后，比如说在初始的 $\mathcal{K}$-蛇中从 $\pi^{M_{2n+1}}$ 得到 π^1 是通过将元素 x 推至顶端所得到的，那么新的蛇的最后一步也是推这个元素，得到 $\pi^1_{\uparrow,2n+2}$. 循环的构成也将自然成立，因为对最后一个置换 $\pi^1_{\uparrow,2n+2}$ 做 t_{2n+2}，回到了最开始的 $\pi^1_{\uparrow,1}$. 构造完毕。

定理29. *对于 $n\ge 4$，上述构造得到 S_{2n+2} 中的 $\mathcal{K}$-蛇，长度近似达到 $\frac{1}{4}|S_{2n+2}|$.*

证明. 回顾关于 $d_K(\sigma,\pi)$ 的一个表达式[77]：

$$d_K(\sigma,\pi) = |\{(i,j) : \sigma^{-1}(i) < \sigma^{-1}(j) \wedge \pi^{-1}(i) > \pi^{-1}(j)\}|.$$

利用此式对所构造的蛇形码中的置换检验其两两之间的距离。$d_K(\sigma,\pi) \ge d_K(\sigma_\downarrow, \pi_\downarrow)$，则若 $\sigma_\downarrow$ 和 $\pi_\downarrow$ 不同的话，那因为它们出现在原初始的蛇形码中，则易知 $d_K(\sigma_\downarrow,\pi_\downarrow)\ge 2$.

而当 $\sigma_\downarrow$ 与 $\pi_\downarrow$ 相同时，则它们之间的 Kendall's τ-距离恰为“$2n+2$”这个元素的位置指标之差。对于初始的蛇形码中的任意置换 $\pi\in S_{2n+1}$，定义 $I(\pi) = \{1\le i\le 2n+2 : \pi_{\uparrow,i}$ 是所构造的蛇形码中的一个置换$\}$. 我们只需证明 $I(\pi)$ 不包含连续的整数。例如，由构造方式显然有 $I(\pi^1) = \{1,4,6,8,\ldots,2n-4,2n-1,2n+2\}$.

对于除却 π^1 之外的置换 π，最后一个复制品对于 $I(\pi)$ 的贡献仅为一个单独的数字 x，其中 $x\in\{2n,2n+1,2n+2\}$. 其它复制品对于 $I(\pi)$ 的贡献中没有大于 $2n-2$ 的整数。于是可以忽略最后一个复制品的影响，只关注于前面 $n-2$ 个复制品，将这些复制品分别记为 $R_1,\ldots,R_{n-2}$. 对于 $1\le j\le n-3$，可以验证下列事实：

- 若 $\pi_{\uparrow,i}\in R_j$，$4\le i\le 2n-3$，则 $\pi_{\uparrow,i-2}\in R_{j+1}$；
- 若 $\pi_{\uparrow,1}\in R_j$ 且 $\pi_{\uparrow,2n-2}\in R_j$，则 $\pi_{\uparrow,2n-4}\in R_{j+1}$；

• 若 $\pi_{\uparrow,2} \in R_j$，则 $\pi_{\uparrow,2n-3} \in R_{j+1}$；

• 若 $\pi_{\uparrow,3} \in R_j$，则 $\pi_{\uparrow,1} \in R_{j+1}$ 且 $\pi_{\uparrow,2n-2} \in R_{j+1}$，唯一的例外是 $\pi_{\uparrow,3}^{M_{2n+1}} \in R_{n-3}$，但是 $\pi_{\uparrow,1}^{M_{2n+1}} \notin R_{n-2}$).

利用以上事实可检验，对于初始的蛇形码中的任意置换 $\pi \in S_{2n+1}$，$I(\pi)$ 不包含连续的整数。综上所述，所构造的蛇形码中的置换两两的 Kendall's τ-距离至少为 2.

接下来估算一下所构造的 $\mathcal{K}$-蛇的长度。每个复制品长度约为原先整个初始蛇形码的长度，即 M_{2n+1}，则有：

$$M_{2n+2} \approx (n-1)M_{2n+1} \approx \frac{1}{4}|S_{2n+2}|.$$

□

最后我们讨论一下 $n = 1, 2, 3$ 时 S_{2n+2} 中的 $\mathcal{K}$-蛇，这几个情况并不完全符合上述的框架。

对于 $n = 1$，简单的手工操作即可得到最优的 $M_4 = 8$. 示例如下：

$$\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
1 & 4 & 2 & 3 & 4 & 1 & 3 & 2 \\ \hline
2 & 1 & 4 & 2 & 3 & 4 & 1 & 3 \\ \hline
3 & 2 & 1 & 4 & 2 & 3 & 4 & 1 \\ \hline
4 & 3 & 3 & 1 & 1 & 2 & 2 & 4 \\ \hline
\end{array}$$

图 2-7　$M_4 = 8$.

对于 $n = 2$，我们基于上一小节中长度为 57 的 S_5 中的 $\mathcal{K}$-蛇，来构造 S_6 中的 $\mathcal{K}$-蛇。将上述构造中的第一条规则稍微修改，将规则中的“$2n - 2 = 2$”改为“3”。这样即可得到下面所示的长为 $M_6 = 142$ 的 S_6 中的 $\mathcal{K}$-蛇。图示中的 ★ 标记着第二个复制品的起始位置。

对于 $n = 3$，考虑 S_8 中的情形。同上，可以修改第一条规则，将规则中的“$2n - 2 = 4$”改为“5”。则第二个复制品的初始置换为 $\pi_{\uparrow,4}^1$. 为了避免距离上的冲突，要保证所选取的初始的 Horovitz-Etzion 型 $\mathcal{K}$-蛇 $\pi^1, \pi^2, \ldots, \pi^{M_7}$ 有如下性质：其转换序列的第三个操作为 t_7，亦即 $\pi^4 = t_7(\pi^3)$. 通过这种额外的保证，可使得第二个复制品的起始的几个置换形如 $\pi_{\uparrow,4}^1$，$\pi_{\uparrow,5}^2$，$\pi_{\uparrow,6}^3$，$\pi_{\uparrow,7}^4$. 本质目的即是尽快把元素“8”推至下方，以避免同时出现 $\pi_{\uparrow,5}$ 和 $\pi_{\uparrow,6}$ 这一组置换的潜在可能性。如此，我们即得到了 S_8 中的一个 $\mathcal{K}$-蛇，由 S_7 中的 $\mathcal{K}$-蛇的两段复制品所构成。

图 2-8 $M_6 = 142$

2.7 小结

本章的研究主题是置换群上的置换码与蛇形码。对于汉明距离下和 Kendall's τ-距离下的置换码，通过利用图的染色数来分析独立数大小的方法，分别改进了两种码的新的下界。虽然染色方案是明确的，但是寻找码字数目最多的颜色并不直观，似乎仍需对所有置换进行遍历染色之后再进行计数比较。于是从构造意义上讲，这仍是一个指数时间的构造方法，更便利的构造方法有待探索。对于蛇形码的研究，在奇数阶和偶数阶置换群上有明显区别，我们在两个方面都分别给出了一定推进。最近，在文献[72] 中用异于 Horovitz-Etzion 蛇形码的思路，得到了奇数阶上的完美蛇形码，从而在奇数阶上彻底解决了此问题。

3 数字指纹：合谋-安全码及相关哈希函数族

3.1 介绍

在数字产品的版权保护问题中，产品的发布者可以在数字产品中附加一些码字作为数字指纹。这将使得发布者在发现盗版产品时，可以通过调查所嵌入的数字指纹而追查到盗版的源头。然而，多个盗版者可进行协助、合谋攻击，通过对各自数字产品的组合而产出盗版产品，这也同时将各自的数字指纹做了整合，加大了追查盗版源头的难度。为了抵抗这种合谋攻击，近年来设计出很多合谋-安全码，比如防诬陷码、可确定性父元码、追踪码、可分离码等等。分离哈希函数族是一类重要的组合结构，在各种合谋-安全码的研究中有着重要的应用。通常来说，各种合谋-安全码或者是一类特殊参数下的分离哈希函数族，或者可与相关的分离哈希函数族所互相导出。对于合谋-安全码及其相关哈希函数族的研究的主要目标是在给定的参数下构造一个码字数目尽量多的码，或者是直接的清晰构造，或者是用概率方法说明其存在性。本章中，我们将讨论这些码的模型与超图之间的联系，利用超图的独立集的结果对一些组合结构的下界进行改进。特别地，这样的一般方法将分别应用于完美哈希函数族、防诬陷码和可分离码。就我们所知，这种利用超图模型的方法尚属首次。首先介绍其相关定义与背景。

3.1.1 分离哈希函数族

粗略地讲，一个哈希函数族是从定义域 Y 到值域 Q 的一族函数的集合。

定义30. 给定正整数 N，n 和 q，一个 $(N;n,q)$-**哈希函数族**是一个由 N 个函数所构成的集合 $\mathcal{F}$，函数的定义域 Y 的大小为 n，值域 Q 的大小为 q.

为叙述简便，一般记定义域 Y 为 $\{1,2,\ldots,n\}$，值域 Q 为 $\{1,2,\ldots,q\}$. 自然地，一个 $(N;n,q)$-哈希函数族可以用一个 $N\times n$ 阵列 $\mathcal{A}$ 来描述，其中列标对应于定义域 Y，行标对应于各个函数 $f\in\mathcal{F}$. 在对应于函数 f 这一行和对应于 $y\in Y$ 的这一列上，阵列中的元素

型	名称	参考文献
$w_i = 1$，任意 i	完美哈希函数族	[6,11,17,20,50] [96,114,121,127]
$\{1, w\}$	防诬陷码	[18,25,35,40,57] [58,88,102,104,110,112,130]
$\{w, w\}$	安全防诬陷码	[39,40,112]
$\{1,1,1\}$ 且 $\{2,2\}$	可确定性父元码	[4,9,71,110,122]
$\{1,\ldots,1,w\}$	强可分离哈希函数族	[102]

表 3-1　分离哈希函数族的特殊情形

为 $f(y) \in Q$. 我们称 $\mathcal{A}$ 为此哈希函数族的**矩阵表示**，将矩阵表示中的每列称为一个码字。

定义31. 一个**分离哈希函数族** *SHF*$(N; n, q, \{w_1, w_2, \ldots, w_t\})$ 是满足下列条件的一个 $(N; n, q)$-哈希函数族 $\mathcal{F}$：对于任意不交的集合 $C_1, C_2, \ldots, C_t \subset \{1, 2, \ldots, n\}$，$|C_1| = w_1, |C_2| = w_2, \ldots, |C_t| = w_t$，存在至少一个函数 $f \in \mathcal{F}$ 使得对任意 $i \neq j$ 有

$$\{f(y) : y \in C_i\} \cap \{f(y) : y \in C_j\} = \emptyset.$$

称此分离哈希函数族的**型**为 $\{w_1, w_2, \ldots, w_t\}$，型的大小为 $w = \sum_{i=1}^{t} w_i$.

对应地，一个分离哈希函数族 SHF$(N; n, q, \{w_1, w_2, \ldots, w_t\})$ 的矩阵表示 $\mathcal{A}$ 将满足下述性质：对任意不相交的列的集合 $C_1, C_2, \ldots, C_t$，$|C_1| = w_1, |C_2| = w_2, \ldots, |C_t| = w_t$，存在 $\mathcal{A}$ 中某个行 r 使得对任意 $i \neq j$ 有

$$\{\mathcal{A}(r, y) : y \in C_i\} \cap \{\mathcal{A}(r, y) : y \in C_j\} = \emptyset.$$

分离哈希函数族已被广泛研究，尤其是值域为二元的情形下。上述的正式的定义最早由 Stinson 等人所提出[112]。许多参数下的分离哈希函数族被应用于密码学上的分析，尤其是对于合谋-安全码。事实上，许多广泛研究的组合结构是特定参数下的某种分离哈希函数族。我们将这些组合结构及其相关的参考文献列于表 3-1.

对于给定的值域大小 q 和特定的型 $\{w_1, \ldots, w_t\}$，我们感兴趣于 n 和 N 的数量关系。即，对于给定的 N，我们想得到最大的 n. 对于绝大多数的型，很难精确刻画 n 的最大值，而研究其上下界是相对更现实的一个研究路线[19,88,110,113,115]. 最近，Bazrafshan 和 Trung[12,13] 对多数先前已知的上界做出改进，甚至通过确定性的构造证明了当 N 接近型

的大小时，有些结果是紧的。利用概率方法中的一个基本技巧“删除方法”，Stinson 等人[113] 给出了一个存在性的证明，得到了任意型的分离哈希函数族在其它参数给定时的 n 的最大值的下界。

3.1.2 可分离码

可分离码是一种特殊的合谋-安全码，由 Cheng 和 Miao[37] 所定义，用来抵抗合谋者的平均攻击策略。

定义32. 对于整数 N，n，q，令 Q 为字母表 $\{1,2,\ldots,q\}$. 称 $\mathcal{C}=\{c_1,c_2,\ldots,c_n\}\subset Q^N$ 为一个 (N,n,q)-码，如果每个 c_i 为一个长为 N 的码字。

令 $c(i)$ 代表向量 $c\in Q^N$ 的第 i 位，$1\le i\le N$. 对于任意码 $\mathcal{C}\subset Q^N$，定义 $\mathcal{C}(i)=\{c(i)\in Q|c\in\mathcal{C}\},1\le i\le n$. 对于任意码的一个子集 $\mathcal{C}_0\subset\mathcal{C}$，定义其**后代码**为 $\mathrm{desc}(\mathcal{C}_0)=\{x\in Q^n|x(i)\in\mathcal{C}_0(i),1\le i\le n\}$. 亦即，码字集合 $\mathrm{desc}(\mathcal{C}_0)$ 包含了可以由拥有 $\mathcal{C}_0$ 中码字的一组合谋用户所生成的 n 元组，$\mathrm{desc}(\mathcal{C}_0)=\mathcal{C}_0(1)\times\cdots\times\mathcal{C}_0(n)$.

定义33. 假设 $\mathcal{C}$ 为一个 (N,n,q)-码，整数 $t\ge 2$. 若对于任意的 $\mathcal{C}_1$，$\mathcal{C}_2\subset\mathcal{C}$，$|\mathcal{C}_1|\le t$，$|\mathcal{C}_2|\le t$ 且 $\mathcal{C}_1\ne\mathcal{C}_2$，有 $\mathrm{desc}(\mathcal{C}_1)\ne\mathrm{desc}(\mathcal{C}_2)$，则称 $\mathcal{C}$ 为一个 $\bar{t}$-**可分离码**。亦即，存在至少一个指标 i，$1\le i\le N$，使得 $\mathcal{C}_1(i)\ne\mathcal{C}_2(i)$.

给定 N，q，t，我们感兴趣于研究可分离码的最大码字数目 n. 不幸的是，可分离码的构造非常困难，目前仅有关于码长为 2 和 3 时的最优 $\bar{2}$-可分离码的构造。对于其它参数，可分离码码字数目的上下界之间有很大的鸿沟。最近，Gao 和 Ge[65] 分别通过概率方法和组合技巧改进了 $\bar{2}$-可分离码的上下界，甚至证明在 N 取定，q 比较大时，他们的下界是渐进最优的。

本章的结构如下。在第 3.2 小节中，我们建立码的问题与超图独立集问题的相关关联，介绍后文中将要涉及的关于超图独立集的一些结果。在第 3.3、3.4、3.5 小节，将应用这套方法分别改进某些参数下完全哈希函数族、防诬陷码、可分离码的下界。第 3.6 小节对本章进行总结。

3.2 码字数目问题与（超）图的独立集的联系

在本节中，我们介绍码字数目问题与（超）图的独立集之间的联系。

一个超图由点集与边集组成，记 $\mathcal{V}$ 为一个有限的顶点集，$\mathcal{E}$ 为边集，每条边是 $\mathcal{V}$ 的一个子集。一般的图即是每条边数目均为 2 的超图。超图的一个独立集是点集的一个子集，不包含超图中的任何一条边。超图的独立数即为最大的独立集的大小。

所谓码，可以看作其元素所在的基础集合（比如常见的，所有 n 长 q 元向量）中的满足限定条件一个子集。限定条件可能是针对一个码字的，比如极小汉明重量，或者是针对多个码字之间的，比如两个码字之间的距离。编码理论的本质问题就是研究满足给定的限定条件的最大子集的大小。现在我们将码字数目问题转化到超图的语言上来描述。令基础集合中的每个元素为超图中的一个点，点集的任意子集构成一条边当且仅当对应的码字的同时出现会违背至少一条限定条件。这里边的选取是在“极小”意义下的，亦即一条边中任意删除一点之后，余下的点对应的码字的同时出现不会违背限定条件。此超图的一个独立集所对应的码字则可构成符合要求的码，于是码字数目问题转化成为了寻找此对应超图中的独立集的问题。例如，如果唯一的限定条件是任意两个码字之间的极小距离大于等于 d，则对应的图中两点之间有边当且仅当它们的距离小于 d. 这样的方法已经有多次使用，比如 Jiang 和 Vardy[78] 以及之后 Vu 和 Wu[126] 用 Bollobás 的针对局部稀疏图的独立数的一个结论，分别改进了非线性二元码和 q 元码的 Gilbert-Varshamov 型下界。Gao 等人[66] 利用 Li 和 Rousseau[89] 的一个独立数的结果改进了汉明距离下置换码的 Gilbert-Varshamov 型下界。另外的例子即是上一章中我们对于两种距离下的置换码下界的改进。上述的所有例子都是只有码字之间两两的距离这一限制，所以都是在普通图的模型上操作的。本章中我们考虑的问题中，码的限定要求都将涉及多于两个码字，则我们需要在超图模型下考虑问题。

关于超图的独立数也有很多研究结果[1,2,53,85,98]. 我们将利用的是 Duke 等人[53] 所提出的下界。在叙述他们的定理之前，我们先给出超图上的一些概念与符号。令超图 $\mathcal{H}(\mathcal{V},\mathcal{E})$ 的点集为 $\mathcal{V}$，边集为 $\mathcal{E}$. 若所有边的大小均为 k，则称 $\mathcal{H}$ 为 k-超图。对于任意点 v，定义 v 的度数为包含点 v 的边的数目，表示为 $d(v)$. 遍历所有点的最大的 $d(v)$ 的值称为 $\mathcal{H}$ 的最大度，记为 $\Delta(\mathcal{H})$. 对于点集的一个 w 元子集 $\mathcal{W}$，定义 $\mathcal{W}$ 的 w- 度为包含 $\mathcal{W}$ 的边的数目。在一个 k-超图 $\mathcal{H}$ 中，对任意整数 j，$2 \le j \le k-1$，交集大小为 j 的一对无序的边 $\{e,e'\}$ 称为一个 $(2,j)$-圈。$\mathcal{H}$ 中的 $(2,j)$-圈的数目记为 $s_j(\mathcal{H})$.

