分类号: O157 密级: 无
单位代码: 10028 学号: 2190501016

首都师范大学博士学位论文

加法组合与离散几何中若干问题的研究

Several problems in additive combinatorics and discrete geometry

研 究 生: 谢城飞

指导教师: 葛根年 教授

学科专业: 应 用 数 学

学科方向: 组合数学与信息安全

2023 年 3 月

首都师范大学学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：

日期：　　年　月　日

首都师范大学学位论文授权使用声明

本人完全了解首都师范大学有关保留、使用学位论文的规定，学校有权保留学位论文并向国家主管部门或其指定机构送交论文的电子版和纸质版。有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅。有权将学位论文的内容编入有关数据库进行检索。有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

学位论文作者签名：

导师签名：

日期：　　年　月　日

摘　要

作为近年来组合数学最活跃的分支之一，加法组合与离散几何受到了广泛关注。处理其中问题的工具涉及数学的各个分支，而其深刻的理论又能应用于其他数学领域。在本学位论文中，我们主要研究了加法组合与离散几何中的问题并做了一定的推进，包括加乘估计问题，球堆积问题，接触数问题，有限域上的相似构型问题。我们使用了许多深刻的数学工具，包括谱图论工具，线性代数方法，编码理论思想等。

在第一章绪论部分，我们将简要介绍本文所研究问题的背景，并总结我们对这些问题所做的推进。

在第二章中，我们考察了有限域上的矩阵环中的加乘估计问题。我们用$M_n(\mathbb{F}_q)$表示$\mathbb{F}_q$上的n阶矩阵的集合。首先，对于$A,B,C\subseteq M_n(\mathbb{F}_q)$，只要$|A||B||C|\gtrsim q^{3n^2-\frac{n+1}{2}}$，就有

$$|A+BC|\gtrsim q^{n^2}。$$

然后，如果$M_n(\mathbb{F}_q)$的子集A满足$|A|\geq C(n)q^{n^2-1}$，其中$C(n)$是一个充分大的常数，那么

$$\max\{|A+A|,|AA|\}\gtrsim \min\left\{\frac{|A|^2}{q^{n^2-\frac{n+1}{4}}},q^{n^2/3}|A|^{2/3}\right\}。$$

这些结论改进了The和Vinh在2020年的结果，并推广了Mohammadi等人在2021年的结果。此外，通过更加细致地考察能量不等式，我们进一步改进了$\max\{|A+A|,|AA|\}$，$|A+BC|$，以及$|A(B+C)|$的下界。我们用到的工具涉及谱图论与线性代数。

在第三章中，我们研究了超球的堆积问题。对于$0=k_1<k_2<\cdots<k_{m+1}=n$，我们定义

$$\left\{\boldsymbol{x}\in\mathbb{R}^n:\sum_{j=1}^{m}\left(x_{k_j+1}^2+x_{k_j+2}^2+\cdots+x_{k_{j+1}}^2\right)^{p/2}\leq r^p\right\}$$

为$\mathbb{R}^n$中半径为r、球心为$\mathbf{0}$的超球。它是ℓ_p球的一种推广。当$1<p\leq 2$时，Schmidt证明了超球的堆积密度为$\Omega(n/2^n)$。后来Rogers和Schmidt分别对常数因子做了改进。我们给出了两种新的证明，证明超球的堆积密度为$\Omega(n/2^n)$。我们的第一个证明基

于刚性超球模型，第二个证明基于图的独立数。我们也研究了堆积的熵密度和压力，这些指标衡量了堆积的丰富程度。

在第四章中，我们研究了ℓ_p球的接触数问题。通过编码理论的思想，我们给出了ℓ_p球的最大接触数新的下界。这些结果改进了Xu在2007年的工作。

在第五章中，我们研究了有限域上的相似构型的问题。设$G = (V, E)$是一个图，其中$V = \{1, 2, \ldots, n\}$，$E \subseteq \binom{V}{2}$。对于$\mathbb{F}_q^d$的子集$\mathcal{E}$，我们称$\mathcal{E}$包含一对相似比为r的图G，如果存在不同的$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in \mathcal{E}$和不同的$\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n \in \mathcal{E}$，使得对任意$\{i, j\} \in E$，都有$\|\boldsymbol{y}_i - \boldsymbol{y}_j\| = r\|\boldsymbol{x}_i - \boldsymbol{x}_j\| \neq 0$，其中对$\boldsymbol{x} = (x_1, x_2, \ldots, x_d) \in \mathbb{F}_q^d$，$\|\boldsymbol{x}\| := x_1^2 + x_2^2 + \cdots + x_d^2$。我们证明了如果$\mathcal{E}$的基数至少为$C_k q^{d/2}$，那么$\mathcal{E}$包含一对相似比为$r$的$k$星；如果$\mathcal{E}$的基数至少为$C \cdot \min\left\{q^{(2d+1)/3}, \max\left\{q^3, q^{d/2}\right\}\right\}$，那么$\mathcal{E}$包含一对相似比为$r$的4长路径。我们的方法基于计数组合与图论。

在第六章中，我们将对其他成果及部分在研问题做简要介绍。

关键词: 加乘估计，有限域，球堆积，刚性超球模型，一致凸性，独立数，接触数，Gilbert-Varshamov型界，相似构型

Abstract

Among the most active branches in combinatorics, additive combinatorics and discrete geometry receive a lot of attention. Dealing with these problems involves several branches in mathematics, and these theories also have wide application in other fields. In this thesis, we mainly investigate several problems in additive combinatorics and discrete geometry, including sum-product estimates, sphere packing, kissing number, similar configurations in finite fields. We use techniques from spectral graph theory, linear algebra, coding theory and so on.

In Chapter 1, we will briefly introduce the backgrounds of problems discussed in this thesis and summarize our main contributions towards these problems.

In Chapter 2, we study some sum-product problems over matrix rings. Let $M_n(\mathbb{F}_q)$ be the set of matrices of order n over $\mathbb{F}_q$. Firstly, for $A, B, C \subseteq M_n(\mathbb{F}_q)$, we have

$$|A + BC| \gtrsim q^{n^2},$$

whenever $|A||B||C| \gtrsim q^{3n^2-\frac{n+1}{2}}$. Secondly, if a set A in $M_n(\mathbb{F}_q)$ satisfies $|A| \geq C(n)q^{n^2-1}$ for some sufficiently large $C(n)$, then we have

$$\max\{|A+A|, |AA|\} \gtrsim \min\left\{\frac{|A|^2}{q^{n^2-\frac{n+1}{4}}}, q^{n^2/3}|A|^{2/3}\right\}.$$

These results improve those of The and Vinh (2020), and generalize those of Mohammadi, Pham, and Wang (2021). Moreover, paying more attention to the energy inequalities, we give further improvement for the lower bounds of $\max\{|A+A|, |AA|\}$, $|A+BC|$, and $|A(B+C)|$. Our method is based on spectral graph theory and linear algebra.

In Chapter 3, we study the superball packing problem. For $0 = k_1 < k_2 < \cdots < k_{m+1} = n$, we define the superball with radius r and center $\mathbf{0}$ in $\mathbb{R}^n$ to be the set

$$\left\{\boldsymbol{x} \in \mathbb{R}^n : \sum_{j=1}^{m}\left(x_{k_j+1}^2 + x_{k_j+2}^2 + \cdots + x_{k_{j+1}}^2\right)^{p/2} \leq r^p\right\},$$

which is a generalization of ℓ_p-balls. We give two new proofs for the celebrated result that for $1 < p \leq 2$, the translative packing density of superballs in $\mathbb{R}^n$ is

$\Omega(n/2^n)$. This bound was first obtained by Schmidt, with subsequent constant factor improvement by Rogers and Schmidt, respectively. Our first proof is based on the hard superball model, and the second proof is based on the independence number of a graph. We also investigate the entropy of packings, which measures how plentiful such packings are.

In Chapter 4, we give new lower bounds for the kissing number of ℓ_p-spheres. These results improve the previous work due to Xu (2007). Our method is based on coding theory.