定理34. [53] *令 $\mathcal{H}=(\mathcal{V},\mathcal{E})$ 为 n 个点上的 k-超图，满足 $\Delta(\mathcal{H}) \le t^{k-1}$，其中 $t \gg k$. 若对于*

$j = 2, 3, \ldots, k-1$ 存在 $\gamma > 0$ 满足

$$s_j(\mathcal{H}) \leq n \cdot t^{2k-j-1-\gamma} \tag{3-1}$$

则有

$$\alpha(\mathcal{H}) \geq c(k,\gamma) \cdot \frac{n}{t} \cdot (\ln t)^{\frac{1}{k-1}}$$

其中 $c(k,\gamma)$ 为一个依赖于 k 和 γ 的常数。

特别地，我们取 $t = \Delta^{1/(k-1)}$，对上述定理中的整数部分做重新整合（这里 k 也是一个给定的常数），则可得到

$$\alpha(\mathcal{H}) \geq c(k,\gamma) \cdot \frac{n}{\Delta^{\frac{1}{k-1}}} \cdot (\ln \Delta)^{\frac{1}{k-1}}. \tag{3-2}$$

接下来，我们将利用上述定理分析完美哈希函数族、防诬陷码和可分离码的下界。

3.3　完美哈希函数族

一个分离哈希函数族 SHF$(N; n, q, \{w_1, w_2, \ldots, w_t\})$，若其型为对于任意 i 有 $w_i = 1$，则称为一个完美哈希函数族，记为 PHF$(N; n, q, t)$. 回忆对于哈希函数族的矩阵表示，我们称矩阵的每一个列为一个码字。对于给定的 N，q 和 t，我们想要得到最大的码字数目 n. 注意到由可分离的要求，没有两个码字是完全相同的。

构造对应的超图模型 $\mathcal{H}(\mathcal{V}, \mathcal{E})$ 如下。令点集 $\mathcal{V}$ 为基础集合 Q^N，任意 t 个点构成一条边当且仅当它们不可分离，亦即对于任意的指标 $i \in [N]$，这 t 个点中的至少两个点 x 和 y 对应的分量为 $x_i = y_i$. 则此超图中的一个大小为 n 的独立集即对应于一个完美哈希函数族 PHF$(N; n, q, t)$.

为利用定理 34，我们需要计算下面两个数值。对 Q^N 中的任意 t 个向量，如果它们在第 i 位上的分量两两皆不相同，则我们称它们**在第 i 指标上相异**。对于 $1 \leq j \leq t-1$，$0 \leq m \leq N$，对于某 j 个点组成的集合，如果这 j 个点恰好在 m 个指标上相异，则称之为一个 (j,m)-组。记 $C_t(j,m)$ 为 (j,m)-组的数目，记 $D_t(j,m)$ 为所有 (j,m)-组的最大 j-度。我们现在计算这两个数量，利用归纳和算两次的方法。

引理35. 对于 $2 \leq j \leq t-1$，$0 \leq m \leq N$，有

$$C_t(j,m) = \frac{1}{j!} q^N \binom{N}{m} \varphi_j^m (q^{j-1} - \varphi_j)^{N-m},$$

其中 $\varphi_j = \prod_{i=1}^{j-1}(q-i)$.

证明. 利用归纳法证明。为计算 $C_t(2,m)$，只需计数恰好在 m 个指标上相异的无序点对的数目。首先任意取定第一个点，这有 q^N 种选择。对第二个点的选择分几步，首先选定 m 个指标，这有 $\binom{N}{m}$ 种选择方式；在这些位置上，第二个点应取 Q 中与第一个点不相同的元素，而在其它 $N-m$ 个位置上应取与第一个点相同的元素。注意到点对的无序性，每个序对实际上如此计算了两次。综上有 $C_t(2,m)=\frac{1}{2}q^N\binom{N}{m}(q-1)^m$.

对于一个给定的 (j,m)-组，记作 A，通过删除这 j 个点中的任何一个，都可以得到一个 $(j-1,l)$-组，记为 B，其中 $l\geq m$. 称 B 为 A 的一个**子组**。我们对这样的序对 (A,B) 的数目进行两次不同的计数。显然，每个 (j,m)-组 A 有 j 个子组，则序对数目为 $jC_t(j,m)$. 换一种计算方式如下。首先选取一个 $(j-1,l)$-组 B，其中 $l\geq m$，再计算使得 $A=\{v\}\bigcup B$ 为 (j,m)-组的点 v 的数目。对于给定的 $(j-1,l)$-组 B，从这 $j-1$ 个点本身相异的 l 个指标中选取出 m 个，然后如下选择 v 点。在 B 中的 $j-1$ 个点已经有所重复的那 $N-l$ 个指标上，对应的 v 的分量可以是任取的；在所选出的 m 个指标上，要保持 A 在这些指标上相异，则对应的 v 的分量各自有 $q-j+1$ 种选择方式；在余下的 $l-m$ 个指标上，本身 B 中的 $j-1$ 个点在此相异，要使得 A 在这些指标上不再相异，则对应的 v 的分量各自有 $j-1$ 种选择方式。总计的 v 的数目为 $\binom{l}{m}q^{N-l}(q-j+1)^m(j-1)^{l-m}$. 则我们有等式

$$jC_t(j,m)=\sum_{l=m}^{N}C_t(j-1,l)\binom{l}{m}q^{N-l}(q-j+1)^m(j-1)^{l-m}.$$

于是归纳的过程如下：

$$\begin{aligned}
&C_t(j,m)\\
&=\frac{1}{j}\sum_{l=m}^{N}C_t(j-1,l)\binom{l}{m}q^{N-l}(q-j+1)^m(j-1)^{l-m}\\
&=\frac{1}{j!}q^{2N}(q-j+1)^m\sum_{l=m}^{N}\binom{N}{l}\binom{l}{m}q^{-l}(j-1)^{l-m}\varphi_{j-1}^l(q^{j-2}-\varphi_{j-1})^{N-l}\\
&=\frac{1}{j!}q^{2N}(q-j+1)^m\sum_{l=m}^{N}\binom{N}{m}\binom{N-m}{l-m}q^{-l}(j-1)^{l-m}\varphi_{j-1}^l(q^{j-2}-\varphi_{j-1})^{N-l}\\
&=\frac{1}{j!}q^{2N-m}(q-j+1)^m\binom{N}{m}\varphi_{j-1}^m\sum_{l=0}^{N-m}\binom{N-m}{l}q^{-l}(j-1)^{l}\varphi_{j-1}^l(q^{j-2}-\varphi_{j-1})^{N-m-l}\\
&=\frac{1}{j!}q^{2N-m}(q-j+1)^m\binom{N}{m}\varphi_{j-1}^m(q^{j-2}-\varphi_{j-1}+\frac{(j-1)\varphi_{j-1}}{q})^{N-m}\\
&=\frac{1}{j!}q^{N}\binom{N}{m}\varphi_{j}^m(q^{j-1}-\varphi_{j})^{N-m}.
\end{aligned}$$

□

引理36. 对于 $2 \le j \le t-1$，$0 \le m \le N$，有

$$D_t(j,m) \le \frac{1}{(t-j)!} q^{(t-j)(N-m)} (q^{t-j} - \phi_j)^m,$$

其中 $\phi_j = \prod_{i=j}^{t-1}(q-i)$. 特别地，$D_t(1,N) < \frac{1}{(t-1)!}(q^{t-1} - \phi_1)^N$.

证明. 对 $t-j$ 做归纳。对于给定的一个 (j,m)-组 A，其 j-度为可使得 $A \bigcap B = \emptyset$ 且 $A \bigcup B$ 构成超图中的一条边的 $(t-j)$ 元集合 B 的数目。归纳的起始为 $D_t(t-1,m) \le q^{N-m}(t-1)^m$，这是由于当 $j = t-1$ 时，B 即一个单独的点 v 满足：在所给定的 $t-1$ 个点相异的那 m 个指标上，对应的 v 的分量即取作与这 $t-1$ 个点中的某个相同；在其它的 $N-m$ 个指标上，原 $t-1$ 个点的分量已有若干重复，此时对应的 v 的分量可任取。

给定一个 (j,m)-组 A，我们对序对 (B,v) 进行计数，其中 B 是一个 $(t-j)$ 个点组成的集合，$A \bigcup B$ 构成超图中的一条边，且 v 为 B 中的一个点。令 $D_t(A)$ 表示 A 的 j- 度。显然，由定义知此数值等于 $(t-j)D_t(A)$. 计数的另一方式是先数 v，注意到 v 会出现于上述序对之中当且仅当下述两个条件成立。

1) 在 A 中的 j 个点所相异的 m 个指标其中的 k 个上，对应的 v 的分量取异于 j 个点的值，而在另外 $m-k$ 个指标上，对应的 v 的分量取作与原 j 个点中的某个相同。

2) 在其它的 $N-m$ 个指标上，原 j 个点的分量已有若干重复，此时对应的 v 的分量可任取。

于是总共有 $q^{N-m}\binom{m}{k}(q-j)^k j^{m-k}$ 个合适的 v. 进而 $A \bigcup \{v\}$ 是一个 $(j+1,k)$-组，其 $(j+1)$-度即等于要计数的 (B,v) 的数目。注意当 $k=0$ 时，上述过程可能会取到 A 自身的一个点作为 v，这是要排除的情形，因此我们有下面的不等式，而非等式：

$$(t-j)D_t(j,m) < \sum_{k=0}^{m} D_t(j+1,k) \binom{m}{k} q^{N-m}(q-j)^k j^{m-k}.$$

归纳的过程如下：

$$
\begin{aligned}
&D_t(j,m)\\
&< \frac{1}{t-j}\sum_{k=0}^{m} D_t(j+1,k)\binom{m}{k}q^{N-m}(q-j)^k(j)^{m-k}\\
&< \frac{1}{(t-j)!}q^{N-m}j^m\sum_{k=0}^{m}\binom{m}{k}q^{(t-j-1)(N-k)}(q-j)^k j^{-k}(q^{t-j-1}-\phi_{j+1})^k\\
&= \frac{1}{(t-j)!}q^{(t-j)N-m}j^m\sum_{k=0}^{m}\binom{m}{k}q^{(t-j-1)(-k)}(q-j)^k j^{-k}(q^{t-j-1}-\phi_{j+1})^k\\
&= \frac{1}{(t-j)!}q^{(t-j)N-m}j^m(\frac{(q-j)(q^{t-j-1}-\phi_{j+1})}{jq^{t-j-1}}+1)^m\\
&= \frac{1}{(t-j)!}q^{(t-j)(N-m)}(q^{t-j}-\phi_j)^m.
\end{aligned}
$$

□

现在可以进行 Δ 和 $s_j(\mathcal{H})$ 的计算，$j=2,3,\ldots,t-1$.

$$\Delta = D_t(1,N) < \frac{1}{(t-1)!}(q^{t-1}-\phi_1)^N.$$

$$
\begin{aligned}
&s_j(\mathcal{H}) < \sum_{m=0}^{N} C_t(j,m)\binom{D_t(j,m)}{2}\\
&< \frac{1}{j!}\frac{1}{(t-j)!^2}q^N q^{2(t-j)N}\sum_{m=0}^{N}\binom{N}{m}(q^{2(t-j)})^{-m}\varphi_j^m(q^{j-1}-\varphi_j)^{N-m}(q^{t-j}-\phi_j)^{2m}\\
&= \frac{1}{j!}\frac{1}{(t-j)!^2}q^N q^{2(t-j)N}(\varphi_j(1-\frac{\phi_j}{q^{t-j}})^2+q^{j-1}-\varphi_j)^N\\
&= \frac{1}{j!}\frac{1}{(t-j)!^2}q^N(q^{2t-j-1}-2q^{t-j}\varphi_j\phi_j+\varphi_j\phi_j^2)^N.
\end{aligned}
$$

由式子 (3-2)，对于 q 的限制为：存在$\gamma>0$，对于任意 $j=2,3,\ldots,t-1$ 有 $s_j(\mathcal{H}) \le q^N\Delta^{\frac{2t-j-1-\gamma}{t-1}}$.

例如，当 $t=3$ 时，我们有 $\Delta < \frac{1}{2}(q^2-(q-1)(q-2))^N \sim (3q-2)^N$，$s_2(\mathcal{H}) < \frac{1}{2}q^N(q^2+4q-4)^N$，限制条件转化为

$$(q^2+4q-4)^N < (3q-2)^{3N/2}.$$

这在 $q=3,4,\ldots,15$ 时成立，则这种情况下可以导出

$$\alpha(\mathcal{H}) \ge c\frac{q^N}{(3q-2)^{N/2}}N^{\frac{1}{2}}.$$

于是我们有下述定理，将 Stinson 等人[113] 的结果提高了 $N^{\frac{1}{2}}$ 倍。

定理37. *对于充分大的 N 和 $q=3,4,\ldots,15$，只要*

$$n \le c\left(\frac{q^2}{3q-2}\right)^{\frac{N}{2}} N^{\frac{1}{2}},$$

其中 c 为一个常数，则存在完美哈希函数族 $PHF(N;n,q,3)$.

当 $t=4$ 时，我们有

$$\begin{aligned}\Delta &< \frac{1}{6}(q^3-(q-1)(q-2)(q-3))^N \sim (6q^2-11q+6)^N,\\ s_3(\mathcal{H}) &< \frac{1}{6}q^N(3q^3+7q^2-27q+18)^N,\\ s_2(\mathcal{H}) &< \frac{1}{2}q^N(q^4+25q^3-85q^2+96q-36)^N.\end{aligned}$$

限制条件为

$$\begin{aligned}(3q^3+7q^2-27q+18)^N &< (6q^2-11q+6)^{\frac{4N}{3}},\\ (q^4+25q^3-85q^2+96q-35)^N &< (6q^2-11q+6)^{\frac{5N}{3}}.\end{aligned}$$

这在 $q=4,5,\ldots,31$ 时成立，则这种情况下可以导出

$$\alpha(\mathcal{H}) \ge c\frac{q^N}{(6q^2-11q+6)^{N/3}}N^{\frac{1}{3}}.$$

于是我们有下述定理，将 Stinson 等人[113] 的结果提高了 $N^{\frac{1}{3}}$ 倍。

定理38. *对于充分大的 N 和 $q=4,5,\ldots,31$，只要*

$$n \le c\left(\frac{q^3}{6q^2-11q+6}\right)^{\frac{N}{3}} N^{\frac{1}{3}},$$

其中 c 为一个常数，则存在完美哈希函数族 $PHF(N;n,q,4)$.

对于一般的 t 可类似进行这样的过程。

3.4　2-防诬陷码

一个 2-防诬陷码是型为 $\{1,2\}$ 的分离哈希函数族。与上一小节类似，我们构造的超图以 Q^N 为点集。超图中的边相对前一个例子来说稍微复杂一些。这是由于，在之前完美哈

希函数族的问题上，超图中的边的每个顶点的地位是相同的，而在 2-防诬陷码的情形下，由于型中有“1”和“2”之分，则每条边中的点有不同的意义。特别地，三个点 (a,b,c) 构成一条边当且仅当下述条件至少一个成立。

- $\forall i \in [N]$，$a_i = b_i$ 或 $a_i = c_i$;
- $\forall i \in [N]$，$b_i = a_i$ 或 $b_i = c_i$;
- $\forall i \in [N]$，$c_i = a_i$ 或 $c_i = b_i$.

为突出强调每个点的角色，将上述三种边分别记为 $((b,c),a)$，$((a,c),b)$ 和 $((a,b),c)$. 注意到这三种情况实际上是不交的。这是由于，一条 $((a,b),c)$ 型的边蕴含了存在 i 使得 $a_i = c_i \neq b_i$ 这个事实，于是它不会同时是一条 $((a,c),b)$ 型的边。

对任何顶点 a，首先选取顶点 b，与 a 恰好在 $N-i$ 个指标上相同，$i = 1,2,\ldots,N$. 则对于每个 i 共 $\binom{N}{i}(q-1)^i$ 种对于 b 的选取方式。在选定一个序对 (a,b) 后，计算可使得 (a,b,c) 组成边的点 c 的数目。亦即，(a,b) 的 2-度。

情形1：$((a,b),c)$ 型的边。

在这种情形下，对于取 $a_i = b_i$ 的 $N-i$ 个指标，c_i 也取同样的值。对于其它的指标 j，c_j 可以取作 a_j 或 b_j. 注意到我们要求 $c \neq a$，$c \neq b$，则共有 $2^i - 2$ 种对 c 的选取。

情形2：$((b,c),a)$ 型的边。

在这种情形下，对于取 $a_i = b_i$ 的 $N-i$ 个指标，c_i 的取值任意。对于其它的指标 j，$a_j \neq b_j$，c_j 要等同于 a_j. 注意到我们要求 $c \neq a$，则共有 $q^{N-i} - 1$ 种对 c 的选取。

情形3：$((a,c),b)$ 型的边。

与情形 2 是一样的。

综上，给定的一个恰好在 $N-i$ 个指标上相同序对 (a,b) 的 2-度为 $2^i + 2q^{N-i} - 4$.

在取定 a 后，上述的计数过程中对于每条边 (a,b,c) 计数了两次。则有，

$$\Delta = \frac{1}{2}\sum_{i=1}^{N}\binom{N}{i}(q-1)^i(2^i + 2q^{N-i} - 4) \sim (2q-1)^N$$

且

$$\begin{aligned} s_2(\mathcal{H}) &= \frac{1}{2}q^N\sum_{i=1}^{N}\binom{N}{i}(q-1)^i\binom{2^i + 2q^{N-i} - 4}{2} \\ &\sim q^N(q^2+q-1)^N. \end{aligned}$$

为运用定理 34，需要满足，存在 $\gamma > 0$ 使得，

$$s_2(\mathcal{H}) \leq q^N \Delta^{3/2-\gamma},$$

即

$$(q^2+q-1)^N < (2q-1)^{\frac{3N}{2}}.$$

当 $q = 3$ 时限制条件成立，此时可导出

$$\alpha(\mathcal{H}) \geq c\frac{q^N}{(2q-1)^{N/2}} N^{\frac{1}{2}}.$$

于是我们有下述定理，将 Stinson 等人[113] 的结果提高了 $\sqrt{N}$ 倍。

定理39. *对于充分大的 N，只要*

$$n \leq c\sqrt{N}\left(\frac{9}{5}\right)^{\frac{N}{2}},$$

其中 c 为一个常数，则存在码长为 N 的三元 2-防诬陷码，码字数目为 n.

3.5　可分离码

在本小节中我们分析 $\overline{2}$-可分离码的下界。虽然按照定义，$\overline{t}$-可分离码的限制是针对于任意的 $\mathcal{C}_1, \mathcal{C}_2 \subset \mathcal{C}$，$|\mathcal{C}_1| \leq t$，$|\mathcal{C}_2| \leq t$，$\mathcal{C}_1 \neq \mathcal{C}_2$. 但在 $t = 2$ 这一情形下，容易分析得出[37] 只需要限制于不交的 $\mathcal{C}_1, \mathcal{C}_2 \subset \mathcal{C}$，$|\mathcal{C}_1| = 2$，$|\mathcal{C}_2| = 2$ 即可。

构造一个 4-超图 $\mathcal{H}(\mathcal{V}, \mathcal{E})$，其中 $\mathcal{V}$ 仍然是 Q^N. 对于四个点 (a, b, c, d)，如果对于 $\forall j = 1, 2, \ldots, n$ 有 $\{a_j, b_j\} = \{c_j, d_j\}$，则它们组成一条边。注意到这个定义中的 4 个点也是分为两组的，表示为 $((a, b), (c, d))$ 型的边。

对任意点 a，首先寻找与它同组的同伴 b，恰与 a 在 $N - i$ 个指标上相同，$i = 1, 2, \ldots, N$. 对于每个 i 总计有 $\binom{N}{i}(q-1)^i$ 种对于 b 的选取。对于取定的序对 (a, b)，计算可使得 $((a, b), (c, d))$ 构成一条边的序对 (c, d) 的数目。对于取 $a_i = b_i$ 的 $N - i$ 个指标，c_i 和 d_i 也要是同样的相同的取值。对于其它指标，$a_k \neq b_k$，则 c_k 在 a_k 和 b_k 两者之间取一。一旦 c_k 取定为其中之一，则 d_k 需为另外一个值。再考虑到对称性以及 $c \neq a, b$ 的要求，有

$$\Delta = \sum_{i=1}^{N} \binom{N}{i} (q-1)^i (2^{i-1} - 1) \sim (2q-1)^N.$$

接下来，可以观察到 $s_3(\mathcal{H}) = 0$. 这是因为如果有两条边 (a, b, c, d) 和 (a, b, c, e) 的话，考虑边内部基于不同分组的下面两种情形：

情形1：$((a,b),(c,d))$ 和 $((a,b),(c,e))$，这显然可推出 $d=e$.

情形2：$((a,b),(c,d))$ 和 $((a,c),(b,e))$，从第一条边的分组可知在某些指标上 a 和 c 的分量相同，而 b 对应的分量异于它们，这说明第二条边那种形式是不可能存在的。

上述 $s_3(\mathcal{H})=0$ 这一事实也同时简化了计算 $s_2(\mathcal{H})$ 这一任务，因为我们可以只基于一个给定的序对 (a,b)，来计算交于这两点的边的数目，然后进行加和，而不用担心重复计算。对于给定的恰好在 $N-i$ 个指标上相同的点对 (a,b)，分别计数下面两类边。

情形1：$((a,b),(c,d))$，由上文的分析可得此类型的边的数目为 $2^{i-1}-1$.

情形2：$((a,c),(b,d))$，在 $a_k\neq b_k$ 的 i 个指标上，需要有 $c_k=b_k$ 和 $d_k=a_k$. 对于其它的 $N-i$ 个指标上，对应的 c 和 d 的分量取作相同的任意元素即可。再稍注意保证 $c\neq b$，则共有 $q^{N-i}-1$ 种选择。

$$\begin{aligned} s_2(\mathcal{H}) &= \sum_{i=1}^{N} q^N \binom{N}{i} (q-1)^i \binom{2^{i-1}+q^{N-i}-2}{2} /2 \\ &\sim q^N (q^2+q-1)^N. \end{aligned}$$

为运用定理 34，需要满足，存在$\gamma>0$ 使得，

$$s_2(\mathcal{H}) \leq q^N \Delta^{5/3-\gamma}$$

即

$$(q^2+q-1)^N < (2q-1)^{5N/3}.$$

在 $q=2,3,\ldots,26$ 时限制条件成立，可推导出

$$\alpha(\mathcal{H}) \geq c\frac{q^N}{(2q-1)^{N/3}} N^{\frac{1}{3}}.$$

于是我们有下述定理，将 Gao 等人[65] 的结果提高了 $N^{\frac{1}{3}}$ 倍。

定理40. *对于充分大的 N，$q=2,3,\ldots,26$，只要*

$$n \leq c\frac{q^N}{(2q-1)^{N/3}} N^{\frac{1}{3}},$$

其中 c 为一个常数，则存在 $(N,n,q)-\overline{2}$-可分离码。

3.6　总结

本章中我们介绍了利用超图的独立数来考虑组合结构的下界这一方法，并将其用在了对完美哈希函数族、防诬陷码和可分离码的下界改进上。我们相信此方法有更多的用武之地，只要所研究的组合结构对应的超图的边集大小一致。难点在于，所采取的图论工具中某些参数计算稍显困难。对超图的独立数的研究本身是非常有价值的问题，如何将这方面的其它研究结果（如文献[85]）灵活运用也是值得探讨的课题。

4 源于密码学背景的可逆矩阵问题

4.1 介绍

本章考虑的问题，简而言之是一个纯粹的组合问题。考虑在一个二元的可逆矩阵之中，最多有多大比例的 2×2 可逆子矩阵。

这个问题最本原的动机要追溯到图灵奖得主 Ron Rivest 在[101] 中所提出的 AONT 变换（All-or-nothing transforms），用来作为使用分组密码之前的一个预处理过程。Stinson[111] 将原先 Rivest 最初的计算安全性背景改变为无条件安全性背景，之后 Stinson 等人又在[43] 中进一步提出了广义的 AONT 的概念，定义如下：

定义41. 令 X 为一个有限的字母集。令 s 为一个正整数，考虑映射 $\phi : X^s \to X^s$. 对于此映射的任意一个 s 元组的输入，比如说 $x = (x_1, \ldots, x_s)$，ϕ 将其映射成为一个 s 元组的输出，比如说 $y = (y_1, \ldots, y_s)$，其中 $x_i, y_i \in X$，$1 \le i \le s$. 如果下述性质成立，则称映射 ϕ 为一个无条件安全的 ***AONT* 变换**：

- ϕ 是双射。
- 如果输出的 $y_1, \ldots, y_s$ 中任何 $s - t$ 个值被固定下来，则输入的 $x_i\ (1 \le i \le s)$ 中的任何 t 位的信息 $x_i\ (1 \le i \le s)$ 在信息理论的意义下的是完全无法决定的。

我们将这样的映射 ϕ 记为 (t, s, v)-AONT，其中 $v = |X|$. 且当 s 和 v 可从上下文明显推定时，符号中将其省略，简记为 t-AONT.

Rivest 在[101] 中所提出的，即对应于上述定义在 $t = 1$ 时的特殊情形。1-AONT 可以在分组密码的使用之前提供一个被称为“包变换（package transform）”的预处理过程。假设我们想要加密的明文是 $(x_1, \ldots, x_s)$. 首先借由一个 1-AONT，将其转化为 $(y_1, \ldots, y_s) = \phi(x_1, \ldots, x_s)$. 要注明的是 ϕ 这个变换本身并不需要是秘密的。接下来用一个分组密码对 $(y_1, \ldots, y_s)$ 进行加密，将其转化成密文 $z_i = e_K(y_i)$，$1 \le i \le s$，其中 e_K 代表加密所使用的函数。密文的接收者可以对密文进行解密，再利用原 1-AONT 的逆变换 ϕ^{-1}

得到原始的明文。但是，对于任何一个窃听者而言，想得到明文中的任意一位信息，都必须对密文解密（比如穷尽搜索的方法）得到整体的 $(y_1, \ldots, y_s)$ 的信息才可以。换言之，由于 1-AONT 的性质，仅仅部分的破译对于得到明文中的任意一位信息没有任何帮助。在这种意义上，1-AONT 的应用为分组密码提供了一层额外的安全保护。这种方法的延伸扩展也在[30,45]中有相关研究。AONT 也在密码学方面有诸多其它应用。比如，它被应用在网络编码[31,70]，安全数据传输[124]，抗干扰技术[99]，安全的分布式云存储[91,109]，安全的秘密分享方案[100]等。

然而，1-AONT 的性质并不能保证输入的多位信息的线性组合是否有部分信息的潜在泄露，比如说，有一定可能通过若干输出的信息，得知输入的信息中某两个位置的线性叠加的准确值。针对这种潜在的风险，Stinson 等人提出了 t-AONT 这一概念。类似上文所述，如果利用一个 t-AONT 在分组密码的使用之前对明文进行预处理，则任意窃听者若想得到关于明文的任何 t 位信息的任何布尔函数组合的部分信息，就必须至少得对密文解密得到 $(y_1, \ldots, y_s)$ 中多于 $s-t$ 信息才行。

线性的 AONT 的研究最为受到青睐。令字母表为有限域 $\mathbb{F}_q$. 其上的一个 (t, s, q)-AONT 被称为线性的，如果每个 y_i 都是 $(x_1, \ldots, x_n)$ 的一个 $\mathbb{F}_q$-线性函数。则它可以被表示为一个 $\mathbb{F}_q$ 上的 $s \times s$ 阶可逆矩阵 M. t-AONT 的第二个性质即要求 M 的任意 $t \times t$ 子矩阵也是可逆的。在[43] 中指出，当 $q \geq 2s$ 时，满足这样性质的矩阵是存在的。然而，当我们想要在 $\mathbb{F}_2$ 上考虑类似的问题时，容易发现，对于 $s > 1$，并不存在线性的 $(1, s, 2)$-AONT，对于 $s > 2$，也并不存在线性的 $(2, s, 2)$-AONT. 于是 D'Arco 等人提出的问题是如何得到一个尽量拥有 t-AONT 性质的矩阵，亦即，对给定的正整数 $t \leq s$，在一个 s 阶的二元可逆矩阵 M 中，最多有多大比例的 t 阶的可逆子矩阵? 下文中，我们提到矩阵可逆都是在 $\mathbb{F}_2$ 上来考虑的。沿用[43] 中的符号，我们有：

$$N_t(M) = M \text{ 的可逆 } t \times t\text{-子矩阵数目，}$$

$$R_t(M) = \frac{N_t(M)}{\binom{s}{t}^2},$$

$$R_t(s) = \max\{R_t(M) : M \text{ 是一个 } s \times s \text{ 可逆二元矩阵}\}。$$

在[43] 中证明了 $R_1(s) = 1 - \frac{s-1}{s^2}$，同时也分析了 $R_2(s)$ 的上下界，并猜想 $\lim_{s\to\infty} R_2(s)$ 这个极限值存在且位于 0.494 和 0.625 之间。本章的目标即完整解决这个问题，给出 $\lim_{s\to\infty} R_2(s) = 0.5$. 本章的结构如下。在第 4.2 小节我们分析建立整数规划，以分析 $R_2(s)$ 的上界，得到 $\lim_{s\to\infty} R_2(s) \leq 0.5$. 在第 4.3 小节我们利用概率方法分析 $R_2(s)$ 的下界，得到 $\lim_{s\to\infty} R_2(s) \geq 0.5$. 在第 4.4 小节我们给出一个基于分圆的构造的例子。第 4.5 小节对本章进行总结。

4.2　基于整数规划的上界分析

本小节中我们分析 $\lim_{s\to\infty} R_2(s)$ 的上界。在分析上界时可以暂时放宽条件，忽略矩阵整体本身可逆的限制。一个 2×2 的二元矩阵可逆当且仅当它为如下形式之一：

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}.$$

取定一个整数 c，先对恰好包含 c 个“1”的矩阵进行分析，分析这些“1”应当如何分布，以使得 2×2 的可逆子矩阵数目尽量多。对于 $1\le i\le n$，令 x_i 为第 i 行的重量（重量即为“1”的数目，下同），令 y_i 为第 i 列的重量。对于 $1\le i<j\le n$，令 $z_{i,j}$ 为第 i 和第 j 行的交错数，定义为 $z_{i,j}=|\{k : M_{i,k}=M_{j,k}=1\}|$. 除却自然的限制 $\sum_{i=1}^n x_i=\sum_{i=1}^n y_i=c$ 之外，利用标准的算两次的方法，可以得到一个附加的限制 $\sum_{1\le i<j\le n} z_{i,j}=\sum_{i=i}^n \binom{y_i}{2}$. 则由第 i 和第 j 行所提供的 2×2 可逆矩阵的数目为

$$z_{i,j}(x_i-z_{i,j})+z_{i,j}(x_j-z_{i,j})+(x_i-z_{i,j})(x_j-z_{i,j})=x_ix_j-z_{i,j}^2.$$

于是我们只需要对下面的整数规划问题进行求解。

$$\begin{aligned}\text{maximize}: &\sum_{1\le i<j\le s} x_ix_j-z_{i,j}^2\\ \text{subject to}: &\sum_{1\le i\le s} x_i=\sum_{1\le i\le s} y_i=c,\\ &\sum_{1\le i<j\le s} z_{i,j}=\sum_{1\le i\le s}\binom{y_i}{2},\\ &x_i,y_i,z_{i,j}\in\mathbb{N},1\le i<j\le s,\\ &c\in\mathbb{N},0\le c\le s^2.\end{aligned}$$

此规划的最优值，除以 $\binom{s}{2}^2$ 即为 $R_2(s)$ 的一个上界。这个上界是否可以精确达到并不是一个显然的问题，因为满足参数 $x_i,y_i,z_{i,j}$ 的可逆矩阵并不一定存在。一般来说，对每个 s 去决定最大的 $R_2(s)$ 的准确值是困难的，需要具体问题具体分析。下面我们以 $s=10$ 作为一个例子。

记一个多重集合的型为 $a_1^{n_1}\dots a_k^{n_k}$ 代表着此多重集合中每个元素 a_i 出现 n_i 次。对于 $s=10$ 这一情形，整数规划所得的最优值为 1216，对应的行重集合与列重集合的型都是 8^27^8，交叉数集合的型为 $5^{44}4^1$. 但是，满足这样参数的矩阵是不存在的，因为两个重量为

8 的行的交叉数必然至少为 6，这与交叉数集合的型相矛盾。那么退而求其次，此规划的第二最优值 1215 可以在行重集合与列重集合的型为 7^{10} 且交叉数集合的型为 $5^{30}4^{15}$ 时取到。设定 $S=\{1,2,4\}$，做如下二元矩阵 M，$M_{i,j}=1$ 当且仅当 $i-j\notin S \pmod{10}$. 此矩阵符合上述要求。所以我们得到 $R_2(10)=\frac{1215}{2025}=0.6$.

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0\\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0\\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1\\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0\\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1\\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1\\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1\\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1\\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1
\end{pmatrix}$$

尽管对每个 s 想去找到 $R_2(s)$ 的准确值是较为繁琐的，但对于我们的目标寻找 $\lim_{s\to\infty}R_2(s)$ 的上界而言，对这个整数规划做近似的求解即可。

定理42. $\lim_{s\to\infty}R_2(s)\le 0.5$.

证明. 考虑这个整数规划的松弛线性规划。显然，最大值在每个集合 $\{x_i\}_{1\le i\le s}$，$\{y_i\}_{1\le i\le s}$ 和 $\{z_{i,j}\}_{1\le i<j\le s}$ 都尽量平均分布时取到。亦即，对于给定的 c，$x_i=y_i=\frac{c}{s}$，$z_{i,j}=\frac{c(c-s)}{s^2(s-1)}$ 且目标函数达到 $\binom{s}{2}(\frac{c^2}{s^2}-\frac{c^2(c-s)^2}{s^4(s-1)^2})$. 这个值在 $c=\frac{3s+\sqrt{8s^4-16s^3+9s^2}}{4}$ 时取到。于是渐进意义下取 $c\sim\frac{\sqrt{2}s^2}{2}$ 可以得到 $\lim_{s\to\infty}R_2(s)\le 0.5$. □

4.3 基于概率方法的下界分析

在本小节中，我们利用概率方法分析 $\lim_{s\to\infty}R_2(s)$ 的下界。在[43] 中已经提出来随机构造的想法，以概率 $p=\sqrt{\frac{1}{2}}$ 取矩阵的每个项为“1”，各项之间独立同分布，所得到的矩阵的 2×2 可逆子矩阵数目的期望则为 $\frac{1}{2}\binom{s}{2}\binom{s}{2}$. 然而，他们并没有将此思路继续下去，没有深究是否存在一个可逆矩阵，其 2×2 可逆子矩阵数目达到这个期望值。实际上，有两种方式来解决这个问题，一种方法将在下一小节的具体构造中给出调节方式，另一种方法将如下文所述，综合利用了一个标准的二阶矩方法以及[42] 中的一个强力的结论。

引理43. [42] 令 M 为一个随机的 $s \times s$ 二元矩阵，每个矩阵的项独立同分布，服从概率 $\Pr[M_{i,j}=1]=p(s)$，$\Pr[M_{i,j}=0]=1-p(s)$. 如果对于任何 $d(s)\to\infty$ 有 $\min\{p(s),1-p(s)\} \geq (\log s + d(s))/s$，则 $\Pr[M \text{ 可逆}]$ 趋近于一个常数 $c \approx 0.28879$.

定理44. 对于任意 $\epsilon > 0$, 存在充分大的 S，使得对任意 $s > S$，存在可逆矩阵 M 满足 $R_2(M) > \frac{1}{2} - \epsilon$. 因此，$\lim_{s\to\infty} R_2(s) \geq 0.5$.

证明. 对于 $1 \leq i < j \leq s$，$1 \leq k < l \leq s$，令 $X_{i,j;k,l}$ 为随机事件“由第 i 行第 j 行和第 k 列第 l 列共同生成的 2×2 子矩阵可逆”的指示变量，亦即，$X_{i,j;k,l}=1$ 当且仅当此事件发生，否则 $X_{i,j;k,l}=0$. 令 $X=\sum_{1\leq i<j\leq s}\sum_{1\leq k<l\leq s} X_{i,j;k,l}$. X 是对总共的 2×2 可逆子矩阵的计数。令矩阵的每个项独立同分布，以概率 p 取“1”. 由期望的线性性可得

$$E[X]=\sum_{1\leq i<j\leq s}\sum_{1\leq k<l\leq s} E[X_{i,j;k,l}]=\binom{s}{2}^2(4p^3(1-p)+2p^2(1-p)^2)=\binom{s}{2}^2(2p^2-2p^4).$$

取概率 $p=\sqrt{\frac{1}{2}}$，可以将期望值最大化为 $E[X]=\frac{1}{2}\binom{s}{2}^2$. 接下来考虑随机变量 X 的方差。注意到两个指示变量 $X_1 := X_{i_1,j_1;k_1,l_1}$ 和 $X_2 := X_{i_2,j_2;k_2,l_2}$ 之间的协方差为

$$\mathrm{Cov}[X_1,X_2]=E[(X_1-E[X_1])(X_2-E[X_2])]=\frac{1}{4}(\Pr[X_1=X_2]-\Pr[X_1\neq X_2])=\frac{1}{4}(2\Pr[X_1=X_2]-1).$$

这个协方差的具体值依据两个子矩阵的交集大小而分为以下三种情形：

1) 两个子矩阵不交。则两个指示变量相互独立，协方差为 0.

2) 两个矩阵有一个公共元时，接下来的计算再分如下两部分：

- 令 $\mathcal{A}$ 为事件“公共元为 0”，此事件发生的概率为 $1-p$，在此情形下，

$$\Pr[X_1=1\mid\mathcal{A}]=\Pr[X_2=1\mid\mathcal{A}]=p^2(1-p)+p^3=\frac{1}{2},$$

$$\begin{aligned}\Pr[X_1=X_2\mid\mathcal{A}]&=\Pr[X_1=1\mid\mathcal{A}]\Pr[X_2=1\mid\mathcal{A}]+\Pr[X_1=0\mid\mathcal{A}]\Pr[X_2=0\mid\mathcal{A}]\\&=\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}=\frac{1}{2}.\end{aligned}$$

- 令 $\mathcal{B}$ 为事件“公共元为 1”，此事件发生的概率为 p，在此情形下，

$$\Pr[X_1=1\mid\mathcal{B}]=\Pr[X_2=1\mid\mathcal{B}]=3p^2(1-p)+p(1-p)^2=\frac{1}{2},$$

$$\begin{aligned}\Pr[X_1=X_2\mid\mathcal{B}]&=\Pr[X_1=1\mid\mathcal{B}]\Pr[X_2=1\mid\mathcal{B}]+\Pr[X_1=0\mid\mathcal{B}]\Pr[X_2=0\mid\mathcal{B}]\\&=\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}=\frac{1}{2}.\end{aligned}$$

则这种情形下的协方差仍然为 0.