In Chapter 5, we study problems about the similar configurations in $\mathbb{F}_q^d$. Let $G = (V, E)$ be a graph, where $V = \{1, 2, \ldots, n\}$ and $E \subseteq \binom{V}{2}$. For a set $\mathcal{E}$ in $\mathbb{F}_q^d$, we say that $\mathcal{E}$ contains a pair of G with dilation ratio r if there exist distinct $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in \mathcal{E}$ and distinct $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n \in \mathcal{E}$ such that $\|\boldsymbol{y}_i - \boldsymbol{y}_j\| = r\|\boldsymbol{x}_i - \boldsymbol{x}_j\| \neq 0$ whenever $\{i, j\} \in E$, where $\|\boldsymbol{x}\| := x_1^2 + x_2^2 + \cdots + x_d^2$ for $\boldsymbol{x} = (x_1, x_2, \ldots, x_d) \in \mathbb{F}_q^d$. We show that if $\mathcal{E}$ has size at least $C_k q^{d/2}$, then $\mathcal{E}$ contains a pair of k-stars with dilation ratio r, and that if $\mathcal{E}$ has size at least $C \cdot \min\left\{q^{(2d+1)/3}, \max\left\{q^3, q^{d/2}\right\}\right\}$, then $\mathcal{E}$ contains a pair of 4-paths with dilation ratio r. Our method is based on enumerative combinatorics and graph theory.

In Chapter 6, we briefly introduce several other results including topics still under investigation.

Key words: sum-product estimates, finite field, sphere packing, hard superball model, uniform convexity, independence number, kissing number, Gilbert-Varshamov type bound, similar configurations

目录

摘要 **i**

Abstract **iii**

第 1 章 绪论 **1**

1.1 $M_n(\mathbb{F}_q)$上的加乘估计问题 1

1.2 高维超球堆积密度的下界 5

1.3 高维ℓ_p球的接触数的下界 7

1.4 有限域上的相似图形 8

第 2 章 $M_n(\mathbb{F}_q)$上的加乘估计问题 **11**

2.1 简介 11

2.1.1 初步的改进 12

2.1.2 进一步的改进 13

2.1.3 本章的结构 16

2.2 准备工作 17

2.3 主要引理 18

2.4 定理2.5和2.6的证明 24

2.5 定理2.4的证明 27

2.6 定理2.7和定理2.8的证明 32

2.7 定理2.9的证明 38

2.8 定理2.10的证明 39

第 3 章 高维超球堆积密度的下界 **43**

3.1 简介 43

3.2 一致凸空间 46

3.3 刚性超球模型 52

3.4 定理3.2的另一种证明 63

3.5 熵密度和压力的下界 68

第 4 章 高维ℓ_p球的接触数的下界 **73**

4.1 简介 73
4.2 改进的Gilbert-Varshamov型界 74
4.3 当p比较小时的数值结果 78
4.3.1 r的值 78
4.3.2 $F_p(\sigma)$的渐进行为 79
4.3.3 对于特定的p的数值结果 80
4.4 当p比较大时的数值结果 81
4.4.1 $|J_1'(n,n)|$的改进下界 81
4.4.2 对于特定的p的数值结果 82
4.5 进一步的讨论 83

第 5 章 有限域上的相似图形 **85**

5.1 简介 85
5.2 定理5.5的证明 88
5.3 定理5.6的证明 91
5.3.1 $2 \le d \le 4$的情况 97
5.3.2 $d = 5$的情况 98
5.3.3 $d \ge 6$的情况 99
5.3.4 完成定理5.6的证明 100
5.4 进一步的讨论 103

第 6 章 其他在研问题 **105**

6.1 Grassmannian覆盖码 105
6.2 有限域上的线性空间中的内积链 107
6.3 $(\mathbb{Z}/N\mathbb{Z})^n$上的Furstenberg集 108

参考文献 **111**

致谢 **117**

攻读博士学位期间的研究成果 **119**

第 1 章　绪论

§ 1.1　$M_n(\mathbb{F}_q)$上的加乘估计问题

令$\mathbb{F}_q$为q个元素的域，$M_n(\mathbb{F}_q)$为$\mathbb{F}_q$上所有$n\times n$矩阵构成的环，$Z_n(\mathbb{F}_q)$ 为$\mathbb{F}_q$上所有$n\times n$的不可逆矩阵构成的集合，$GL_n(\mathbb{F}_q)$为$\mathbb{F}_q$上所有$n\times n$的可逆矩阵构成的集合。对于变量X和Y，如果存在一个常数$C(n)$（可能与n有关，但与q无关）使得$X\leq C(n)Y$，那么我们就记作$X\lesssim Y$。如果$X\lesssim Y$且$Y\lesssim X$，那么我们记作$X\sim Y$。对于$A,B\subseteq M_n(\mathbb{F}_q)$，我们定义$A+B=\{a+b:a\in A,b\in B\}$，$AB=\{ab:a\in A,b\in B\}$。

在环R中，设$A\subseteq R$是一个有限集。如果A是一个等差数列，那么一般来说$|A+A|\sim|A|$且$|AA|\sim|A|^2$。如果A是一个等比数列，那么一般来说$|AA|\sim|A|$且$|A+A|\sim|A|^2$。我们观察到$|A+A|$和$|AA|$中似乎总有一个值会比较大（相对于$|A|$）。加乘估计的问题是指在一定条件下估计$\max\{|A+A|,|AA|\}$的下界。在有限域中，我们通常研究两类问题：$|A|$相对于q比较小时估计$\max\{|A+A|,|AA|\}$的下界，以及$|A|$需要多大才能保证$\max\{|A+A|,|AA|\}$相对于q比较大。Bourgain，Katz和Tao[4]证明了当p是素数，并且给定$A\subseteq\mathbb{F}_p$满足$p^\delta<|A|<p^{1-\delta}$时，那么我们有

$$\max\{|A+A|,|AA|\}\geq C_\delta|A|^{1+\epsilon},$$

其中$\epsilon=\epsilon(\delta)$是某个只与$\delta$有关的常数。

最近，Mohammadi和Stevens[52]证明了当$q=p^r$并且$A\subseteq\mathbb{F}_q$满足$|A|\lesssim p^{1/2}$时，有$\max\{|A+A|,|AA|\}\gtrsim|A|^{5/4}$。

在矩阵环中，The和Vinh[78]证明了下列结果。

定理1.1 ([78]). 对任意正整数n, 存在常数$C(n)$使得下述命题成立。若$A \subseteq M_n(\mathbb{F}_q)$满足$|A| \geq C(n)q^{n^2-1}$, 那么我们有

$$\max\{|A+A|, |AA|\} \gtrsim \min\left\{\frac{|A|^2}{q^{n^2-1/2}}, q^{n^2/2}|A|^{1/2}\right\}。$$

定理1.2 ([78]). 对于$A, B, C \subseteq M_n(\mathbb{F}_q)$, 我们有

$$|A+BC| \gtrsim \min\left\{q^{n^2}, \frac{|A||B||C|}{q^{2n^2-1}}\right\}。$$

定理1.3 ([78]). 对于$A \subseteq GL_n(\mathbb{F}_q)$和$B, C \subseteq M_n(\mathbb{F}_q)$, 我们有

$$|A(B+C)| \gtrsim \min\left\{q^{n^2}, \frac{|A||B||C|}{q^{2n^2-1}}\right\}。$$

这些定理的证明用到了图论和线性代数的知识。首先将问题转化为一些能量方程，并将其嵌入到二部图中。使用线性代数的知识可以得出该二部图的一些性质，例如公共邻点。最终得到结果。文献[51, 54, 56]中也有相关结果。

通过考察不同的能量方程，我们给出了加乘估计的一些新结果。

定理1.4. 对于$A, B, C \subseteq M_n(\mathbb{F}_q)$, 我们有

$$|A+BC| \gtrsim \min\left\{q^{n^2}, \frac{|A||B||C|}{q^{2n^2-\frac{n+1}{2}}}\right\}。$$

特别地, 若$|A||B||C| \gtrsim q^{3n^2-\frac{n+1}{2}}$, 那么$|A+BC| \gtrsim q^{n^2}$。

当$|A||B||C| \lesssim q^{3n^2-1}$且$|B|\cdot|C| \gtrsim q^{2n^2-\frac{n+1}{2}}$时，定理1.4的结果比定理1.2更好。