3) 两个矩阵有两个公共元（两个公共元或者同行，或者同列）。注意到对于每个 $X_{i,j;k,l}$，其它与之交于两个公共元的指示变量数目为 $4(s-2)$. 于是至多有 $2(s-2)\binom{s}{2}^2$ 个这样的无序对。接下来的计算再分如下三部分：

• 令 $\mathcal{C}$ 为事件“两公共元皆为 1”，此事件发生的概率为 p^2，在此情形下，

$$\begin{aligned}\Pr[X_1 = 1 \mid \mathcal{C}] &= \Pr[X_2 = 1 \mid \mathcal{C}] = 2p(1-p) = 2p-1,\\ \Pr[X_1 = X_2 \mid \mathcal{C}] &= \Pr[X_1 = 1 \mid \mathcal{C}]\Pr[X_2 = 1 \mid \mathcal{C}] + \Pr[X_1 = 0 \mid \mathcal{C}]\Pr[X_2 = 0 \mid \mathcal{C}]\\ &= (2p-1)^2 + (2-2p)^2 = 9-12p.\end{aligned}$$

• 两公共元皆为 0（此事件发生概率为 $(1-p)^2$），此情形下 X_1 和 X_2 总为 0，$\Pr[X_1 = X_2] = 1$;

• 令 $\mathcal{D}$ 为事件“两公共元一个为 1 另一个为 0”，此事件发生的概率为 $2p(1-p)$，在此情形下，

$$\begin{aligned}\Pr[X_1 = 1 \mid \mathcal{D}] &= \Pr[X_2 = 1 \mid \mathcal{D}] = p^2 + pq = p,\\ \Pr[X_1 = X_2 \mid \mathcal{D}] &= \Pr[X_1 = 1 \mid \mathcal{D}]\Pr[X_2 = 1 \mid \mathcal{D}] + \Pr[X_1 = 0 \mid \mathcal{D}]\Pr[X_2 = 0 \mid \mathcal{D}]\\ &= p^2 + (1-p)^2 = 2-2p.\end{aligned}$$

则这种序对之间的协方差为

$$\frac{1}{4}(p^2 \times (17-24p) + (1-p)^2 \times 1 + 2p(1-p) \times (3-4p)) = \frac{3}{4} - p.$$

接下来可以计算 X 的方差如下。

$$\mathrm{Var}[X] = \sum_{1\le i<j\le s}\sum_{1\le k<l\le s}\mathrm{Var}[X_{i,j;k,l}] + 2(s-2)\binom{s}{2}^2 \times (\frac{3}{4} - p) \sim s^5.$$

下面利用切比雪夫不等式。对任意 $\lambda > 0$，$\Pr[|X - E[X]| \ge \lambda\sigma] \le \frac{1}{\lambda^2}$，其中 $\sigma = \sqrt{\mathrm{Var}[X]}$ 为标准差。对任意的 $\epsilon > 0$，设置 $\lambda\sigma = \epsilon\binom{s}{2}^2$. 由 $\sigma \sim s^{5/2}$ 可知 $\lambda \sim s^{3/2}$. 则 $\Pr[|X - E[X]| \ge \epsilon\binom{s}{2}^2] \le \frac{1}{s^3} \to 0$ $(s \to \infty)$. 于是对于充分大的 s，由引理 43 可得，$\Pr[M \text{ 可逆}] + \Pr[X > (\frac{1}{2} - \epsilon)\binom{s}{2}^2] > 0$. 于是对任意的 $\epsilon > 0$ 有 $R_2(s) > \frac{1}{2} - \epsilon$. 综上所述，$\lim_{s\to\infty} R_2(s) \ge 0.5$. □

以上的定理 42 和定理 44 结合起来得到了我们的主要结论：

定理45. 令 $R_2(s)$ 为一个 $s \times s$ 可逆二元矩阵中 2×2 可逆子矩阵的最大比例，则有：

$$\lim_{s\to\infty} R_2(s) = 0.5.$$

4.4　近似最优的矩阵的明确构造

上一小节的概率分析仅仅是一个存在性结论，并没有给具体构造矩阵的方式。直接的去随机化方法并不现实，因为在逐步决定每个元时去计算条件期望本身也是很困难的。本小节中，我们讨论一种明确构造近似最优的矩阵的方式。

此构造过程首先包含一个主要步骤，构造 M 的核心结构，接下来是一个调整步骤，以保证最后所构造的矩阵 M 确实为可逆的，同时在渐进意义下并不影响 $R_2(M)$ 的值。

回忆对于上界的证明，最优的矩阵应该有均衡的行重，均衡的列重，均衡的交叉数。回忆下界的证明，矩阵中总共的“1”的数目需要接近于 $\sqrt{\frac{1}{2}}s^2$. 构造近似最优矩阵也需要以此两条为准则。

令 $\mathcal{S}$ 为 $\{1, 2, \ldots, s\}$ 的一个子集。我们构造这样的矩阵 M，$M_{i,j} = 1$ 当且仅当 $i-j \notin \mathcal{S}$, $(\mathrm{mod}\ s)$. 上述的两条准则，提示我们应该：

- 选取的子集 $\mathcal{S}$ 大小约为 $(1 - \sqrt{\frac{1}{2}})s$.
- 令 $\Delta(\mathcal{S})$ 为多重集合 $\{x - y : x, y \in \mathcal{S}, x \neq y\}$. 令 m_i 为 i 在 $\Delta(\mathcal{S})$ 中的重数，$1 \leq i \leq s-1$. 这些重数应当接近完全相同。

构造的核心关键即为寻找这样合适的 $\mathcal{S}$，对于这个问题，分圆是一个非常有用的工具。实际上，在[43] 中，其作者就使用了 4 阶分圆构造了一系列矩阵，达到了 $R_2(M) \approx 0.492$. 我们模仿他们的方式，采用 7 阶分圆。我们的结果更加接近 0.5，因为对比而言我们的 $\mathcal{S}$ 的大小更加接近 $(1 - \sqrt{\frac{1}{2}})s$.

4.4.1　主要步骤：基于分圆的构造

令 p 为素数，γ 为任意取定的一个 $\mathbb{F}_p$ 中的本原元。令 $N > 1$ 为 $p-1$ 的一个因子。定义 $\mathbb{F}_p$ 的 N 阶分圆类 $C_0, C_1, \ldots, C_{N-1}$ 为

$$C_i = \left\{ \gamma^{jN+i} \mid 0 \leq j \leq \frac{p-1}{N} - 1 \right\},$$

其中 $0 \le i \le N-1$. 亦即，C_0 是模 p 的 N 次剩余，$C_i = \gamma^i C_0$，$1 \le i \le N-1$. 对于整数 i, j，$0 \le i, j < N$，N 阶分圆数的定义为

$$(i,j)_N = |(C_i + 1) \bigcap C_j|.$$

下面的引理概括了分圆数的一些基本性质。

引理46. [16] 令 $p = ef + 1$ 为奇素数。

- $(i,j)_e = (i',j')_e$，若 $i \equiv i' \pmod e$ 且 $j \equiv j' \pmod e$.
- $(i,j)_e = \begin{cases} (j,i)_e, & \text{若 } f \text{ 为偶数;} \\ (j+e/2, i+e/2)_e, & \text{若 } f \text{ 为奇数。} \end{cases}$
- $\sum_{i=0}^{e-1}(i,j)_e = f - \delta_j$, 其中当 $j \equiv 0 \pmod e$ 时 $\delta_j = 1$，否则 $\delta_j = 0$.

在此小节中，我们总是假设 $p = 7f + 1$ 为素数。我们需要下面的关于 7 阶分圆数的结论。

引理47. [86,87] 若 $p \equiv 1 \pmod 7$，则对于 $0 \le i, j \le 6$ 有 $\lim_{p\to\infty} \frac{(i,j)_7}{p} = \frac{1}{49}$.

我们设定矩阵 $M' = (m_{ij})$ 为 $\mathbb{F}_2$ 上的一个 $p \times p$ 矩阵，行与列的标记为 $\mathbb{F}_p$，且

$$m_{ij} = \begin{cases} 1, & \text{若 } j - i \in C_0 \bigcup C_1; \\ 0, & \text{其它情况.} \end{cases}$$

令 M 为 M' 的补矩阵（0 对应于 1，1 对应于 0）。

首先考虑矩阵 M'. 显然，第 i_1 与 i_2 行中所包含的 2×2 可逆矩阵的数目只由 $i_1 - i_2$ 所决定。则只需考虑第 0 与 i 行。定义

$$n_i = \{j \mid m_{0j} = m_{ij} = 1\}.$$

则可计算得到

$$\begin{aligned} n_i &= |(C_0 \bigcup C_1) \bigcap ((C_0 \bigcup C_1) + i)| \\ &= |C_0 \bigcap (C_0 + i)| + |C_0 \bigcap (C_1 + i)| + |C_1 \bigcap (C_0 + i)| + |C_1 \bigcap (C_1 + i)| \\ &= |i^{-1}C_0 \bigcap (i^{-1}C_0 + 1)| + |i^{-1}C_0 \bigcap (i^{-1}C_1 + 1)| + |i^{-1}C_1 \bigcap (i^{-1}C_0 + 1)| + |i^{-1}C_1 \bigcap (i^{-1}C_1 + 1)|. \end{aligned}$$

令 $i^{-1}C_0 = C_m$，其中 $0 \le m \le 6$，则 $i^{-1}C_1 = C_{m+1}$. 由引理 46，我们有

$$\begin{aligned} n_i &= |C_m \bigcap (C_m + 1)| + |C_m \bigcap (C_{m+1} + 1)| + |C_{m+1} \bigcap (C_m + 1)| + |C_{m+1} \bigcap (C_{m+1} + 1)| \\ &= (m,m)_7 + (m,m+1)_7 + (m+1,m)_7 + (m+1,m+1)_7, \\ &= (m,m)_7 + 2(m,m+1)_7 + (m+1,m+1)_7. \end{aligned}$$

在 M 的第 0 与 i 行，假设有 $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ 出现 a_0 次，$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ 出现 a_1 次，$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ 出现 a_2 次，$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ 出现 a_3 次。注意到 M 为 M' 的补矩阵，则有

$$\begin{aligned} a_0 &= n_j, \\ a_1 = a_2 &= 2f - n_j, \\ a_3 &= p - 4f + n_d = 3f + 1 + n_j. \end{aligned}$$

于是我们得到

$$a_1a_2 + a_1a_3 + a_2a_3 = 16f^2 - 6fn_j + 4f - n_j^2 - 2n_j.$$

所以，M 中的 2×2 可逆子矩阵的数目总计为

$$\begin{aligned} &\frac{p(p-1)}{14} \sum_{m=0}^{6} (16f^2 - 6fn_j + 4f - n_j^2 - 2n_j) \\ &= \frac{p(p-1)}{14} \sum_{m=0}^{6} (16f^2 + 4f - (6f+2)((m,m)_7 + 2(m,m+1)_7 + (m+1,m+1)_7) - \\ &((m,m)_7 + 2(m,m+1)_7 + (m+1,m+1)_7)^2). \end{aligned}$$

由引理 47 可知，对任意 $0 \le m \le 6$，当 f 趋于无穷时，$\frac{(m,m)_7}{f} = \frac{(m,m+1)_7}{f} = \frac{1}{7}$. 于是有

$$\begin{aligned} &\lim_{p \to \infty} \frac{2}{7p(p-1)} \sum_{m=0}^{6} (16f^2 + 4f - (6f+2)((m,m)_7 + 2(m,m+1)_7 + (m+1,m+1)_7) - \\ &((m,m)_7 + 2(m,m+1)_7 + (m+1,m+1)_7)^2) \\ &= \lim_{f \to \infty} \frac{2}{7(7f+1)7f} \sum_{m=0}^{6} (16f^2 + 4f - (6f+2)(\frac{4f}{7} + o(f)) - (\frac{4f}{7} + o(f))^2) \\ &= \frac{1200}{2401}. \end{aligned}$$

4.4.2 调整步骤

仍然需要分析上述构造的矩阵是否本身是可逆的。我们声称，即便 M 本身并不可逆的话，我们可以通过些许调整将其转化成为一个可逆矩阵，且同时在渐近意义下不影响 $R_2(M)$ 的值。

引理48. *每个二元矩阵 M 可以通过调节其对角线上的元素使之成为一个可逆矩阵。*

证明. 采用数学归纳法。首先将 $M_{1,1}$ 这一项设定为“1”，在假定已经将 k 阶主子式（记为 P_k）调整成可逆的前提下，考虑如何选择 $M_{k+1,k+1}$ 这一项。计算 P_{k+1} 的行列式时，依据第 $(k+1)$ 行进行展开。整个加和中包含了一项 $\det(P_k) \times M_{k+1,k+1}$. 由于已经假定 $\det(P_k) \neq 0$，则可以通过调整 $M_{k+1,k+1}$ 的取值以保证 $\det(P_{k+1}) \neq 0$. □

由于至多调整了 p 个元素，每个元素包含于 $(p-1)(p-1)$ 个 2×2 子矩阵之中，所以整个调整步骤所影响到的 2×2 子矩阵数目至多为 $p(p-1)^2 \sim p^3 = o(p^4)$. 对于充分大的$p$, 渐进意义上这个误差可以忽略，不影响 $R_2(M)$ 的值。

综上所述，通过分圆的主要步骤辅以在对角线上的调整步骤，可以得到一系列近似最优的矩阵：

定理49. *对任意素数 p，$p \equiv 1 \pmod 7$，上述构造给出矩阵 M_p，满足*

$$\lim_{p\to\infty} R_2(M_p) = \frac{1200}{2401} \approx 0.4997917.$$

4.5 小结

本章证明了 $\lim_{s\to\infty} R_2(s) = 0.5$，完整回答了 D'Arco 等人所提出的问题。对此问题的进一步思考是去考虑一般的可逆 $t \times t$ 子矩阵数目。随机选取辅以二阶矩方法的讨论仍会给出问题的一个下界，比如 $\lim_{s\to\infty} R_3(s) \geq 0.38817$（每个元独立同分布，以概率 $p \approx 0.63056$ 选取为“1”）。但是，对上界的讨论，类似的用整数规划的方法去处理略显困难。然而我们猜测对任何 $t \leq s$，$\lim_{s\to\infty} R_t(s)$ 的准确值很可能就是通过概率方法所能分析得到的下界。对应的最优的矩阵应当保持着平衡性，即任意 $r \leq t$ 列（行）的交叉数约为 sp^r，其中 p 为概率分析中所得的取每项为“1”的最优概率。

5 量子信息中的不可扩展乘积基

5.1 介绍

$\mathbb{C}$ 代表复数域。在张量空间 $\bigotimes_{i=1}^{m}\mathbb{C}^{k_i}$ 中的一个向量 $\mathbf{v}$，如果可以写成 $\mathbf{v}=\mathbf{v_1}\otimes\mathbf{v_2}\otimes\cdots\otimes\mathbf{v_m}$ 这样的形式，其中 $\mathbf{v_i}\in\mathbb{C}^{k_i}$，那么我们称这个向量 $\mathbf{v}$ 为一个**纯态**。如果这样的分解不存在，则称之为**纠缠态**。对于两个 $\bigotimes_{i=1}^{m}\mathbb{C}^{k_i}$ 中的纯态向量 $\mathbf{u}=\mathbf{u_1}\otimes\mathbf{u_2}\otimes\cdots\otimes\mathbf{u_m}$ 和 $\mathbf{v}=\mathbf{v_1}\otimes\mathbf{v_2}\otimes\cdots\otimes\mathbf{v_m}$，定义它们的内积为

$$(\mathbf{u},\mathbf{v})=\prod_{i=1}^{m}(\mathbf{u_i},\mathbf{v_i}),$$

于是 $(\mathbf{u},\mathbf{v})=0$ 当且仅当存在至少一个指标 i，使得 $(\mathbf{u_i},\mathbf{v_i})=0$.

在文献[15] 与[51]中，首次提出了不可扩展乘积基的概念。在 $\bigotimes_{i=1}^{m}\mathbb{C}^{k_i}$ $(k_i\geq 2)$ 中的一个**不可扩展乘积基**（Unextendible product bases，以下简称为 UPB），是由此张量空间中若干非零纯态向量所组成的集合 $\mathcal{F}$，满足：

- （正交限定）$\mathcal{F}$ 中的任何两个纯态向量正交；
- （不可扩展限定）不存在 $\bigotimes_{i=1}^{m}\mathbb{C}^{k_i}$ 中的一个非零纯态向量，与 $\mathcal{F}$ 中的所有向量正交。

除却最初在[51,105,108] 中对 Bound 纠缠态的构造这一动机之外，不可扩展乘积基在量子信息的诸多领域中有重要应用，包括：构造不可约正算子[120]，生成无量子违背的 Bell 不等式[7,8]，构造低维度的局部不可区分子空间[52]，以及无纠缠态下的量子非局域性的现象的存在性[14]。

上述量子信息中的诸多应用引出了 UPB 的最小规模问题。令 $f_m(k_1,\ldots,k_m)$ 代表 $\bigotimes_{i=1}^{m}\mathbb{C}^{k_i}$ 中的规模最小的 UPB 的大小。称每个 $\mathbb{C}^{k_i}$ 为一个**局部空间**。当局部空间的数目 m 可由上下文明确指定时，我们在记号中省略掉它，即 $f(k_1,\ldots,k_m)$.