定理1.5. 对于任意正整数n, 存在$C(n)$使得下述命题成立。若$A, B \subseteq M_n(\mathbb{F}_q)$满足$|A| \geq C(n)q^{n^2-1}$, 那么我们有

$$\max\{|A+B|, |AB|\} \gtrsim \min\left\{\frac{|A||B|}{q^{n^2-\frac{n+1}{4}}}, q^{n^2/3}|B|^{2/3}\right\},$$

以及

$$\max\{|A+B|, |BA|\} \gtrsim \min\left\{\frac{|A||B|}{q^{n^2-\frac{n+1}{4}}}, q^{n^2/3}|B|^{2/3}\right\}。$$

在定理1.5中，若取$A=B$，那么我们就得到下列推论。

推论1.1. 对于任意正整数n，存在$C(n)$使得下述命题成立。若$A \subseteq M_n(\mathbb{F}_q)$ 满足$|A| \geq C(n)q^{n^2-1}$，那么我们有

$$\max\{|A+A|, |AA|\} \gtrsim \min\left\{\frac{|A|^2}{q^{n^2-\frac{n+1}{4}}}, q^{n^2/3}|A|^{2/3}\right\}。$$

当$q^{n^2-\frac{n+1}{4}} \lesssim |A| \lesssim q^{n^2-\frac{3}{8}}$且$n \geq 2$时，推论1.1的结果比定理1.1更好。

如果我们更加细致地考察能量不等式，我们可以进一步改进我们的结果。

首先，当$n=2$和$n=3$时，我们可以改进$\max\{|A+B|, |BA|\}$的下界。我们有下列定理。

定理1.6. 存在一个常数C_0使得下述命题成立。设$A, B \subseteq M_2(\mathbb{F}_q)$满足$|A| \geq C_0 q^3$。

- 若$q^{\frac{55}{4}} \lesssim |A|^3|B| \lesssim q^{16}$，那么

$$\max\{|A+B|, |BA|\} \gtrsim q^{\frac{4}{3}}|B|^{\frac{2}{3}}。$$

- 若$|A|^{2+\frac{2}{t_0}}|B| \lesssim q^{9+\frac{19}{2t_0}}$且$|A|^{2+\frac{1}{t_0}}|B| \gtrsim q^{9+\frac{19}{4t_0}}$，那么

$$\max\{|A+B|, |BA|\} \gtrsim \max\left\{\frac{|A||B|}{q^{3+\frac{1}{2t_0}}}, q^{\frac{4}{3t_0}}|A|^{\frac{t_0-1}{3t_0}}|B|^{\frac{2}{3}}\right\},$$

其中$t_0 \geq 2$是2的幂。

定理1.7. 存在一个常数C_0使得下述命题成立。设$A, B \subseteq M_3(\mathbb{F}_q)$满足$|A| \geq C_0 q^8$。

- 若$q^{33} \lesssim |A|^3|B| \lesssim q^{36}$，那么

$$\max\{|A+B|, |BA|\} \gtrsim q^3|B|^{\frac{2}{3}}。$$

- 若$|A|^3|B| \lesssim q^{33}$且$|A|^{10}|B|^4 \gtrsim q^{111}$，那么

$$\max\{|A+B|, |BA|\} \gtrsim \max\left\{\frac{|A||B|}{q^8}, q^{\frac{3}{2}}|A|^{\frac{1}{6}}|B|^{\frac{2}{3}}\right\}。$$

特别地，取$A=B$，那么我们就得到下列推论。

推论1.2. 设C_0是定理*1.6*中的常数，$A \subseteq M_2(\mathbb{F}_q)$满足$|A| \geq C_0 q^3$。

- 若$q^{\frac{55}{16}} \lesssim |A| \lesssim q^4$，那么

$$\max\{|A+A|, |AA|\} \gtrsim q^{\frac{4}{3}}|A|^{\frac{2}{3}}。$$

- 若$q^{\frac{36t_0+19}{12t_0+4}} \lesssim |A| \lesssim q^{\frac{18t_0+19}{6t_0+4}}$，那么

$$\max\{|A+A|, |AA|\} \gtrsim \max\left\{\frac{|A|^2}{q^{3+\frac{1}{2t_0}}}, q^{\frac{4}{3t_0}}|A|^{1-\frac{1}{3t_0}}\right\},$$

其中$t_0 \geq 2$是2的幂。

当$n=2$，$q^3 \lesssim |A| \lesssim q^{\frac{47}{14}}$时，推论1.2给出的$\max\{|A+A|, |AA|\}$的下界比推论1.1更好。当$n=2$，$q^3 \lesssim |A| \lesssim q^{\frac{29}{8}}$时，推论1.2的结果比定理1.1更好。

推论1.3. 设C_0是定理*1.7*中的常数，$A \subseteq M_3(\mathbb{F}_q)$满足$|A| \geq C_0 q^8$。

- 若$q^{\frac{33}{4}} \lesssim |A| \lesssim q^9$，那么

$$\max\{|A+A|, |AA|\} \gtrsim q^3|A|^{\frac{2}{3}}。$$

- 若$q^8 \lesssim |A| \lesssim q^{\frac{33}{4}}$，那么

$$\max\{|A+A|, |AA|\} \gtrsim \max\left\{\frac{|A|^2}{q^8}, q^{\frac{3}{2}}|A|^{\frac{5}{6}}\right\}。$$

当$n=3$，$q^8 \lesssim |A| \lesssim q^{\frac{57}{7}}$时，推论1.3给出的$\max\{|A+A|, |AA|\}$的下界比推论1.1更好。当$n=3$，$q^8 \lesssim |A| \lesssim q^{\frac{69}{8}}$时，推论1.3的结果比定理1.1更好。

接着，我们改进$|A+BC|$的下界，其中$A, B, C \subseteq M_n(\mathbb{F}_q)$。

定理1.8. 对于$A, B, C \subseteq M_n(\mathbb{F}_q)$，我们有

$$|A+BC| \gtrsim \max_{t\text{是2的幂}}\left\{\min\left\{q^{\frac{2n^2}{t}}|A|^{1-\frac{2}{t}}, \frac{|A||B||C|}{q^{2n^2-\frac{(t-1)n+1}{t}}}\right\}\right\}。$$

- 若$|A||B||C| \gtrsim q^{3n^2-\frac{n+1}{2}}$，那么

$$|A+BC| \gtrsim q^{n^2}。$$

- 若$|A|^{\frac{2}{t_0}}|B||C| \lesssim q^{2n^2+\frac{2n^2}{t_0}-\frac{(t_0-1)n+1}{t_0}}$且$|A|^{\frac{1}{t_0}}|B||C| \gtrsim q^{2n^2+\frac{n^2}{t_0}-\frac{(2t_0-1)n+1}{2t_0}}$，那么

$$|A+BC| \gtrsim \max\left\{\frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}, q^{\frac{n^2}{t_0}}|A|^{1-\frac{1}{t_0}}\right\},$$

其中$t_0 \geq 2$是2的幂。

当$|A|^{\frac{1}{2}}|B||C| \lesssim q^{\frac{5n^2-n-1}{2}}$且$|B||C| \gtrsim q^{2n^2-n}$时，定理1.8给出的$|A+BC|$的下界比定理1.4更好。当$|A||B||C| \lesssim q^{3n^2-1}$且$|B||C| \gtrsim q^{2n^2-n}$时，定理1.8的结果比定理1.2更好。

最后，我们改进$|A(B+C)|$的下界，其中$A \subseteq GL_n(\mathbb{F}_q)$，$B, C \subseteq M_n(\mathbb{F}_q)$。

定理1.9. 对于$A \subseteq GL_n(\mathbb{F}_q)$，$B, C \subseteq M_n(\mathbb{F}_q)$我们有

$$|A(B+C)| \gtrsim \max_{t\text{是2的幂}}\left\{\min\left\{q^{\frac{n^2}{t}}|B|^{\frac{1}{2}}|C|^{\frac{1}{2}-\frac{1}{t}}, \frac{|A||B||C|}{q^{2n^2-\frac{(t-1)n+1}{t}}}\right\}\right\}。$$

- 若$|A||B|^{\frac{1}{2}}|C| \gtrsim q^{\frac{5n^2-n-1}{2}}$，那么

$$|A(B+C)| \gtrsim q^{\frac{n^2}{2}}|B|^{\frac{1}{2}}。$$

- 若$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}+\frac{1}{t_0}} \lesssim q^{2n^2+\frac{n^2}{t_0}-\frac{(t_0-1)n+1}{t_0}}$且$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}+\frac{1}{2t_0}} \gtrsim q^{2n^2+\frac{n^2}{2t_0}-\frac{(2t_0-1)n+1}{2t_0}}$，那么

$$|A(B+C)| \gtrsim \max\left\{\frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}, q^{\frac{n^2}{2t_0}}|B|^{\frac{1}{2}}|C|^{\frac{1}{2}-\frac{1}{2t_0}}\right\},$$

其中$t_0 \geq 2$是2的幂。

若对于某个t有$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}+\frac{1}{t}} \lesssim q^{2n^2+\frac{n^2}{t}-1}$，那么定理1.9的结果比定理1.3更好。例如，取$|A| = |B| = |C| \sim q^{n^2-1}$且$t = 2$，此时定理1.3只给出平凡的结果，而定理1.9给出非平凡下界$|A(B+C)| \gtrsim q^{n^2-\frac{1}{2}}$（在$n \geq 10$的时候）。

关于$M_n(\mathbb{F}_q)$上的加乘估计问题，我们共撰写了2篇文章。其中，定理1.4，定理1.5，以及推论1.1已发表在《Finite Fields and Their Applications》。

§1.2 高维超球堆积密度的下界

球堆积（sphere packing）问题指的是如何在空间$\mathbb{R}^n$中最紧密地堆积相同大小的球。这个问题目前已知的确切结果只有1维，2维，3维，8维，以及24维。

令$\Delta_2(n)$为欧几里得空间$\mathbb{R}^n$中相同大小的球的最大平移堆积密度。在高维的情况，$\Delta_2(n)$的最佳上界由Kabatjanskiĭ和Levenšteĭn[36]得到：$\Delta_2(n) \leq 2^{(-0.599\ldots+o(1))n}$。Cohn和Zhao[9]以及Sardari和Zargar[70]进一步改进了常数因子。下界方面，$\Delta_2(n) \geq 2^{-n}$是平凡的。Rogers[60]将下界改进为$n2^{-n}$。Ball[1]构造了密度为$2(n-1)2^{-n}\zeta(n)$的格球堆积。目前已知最佳的下界由Venkatesh[80]得出，为$(65963+o(1))n2^{-n}$。

我们考虑超球的堆积密度。设$k \in \mathbb{N}$，$p \geq 1$为实数。记$\|\cdot\|_2$为ℓ_2范数。再令$\boldsymbol{k}=(k_1,k_2,\ldots,k_{m+1})$满足$0=k_1<k_2<\cdots<k_{m+1}=n$。我们用

$$B^n_{p,\boldsymbol{k}}(\boldsymbol{x},r)=\left\{\boldsymbol{y}:\left(\sum_{j=1}^{m}\left\|\left(x_{k_j+1}-y_{k_j+1},x_{k_j+2}-y_{k_j+2},\ldots,x_{k_{j+1}}-y_{k_{j+1}}\right)\right\|_2^p\right)^{\frac{1}{p}}\leq r\right\}$$

表示$\mathbb{R}^n$中半径为r、球心为$\boldsymbol{x}$的超球，其中$\boldsymbol{x}=(x_1,x_2,\ldots,x_n)$，$\boldsymbol{y}=(y_1,y_2,\ldots,y_n)$。如果超球的球心为原点$\mathbf{0}$，那么我们简记为$B^n_{p,\boldsymbol{k}}(r)=B^n_{p,\boldsymbol{k}}(\mathbf{0},r)$。

假设用于堆积的超球的体积为1，并用$r_{p,\boldsymbol{k},n}$表示体积为1的超球的半径。我们用$\Delta_{p,\boldsymbol{k}}(n)$表示体积为1的超球的最大平移堆积密度，即

$$\Delta_{p,\boldsymbol{k}}(n)=\limsup_{R\to\infty}\sup_{\mathcal{P}}\frac{\mathrm{vol}(\mathcal{P}\cap B^n_{p,\boldsymbol{k}}(R))}{\mathrm{vol}(B^n_{p,\boldsymbol{k}}(R))},$$

其中$\mathrm{vol}(\mathcal{P}\cap B^n_{p,\boldsymbol{k}}(R))$是$B^n_{p,\boldsymbol{k}}(R)$中的被体积为1、球心在$\mathcal{P}$的超球所覆盖的体积，上确界取遍所有的点集$\mathcal{P}\subseteq\mathbb{R}^n$，只要球心在$\mathcal{P}$的超球互不重叠。

特别地，取$\boldsymbol{k}=\boldsymbol{k}_n:=(0,1,2,\ldots,n)$，此时，

$$B^n_{p,\boldsymbol{k}_n}(\boldsymbol{x},r)=\left\{\boldsymbol{y}\in\mathbb{R}^n:\left(\sum_{j=1}^{n}|x_j-y_j|^p\right)^{1/p}\leq r\right\}$$

是$\mathbb{R}^n$中的ℓ_p球。令$\Delta_p(n):=\Delta_{p,\boldsymbol{k}_n}(n)$为$\ell_p$球的最大堆积密度。$\Delta_p(n)$的上界首先由van der Corput和Schaake[79]得到：当$p\geq 2$时，$\Delta_p(n)\leq\frac{1+n/p}{2^{n/p}}$；当$1\leq p\leq 2$时，$\Delta_p(n)\leq\frac{1+(1-1/p)n}{2^{n/p}}$。当$p\geq 1.494\ldots$时，Sah等人[69]做了指数型的改进。Minkowski-Hlawka定理[30]给出了下界$\Delta_{p,\boldsymbol{k}}(n)\geq\zeta(n)2^{-n+1}$，其中$\zeta(n)$是黎曼$\zeta$函数。在$p\geq 3$的情况下，Rush和Sloane[68]改进了$\ell_p$球的Minkowski-Hlawka界，如$\Delta_3(n)\geq 2^{-0.8226\ldots n+o(n)}$。对关于坐标平面对称的任意凸体，Rush[64]构造了密度为$2^{-n+o(n)}$的格堆积。后来，在$p>2$的情况下，Elkies等人[17]对超球的Minkowski-Hlawka界做了指数型的改进。他们的结果也适用于更一般的凸体。Rush[65–67]以及Liu和Xing[50]还尝试用纠错码来构造下界。

我们主要关注$1 < p \leq 2$时的下界。在这种情况下，Minkowski-Hlawka界仍然没有指数型的改进。Rogers[61]得到了$\Omega(\sqrt{n}/2^n)$的下界。Schmidt[71]得到了$\Omega(n/2^n)$的下界。后来，Rogers[62]以及Schmidt[72]分别对常数因子做了改进。目前最佳的结果由Schmidt[73]得到，其中的常数因子为$\log\sqrt{2} \approx 0.346$。我们对$\ell_p$球的堆积密度的下界$\Omega(n/2^n)$给出了两个新的证明。

定理1.10. *对任意$1 < p \leq 2$，存在常数$c_p \in (0,2)$使得*

$$\Delta_p(n) \geq (1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}。$$

事实上，我们的结论对上述定义的超球的堆积密度$\Delta_{p,\boldsymbol{k}}(n)$均成立。

定理1.11. *对任意$p \in (1,2]$，存在常数$c_p \in (0,2)$使得下述命题成立。对任意$\boldsymbol{k} = (k_1, k_2, \ldots, k_{m+1})$满足$k_j \in \mathbb{N}\cup\{0\}$且$0 = k_1 < k_2 < \cdots < k_{m+1} = n$，我们有*

$$\Delta_{p,\boldsymbol{k}}(n) \geq (1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}。$$

当$\boldsymbol{k}$取不同值的时候，用于堆积的凸体也不同，但是我们的下界与$\boldsymbol{k}$无关。所以这个结论的意思是，只要给定$1 < p \leq 2$，再让n取得比较大，那么对于任意的$\boldsymbol{k} = (k_1, k_2, \ldots, k_{m+1})$，只要$k_j \in \mathbb{N}\cup\{0\}$且$0 = k_1 < k_2 < \cdots < k_{m+1} = n$，$B^n_{p,\boldsymbol{k}}(\mathbf{0}, r_{p,\boldsymbol{k},n})$的平移堆积密度总是渐进大于$\frac{\log(2/c_p)n}{2^n}$。