文献[15] 在提出此定义的同时也立即提出了此问题的平凡下界 $f(k_1,k_2,\ldots,k_m)\geq\sum_{i=1}^{m}(k_i-1)+1$. 假设 $\mathcal{F}$ 仅包含 $\mathbf{v_j}=\mathbf{v_{j,1}}\otimes\cdots\otimes\mathbf{v_{j,m}}$, $\mathbf{v_{j,s}}\in\mathbb{C}^{k_s}$, $1\leq j\leq\sum_{i=1}^{m}(k_i-1)$,

$1 \le s \le m$ 这些向量。将指标集 $J = \{1, 2, \ldots, \sum_{i=1}^{m}(k_i - 1)\}$ 划分为 m 个两两不交的子集 $J_1, J_2, \ldots, J_m$，使得 $|J_s| = k_s - 1, 1 \le s \le m$. 寻找一个非零向量 $\mathbf{u_s} \in \mathbb{C}^{k_s}$ 与每个 $\mathbf{v_{j,s}}$，$j \in J_s$ 都正交，这样的向量显然存在，因为 $\{\mathbf{v_{j,s}}\}_{j \in J_s}$ 这族向量仅仅能张成 $\mathbb{C}^{k_s}$ 的非平凡子空间。进而，我们得到一个非零纯态向量 $\mathbf{u} = \mathbf{u_1} \otimes \cdots \otimes \mathbf{u_m}$ 与所有 $\mathbf{v_j}$ 都正交，这与定义中的不可扩展限定相矛盾。于是，$f(k_1, k_2, \ldots, k_m) \ge \sum_{i=1}^{m}(k_i - 1) + 1$ 成立。 Alon 与 Lovász 在[5] 中给出了此平凡下界可达到的充分必要条件：

定理50. [5] *令 $m \ge 2$ 且 $2 \le k_1 \le \cdots \le k_m$. 则 $f(k_1, \ldots, k_m) > \sum_{i=1}^{m}(k_i - 1) + 1$ 当且仅当 $(k_1, \ldots, k_m)$ 满足下述情形之一：*

1) $m = 2$ 且 $k_1 = 2$；

2) $\sum_{i=1}^{m}(k_i - 1) + 1$ 为奇数且至少一个 k_i 为偶数。

对于上述第一种情形，Feng [61] 给出了 $f(2, k) = 2k$. 对于第二种情形，$f(k_1, \ldots, k_m) \ge \sum_{i=1}^{m}(k_i - 1) + 2$，准确的值的分析较为困难。我们首先列举一些已知结果如下。

首先，所有局部空间的维度均为 2 的情形在量子信息中颇受关注。令 $f(2^{[t]})$ 代表 $(\mathbb{C}^2)^{\otimes t}$ 中规模最小的 UPB 的大小。当 t 为奇数时，定理 50 给出了 $f(2^{[t]}) = t + 1$. 之后 Feng [61] 给出了 $f(2^{[4]}) = 6$ 以及对任何自然数 m 有 $f(2^{[4m+2]}) = 4m + 4$. 最后 Johnston 完全解决了余下的情形。上述结果总结如下：

定理51. [5,61,80,81] *令 $f(2^{[t]})$ 代表 $(\mathbb{C}^2)^{\otimes t}$ 中规模最小的 UPB 的大小，则有*

1) *若 t 为奇数，则 $f(2^{[t]}) = t + 1$；*

2) *若 $t = 4$ 或 $t \equiv 2 \pmod 4$，则 $f(2^{[t]}) = t + 2$；*

3) *若 $t = 8$，则 $f(2^{[t]}) = t + 3$；*

4) *其它情形下，$f(2^{[t]}) = t + 4$.*

在所有局部空间的维度均为 2 的这一情形解决之后，自然而然考虑的下一个情形是仅有一个非二维局部空间的情形。假设有 $t \ge 2$ 个维度为 2 的局部空间，另有一个维度为 $s \ge 3$ 的局部空间，令 $f(2^{[t]}, s)$ 代表此情形下规模最小的 UPB 的大小。当 $t + s$ 为偶数时，定理 50 给出了 $f(2^{[t]}, s) = t + s$. 除此之外，Feng[61] 给出了 $f(2^{[2]}, 3) = 6$, $f(2^{[2]}, 5) = 8$, $f(2^{[3]}, 4) = 8$ 和 $f(2^{[4]}, 5) = 10$ 这几个零星的例子。Chen 与 Johnston[36] 将 $f(2, 2, 5) = 8$ 这个结果演化为如下更一般的结论：

定理52. [36] *对于正整数 k 有 $f(2, 2, 4k + 1) = 4k + 4$.*

自然地，下一个需要考虑解决的问题为决定 $f(2,2,4k-1)$ 的值，这也在[36] 中被列为一个公开问题：**是否可以将 $f(2,2,3)=6$ 扩展得到 $f(2,2,4k-1)=4k+2$ 这样的一般结论?**

以上所列举的为关于最小规模 UPB 的目前仅有的结果。其研究方法使用的皆是纯粹的组合技巧。需要说明的是，[36] 的作者尝试利用了代数几何的思想去构造 UPB 的向量，并给出了一个针对一大类参数的结论。虽然他们的结果的正确性符合想象，但是他们基于代数几何的证明是不严谨的。于是我们暂时并不能完全承认他们的结论的正确性。

在本章，我们将回归到纯粹的组合手法，利用包括图的正交表示、循环图的连通性、图的 1-因子分解等图论工具。我们的第一个结果是对于上述关于 $f(2,2,4k-1)$ 问题的肯定的回答。

定理53. *对于正整数 k 有 $f(2,2,4k-1)=4k+2$.*

第二个结果是针对更一般的 $f(2^{[t]},s)$ 的问题。我们给出下面的定理，解决了此问题的一半情形。

定理54. *对于正整数 t，s，$t\geq 3$ 且 $s\geq 3$，如果 $t+s+1$ 是 4 的倍数，则有 $f(2^{[t]},s)=t+s+1$.*

在研究此定理的过程中，对于相关图论工具的进一步充分应用可以得到下面一个更为复杂的结果。虽然此结论形式上显得杂乱，然而它能充分体现出我们的方案对于最小规模 UPB 这一问题研究的作用。

定理55. *令 t 为一个正奇数。令 $a_1,a_2,\ldots,a_k$ 为一族正奇数，b 为一个正偶数。假设以下两个条件至少一个成立：$a_1,a_2,\ldots,a_k$ 并不完全相同或 $t\geq 3$. 如果 $t+\sum_{i=1}^{k}(a_i-1)+b+1$ 是 4 的倍数，则有 $f(2^{[t]},a_1,\ldots,a_k,b)=t+\sum_{i=1}^{k}(a_i-1)+b+1$.*

本章的结构如下。在第 5.2 小节，我们将简要介绍相关术语并讨论最小规模 UPB 的构造的基本思路。在第 5.3 小节，由于其思路与后文的显著不同，我们将单独列出定理 53 的证明。第 5.4 小节将介绍一些图论工具，主要围绕循环图的连通性。利用这些工具，我们在第 5.5 小节进行定理 54 和 55 的证明。第 5.5 小节对本章进行总结。

5.2 预备工作

给定一个 $\bigotimes_{i=1}^{m}\mathbb{C}^{k_i}$ 中的大小为 n 的 UPB，我们可以构造一族图 G_i，$i=1,\ldots,m$，用来辅助视觉化这族向量之间的正交关系。每个图 G_i 的点集 V 包含了 n 个点，对应于这组 UPB 中的 n 个向量。在本章之中，我们以粗体表示与点 v 相对应的向量 $\mathbf{v}=\mathbf{v_1}\otimes\mathbf{v_2}\otimes\cdots\otimes\mathbf{v_m}$, $\mathbf{v_i}\in\mathbb{C}^{k_i}$. 两个点 v 与 u 在图 G_i 中有一条边相连当且仅当 $(\mathbf{v_i},\mathbf{u_i})=0$. 于是图 G_i 实际上代表了第 i 个局部空间上的正交关系，被称为这个局部空间上的**正交图**。显然，全体正交图的并是整个完全图 K_n. 最小规模 UPB 的构造的基本思路包含以下三个方面。

- 对于每个局部空间 $\mathbb{C}^{k_i}$ 选取一张**初始图** H_i. 每张初始图的点集 V 包含了 n 个点，对应于这组 UPB 中的 n 个向量。且所有初始图构成了整个完全图 K_n 的一组不交并。

- 在每个局部空间 $\mathbb{C}^{k_i}$ 中，对初始图 H_i 的每个点赋予一个向量，使得 H_i 中任意相邻两点所赋予的向量正交。对每个顶点 v，记其在局部空间 $\mathbb{C}^{k_i}$ 中所被赋予的向量为 $\mathbf{v_i}$. 构造一个大小为 n 的 UPB，其中每个顶点 v 对应的纯态向量为 $\mathbf{v}=\mathbf{v_1}\otimes\mathbf{v_2}\otimes\cdots\otimes\mathbf{v_m}$. 则这个 UPB 的每个正交图 G_i 皆包含 H_i 作为一张子图。于是全体正交图的并也如预期一样是整个完全图 K_n.

- 证明上述构造满足不可扩展限定。在每个局部空间 $\mathbb{C}^{k_i}$ 中，对于点集的任一个子集 $S_i\subset V$，如果它所对应的向量不能张成整个局部空间 $\mathbb{C}^{k_i}$，则我们称之为**不饱和的**。于是可以找到一个非零向量 $\mathbf{w_i}\in\mathbb{C}^{k_i}$ 与 $\{\mathbf{v}:v\in S_i\}$ 这一族向量皆正交。证明一个构造的 UPB 的确满足不可扩展限定，等同于说明，对于任何一组 $S_1,S_2,\ldots,S_m$ 的选取（其中每个 S_i 是如上所定义的一个不饱和的子集），它们的并集不等于整个点集 V. 要注意的是，我们并不一定要保证 $G_i=H_i$，但是一般情况下，不可扩展限定会强制要求 $G_i=H_i$ 成立。

综上所述，对于 UPB 的构造既要选取合适的初始图，又要根据初始图在每个局部空间中选取合适的向量。其中后者选取合适的向量这一问题相对比较棘手。在 Lovász 研究图的香农容量的文章[92] 中所提出的图的正交表示这一概念，对于这一问题的帮助很大。给定一张图 $G(V,E)$，其中 V 代表点集，E 代表边集，它**在** $\mathbb{R}^d$ **上的正交表示**是一个映射：$f:V\to\mathbb{R}^d$，使得不相邻的点上的向量正交。于是，基于初始图 H_i 来选择合适的向量使其正交图 G_i 包含 H_i 这一问题，等价于寻找 H_i 的补图 $\overline{H}_i$ 上的一个正交表示的问题。图的正交表示这一概念与图的连通性密切相关。对于一个连通图，如果去掉某些 k 个点及相关

的边之后会使得这个图不再连通，然而去掉任意少于 k 个点及相关的边之后余下的图依然连通，那么我们称这个图是 k-**连通**的。Lovász，Saks 与 Schrijver[93] 证明了下述结论。

引理56. [93] 令图 G 的顶点数为 n，则 G 是 k-连通的当且仅当存在图 G 的一个在 $\mathbb{R}^{n-k}$ 上的正交表示，并且使得任意 $n-k$ 个向量线性无关。

上述引理的强大之处不光在于它联系了图的连通性与正交表示这两个方面，还尤其在于它对于这组正交表示提供了更多的线性无关性的相关信息，这对于之后不可扩展限定的分析有很大帮助。例如，在定理 50 的证明中，Alon 和 Lovász[5] 选取了合适的初始图 H_i，其中每个 $\overline{H}_i$ 都是 $(n-k_i)$-连通的，$n=\sum_{i=1}^{m}(k_i-1)+1$. 则对应的向量选取可由引理 56 保证。最后，为证明不可扩展限定的成立，只需要说明每个不饱和集 S_i 的大小不超过 k_i-1 即可，这同样是由引理 56 所保证的。

我们现在着眼于平凡下界不可达到的情形，为了证明下一个最小值 $\sum_{i=1}^{m}(k_i-1)+2$ 可以达到，我们首先分析一下如果这种 UPB 存在的话，它的正交图应当满足怎样的性质。每个正交图 G_i 的最小度数至少为 k_i-1，否则若 $deg(v)<k_i-1$，则我们可以找到一个非零向量 $\mathbf{w_i}\in\mathbb{C}^{k_i}$ 使得它与 $\{\mathbf{u_i}:u\text{ 与 }v\text{ 在 }G_i\text{ 中相邻}\}\bigcup\{\mathbf{v_i}\}$ 皆正交。进而，一个纯态向量 $\mathbf{v_1}\otimes\cdots\otimes\mathbf{v_{i-1}}\otimes\mathbf{w_i}\otimes\mathbf{v_{i+1}}\otimes\cdots\otimes\mathbf{v_m}$ 将与这个假定的 UPB 中的所有向量正交，这与不可扩展限定相矛盾。每个正交图 G_i 的最大度数至多为 k_i-1，否则我们可以通过类似于对平凡下界的分析方法得到矛盾。于是，在对于初始图的选择中，我们要求对每个点 v，恰好在一个初始图中度数为 $deg(v)=k_i$，其它图中皆为 $deg(v)=k_i-1$.

对于一个最大度为 k_i 的初始图 H_i 而言，其对应的向量的赋予相对困难，因为此时我们将无法借助引理 56 的辅助。于是，一个自然的想法就是设置其中一个初始图为 k_i-正则的，其它皆为 (k_i-1)-正则的。在绝大多数已知的结果以及接下来对定理 54 和 55 的证明中就贯彻了这样的想法。然而，有些情形下，只有选择非正则的初始图，才能分析得到期望的 UPB 的存在。下一小节对于 $f(2,2,4k-1)=4k+2$ 的证明即是这样的情况之一。基于此结果的相对特殊性，以及它的证明与其它结果的证明有显著不同，我们将它单列一个小节。

5.3　定理 53 的证明

本小节中我们将讨论 $f(2,2,4k-1)$. 当 $k=1$ 时，$f(2,2,3)=6$ 已由 Feng 给出构造[61]。现在我们将对于一般的 $k\geq 2$ 对定理 53展开证明。

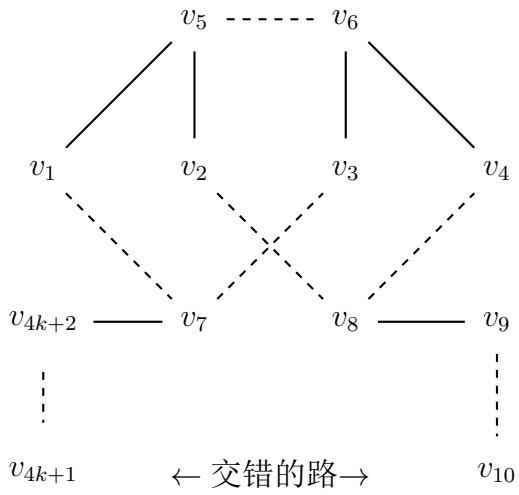

图 5-1　初始图 $H_1 \bigcup H_2$.

对两个二维的局部空间，选取初始图 H_1 与 H_2，记 H_3 为 $4k-1$ 维度的局部空间的初始图。点集表示为 $V = \{v_1, v_2, \ldots, v_{4k+2}\}$. 前两张初始图的并在图 5-1 中画出，实线代表 H_1 中的边，虚线代表 H_2 中的边。余下的从 v_{10} 到 v_{4k+1} 的交错路径未予画出。令 H_1 有以下四条边：$v_1 \sim v_5$，$v_2 \sim v_5$，$v_3 \sim v_6$，$v_4 \sim v_6$. 令 H_2 有以下五条边：$v_1 \sim v_7$，$v_3 \sim v_7$，$v_2 \sim v_8$，$v_4 \sim v_8$，$v_5 \sim v_6$. 余下的 H_1 中的 $2k-2$ 条边和 H_2 中的 $2k-3$ 条边一同构成了从 v_8 到 v_7 的一条交错的路径。不失一般性，设定此路径为 $v_8 \sim v_9 \sim \cdots \sim v_{4k+1} \sim v_{4k+2} \sim v_7$. 则 H_3 也被精确的决定出，即所绘图的补图，$H_3 = \overline{H_1 \bigcup H_2}$.

对于 H_1 和 H_2 上所应赋予的向量是显而易见的。仅需考虑选取 $\mathbb{C}^{4k-1}$ 中的合适的向量以满足 H_3 所指定的正交关系。在余下的证明中我们用 $\mathbf{v_i} \in \mathbb{C}^{4k-1}$ 表示对点 v_i 所赋予的向量。注意到任何 $s \leq 4k$ 个向量需要张成一个维度为 $s-1$ 或 s 的空间，否则模仿对平凡下界的分析将很容易得到与不可扩展限定相冲突的矛盾。

首先关注在图 H_3 中每个顶点 v_i 的邻域 N_i. $N_9 = V\backslash\{v_8, v_9, v_{10}\}$ 包含了$4k-1$ 个顶点，对应的向量需要张成一个 $4k-2$-维的子空间。类似地，$N_{10} = V\backslash\{v_9, v_{10}, v_{11}\}$ 包含了 $4k-1$ 个顶点，对应的向量需要张成一个 $4k-2$-维的子空间。它们的交集 $N_9 \bigcap N_{10} = V\backslash\{v_8, v_9, v_{10}, v_{11}\}$ 包含了 $4k-2$ 个顶点。我们声称这些对应于 $N_9 \bigcap N_{10}$ 的向量应当张成一个维度为 $4k-3$ 的空间。这是由于如果维数可以达到 $4k-2$ 的话，那么 $\mathbf{v_8}$ 和 $\mathbf{v_{11}}$ 两者都可以写成 $\mathbf{V}\backslash\{\mathbf{v_8}, \mathbf{v_9}, \mathbf{v_{10}}, \mathbf{v_{11}}\}$ 的线性组合。则 $\mathbf{V}\backslash\{\mathbf{v_9}, \mathbf{v_{10}}\}$ 包含了 $4k$ 个向量，但仅仅张成了一个 $4k-2$-维空间，这将导致与不可扩展限定的矛盾。这个思路延续下去，我们分别考虑 $N_9 \bigcap N_{10} \bigcap N_{11}$，$N_9 \bigcap N_{10} \bigcap N_{11} \bigcap N_{12}$，... 直到最后 $N_9 \bigcap N_{10} \bigcap \cdots \bigcap N_{4k+2}$ 所分别张成的空间的维数. 最终的结论是由 $\{\mathbf{v_1}, \mathbf{v_2}, \mathbf{v_3}, \mathbf{v_4}, \mathbf{v_5}, \mathbf{v_6}\}$

张成的空间的维度为 5. 于是我们应这样选取向量：

$$\mathbf{v_1} = (1,0,0,0,0,0,\ldots,0),$$

$$\mathbf{v_2} = (0,1,0,0,0,0,\ldots,0),$$

$$\mathbf{v_3} = (0,0,1,0,0,0,\ldots,0),$$

$$\mathbf{v_4} = (0,0,0,1,0,0,\ldots,0),$$

$$\mathbf{v_5} = (1,1,0,0,1,0,\ldots,0),$$

$$\mathbf{v_6} = (0,0,1,1,1,0,\ldots,0).$$

接下来我们选择 $\mathbf{v_7}$ 与 $\mathbf{v_8}$：

$$\mathbf{v_7} = (1,0,1,0,-1,\lambda\mathbf{w_7}),$$

$$\mathbf{v_8} = (0,1,0,1,-1,\tau\mathbf{w_8}),$$

其中 $\mathbf{w_7}$ 与 $\mathbf{w_8}$ 为 $\mathbb{C}^{4k-6}$ 中的向量，λ 与 τ 是待定的非零参数。最后，其它向量形如 $\mathbf{v_i} = (0,0,0,0,0,\mathbf{w_i}), 9 \leq i \leq 4k+2$，其中 $\mathbf{w_i} \in \mathbb{C}^{4k-6}$. 可以检查得到，$H_3$ 所要求的正交限定中，涉及 $\mathbf{v_1},\ldots,\mathbf{v_6}$ 的已经全部满足。

只要 $\mathbf{w_7}$ 与 $\mathbf{w_8}$ 不正交的话，那么我们就可以通过调节系数 λ 和 τ 的选取，使得 $(\mathbf{v_7},\mathbf{v_8}) = 1+\lambda\tau(\mathbf{w_7},\mathbf{w_8}) = 0$. 于是余下的工作仅仅是选择 $\mathbf{w_7},\ldots,\mathbf{w_{4k+2}}$，使得其正交关系满足 H_3 中余下的边。等价于说，寻找圈图 $C = v_7 \sim v_8 \sim v_9 \sim \cdots \sim v_{4k+1} \sim v_{4k+2} \sim v_7$ 在 $\mathbb{C}^{4k-6}$ 上的一个正交表示。为此重新考虑引理 56 的作用。圈图 C 有 $4k-4$ 个顶点。由于圈是一个 2-连通的图，则引理 56 保证了 C 在 $\mathbb{C}^{4k-6}$ 上的一个正交表示，且同时保证了 $\{\mathbf{w_7},\ldots,\mathbf{w_{4k+2}}\}$ 这 $4k-4$ 个向量中的任意 $4k-6$ 个线性无关。

最后我们证明所构造的 UPB 满足不可扩展限定。第一个不饱和集 S_1 为 $\{v_1,v_2\}$ 或者 $\{v_3,v_4\}$ 或者任意一个单点集。第二个不饱和集 S_2 为 $\{v_1,v_3\}$ 或者 $\{v_2,v_4\}$ 或者任意一个单点集。对第三个不饱和集的限制条件由下述引理给出。

引理57. *对上述所构造的向量，选取合适的 λ 与 τ，可使得第三个不饱和集 S_3 满足：$|S_3| \leq 4k-1$ 且等号成立时必须有 $|S_3 \bigcap \{v_1,v_2,v_3,v_4\}| \geq 3$.*

证明. 将上述向量排成一个大小为 $(4k+2)\times(4k-1)$ 的矩阵 A，其中矩阵第 i 行对应于向量 $\mathbf{v_i}$. 我们说明任意的 $(4k)\times(4k-1)$ 阶子矩阵 A' 的秩为 $4k-1$. 比较 A' 与 A 并假定所缺失的两行的指标为 i 和 j.