对$p > 2$的情况，我们的方法也可以给出下界$\Omega_p(n/2^n)$。

我们将用两种方法证明定理1.11。我们的第一个证明方法叫做刚性超球模型（hard superball model）。这个方法由统计物理发展而来。Jenssen等人用该方法证明了接触数的下界[33]和欧几里得球体的堆积密度的下界[34]。在他们的文章中，该方法被分别称为刚性球盖模型（hard cap model）和刚性球面模型（hard sphere model）。我们的第二个证明用到图的独立数。我们也会用到一致凸性的概念来克服非欧球体所带来的困难。

我们还研究了球堆积的熵密度和压力，这些指标衡量了球堆积的丰富程度。

该工作已投稿。

§1.3 高维ℓ_p球的接触数的下界

记S^{n-1}为$\mathbb{R}^n$中的单位球面。接触数（kissing number）的问题是指最多能有多

少个互不重叠的平移$S^{n-1}+\boldsymbol{x}$同时与S^{n-1}相切。这个问题目前已知的确切结果只有1维，2维，3维，4维，8维，以及24维。

用$K_2(n)$表示S^{n-1}的最大接触数。在高维时，$K_2(n)$的最佳上界由Kabatjanskiĭ和Levenšteĭn[36]得到：$K_2(n)\le 2^{0.401n(1+o(1))}$。利用球面覆盖的方法，Shannon[75]和Wyner[84]得到了下界$K_2(n)\ge c\sqrt{n}(2/\sqrt{3})^n$。最近，Jenssen等人[33]将下界改进为$\Omega\left(n^{3/2}(2/\sqrt{3})^n\right)$。Fernández等人[22]又进一步改进了常数因子。

我们考虑ℓ_p球的最大接触数。对于$p\ge 1$，记$S_p^{n-1}(R)$为$\mathbb{R}^n$中半径为R、球心为$\mathbf{0}$的ℓ_p球，即$S_p^{n-1}(R):=\{\boldsymbol{x}\in\mathbb{R}^n:\|\boldsymbol{x}\|_p=R\}$，其中$\ell_p$范数$\|\cdot\|_p$定义为$\|\boldsymbol{x}\|_p=(\sum_{i=1}^n|x_i|^p)^{1/p}$，$\boldsymbol{x}=(x_1,x_2,\dots,x_n)$。我们简记$S_p^{n-1}=S_p^{n-1}(1)$。令$K_p(n)$为$S_p^{n-1}$的最大接触数。Minkowski-Hadwiger定理[26]给出了上界$K_p(n)\le 3^n-1$。在$p\ge 2$时，Sah等人[69]对这个界做了改进。当p在1到2之间时，已知的上界很少。

在下界方面，Larman和Zong[46]证明了$K_p(n)\ge(9/8)^{n(1+o(1))}=2^{0.1699n(1+o(1))}$。Xu[85]改进了他们的结果，例如$K_3(n)\ge 2^{0.4564n(1+o(1))}$。我们的工作进一步改进了Xu的结果。因为我们的结果没有显式表达式，所以我们在这里列出一些数值结果：

$$K_1(n)\ge 2^{0.1247n(1+o(1))}+2^{0.1825n(1+o(1))}+2^{0.1554n(1+o(1))}+\cdots;$$

$$K_2(n)\ge 2^{0.2059n(1+o(1))}+2^{0.1381n(1+o(1))}+2^{0.0584n(1+o(1))}+\cdots;$$

$$K_3(n)\ge cn2^{0.4564n(1+o(1))}+2^{0.1562n(1+o(1))}+2^{0.0425n(1+o(1))}+\cdots。$$

我们的方法来源于编码理论。最大接触数$K_p(n)$与最小距离为1的ℓ_p球面码的最大基数相等。我们从S_p^{n-1}上选取一个离散的集合X。利用编码理论中的思想，我们可以找到X的一个比较大的子集，其中的点两两之间距离不小于1。这就给出了$K_p(n)$的一个下界。

§1.4 有限域上的相似图形

离散几何中的许多问题都问一个集合的最小基数，使得这个集合中必定会有某种给定的结构。Falconer猜想便是其中之一。Falconer猜想指的是如果$\mathbb{R}^d$的一个子集$\mathcal{E}$的Hausdorff维数严格大于$d/2$，那么$\mathcal{E}$中任意两点之间的距离构成的集合具有正Lebesgue测度。目前已知最佳的结果可以参考文献[14, 15, 24]。

设$\mathbb{F}_q$为q个元素的域。在有限域中，Iosevich等人[31]考察了距离集的商集

$$\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})} := \left\{\frac{a}{b} : a \in \Delta(\mathcal{E}), b \in \Delta(\mathcal{E}) \setminus \{0\}\right\},$$

其中$\Delta(\mathcal{E}) := \{a_1^2 + a_2^2 + \cdots + a_d^2 : (a_1, a_2, \ldots, a_d) \in \mathcal{E}\}$，并得到如下定理。

定理1.12 ([31]). 设$\mathcal{E} \subseteq \mathbb{F}_q^d$，且$d$是大于等于2的偶数。若$|\mathcal{E}| \geq 9q^{d/2}$，则

$$\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})} = \mathbb{F}_q。$$

定理1.13 ([31]). 设$\mathcal{E} \subseteq \mathbb{F}_q^d$，且$d$是大于等于3的奇数。若$|\mathcal{E}| \geq 6q^{d/2}$，则

$$\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})} \supseteq \mathbb{F}_q^+ \cup \{0\},$$

其中$\mathbb{F}_q^+$表示$\mathbb{F}_q$中的非零二次剩余的集合。

定理1.12的结论意味着对任意$r \in \mathbb{F}_q^*$，存在$\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}', \boldsymbol{y}' \in \mathcal{E}$，使得$\|\boldsymbol{y}' - \boldsymbol{y}\| = r\|\boldsymbol{x}' - \boldsymbol{x}\| \neq 0$。换句话说，$K_{|\mathcal{E}|}$包含一对长度比为$r$的边。确切地说，我们给出以下定义。

定义1.1. 设$G = (V, E)$是一个图，$V = \{1, 2, \ldots, n\}$，$E \subseteq \binom{V}{2}$。对于$\mathbb{F}_q^d$的一个子集$\mathcal{E}$，我们称$\mathcal{E}$包含一对相似比为r的图G，如果存在不同的$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in \mathcal{E}$和不同的$\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n \in \mathcal{E}$，使得对任意$\{i, j\} \in E$，都有$\|\boldsymbol{y}_i - \boldsymbol{y}_j\| = r\|\boldsymbol{x}_i - \boldsymbol{x}_j\| \neq 0$。

最近，Rakhmonov[59]针对特定的图G，考察了$\mathcal{E}$的最小基数条件。记$\mathbb{F}_q^*$为$\mathbb{F}_q$中的非零元素构成的集合。Rakhmonov得到了下列结论。

定理1.14 ([59]). 若$r \in \mathbb{F}_p^*$，p是一个素数且$p \equiv 3 \pmod 4$，$\mathcal{E} \subseteq \mathbb{F}_p^2$且$|\mathcal{E}| > (\sqrt{3}+1)p$，则$\mathcal{E}$包含一对相似比为$r$的2长路径。

定理1.15 ([59]). 若$r \in \mathbb{F}_p^*$，p是一个素数且$p \equiv 3 \pmod 4$，$\mathcal{E} \subseteq \mathbb{F}_p^2$且$|\mathcal{E}| > 4\sqrt{3}p^{3/2}$，则$\mathcal{E}$包含一对相似比为$r$的4圈。

我们关注k星（k-star）和4长路径（4-path）这两类情况。我们的主要结果是以下定理。

定理1.16. 设q是一个奇素数的幂，$\mathcal{E} \subseteq \mathbb{F}_q^d$，且$k \geq 2$为整数。

- 若$q \geq 5$，$d \geq 2$为偶数，$r \in \mathbb{F}_q^*$，且$\mathcal{E}$的基数至少是$\left(31 + 10\binom{k}{2}\right) q^{d/2}$，则$\mathcal{E}$包含一对相似比为$r$的$k$星。

- 若$d \geq 3$为奇数，$r \in \mathbb{F}_q^+$，且$\mathcal{E}$的基数至少是$\left(4 + \sqrt{3}\binom{k}{2}\right) q^{d/2}$，则$\mathcal{E}$包含一对相似比为$r$的$k$星。