如果集合 $X=\{1,2,3,4,5,6\}\backslash\{i,j\}$ 的大小为 $|X|\geq 5$，则利用指标包含于 X 的任意五行对矩阵做初等行变换中的消法变换，则可以将前五列中其它位置全部清零，将矩阵 A' 转化成为分块矩阵 $\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$，其中 B 是秩为 5 的 5×5 阶矩阵，C 是秩为 $4k-6$ 的 $(4k-5)\times(4k-6)$ 阶矩阵。否则，当 $|X|=4$ 时，利用指标为 $\{9,\ldots,4k+2\}$ 的行对矩阵做初等行变换中的消法变换，同样可以将矩阵 A' 转化成为分块矩阵 $\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$，其中 B 是秩为 5 的 6×5 阶矩阵，C 是秩为 $4k-6$ 的 $(4k-6)\times(4k-6)$ 阶矩阵。于是，A 的任意 $(4k)\times(4k-1)$ 阶子矩阵 A' 的秩为 $4k-1$，这等价于说任何不饱和集 S_3 满足 $|S_3|\leq 4k-1$.

接下来我们考虑 A 的任意 $(4k-1)\times(4k-1)$ 阶子矩阵 A'，研究它何时会是非满秩的。假定所缺失的三行的指标为 i,j,l. 如果 $|\{i,j,l\}\bigcap\{1,2,3,4\}|=3$，或者如果 $\{i,j\}\subset\{1,2,3,4\}$ 且 $l\in\{7,8\}$，则与上段类似，利用指标为 $\{9,\ldots,4k+2\}$ 的行对矩阵做初等行变换中的消法变换可推出 $rank(A')=4k-1$. 如果 $\{i,j\}\subset\{1,2,3,4\}$ 且 $l\in\{9,\ldots,4k+2\}$，那么在向量选取中不够细致的话，会有 $rank(A')<4k-1$ 的风险。这种潜在的风险仅仅伴随着下面这种情况——当对矩阵做初等行变换，寄希望于尽量将矩阵转化为分块矩阵之时，却不得已地发现，第七与第八行只能被变换为线性相关的两行 $(\mathbf{v},\lambda\mathbf{w})$ 和 $(\gamma\mathbf{v},\tau\mathbf{w})$，其中 $\tau/\lambda=\gamma$，导致了 $rank(A')<4k-1$. 然而，注意到我们之前保持了系数 λ 与 τ 的灵活性，唯一的约束是它们的乘积为固定的常数。那么通过对这两个参数的调节，比如调整为 $\alpha\lambda$ 和 τ/α，则之前的初等行变换过程会将第七与第八行变换为线性无关的两行 $(\mathbf{v},\alpha\lambda\mathbf{w})$ 和 $(\gamma\mathbf{v},\tau/\alpha\mathbf{w})$. 由于三元组 $\{i,j,l\}$ 的数目是有限的，每个选取仅对应于一个对 τ/λ 所禁止的取值，则总共所禁止的取值有限，总可以有合适的调节参数的方式。综上所述，如果 $|S_3|=4k-1$ 则必有 $|\{i,j,l\}\bigcap\{1,2,3,4\}|\leq 1$，等价于 $|S_3\bigcap\{v_1,v_2,v_3,v_4\}|\geq 3$. □

于是，无论怎样选取不饱和集 S_1，S_2 和 S_3，它们的并集将不会是整个点集 V. 不可扩展限定的说明完毕，这组向量构成我们所想要的 UPB，完成了对定理 53 的证明。

作为示例，我们列出 $\mathbb{C}^2\bigotimes\mathbb{C}^2\bigotimes\mathbb{C}^7$ 中的一个大小为 10 的 UPB:

$$\mathbf{v_1}=\mathbf{a}\otimes\mathbf{e}\otimes(1,0,0,0,0,0,0), \qquad \mathbf{v_2}=\mathbf{a}\otimes\mathbf{f}\otimes(0,1,0,0,0,0,0),$$
$$\mathbf{v_3}=\mathbf{b}\otimes\mathbf{e}\otimes(0,0,1,0,0,0,0), \qquad \mathbf{v_4}=\mathbf{b}\otimes\mathbf{f}\otimes(0,0,0,1,0,0,0),$$
$$\mathbf{v_5}=\mathbf{a}^{\perp}\otimes\mathbf{h}\otimes(1,1,0,0,1,0,0), \qquad \mathbf{v_6}=\mathbf{b}^{\perp}\otimes\mathbf{h}^{\perp}\otimes(0,0,1,1,1,0,0),$$
$$\mathbf{v_7}=\mathbf{c}\otimes\mathbf{e}^{\perp}\otimes(1,0,1,0,-1,2,0), \qquad \mathbf{v_8}=\mathbf{d}^{\perp}\otimes\mathbf{f}^{\perp}\otimes(0,1,0,1,-1,-1/2,-1/2),$$
$$\mathbf{v_9}=\mathbf{d}\otimes\mathbf{g}^{\perp}\otimes(0,0,0,0,0,0,1), \qquad \mathbf{v_{10}}=\mathbf{c}^{\perp}\otimes\mathbf{g}\otimes(0,0,0,0,0,1,-1).$$

5.4　图论工具：循环图的连通性和图的 1-因子分解

本小节中我们介绍一些图论相关的工具，以为后文分析 UPB 做好准备。回忆在第 5.2 小节所述的基本思路之中，我们要求恰好一个初始图为 k_i-正则的。在这个图上赋予合适的向量是一个棘手的问题。然而，有一个非常简单的特例。在一个二维的局部空间上，如果点的数目满足 $n = 4k$ 的话，则可以选定一个 2-正则的初始图——k 份 $K_{2,2}$ 的并。为这个初始图赋予向量的方法是显而易见的。利用这张图的话，问题则转化为，可否将一个完全图 K_n 分解成若干个图，其中之一为上述 k 份 $K_{2,2}$ 的并，另外的图的补图皆有良好的连通性质以使得引理 56 可以利用。循环图符合我们的要求。

给定 $\mathbb{Z}_n$ 的一个对称的子集 $S \subseteq \mathbb{Z}_n$（对称的意思是如果 $g \in S$ 那么 $-g \in S$），**循环图** $\Gamma(\mathbb{Z}_n, S)$ 有 n 个顶点，对应于 $\mathbb{Z}_n$ 的各个元素，其中有边 $g \sim h$ 当且仅当 $g - h \in S$. 循环图是正则图，且度数为集合 S 的大小。如果一个循环图的连通度的等于它的度数，则称它**有最大连通性**。一个循环图有最大连通性的充分必要条件由 Boesch 和 Tindell 在[21] Theorem 1 中给出，但是利用他们给的标准来判定一个具体的循环图是否有最大连通性一般是不切实际的，因为他们的标准要对 n 的所有真因子做逐个检验。于是我们需要一些其它判定一个具体的循环图是否有最大连通性的技巧方法。下面的初步结果在[5] 中给出。

引理58. *对于 $2t \leq n$，循环图 $\Gamma(\mathbb{Z}_n, T = \{\pm 1, \ldots, \pm t\})$ 是 $|T|$-连通的。对于 $2t \leq n-3$，循环图 $\Gamma(\mathbb{Z}_n, S = \mathbb{Z}_n \backslash (T \bigcup \{0\}))$ 是 $|S|$-连通的。*

我们接下来给出另外三个有关 $\mathbb{Z}_{4k}$ 上的循环图的连通性的引理，这些都将在接下来主要定理的证明中用到。将点集标记为 $V = \{v_0, v_1, \ldots, v_{4k-1}\}$ 且下文中指标上的加减法都在模 $4k$ 意义下运算。对于一部分点集 $W \subset V$ 和一个整数集合 B，定义 $W + B$ 为 $\{v_{j+b} : v_j \in W, b \in B\}$.

引理59. *对于整数 m 和 p，$1 \leq m$，$p < 2k$，$m < 2k-p$，$m \neq p$，循环图 $\Gamma(\mathbb{Z}_{4k}, \{\pm 1, \ldots, \pm m\} \bigcup \{\pm(2k-p), \ldots, \pm(2k-1), 2k\})$ 是 $(2m + 2p + 1)$-连通的。*

证明. 令 $B = \{\pm 1, \ldots, \pm m\} \bigcup \{\pm(2k-p), \ldots, \pm(2k-1), 2k\} \bigcup \{0\}$. 如果此图非 $(2m+2p+1)$-连通，则存在集合 $W \subset V$ 满足 $W + B \neq \mathbb{Z}_{4k}$，$|W| \geq 2$ 且 $|(W + B) \backslash W| \leq 2m + 2p$. 下面说明这会导致矛盾。

仅证明 $m > p$ 的情况。否则我们可以稍作变动，令 $B' = B + 2k = \{\pm(2k -$

$1),\ldots,\pm(2k-m)\}\bigcup\{\pm p,\ldots,\pm 1,0\}\bigcup\{2k\}$，这样交换了 m 和 p 的角色。由 $|(W+B)\backslash W| = |(W+B')\backslash W|$，则我们可以将以下的分析过程作用于 $(W+B')\backslash W$ 即可。

不失一般性假设 $0\notin(W+B)$. 则 $\{v_1,\ldots,v_m,v_{2k-p},\ldots,v_{2k+p},v_{4k-m},\ldots,v_{4k-1}\}$ 中的每个点都不是 W 中的点。可以找到这样的指标 $m<z<z'<4k-m$ 使得：

- $v_z\in W$ 且对每一个 $m<i<z$，$v_i\notin W$.
- $v_{z'}\in W$ 且对每一个 $z'<j<4k-m$，$v_j\notin W$.

余下的讨论取决于 v_z 和 $v_{z'}$ 的位置，分两种情况进行。

情形1：$m<z<z'<2k-p$，亦即，整个 $\{v_{2k-p},\ldots,v_{4k-1}\}$ 与 W 没有公共点。于是可以找到如下不同的 $(W+B)\backslash W$ 中的点：$\{v_{z-m},\ldots,v_{z-1}\}$，$\{v_{z'+1},\ldots,v_{z'+m}\}$，$\{v_{z'+2k-p},\ldots,v_{z'+2k+p}\}$，共计 $2m+2p+1$ 个点。这即导致了与 $|(W+B)\backslash W|\le 2m+2p$ 的矛盾。对称的另一个情形 $2k+p<z<z'<4k-m$ 同样遵循此分析。

情形2：否则，$m<z<2k-p$ 且 $2k+p<z'<4k-m$. 则可以进一步找到这样的指标 y，$z\le y<2k-p$，$v_y\in W$ 且对任意 $y<j<2k-p$，$v_j\notin W$. 类似地可以找到指标 y'，$2k+p<y'\le z'$，$v_{y'}\in W$ 且对任意 $2k+p<j<y'$，$v_j\notin W$. 于是可以找到如下不同的 $(W+B)\backslash W$ 中的点：$\{v_{z-m},\ldots,v_{z-1}\}$，$\{v_{y+1},\ldots,v_{y+m}\}\bigcup\{v_{y'-m},\ldots,v_{y'-1}\}$，$\{v_{z'+1},\ldots,v_{z'+m}\}$. 其中第二个集合或者包含了 $2m$ 个不同的点（当 $y+m<y'-m$ 时），或者它包含了整段 $\{v_{2k-p},\ldots,v_{2k+p}\}$. 于是我们找到了 $m+\min\{2m,2p+1\}+m>2m+2p$ 个点，再次导致了与 $|(W+B)\backslash W|\le 2m+2p$ 的矛盾。 □

引理60. 对于整数 $1\le m<k-1$，循环图 $\Gamma(\mathbb{Z}_{4k},\{\pm1,\pm2,\ldots,\pm m\}\bigcup\{\pm k\})$ 是 $(2m+2)$-连通的。

证明. 令 $B=\{\pm1,\ldots,\pm m\}\bigcup\{\pm k\}\bigcup\{0\}$. 如果此图非 $(2m+2)$-连通，则存在集合 $W\subset V$ 满足 $W+B\neq\mathbb{Z}_{4k}$，$|W|\ge 2$ 且 $|(W+B)\backslash W|\le 2m+1$. 下面说明这会导致矛盾。

不失一般性假设 $0\notin(W+B)$. 则 $\{v_1,\ldots,v_m,v_k,v_{3k},v_{4k-m},\ldots,v_{4k-1}\}$ 中的每个点都不是 W 中的点。可以找到这样的指标 $m<z<z'<4k-m$ 使得：

- $v_z\in W$ 且对每一个 $m<i<z$，$v_i\notin W$.
- $v_{z'}\in W$ 且对每一个 $z'<j<4k-m$，$v_j\notin W$.

此时我们可以找到 $\{v_{z-m},\ldots,v_{z-1}\}\subset(W+B)\backslash W$ 且 $\{v_{z'+1},\ldots,v_{z'+m}\}\subset(W+B)\backslash W$，共计 $2m$ 个不同的点。如果 $z>k$，则另可以找到 $v_{z-k}\in(W+B)\backslash W$. 否则 $z<k$，那么必存在 v_i，$z<i\le k$，属于 $(W+B)\backslash W$，因为 $v_z\in W$ 且 $v_k\notin W$. 类似地可以找到 $v_{z'+k}$

或者一个点 v_j，$3k \le j < z'$，分别取决于是 $z' < 3k$ 还是 $z' > 3k$. 综上总共找到了至少 $(2m+2)$ 个不同的 $(W+B)\backslash W$ 中的点，导致了与 $|(W+B)\backslash W| \le 2m+1$ 的矛盾。　□

引理61. 对于整数 $0 \le m < k-1$，$0 \le p < k-1$，$m \ne p$，循环图 $\Gamma(\mathbb{Z}_{4k}, \{\pm 1, \ldots, \pm m\} \bigcup \{\pm k\} \bigcup \{\pm(2k-p), \ldots, \pm(2k-1), 2k\})$ 是 $(2m+2p+3)$-连通的。

证明. 令 $B = \{\pm 1, \ldots, \pm m\} \bigcup \{\pm k\} \bigcup \{\pm(2k-p), \ldots, \pm(2k-1), 2k\} \bigcup \{0\}$. 如果此图非 $(2m+2p+3)$-连通，则存在集合 $W \subset V$ 满足 $W + B \ne \mathbb{Z}_{4k}$，$|W| \ge 2$ 且 $|(W+B)\backslash W| \le 2m+2p+2$. 下面说明这会导致矛盾。

仅证明 $m > p$ 的情况。否则我们可以稍作变动，令 $B' = B + 2k$ 以交换了 m 和 p 的角色。由 $|(W+B)\backslash W| = |(W+B')\backslash W|$，则我们可以将以下的分析过程作用于 $(W+B')\backslash W$ 即可。

不失一般性假设 $0 \notin (W+B)$. 则 $\{v_1, \ldots, v_m, v_k, v_{2k-p}, \ldots, v_{2k+p}, v_{3k}, v_{4k-m}, \ldots, v_{4k-1}\}$ 中的每个点都不是 W 中的点。可以找到这样的指标 $m < z < z' < 4k-m$ 使得：

- $v_z \in W$ 且对每一个 $m < i < z$，$v_i \notin W$.
- $v_{z'} \in W$ 且对每一个 $z' < j < 4k-m$，$v_j \notin W$.

余下的讨论取决于 v_z 和 $v_{z'}$ 的位置，分两种情况进行。

情形1：$m < z < z' < 2k-p$，亦即，整个 $\{v_{2k-p}, \ldots, v_{4k-1}\}$ 与 W 没有公共点。于是可以找到如下不同的 $(W+B)\backslash W$ 中的点：$\{v_{z-m}, \ldots, v_{z-1}\}$, $\{v_{z'+1}, \ldots, v_{z'+m}\}$，$v_{z'+k}$，$\{v_{z'+2k-p}, \ldots, v_{z'+2k+p}\}$，共计 $2m+2p+2$ 个点。另一个点可以被选取为 v_{z-k}（如果 $k < z < z' < 2k-p$）或者 $v_{z'+3k}$（如果 $m < z < z' < k$）再或者某个 v_j，$z < j < z'$（如果 $m < z < k < z' < 2k-p$）。对称的另一个情形 $2k+p < z < z' < 4k-m$ 同样遵循此分析。

情形2：否则，$m < z < 2k-p$ 且 $2k+p < z' < 4k-m$. 则可以进一步找到这样的指标 y，$z \le y < 2k-p$，$v_y \in W$ 且对任意 $y < j < 2k-p$，$v_j \notin W$. 类似地可以找到指标 y'，$2k+p < y' \le z'$，$v_{y'} \in W$ 且对任意 $2k+p < j < y'$，$v_j \notin W$. 于是可以找到如下不同的 $(W+B)\backslash W$ 中的点：$\{v_{z-m}, \ldots, v_{z-1}\}$，$\{v_{z'+1}, \ldots, v_{z'+m}\}$，$A = \{v_{y+1}, \ldots, v_{y+m}\} \bigcup \{v_{y'-m}, \ldots, v_{y'-1}\}$.

当 $|A| \ge 2p+2$ 时，只需再额外找到 $(W+B)\backslash W$ 中的一个点。这个点可以被选取为 v_{z-k}（如果 $k < z$）或者某个 v_j，$z < j < y$（如果 $z < k < y$）或者 $v_{z'+k}$（如果 $z' < 3k$）或者某个 $v_{j'}$，$y' < j' < z'$（如果 $y' < 3k < z'$）再或者 v_{z+k}（在之前范围之外，则有 $z < y < k$ 且 $3k < y' < z'$，v_{z+k} 这个点并不包含在之前所取的点中，因为 $y+m < z+k < y'-m$）。

当 $|A| = 2p+1$ 时，这仅仅在 $y = 2k-p-1$ 且 $y' = 2k+p+1$ 时才会发生。此时需要再额外找到 $(W+B)\backslash W$ 中的两个点。其一可以为 v_{z-k}（如果 $k < z$）或者某个 v_j，$z < j < y$（如果 $z < k < y$）。其二可以为 $v_{z'+k}$（如果 $z' < 3k$）或者某个 $v_{j'}$，$y' < j' < z'$（如果 $y' < 3k < z'$）。

综上总共找到了至少 $(2m+2p+3)$ 个不同的 $(W+B)\backslash W$ 中的点，导致了与 $|(W+B)\backslash W| \leq 2m+2p+2$ 的矛盾。 □

在预备好这些与循环图连通性相关的结论之后，我们离完全准备好进行定理 54 和 55 的证明只差一步。最后的预备内容是关于图的 1-因子分解。对于有 $2n$ 个顶点的图 $G = (V, E)$，它的一个 **1-因子**（亦称为一个完美匹配）是 G 中的 n 条两两无公共点的边。G 的 **1-因子分解**是指将整个边集 E 分解为不交并 $\{E_1, \ldots, E_l\}$ 使得每个 E_i 都是图 G 的一个 1-因子。在[61] 中指出，当问题中有多个二维的局部空间时，1-因子分解是分析 UPB 的一个方便的工具，因为一个 1-因子可以用来做某个二维局部空间的初始图。我们需要下述引理。

引理62. [116] *对每个偶数阶的阿贝尔群 G 和它的任何对称子群 S，凯莱图 $\Gamma(G, S)$ 有 1-因子分解。*

5.5 定理 54 和 55 的证明

本小节中，我们将利用之前讨论的构造 UPB 的基本思路，以及上一小节中的图论工具，来证明定理 54 和 55.

定理 54 的证明. 令 $t+s+1 = 4k$. 对一个特殊的二维局部空间，选取初始图为 $\Gamma(Z_{4k}, \{\pm k\})$，这恰好是 k 份 $K_{2,2}$ 的并。令 H 为局部空间 $\mathbb{C}^s$ 的初始图。我们首先考虑 t 是奇数 s 是偶数这一情形。令 $p = \frac{t+1}{2}$.

如果 $p+1 > k$，选取 H 为 $\Gamma(\mathbb{Z}_{4k}, \{\pm(p+1), \ldots, \pm(2k-1), 2k\})$，它与 $\Gamma(Z_{4k}, \{\pm k\})$ 的边并不重复。由引理 58，其补图 $\overline{H} = \Gamma(Z_{4k}, \{\pm 1, \ldots, \pm p\})$ 是 $(t+1)$-连通的，于是再由引理 56，我们可以找到 $\overline{H}$ 在 $\mathbb{R}^s$ 上的一个正交表示，且保证任意 s 个向量是线性无关的。其它的二维空间的初始图之并即为 $\Gamma(Z_{4k}, \{\pm 1, \pm 2, \ldots, \pm(k-1), \pm(k+1), \ldots, \pm p\})$. 这一点是可行的，因为由引理 62 此图可以拆分为 $t-1$ 份 1-因子。不可扩展限定是满足的，因为：对于特殊的那个二维局部空间，一个不饱和集的大小至多为 2；s 维的局部空间上的

不饱和集的大小至多为 $s-1$；其它二维空间上，每个不饱和集都仅是单点集。于是无论怎样选取这些不饱和集，它们的并集的大小至多为 $t+s$.

如果 $p+1\leq k$，选取 H 为 $\Gamma(Z_{4k},\{2k,\pm(2k-1),\ldots,\pm(k+1),\pm(k-1),\ldots,\pm p\})$，它与 $\Gamma(Z_{4k},\{\pm k\})$ 的边并不重复。由引理 58，其补图 $\overline{H}=\Gamma(Z_{4k},\{\pm 1,\ldots,\pm(p-1),\pm k\})$ 是 $(t+1)$–连通的，于是再由引理 56，我们可以找到 $\overline{H}$ 在 $\mathbb{R}^s$ 上的一个正交表示，且保证任意 s 个向量是线性无关的。余下的分析同上。

当 t 为偶数 s 为奇数时，令 $q=\frac{s+1}{2}$. 初始图 H 的选取或者是 $\Gamma(Z_{4k},\{\pm 1,\ldots,\pm(q-1)\})$，或者是 $\Gamma(Z_{4k},\{\pm 1,\ldots,\pm(k-1),\pm(k+1),\ldots,\pm q\})$，分别取决于 $q-1<k$ 或者 $q-1\geq k$. 对应的向量赋予将由引理 58，引理 61 和引理 56 所保证。余下的证明同上。 □

定理 55 的证明. 令目标值为 $4k$. 对一个特殊的二维局部空间，选取初始图为 $\Gamma(Z_{4k},\{\pm k\})$，这恰好是 k 份 $K_{2,2}$ 的并。对于维度为 $b=2(p+1)$ 的局部空间，如果 $p<k$ 则选取其初始图为 $\Gamma(\mathbb{Z}_{4k},\{\pm(2k-p),\ldots,\pm(2k-1),2k\})$，否则 $p\geq k$ 时取为 $\Gamma(\mathbb{Z}_{4k},\{\pm(2k-p-1),\ldots,\pm(k-1),\pm(k+1),\pm(2k-1),2k\})$. 对于每一个奇数维度的局部空间，选取其初始图形如 $\Gamma(\mathbb{Z}_{4k},\{\pm a,\pm(a+1),\ldots,\pm(b-1),\pm b\})$，或者不可避免的会有一个初始图形如 $\Gamma(\mathbb{Z}_{4k},\{\pm a,\ldots,\pm(k-1),\pm(k+1),\ldots,\pm b\})$. 保证以上所有图的边没有重复。余下的所有二维局部空间的初始图的并将是之前所选的所有图的并的补图。

对应的向量的赋予以及不可扩展限定的满足将沿用定理 54 的证明思路，并应用引理 56，引理 58，引理 59，引理 60，引理 61 和引理 62. 唯一需要额外注意的是，引理 61 中有着 $m\neq p$ 这一限制。于是，我们不允许有形如 $\Gamma(\mathbb{Z}_{4k},\{\pm m+1,\ldots,\pm(k-1),\pm(k+1),\ldots,\pm(2k-m-1)\})$ 的初始图。在 $a_1,a_2,\ldots,a_k$ 并不完全相同或者 $t\geq 3$ 的时候，容易发现这一点可以通过在初始图的选取之中避免掉。 □

5.6　小结

不可扩展乘积基（UPB）在量子信息中有着广泛的应用。本章中，我们给出了一些关于最小规模 UPB 的大小的新结果。我们首先对于 $f(2,2,4k-1)=4k+2$ 是否成立这一公开问题做出了肯定的回答。之后我们导出了一系列关于某些特殊循环图的连通性的结论，并借助这些结论决定了一系列参数下的最小规模 UPB 的大小的准确值。这些结果或许对各种量子信息的其它理论问题有所帮助。

此问题的难点在于怎样合适选取初始图以及怎样基于初始图所要求的正交关系赋予合适的向量，而对于某个 k 维局部空间上的 k-正则初始图尤其困难。如果有一

个一般性的处理这种初始图上的向量的赋予的方案的话，余下的工作借由引理 56 的辅助将相当简单。比如，我们可以说明 $f(3,4,4) = 10$. 初始图分别选为 $\Gamma(\mathbb{Z}_{10}, \{\pm 3\})$，$\Gamma(\mathbb{Z}_{10}, \{\pm 4, 5\})$ 和 $\Gamma(\mathbb{Z}_{10}, \{\pm 1, \pm 2\})$. 前两张图上向量的赋予可由引理 56 保证。在第三个局部空间上，向量 $\mathbf{v_1}, \ldots, \mathbf{v_{10}}$ 可以被选取为 $(1,0,0,0)$，$(0,1,0,0)$，$(0,0,1,0)$，$(1,0,0,1)$，$(1,x,0,1)$，$(1,-2/x,-4/x,-1)$，$(3,-1,4-x,3-x)$，$(1,2,-1,1)$，$(0,1,1,-1)$，$(0,0,1,1)$，其中 $x = 3\sqrt{2} - 2$. 这仅仅是一个手工搜索出的结果，更一般的思路有待之后的研究。

6 其它在研问题

本章补充简要介绍在攻读博士学位期间的其它研究工作，这些课题或主题稍偏离于本文所讨论的极值构型问题，或因尚在研究初步阶段而未形成完整的成果。限于篇幅，只对这些课题的进展做简要介绍而不再展开论述。

6.1 字符结对码

字符结对码（Symbol-pair codes）的研究背景源于高密度存储设备的兴起。虽然编码过程仍同于往常，但在高密度存储设备上，读取信息时只对单个位置读取是不便的，自然的推广是将码元成对的进行读取。纠错方式也从原先对单个位置的纠错变为对这样一个读取的序对进行纠错。对此问题的最早研究来自 Cassuto 和 Blaum[32]. Chee 等人[34] 提出了字符结对码的 Singleton 型界，并尝试构造了一些达到此上界的码，称为 MDS 字符结对码。

我们对此问题的贡献为，在极小结对距离 $d = 5$ 时，完整地对所有可行的码长 n 构造了 MDS 字符结对码。另分别通过有限几何的工具和代数曲线的工具，对于极小结对距离 d 取 6 和 7 时也给出了一类新的 MDS 字符结对码的构造。本工作已投稿至《IEEE Transactions on Information Theory》.

6.2 分部重复码

随着便携式互联网设备与移动互联网的快速发展，人们对存储的需求日益增长。作为海量存储的主要解决方案，分布式存储正悄然兴起，它采用可扩展的系统结构，利用多台存储服务器分担存储负荷，利用位置服务器定位存储消息，不仅提高了系统的可靠性、可用性和存储效率，而且易于扩展。同时，分布式存储网络提供地理位置上分散的存储节点，以及对其共享存储访问，降低了数据访问的时延。分布式存储系统通常需要保证两个最基本的性能：数据的耐久性和可用性。数据的耐久性是指在系统中存储的数据不会因为永久的节点故障而导致丢失，诸如磁盘故障等等；而可用性意味着系统将能够及时取回数据对象。分布式存储系统主要依赖数据冗余技术来保证这两个性能，这就带来了许多编码

方面的问题。自 2007 年 Dimakis 等人提出了再生码（Regenerating codes）之后，各种基于不同需求的编码问题层出不穷。

分布重复码（Fractional repetition codes）就是在分布式存储研究中所提出的一种码[55]。在文献[59] 中，Etzion 将此问题转化为如下的一个类似于图兰型问题的极值图论问题：给定整数 $d \geq 3$，$n \geq 3$，$n-1 \leq k \leq \binom{n}{2}$，若一张 $d-$正则的图的任意 n 个顶点所诱导的子图中至多有 k 条边，那么这个图最少要有多少点? 记此最优值为 $\eta(n,d,k)$. 作为对此问题的初步尝试，Etzion 近乎完整解决了 $3 \leq n \leq 5$ 的情形[59]。最小的尚未解决的问题为 $\eta(5,d,5)$.

我们对此问题的贡献是给出了 $\eta(5,d,5)$ 的一些新的结果。主要的方法为构造特殊的循环图，使得图中不出现三角形和非平凡的四边形。这等价于要使得循环图的生成集满足某些类似于差集结构的条件。本工作仍在与 Tuvi Etzion 教授的合作下继续展开中。

6.3 序列的复制距离

序列的复制距离（Duplication distance）的研究背景源于对生物进化过程中 DNA 序列的相关性之间的探索。对任何一个二元序列，一个复制过程是将其内任意一段进行复制之后插入到恰与其相邻的位置，如对 101011 的第三到五位进行复制，得到 101011011. 相反的操作称为一个反复制过程。称一个没有任何相邻两段重复的序列为根序列，在二元意义下仅有 $\{0,1,01,10,010,101\}$. 对任意一个序列 s，记 $f(s)$ 为从其根序列经过一步步复制到形成序列 s 的最小步数。对给定的整数 n，$f(n)$ 代表遍历所有 n 长序列 s 中的 $f(s)$ 的最大值。

Bruck 等人对 $f(n)$ 的渐进界的初步研究[3] 将此值确定为 n 的线性级别，$\lim_{n\to\infty}\frac{f(n)}{n}$ 的值被控制在 0.045 和 0.53125 之间。我们对此问题的贡献为设计了两种算法对任意序列 s 估计 $f(s)$ 的上界，进而通过对比两个算法的优劣，建立了一个数学规划问题。最终可将上界修改到 $\frac{1}{3}$. 本工作仍在与 Jehoshua Bruck 教授的合作下继续展开中。

参考文献

[1] M. AJTAI, J. KOMLÓS, J. PINTZ, J. SPENCER, AND E. SZEMERÉDI, *Extremal uncrowded hypergraphs*, J. Combin. Theory Ser. A, 32 (1982), pp. 321–335.

[2] M. AJTAI, J. KOMLÓS, AND E. SZEMERÉDI, *A note on Ramsey numbers*, J. Combin. Theory Ser. A, 29 (1980), pp. 354–360.

[3] N. ALON, J. BRUCK, F. FARNOUD, AND S. JAIN, *On the duplication distance of binary strings*, preprint.

[4] N. ALON, E. FISCHER, AND M. SZEGEDY, *Parent-identifying codes*, J. Combin. Theory Ser. A, 95 (2001), pp. 349–359.

[5] N. ALON AND L. LOVÁSZ, *Unextendible product bases*, J. Combin. Theory Ser. A, 95 (2001), pp. 169–179.

[6] M. ATICI, S. S. MAGLIVERAS, D. R. STINSON, AND W.-D. WEI, *Some recursive constructions for perfect hash families*, J. Combin. Des., 4 (1996), pp. 353–363.

[7] R. AUGUSIAK, T. FRITZ, M. KOTOWSKI, M. KOTOWSKI, M. PAWŁOWSKI, M. LEWENSTEIN, AND A. ACÍN, *Tight bell inequalities with no quantum violation from qubit unextendible product bases*, Physical Review A, 85 (2012), p. 042113.

[8] R. AUGUSIAK, J. STASIŃSKA, C. HADLEY, J. KORBICZ, M. LEWENSTEIN, AND A. ACÍN, *Bell inequalities with no quantum violation and unextendable product bases*, Physical review letters, 107 (2011), p. 070401.

[9] A. BARG AND G. KABATIANSKY, *A class of I.P.P. codes with efficient identification*, J. Complexity, 20 (2004), pp. 137–147.

[10] A. BARG AND A. MAZUMDAR, *Codes in permutations and error correction for rank modulation*, IEEE Trans. Inform. Theory, 56 (2010), pp. 3158–3165.

[11] S. G. BARWICK, W.-A. JACKSON, AND C. T. QUINN, *Optimal linear perfect hash families with small parameters*, J. Combin. Des., 12 (2004), pp. 311–324.

[12] M. BAZRAFSHAN AND T. VAN TRUNG, *Bounds for separating hash families*, J. Combin. Theory Ser. A, 118 (2011), pp. 1129–1135.

[13] ——, *Improved bounds for separating hash families*, Des. Codes Cryptogr., 69 (2013), pp. 369–382.

[14] C. H. BENNETT, D. P. DIVINCENZO, C. A. FUCHS, T. MOR, E. RAINS, P. W. SHOR, J. A. SMOLIN, AND W. K. WOOTTERS, *Quantum nonlocality without entanglement*, Phys. Rev. A (3), 59 (1999), pp. 1070–1091.

[15] C. H. BENNETT, D. P. DIVINCENZO, T. MOR, P. W. SHOR, J. A. SMOLIN, AND B. M. TERHAL, *Unextendible product bases and bound entanglement*, Phys. Rev. Lett., 82 (1999), pp. 5385–5388.

[16] B. C. BERNDT, R. J. EVANS, AND K. S. WILLIAMS, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998.

[17] S. R. BLACKBURN, *Perfect hash families: probabilistic methods and explicit constructions*, J. Combin. Theory Ser. A, 92 (2000), pp. 54–60.

[18] ——, *Frameproof codes*, SIAM J. Discrete Math., 16 (2003), pp. 499–510.

[19] S. R. BLACKBURN, T. ETZION, D. R. STINSON, AND G. M. ZAVERUCHA, *A bound on the size of separating hash families*, J. Combin. Theory Ser. A, 115 (2008), pp. 1246–1256.

[20] S. R. BLACKBURN AND P. R. WILD, *Optimal linear perfect hash families*, J. Combin. Theory Ser. A, 83 (1998), pp. 233–250.

[21] F. BOESCH AND R. TINDELL, *Circulants and their connectivities*, J. Graph Theory, 8 (1984), pp. 487–499.

[22] M. BOGAERTS, *Isometries and construction of permutation arrays*, IEEE Trans. Inform. Theory, 56 (2010), pp. 3177–3179.

[23] ——, *New upper bounds for the size of permutation codes via linear programming*, Electron. J. Combin., 17 (2010), pp. Research Paper 135, 9.

[24] M. BOGAERTS AND P. DUKES, *Semidefinite programming for permutation codes*, Discrete Math., 326 (2014), pp. 34–43.

[25] D. BONEH AND J. SHAW, *Collusion-secure fingerprinting for digital data*, IEEE Trans. Inform. Theory, 44 (1998), pp. 1897–1905.

[26] R. C. BOSE AND S. CHOWLA, *Theorems in the additive theory of numbers*, Comment. Math. Helv., 37 (1962/1963), pp. 141–147.

[27] S. BUZAGLO AND T. ETZION, *Bounds on the size of permutation codes with the Kendall τ-metric*, IEEE Trans. Inform. Theory, 61 (2015), pp. 3241–3250.

[28] S. BUZAGLO, E. YAAKOBI, T. ETZION, AND J. BRUCK, *Systematic codes for rank modulation*, in Information Theory (ISIT), 2014 IEEE International Symposium on, IEEE, 2014, pp. 2386–2390.

[29] P. J. CAMERON AND I. M. WANLESS, *Covering radius for sets of permutations*, Discrete Math., 293 (2005), pp. 91–109.

[30] V. CANDA AND T. VAN TRUNG, *A new mode of using all-or-nothing transforms*, in ISIT, 2002, p. 296.

[31] R. G. CASCELLA, Z. CAO, M. GERLA, B. CRISPO, AND R. BATTITI, *Weak data secrecy via obfuscation in network coding based content distribution*, in Wireless Days, 2008, pp. 1–5.

[32] Y. CASSUTO AND M. BLAUM, *Codes for symbol-pair read channels*, IEEE Trans. Inform. Theory, 57 (2011), pp. 8011–8020.

[33] P. L. ČEBYŠEV, *Mémoire sur les nombres premiers*, Académie Impériale des Sciences, 1850.

[34] Y. M. CHEE, L. JI, H. M. KIAH, C. WANG, AND J. YIN, *Maximum distance separable codes for symbol-pair read channels*, IEEE Trans. Inform. Theory, 59 (2013), pp. 7259–7267.

[35] Y. M. CHEE AND X. ZHANG, *Improved constructions of frameproof codes*, IEEE Trans. Inform. Theory, 58 (2012), pp. 5449–5453.

[36] J. CHEN AND N. JOHNSTON, *The minimum size of unextendible product bases in the bipartite case (and some multipartite cases)*, Comm. Math. Phys., 333 (2015), pp. 351–365.