定理1.17. 设q是一个奇素数的幂，且$\mathcal{E} \subseteq \mathbb{F}_q^d$。

- 若$q \geq 5$，d为2或4，$r \in \mathbb{F}_q^*$，且$\mathcal{E}$的基数至少是$36q^{(2d+1)/3}$，则$\mathcal{E}$包含一对相似比为r的4长路径。

- 若$d = 3$，$r \in \mathbb{F}_q^+$，且$\mathcal{E}$的基数至少是$9q^{(2d+1)/3}$，则$\mathcal{E}$包含一对相似比为r的4长路径。

- 若$d = 5$，$r \in \mathbb{F}_q^+$，且$\mathcal{E}$的基数至少是$12q^3$，则$\mathcal{E}$包含一对相似比为r的4长路径。

- 若$q \geq 5$，$d \geq 6$为偶数，$r \in \mathbb{F}_q^*$，且$\mathcal{E}$的基数至少是$313q^{d/2}$，则$\mathcal{E}$包含一对相似比为r的4长路径。

- 若$d \geq 7$为奇数，$r \in \mathbb{F}_q^+$，且$\mathcal{E}$的基数至少是$313q^{d/2}$，则$\mathcal{E}$包含一对相似比为r的4长路径。

该工作已投稿。

第 2 章　$M_n(\mathbb{F}_q)$上的加乘估计问题

§2.1　简介

令$\mathbb{F}_q$为q个元素的域，$M_n(\mathbb{F}_q)$为$\mathbb{F}_q$上所有$n\times n$矩阵构成的环，$Z_n(\mathbb{F}_q)$ 为$\mathbb{F}_q$上所有$n\times n$的不可逆矩阵构成的集合，$GL_n(\mathbb{F}_q)$为$\mathbb{F}_q$上所有$n\times n$的可逆矩阵构成的集合。对于变量X和Y，如果存在一个常数$C(n)$（可能与n有关，但与q无关）使得$X\leq C(n)Y$，那么我们就记作$X\lesssim Y$。如果$X\lesssim Y$且$Y\lesssim X$，那么我们记作$X\sim Y$。对于$A,B\subseteq M_n(\mathbb{F}_q)$，我们定义$A+B=\{a+b:a\in A,b\in B\}$，$AB=\{ab:a\in A,b\in B\}$，$-A=\{-a:a\in A\}$。若$A\subseteq GL_n(\mathbb{F}_q)$，则记$A^{-1}=\{a^{-1}:a\in A\}$。再令$I_n$为$n\times n$的单位矩阵。

在环R中，设$A\subseteq R$是一个有限集。如果A是一个等差数列，那么一般来说$|A+A|\sim|A|$且$|AA|\sim|A|^2$。如果A是一个等比数列，那么一般来说$|AA|\sim|A|$且$|A+A|\sim|A|^2$。注意到$|A+A|$和$|AA|$中总有一个值会比较大（相对于$|A|$）。加乘估计的问题是指在一定条件下估计$\max\{|A+A|,|AA|\}$的下界。在[19]中，Erdős和Szemerédi证明了存在一个常数ϵ，使得对于任意有限的$A\subseteq\mathbb{Z}$，都有

$$\max\{|A+A|,|AA|\}\gtrsim|A|^{1+\epsilon}。$$

同时他们猜想这个界对于任意$\epsilon<1$和任意充分大的A都成立。

当$A\subseteq\mathbb{R}$时，这个问题上已知最佳的结果由Rudnev和Stevens[63]得出。他们的结果是

$$\max\{|A+A|,|AA|\}\gtrsim|A|^{\frac{4}{3}+\frac{2}{1167}-o(1)}。$$

在有限域中，当$A\subseteq\mathbb{F}_q$相对于q比较大的时候，结果与上述情况有所不同。特别地，当$A=\mathbb{F}_q$时，$|A+A|=|AA|=|A|=q$。所以我们通常研究两类问题：$|A|$相对于q比较小时估计$\max\{|A+A|,|AA|\}$的下界，以及$|A|$需要多大才能保证$\max\{|A+$

$A|, |AA|\}$相对于q比较大。Bourgain，Katz和Tao[4]证明了当p是素数，并且给定$A \subseteq \mathbb{F}_p$满足$p^\delta < |A| < p^{1-\delta}$时，那么我们有

$$\max\{|A+A|, |AA|\} \geq C_\delta |A|^{1+\epsilon},$$

其中$\epsilon = \epsilon(\delta)$是某个只与$\delta$有关的常数。

最近，Mohammadi和Stevens[52]证明了当$q = p^r$并且$A \subseteq \mathbb{F}_q$满足$|A| \lesssim p^{1/2}$时，有$\max\{|A+A|, |AA|\} \gtrsim |A|^{5/4}$。

在矩阵环中，Karabulut等人[37]证明了下面的结果。

定理2.1 ([37]). 如果$A \subseteq M_2(\mathbb{F}_q)$并且$|A| \geq Cq^3$，其中$C$是某个常数，那么我们有

$$\max\{|A+A|, |AA|\} \gtrsim \min\left\{\frac{|A|^2}{q^{7/2}}, q^2|A|^{1/2}\right\}。$$

他们还得到了一些其他的结果。他们的工作被The和Vinh[78]推广。

定理2.2 ([78]). 对任意正整数n，存在常数$C(n)$使得下述命题成立。若$A \subseteq M_n(\mathbb{F}_q)$满足$|A| \geq C(n)q^{n^2-1}$，那么我们有

$$\max\{|A+A|, |AA|\} \gtrsim \min\left\{\frac{|A|^2}{q^{n^2-1/2}}, q^{n^2/2}|A|^{1/2}\right\}。$$

定理2.3 ([78]). 对于$A, B, C \subseteq M_n(\mathbb{F}_q)$，我们有

$$|A+BC| \gtrsim \min\left\{q^{n^2}, \frac{|A||B||C|}{q^{2n^2-1}}\right\}。$$

定理2.4 ([78]). 对于$A \subseteq GL_n(\mathbb{F}_q)$和$B, C \subseteq M_n(\mathbb{F}_q)$，我们有

$$|A(B+C)| \gtrsim \min\left\{q^{n^2}, \frac{|A||B||C|}{q^{2n^2-1}}\right\}。$$

定理2.1−2.4的证明用到了图论和线性代数的知识。首先将问题转化为一些能量方程，并将其嵌入到二部图中。使用线性代数的知识可以得出该二部图的一些性质，例如公共邻点。最终得到结果。文献[51, 54, 56]中也有相关结果。

2.1.1 初步的改进

通过考察不同的能量方程，我们给出了加乘估计的一些新结果。这些结果改进了定理2.1−2.3，同时也推广了文献[51]中的结果。

定理2.5. 对于$A,B,C\subseteq M_n(\mathbb{F}_q)$，我们有

$$|A+BC|\gtrsim \min\left\{q^{n^2},\frac{|A||B||C|}{q^{2n^2-\frac{n+1}{2}}}\right\}。$$

特别地，若$|A||B||C|\gtrsim q^{3n^2-\frac{n+1}{2}}$，那么$|A+BC|\gtrsim q^{n^2}$。

定理2.6. 对于任意正整数n，存在$C(n)$使得下述命题成立。若$A,B\subseteq M_n(\mathbb{F}_q)$满足$|A|\geq C(n)q^{n^2-1}$，那么我们有

$$\max\{|A+B|,|AB|\}\gtrsim \min\left\{\frac{|A||B|}{q^{n^2-\frac{n+1}{4}}},q^{n^2/3}|B|^{2/3}\right\},$$

以及

$$\max\{|A+B|,|BA|\}\gtrsim \min\left\{\frac{|A||B|}{q^{n^2-\frac{n+1}{4}}},q^{n^2/3}|B|^{2/3}\right\}。$$

在定理2.6中，若取$A=B$，那么我们就得到以下推论。

推论2.1. 对于任意正整数n，存在$C(n)$使得下述命题成立。若$A\subseteq M_n(\mathbb{F}_q)$ 满足$|A|\geq C(n)q^{n^2-1}$，那么我们有

$$\max\{|A+A|,|AA|\}\gtrsim \min\left\{\frac{|A|^2}{q^{n^2-\frac{n+1}{4}}},q^{n^2/3}|A|^{2/3}\right\}。$$