[37] M. CHENG, L. JI, AND Y. MIAO, *Separable codes*, IEEE Trans. Inform. Theory, 58 (2012), pp. 1791–1803.

[38] W. CHU, C. J. COLBOURN, AND P. DUKES, *Constructions for permutation codes in powerline communications*, Des. Codes Cryptogr., 32 (2004), pp. 51–64.

[39] G. D. COHEN, S. ENCHEVA, S. LITSYN, AND H. G. SCHAATHUN, *Intersecting codes and separating codes*, Discrete Appl. Math., 128 (2003), pp. 75–83. International Workshop on Coding and Cryptography (WCC 2001) (Paris).

[40] G. D. COHEN AND H. G. SCHAATHUN, *Upper bounds on separating codes*, IEEE Trans. Inform. Theory, 50 (2004), pp. 1291–1295.

[41] C. J. COLBOURN, T. KLØVE, AND A. C. H. LING, *Permutation arrays for powerline communication and mutually orthogonal Latin squares*, IEEE Trans. Inform. Theory, 50 (2004), pp. 1289–1291.

[42] C. COOPER, *On the rank of random matrices*, Random Structures Algorithms, 16 (2000), pp. 209–232.

[43] P. D'ARCO, N. N. ESFAHAN, AND D. R. STINSON, *All or nothing at all*, arXiv:1510.03655, (2015).

[44] D. R. DE LA TORRE, C. J. COLBOURN, AND A. C. H. LING, *An application of permutation arrays to block ciphers*, Congr Numer, (2000), pp. 5–7.

[45] A. DESAI, *The security of all-or-nothing encryption: Protecting against exhaustive key search*, in Advances in Cryptology (CRYPTO 2000), Springer, 2000, pp. 359–375.

[46] M. DEZA AND T. HUANG, *Metrics on permutations, a survey*, J. Combin. Inform. System Sci., 23 (1998), pp. 173–185.

[47] M. DEZA AND S. A. VANSTONE, *Bounds for permutation arrays*, J. Statist. Plann. Inference, 2 (1978), pp. 197–209.

[48] A. DHARWADKER, *The independent set algorithm*, 2006.

[49] C. DING, F.-W. FU, T. KLØVE, AND V. K.-W. WEI, *Constructions of permutation arrays*, IEEE Trans. Inform. Theory, 48 (2002), pp. 977–980.

[50] J. H. DINITZ, A. C. H. LING, AND D. R. STINSON, *Perfect hash families from transversal designs*, Australas. J. Combin., 37 (2007), pp. 233–242.

[51] D. P. DIVINCENZO, T. MOR, P. W. SHOR, J. A. SMOLIN, AND B. M. TERHAL, *Unextendible product bases, uncompletable product bases and bound entanglement*, Comm. Math. Phys., 238 (2003), pp. 379–410.

[52] R. DUAN, Y. XIN, AND M. YING, *Locally indistinguishable subspaces spanned by three-qubit unextendible product bases*, Physical Review A, 81 (2010), p. 032329.

[53] R. A. DUKE, H. LEFMANN, AND V. RÖDL, *On uncrowded hypergraphs*, in Proceedings of the Sixth International Seminar on Random Graphs and Probabilistic Methods in Combinatorics and Computer Science, vol. 6, 1995, pp. 209–212.

[54] P. DUKES AND N. SAWCHUCK, *Bounds on permutation codes of distance four*, J. Algebraic Combin., 31 (2010), pp. 143–158.

[55] S. EL ROUAYHEB AND K. RAMCHANDRAN, *Fractional repetition codes for repair in distributed storage systems*, in 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton), IEEE, 2010, pp. 1510–1517.

[56] E. EN GAD, M. LANGBERG, M. SCHWARTZ, AND J. BRUCK, *Generalized gray codes for local rank modulation*, IEEE Trans. Inform. Theory, 59 (2013), pp. 6664–6673.

[57] S. ENCHEVA AND G. D. COHEN, *Some new p-ary two-secure frameproof codes*, Appl. Math. Lett., 14 (2001), pp. 177–182.

[58] ——, *Frameproof codes against limited coalitions of pirates*, Theoret. Comput. Sci., 273 (2002), pp. 295–304.

[59] T. ETZION, *Regular graphs with forbidden subgraphs of K_n with k edges*, arXiv preprint arXiv:1509.03072, (2015).

[60] F. FARNOUD, V. SKACHEK, AND O. MILENKOVIC, *Error-correction in flash memories via codes in the Ulam metric*, IEEE Trans. Inform. Theory, 59 (2013), pp. 3003–3020.

[61] K. FENG, *Unextendible product bases and 1-factorization of complete graphs*, Discrete Appl. Math., 154 (2006), pp. 942–949.

[62] H. C. FERREIRA AND A. J. H. VINCK, *Interference cancellation with permutation trellis codes*, in IEEE-VTS Fall VTC 2000. 52nd, 2000, pp. 2401–2407.

[63] P. FRANKL AND M. DEZA, *On the maximum number of permutations with given maximal or minimal distance*, J. Combin. Theory Ser. A, 22 (1977), pp. 352–360.

[64] F.-W. FU AND T. KLØVE, *Two constructions of permutation arrays*, IEEE Trans. Inform. Theory, 50 (2004), pp. 881–883.

[65] F. GAO AND G. GE, *New bounds on separable codes for multimedia fingerprinting*, IEEE Trans. Inform. Theory, 60 (2014), pp. 5257–5262.

[66] F. GAO, Y. YANG, AND G. GE, *An improvement on the Gilbert-Varshamov bound for permutation codes*, IEEE Trans. Inform. Theory, 59 (2013), pp. 3059–3063.

[67] E. N. GILBERT, *A comparison of signalling alphabets*, Bell System Technical Journal, 31 (1952), pp. 504–522.

[68] C. GODSIL AND G. ROYLE, *Algebraic graph theory*, vol. 207 of Graduate Texts in Mathematics, Springer-Verlag, New York, 2001.

[69] F. GRAY, *Pulse code communication*, Mar. 17 1953. US Patent 2,632,058.

[70] Q. GUO, M. LUO, L. LI, AND Y. YANG, *Secure network coding against wiretapping and byzantine attacks*, EURASIP Journal on Wireless Communications and Networking, 2010 (2010), p. 17.

[71] H. 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.

[72] A. E. HOLROYD, *Perfect snake-in-the-box codes for rank modulation*, arXiv preprint arXiv:1602.08073, (2016).

[73] M. HOROVITZ AND T. ETZION, *Constructions of snake-in-the-box codes for rank modulation*, IEEE Trans. Inform. Theory, 60 (2014), pp. 7016–7025.

[74] Y.-Y. HUANG, S.-C. TSAI, AND H.-L. WU, *On the construction of permutation arrays via mappings from binary vectors to permutations*, Des. Codes Cryptogr., 40 (2006), pp. 139–155.

[75] I. JANISZCZAK, W. LEMPKEN, P. R. J. ÖSTERGÅRD, AND R. STASZEWSKI, *Permutation codes invariant under isometries*, Des. Codes Cryptogr., 75 (2015), pp. 497–507.

[76] A. JIANG, R. MATEESCU, M. SCHWARTZ, AND J. BRUCK, *Rank modulation for flash memories*, IEEE Trans. Inform. Theory, 55 (2009), pp. 2659–2673.

[77] A. JIANG, M. SCHWARTZ, AND J. BRUCK, *Correcting charge-constrained errors in the rank-modulation scheme*, IEEE Trans. Inform. Theory, 56 (2010), pp. 2112–2120.

[78] T. JIANG AND A. VARDY, *Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes*, IEEE Trans. Inform. Theory, 50 (2004), pp. 1655–1664.

[79] L. JIN, *A construction of permutation codes from rational function fields and improvement to the gilbert-varshamov bound*, IEEE Trans. Inform. Theory, 62 (2016), pp. 159–162.

[80] N. JOHNSTON, *The minimum size of qubit unextendible product bases*, in 8th Conference on the Theory of Quantum Computation, Communication and Cryptography, vol. 22 of LIPIcs. Leibniz Int. Proc. Inform., Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2013, pp. 93–105.

[81] ——, *The structure of qubit unextendible product bases*, J. Phys. A, 47 (2014), pp. 424034, 19.

[82] P. KEEVASH AND C. Y. KU, *A random construction for permutation codes and the covering radius*, Des. Codes Cryptogr., 41 (2006), pp. 79–86.

[83] M. KENDALL AND J. D. GIBBONS, *Rank correlation methods*, A Charles Griffin Title, Edward Arnold, London, fifth ed., 1990.

[84] T. KLØVE, T.-T. LIN, S.-C. TSAI, AND W.-G. TZENG, *Permutation arrays under the Chebyshev distance*, IEEE Trans. Inform. Theory, 56 (2010), pp. 2611–2617.

[85] A. KOSTOCHKA, D. MUBAYI, AND J. VERSTRAËTE, *On independent sets in hypergraphs*, Random Structures Algorithms, 44 (2014), pp. 224–239.

[86] P. A. LEONARD AND K. S. WILLIAMS, *A Diophantine system of Dickson*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8), 56 (1974), pp. 145–150.

[87] ——, *The cyclotomic numbers of order seven*, Proc. Amer. Math. Soc., 51 (1975), pp. 295–300.

[88] P. C. LI, G. H. J. VAN REES, AND R. WEI, *Constructions of 2-cover-free families and related separating hash families*, J. Combin. Des., 14 (2006), pp. 423–440.

[89] Y. LI AND C. C. ROUSSEAU, *On book-complete graph Ramsey numbers*, J. Combin. Theory Ser. B, 68 (1996), pp. 36–44.

[90] F. LIM AND M. HAGIWARA, *Linear programming upper bounds on permutation code sizes from coherent configurations related to the kendall-tau distance metric*, in Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on, IEEE, 2012, pp. 2998–3002.

[91] J. LIU, H. WANG, M. XIAN, AND K. HUANG, *A secure and efficient scheme for cloud storage against eavesdropper*, in Information and Communications Security, Springer, 2013, pp. 75–89.

[92] L. LOVÁSZ, *On the Shannon capacity of a graph*, IEEE Trans. Inform. Theory, 25 (1979), pp. 1–7.

[93] L. LOVÁSZ, M. SAKS, AND A. SCHRIJVER, *Orthogonal representations and connectivity of graphs*, Linear Algebra Appl., 114/115 (1989), pp. 439–454.

[94] F. J. MACWILLIAMS AND N. J. A. SLOANE, *The theory of error-correcting codes*, 9 (1977), pp. 198–205.

[95] A. MAZUMDAR, A. BARG, AND G. ZÉMOR, *Constructions of rank modulation codes*, IEEE Trans. Inform. Theory, 59 (2013), pp. 1018–1029.

[96] K. MEHLHORN, *Data structures and algorithms. 1*, EATCS Monographs on Theoretical Computer Science, Springer-Verlag, Berlin, 1984.

[97] N. PAVLIDOU, A. J. H. VINCK, J. YAZDANI, AND B. HONARY, *Power line communications: State of the art and future trends*, IEEE Communications Magazine, 41 (2003), pp. 34–40.

[98] K. T. PHELPS AND V. RÖDL, *Steiner triple systems with minimum independence number*, Ars Combin., 21 (1986), pp. 167–172.

[99] A. PROANO AND L. LAZOS, *Packet-hiding methods for preventing selective jamming attacks*, IEEE Trans. Dependable Secure Comput., 9 (2012), pp. 101–114.

[100] J. RESCH AND J. PLANK, *AONT-RS: Blending security and performance in dispersed storage systems*, in Proc. 9th USENIX Conference on File and Storage Technologies (FAST), 2011, pp. 191–202.

[101] R. L. RIVEST, *All-or-nothing encryption and the package transform*, in Fast Software Encryption, Springer, 1997, pp. 210–218.

[102] P. SARKAR AND D. R. STINSON, *Frameproof and IPP codes*, in Progress in cryptology—INDOCRYPT 2001 (Chennai), vol. 2247 of Lecture Notes in Comput. Sci., Springer, Berlin, 2001, pp. 117–126.

[103] C. SAVAGE, *A survey of combinatorial Gray codes*, SIAM Rev., 39 (1997), pp. 605–629.

[104] H. G. SCHAATHUN AND G. D. COHEN, *A trellis-based bound on* $(2, 1)$*-separating codes*, in Cryptography and coding, vol. 3796 of Lecture Notes in Comput. Sci., Springer, Berlin, 2005, pp. 59–67.

[105] Ł. SKOWRONEK, *Three-by-three bound entanglement with general unextendible product bases*, J. Math. Phys., 52 (2011), pp. 122202, 32.

[106] D. H. SMITH AND R. MONTEMANNI, *A new table of permutation codes*, Des. Codes Cryptogr., 63 (2012), pp. 241–253.

[107] ——, *Permutation codes with specified packing radius*, Des. Codes Cryptogr., 69 (2013), pp. 95–106.

[108] P. Ø. SOLLID, J. M. LEINAAS, AND J. MYRHEIM, *Unextendible product bases and extremal density matrices with positive partial transpose*, Physical Review A, 84 (2011), p. 042325.

[109] Y.-J. SONG, K.-Y. PARK, AND J.-M. KANG, *The method of protecting privacy capable of distributing and storing of data efficiently for cloud computing environment*, in Computers, Networks, Systems and Industrial Engineering, 2011, pp. 258–262.

[110] 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.

[111] D. R. STINSON, *Something about all or nothing (transforms)*, Des. Codes Cryptogr., 22 (2001), pp. 133–138.

[112] D. R. STINSON, T. VAN 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.

[113] D. R. STINSON, R. WEI, AND K. CHEN, *On generalized separating hash families*, J. Combin. Theory Ser. A, 115 (2008), pp. 105–120.

[114] D. R. STINSON, R. WEI, AND L. ZHU, *New constructions for perfect hash families and related structures using combinatorial designs and codes*, J. Combin. Des., 8 (2000), pp. 189–200.

[115] D. R. STINSON AND G. M. ZAVERUCHA, *Some improved bounds for secure frameproof codes and related separating hash families*, IEEE Trans. Inform. Theory, 54 (2008), pp. 2508–2514.

[116] R. A. STONG, *On* 1*-factorizability of Cayley graphs*, J. Combin. Theory Ser. B, 39 (1985), pp. 298–307.

[117] M. TAIT, A. VARDY, AND J. VERSTRAETE, *Asymptotic improvement of the gilbert-varshamov bound on the size of permutation codes*, arXiv preprint arXiv:1311.4925, (2013).

[118] I. TAMO AND M. SCHWARTZ, *Correcting limited-magnitude errors in the rank-modulation scheme*, IEEE Trans. Inform. Theory, 56 (2010), pp. 2551–2560.

[119] H. TARNANEN, *Upper bounds on permutation codes via linear programming*, European J. Combin., 20 (1999), pp. 101–114.

[120] B. M. TERHAL, *A family of indecomposable positive linear maps based on entangled quantum states*, Linear Algebra and its Applications, 323 (2001), pp. 61–73.

[121] D. TONIEN AND R. SAFAVI-NAINI, *Recursive constructions of secure codes and hash families using difference function families*, J. Combin. Theory Ser. A, 113 (2006), pp. 664–674.

[122] T. VAN TRUNG AND S. MARTIROSYAN, *New constructions for IPP codes*, Des. Codes Cryptogr., 35 (2005), pp. 227–239.

[123] R. R. VARSHAMOV, *Estimate of the number of signals in error correcting codes*, Doklady Akademii Nauk Sssr, 117 (1957), pp. 739–741.

[124] R. VASUDEVAN, A. ABRAHAM, AND S. SANYAL, *A novel scheme for secured data transfer over computer networks*, Journal of Universal Computer Science, 11 (2005), pp. 104–121.

[125] A. J. H. VINCK, *Coded modulation for power line communications*, in AE Int. J. Electron. and Commun, 2011, pp. 45–49.

[126] V. VU AND L. WU, *Improving the Gilbert-Varshamov bound for q-ary codes*, IEEE Trans. Inform. Theory, 51 (2005), pp. 3200–3208.

[127] H. WANG AND C. XING, *Explicit constructions of perfect hash families from algebraic curves over finite fields*, J. Combin. Theory Ser. A, 93 (2001), pp. 112–124.

[128] X. WANG AND F.-W. FU, *Constructions of snake-in-the-box codes under l_∞-metric for rank modulation*, arXiv preprint arXiv:1601.05539, (2016).

[129] Z. WANG AND J. BRUCK, *Partial rank modulation for flash memories*, in Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on, IEEE, 2010, pp. 864–868.

[130] C. XING, *Asymptotic bounds on frameproof codes*, IEEE Trans. Inform. Theory, 48 (2002), pp. 2991–2995.

[131] Y. YEHEZKEALLY AND M. SCHWARTZ, *Snake-in-the-box codes for rank modulation*, IEEE Trans. Inform. Theory, 58 (2012), pp. 5471–5483.

[132] H. ZHOU, M. SCHWARTZ, A. JIANG, AND J. BRUCK, *Systematic error-correcting codes for rank modulation*, IEEE Trans. Inform. Theory, 61 (2015), pp. 17–32.

作者简历

- 张一炜，男，浙江大学数学科学学院博士生，导师：葛根年.
- 通信地址：中国浙江省杭州市浙江大学玉泉校区数学科学学院，310027.
- 联系方式：(+86)18811713631，rexzyw@163.com
- 教育经历：

  2007.9–2011.6，浙江大学竺可桢学院，浙江大学数学科学学院，数学与应用数学专业，理学学士.

  2011.9–今，浙江大学数学科学学院，应用数学专业，理学博士，研究方向：组合数学与编码密码学.
- 研究兴趣：极值组合学，组合设计，编码理论.

攻读博士学位期间主要研究成果

1. Yiwei Zhang, Gennian Ge (2015), "Snake-in-the-box codes for rank modulation under Kendall's τ-metric", IEEE Transactions on Information Theory, vol. 62, no. 1, pp. 151-158, Jan. 2016. (**ZJU TOP100**)

2. Xin Wang, Yiwei Zhang, Yiting Yang, Gennian Ge (2015), "New bounds of permutation codes under Hamming metric and Kendall's τ-metric", submitted.

3. Yiwei Zhang, Gennian Ge (2015), "Snake-in-the-Box codes for rank modulation under Kendall's τ-metric in S_{2n+2}", submitted.

4. Yiting Yang, Yiwei Zhang, Gennian Ge (2015), "New lower bounds for secure codes and related hash families: a hypergraph theoretical approach", submitted.

5. Yiwei Zhang, Tao Zhang, Xin Wang, Gennian Ge (2015), "Invertible binary matrix with maximum number of 2-by-2 invertible submatrices", submitted.

6. Yiwei Zhang, Yiting Yang, Gennian Ge (2015), "New results on the minimum size of unextendible product bases", submitted.

7. Baokun Ding, Gennian Ge, Jun Zhang, Tao Zhang, Yiwei Zhang (2016), "New constructions of MDS symbol-pair codes", submitted.

8. Yiwei Zhang, Gennian Ge, Tuvi Etzion, "New results on an extremal hypergraph problem related to fractional repetition codes", in preparation.

9. Yiwei Zhang, Gennian Ge, Jehoshua Bruck, "On duplication distances", in preparation.