注记2.1. 最近，*Ha*和*Ngo[25]*将定理*2.5*和推论*2.1*推广到了有限链环上。

首先，我们比较定理2.5和定理2.3。当$n=1$时，它们是一样的。当$n\geq 2$时，注意到$|A|\leq |A+BC|\leq q^{n^2}$，所以若$|A||B||C|\lesssim q^{3n^2-1}$且$|B|\cdot|C|\gtrsim q^{2n^2-\frac{n+1}{2}}$，定理2.5的结果比定理2.3更好。

其次，我们比较推论2.1和定理2.2。当$n=1$时，定理2.2的结果更好。当$n\geq 2$时，注意到$\frac{|A|^2}{q^{n^2-\frac{n+1}{4}}}\geq\frac{|A|^2}{q^{n^2-1/2}}$且$q^{n^2/3}|A|^{2/3}\leq q^{n^2/2}|A|^{1/2}$，所以若$q^{n^2/3}|A|^{2/3}\gtrsim\frac{|A|^2}{q^{n^2-1/2}}$，即$|A|\lesssim q^{n^2-\frac{3}{8}}$，推论2.1的结果比定理2.2更好。另一方面，若$|A|\lesssim q^{n^2-\frac{n+1}{4}}$，那么推论2.1只能给出平凡的结果$\max\{|A+A|,|AA|\}\gtrsim|A|$。所以当$q^{n^2-\frac{n+1}{4}}\lesssim|A|\lesssim q^{n^2-\frac{3}{8}}$且$n\geq 2$时，推论2.1的结果比定理2.2更好。

2.1.2 进一步的改进

如果我们更加细致地考察能量不等式，我们可以进一步改进定理2.4-2.6。

2.1.2.1 定理2.6的改进

首先，当$n=2$和$n=3$时，我们可以改进$\max\{|A+B|,|BA|\}$的下界。我们有下列定理。

定理2.7. *存在一个常数C_0使得下述命题成立。设$A,B\subseteq M_2(\mathbb{F}_q)$满足$|A|\geq C_0q^3$。*

- *若$q^{\frac{55}{4}}\lesssim|A|^3|B|\lesssim q^{16}$，那么*

$$\max\{|A+B|,|BA|\}\gtrsim q^{\frac{4}{3}}|B|^{\frac{2}{3}}。$$

- *若$|A|^{2+\frac{2}{t_0}}|B|\lesssim q^{9+\frac{19}{2t_0}}$且$|A|^{2+\frac{1}{t_0}}|B|\gtrsim q^{9+\frac{19}{4t_0}}$，那么*

$$\max\{|A+B|,|BA|\}\gtrsim\max\left\{\frac{|A||B|}{q^{3+\frac{1}{2t_0}}},q^{\frac{4}{3t_0}}|A|^{\frac{t_0-1}{3t_0}}|B|^{\frac{2}{3}}\right\},$$

其中$t_0\geq 2$是2的幂。

定理2.8. *存在一个常数C_0使得下述命题成立。设$A,B\subseteq M_3(\mathbb{F}_q)$满足$|A|\geq C_0q^8$。*

- *若$q^{33}\lesssim|A|^3|B|\lesssim q^{36}$，那么*

$$\max\{|A+B|,|BA|\}\gtrsim q^3|B|^{\frac{2}{3}}。$$

- *若$|A|^3|B|\lesssim q^{33}$且$|A|^{10}|B|^4\gtrsim q^{111}$，那么*

$$\max\{|A+B|,|BA|\}\gtrsim\max\left\{\frac{|A||B|}{q^8},q^{\frac{3}{2}}|A|^{\frac{1}{6}}|B|^{\frac{2}{3}}\right\}。$$

注记2.2. *如果我们将定理2.7和定理2.8中的$\max\{|A+B|,|BA|\}$替换为$\max\{|A+B|,|AB|\}$，也能得到相同的结果（见定理2.15）。*

我们在定理2.7和定理2.8中使用了同一个常数C_0，因为我们可以将它们取成一样，并且我们并不关心这个常数的大小。

在定理2.7和定理2.8中，若取$A=B$，那么我们就得到下列推论。

推论2.2. *设C_0是定理2.7中的常数，$A\subseteq M_2(\mathbb{F}_q)$满足$|A|\geq C_0q^3$。*

- *若$q^{\frac{55}{16}}\lesssim|A|\lesssim q^4$，那么*

$$\max\{|A+A|,|AA|\}\gtrsim q^{\frac{4}{3}}|A|^{\frac{2}{3}}。$$

- 若$q^{\frac{36t_0+19}{12t_0+4}} \lesssim |A| \lesssim q^{\frac{18t_0+19}{6t_0+4}}$，那么

$$\max\{|A+A|,|AA|\} \gtrsim \max\left\{\frac{|A|^2}{q^{3+\frac{1}{2t_0}}}, q^{\frac{4}{3t_0}}|A|^{1-\frac{1}{3t_0}}\right\},$$

其中$t_0 \geq 2$是2的幂。

当$n=2$，$q^3 \lesssim |A| \lesssim q^{\frac{47}{14}}$时，推论2.2给出的$\max\{|A+A|,|AA|\}$的下界比推论2.1更好。当$n=2$，$q^3 \lesssim |A| \lesssim q^{\frac{29}{8}}$时，推论2.2的结果比定理2.2更好。

推论2.3. 设C_0是定理*2.8*中的常数，$A \subseteq M_3(\mathbb{F}_q)$满足$|A| \geq C_0 q^8$。

- 若$q^{\frac{33}{4}} \lesssim |A| \lesssim q^9$，那么

$$\max\{|A+A|,|AA|\} \gtrsim q^3|A|^{\frac{2}{3}}。$$

- 若$q^8 \lesssim |A| \lesssim q^{\frac{33}{4}}$，那么

$$\max\{|A+A|,|AA|\} \gtrsim \max\left\{\frac{|A|^2}{q^8}, q^{\frac{3}{2}}|A|^{\frac{5}{6}}\right\}。$$

当$n=3$，$q^8 \lesssim |A| \lesssim q^{\frac{57}{7}}$时，推论2.3给出的$\max\{|A+A|,|AA|\}$的下界比推论2.1更好。当$n=3$，$q^8 \lesssim |A| \lesssim q^{\frac{69}{8}}$时，推论2.3的结果比定理2.2更好。

2.1.2.2 定理2.5的改进

接着，我们改进$|A+BC|$的下界，其中$A,B,C \subseteq M_n(\mathbb{F}_q)$。

定理2.9. 对于$A,B,C \subseteq M_n(\mathbb{F}_q)$，我们有

$$|A+BC| \gtrsim \max_{t\text{是2的幂}}\left\{\min\left\{q^{\frac{2n^2}{t}}|A|^{1-\frac{2}{t}}, \frac{|A||B||C|}{q^{2n^2-\frac{(t-1)n+1}{t}}}\right\}\right\}。$$

- 若$|A||B||C| \gtrsim q^{3n^2-\frac{n+1}{2}}$，那么

$$|A+BC| \gtrsim q^{n^2}。$$

- 若$|A|^{\frac{2}{t_0}}|B||C| \lesssim q^{2n^2+\frac{2n^2}{t_0}-\frac{(t_0-1)n+1}{t_0}}$且$|A|^{\frac{1}{t_0}}|B||C| \gtrsim q^{2n^2+\frac{n^2}{t_0}-\frac{(2t_0-1)n+1}{2t_0}}$，那么

$$|A+BC| \gtrsim \max\left\{\frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}, q^{\frac{n^2}{t_0}}|A|^{1-\frac{1}{t_0}}\right\},$$

其中$t_0 \geq 2$是2的幂。

当$|A|^{\frac{1}{2}}|B||C| \lesssim q^{\frac{5n^2-n-1}{2}}$且$|B||C| \gtrsim q^{2n^2-n}$时，定理2.9给出的$|A+BC|$的下界比定理2.5更好。当$|A||B||C| \lesssim q^{3n^2-1}$且$|B||C| \gtrsim q^{2n^2-n}$时，定理2.9的结果比定理2.3更好。

2.1.2.3 定理2.4的改进

最后，我们改进$|A(B+C)|$的下界，其中$A \subseteq GL_n(\mathbb{F}_q)$，$B, C \subseteq M_n(\mathbb{F}_q)$。

定理2.10. *对于$A \subseteq GL_n(\mathbb{F}_q)$，$B, C \subseteq M_n(\mathbb{F}_q)$，我们有*

$$|A(B+C)| \gtrsim \max_{t\text{是2的幂}} \left\{ \min \left\{ q^{\frac{n^2}{t}} |B|^{\frac{1}{2}} |C|^{\frac{1}{2}-\frac{1}{t}}, \frac{|A||B||C|}{q^{2n^2-\frac{(t-1)n+1}{t}}} \right\} \right\}。$$

- *若$|A||B|^{\frac{1}{2}}|C| \gtrsim q^{\frac{5n^2-n-1}{2}}$，那么*

$$|A(B+C)| \gtrsim q^{\frac{n^2}{2}} |B|^{\frac{1}{2}}。$$

- *若$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}+\frac{1}{t_0}} \lesssim q^{2n^2+\frac{n^2}{t_0}-\frac{(t_0-1)n+1}{t_0}}$且$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}+\frac{1}{2t_0}} \gtrsim q^{2n^2+\frac{n^2}{2t_0}-\frac{(2t_0-1)n+1}{2t_0}}$，那么*

$$|A(B+C)| \gtrsim \max \left\{ \frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}, q^{\frac{n^2}{2t_0}} |B|^{\frac{1}{2}} |C|^{\frac{1}{2}-\frac{1}{2t_0}} \right\},$$

其中$t_0 \geq 2$是2的幂。

注记2.3. *在定理2.10中，我们可以额外假设$|B| \gtrsim |C|$，否则的话可以交换$|B|$和$|C|$来得到一个较好的界。*

若对于某个t有$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}+\frac{1}{t}} \lesssim q^{2n^2+\frac{n^2}{t}-1}$，那么定理2.10的结果比定理2.4更好。例如，取$|A| = |B| = |C| \sim q^{n^2-1}$且$t = 2$，此时定理2.4只给出平凡的结果，而定理2.10给出非平凡下界$|A(B+C)| \gtrsim q^{n^2-\frac{1}{2}}$（在$n \geq 10$的时候）。

2.1.3 本章的结构

在§ 2.2中，我们介绍两个重要的引理。

在§ 2.3中，通过图论和线性代数方法，我们给出一个重要的不等式，即命题2.1。该不等式一方面关系到方程的解的个数，另一方面又与加乘估计有关。

在§ 2.4中，利用命题2.1，我们将证明定理2.5和定理2.6。

在§ 2.5中，对命题2.1和定理2.5的证明作一定的改动，我们给出定理2.4的一个新的证明。

在§ 2.6中，通过一个递归过程，我们将给出一个新的能量不等式，从而证明定理2.7和定理2.8。

在§ 2.7和§ 2.8中，我们将分别证明定理2.9和定理2.10。

§ 2.2 准备工作

令$G = (U \cup V, E)$是一个二部正则图（biregular graph）。记$\deg(U)$为U中的顶点的度。令A_G为G的邻接矩阵，并设$|\lambda_1| \geq |\lambda_2| \geq |\lambda_3| \cdots \geq |\lambda_n|$为$A_G$的特征值。注意到在一个二部图中，我们有$\lambda_1 = -\lambda_2$。我们称$\lambda_3$为$G$的第三特征值。我们有下列引理。

引理2.1 ([21]). 设G是一个二部正则图，U和V是G的顶点划分。那么，对于每一对$X \subseteq U$和$Y \subseteq V$，若记$e(X,Y)$为X和Y之间的边数，我们有

$$\left| e(X,Y) - \frac{\deg(U)}{|V|}|X||Y| \right| \leq |\lambda_3|\sqrt{|X||Y|},$$

其中λ_3是G的第三特征值。

引理2.2 ([57]). 令G是一个二部正则图，U和V是G的顶点划分，$|U| = m$，$|V| = n$。我们将G中的顶点从1到$|U| + |V|$标号。再设G的邻接矩阵A_G有如下形式

$$A_G = \begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix},$$

其中N是$|U| \times |V|$的矩阵，并且$N_{ij} = 1$当且仅当i和j之间有一条边。令

$$v^3 = (u_1, \ldots, u_m, v_1, \ldots, v_n)^T$$

为A_G的属于特征值λ_3的一个特征向量。那么，我们有

(i) $(u_1, \ldots, u_m)^T$是NN^T的一个特征向量，并且

(ii) $J(u_1, \ldots, u_m)^T = 0$，其中$J$是$m \times m$的全1矩阵。

§2.3 主要引理

给定正整数t（在本章中，我们总是假设t是2的幂）和集合$A_1, A_2, \ldots, A_{2t+2} \subseteq M_n(\mathbb{F}_q)$，记$N(A_1, A_2, \ldots, A_{2t+2})$为如下方程的解的个数

$$a_1a_2 + a_3a_4 + \cdots + a_{2t-1}a_{2t} = a_{2t+1} + a_{2t+2}，\ a_i \in A_i, 1 \leq i \leq 2t+2。 \tag{2.1}$$

我们有下列命题。

命题2.1. *对于任意正整数n，存在$C(n)$使得下述命题成立。对每一个正整数t和集合$A_1, A_2, \ldots, A_{2t}, A_{2t+1}, A_{2t+2} \subseteq M_n(\mathbb{F}_q)$，我们有*

$$N(A_1, A_2, \ldots, A_{2t+2}) \leq C(n)\left(\frac{\prod_{i=1}^{2t+2}|A_i|}{q^{n^2}} + q^{tn^2-\frac{(t-1)n+1}{2}}\sqrt{\prod_{i=1}^{2t+2}|A_i|}\right)。$$

证明. 我们构造一个二部图$G = (U \cup V, E)$，其中$U = V = (M_n(\mathbb{F}_q))^{t+1}$。$(a_1, a_3, \ldots, a_{2t-1}, a_{2t+1}) \in U$和$(a_2, a_4, \ldots, a_{2t}, a_{2t+2}) \in V$之间有一条边当且仅当

$$a_1a_2 + a_3a_4 + \cdots + a_{2t-1}a_{2t} = a_{2t+1} + a_{2t+2}。$$

显然

$$|U| = |V| = (|M_n(\mathbb{F}_q)|)^{t+1} = q^{(t+1)n^2}。$$

给定$(a_1, a_3, \ldots, a_{2t-1}, a_{2t+1}) \in U$和$(a_2, a_4, \ldots, a_{2t}) \in (M_n(\mathbb{F}_q))^t$，

$$a_{2t+2} = a_1a_2 + a_3a_4 + \cdots + a_{2t-1}a_{2t} - a_{2t+1}$$

是唯一确定的。所以$(a_1, a_3, \ldots, a_{2t-1}, a_{2t+1}) \in U$在$G$中的邻点个数为$\deg(U) = q^{tn^2}$，且

$$\frac{\deg(U)}{|V|} = \frac{1}{q^{n^2}}。$$

类似地，$(a_2, a_4, \ldots, a_{2t}, a_{2t+2}) \in V$在$G$中的邻点个数也是$q^{tn^2}$。

对U中任意两个不同的点$(a_1, a_3, \ldots, a_{2t-1}, a_{2t+1})$和$(a_1', a_3', \ldots, a_{2t-1}', a_{2t+1}')$，我们计算它们公共邻点个数，即下列方程的解$(a_2, a_4, \ldots, a_{2t}, a_{2t+2})$ 的个数

$$\begin{cases} a_1a_2 + a_3a_4 + \cdots + a_{2t-1}a_{2t} &= a_{2t+1} + a_{2t+2}， \\ a_1'a_2 + a_3'a_4 + \cdots + a_{2t-1}'a_{2t} &= a_{2t+1}' + a_{2t+2}。 \end{cases} \tag{2.2}$$

我们有

$$(a_1-a_1')a_2+(a_3-a_3')a_4+\cdots+(a_{2t-1}-a_{2t-1}')a_{2t}=a_{2t+1}-a_{2t+1}', \tag{2.3}$$

等价地，

$$\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' \end{pmatrix}\begin{pmatrix} a_2 \\ a_4 \\ \vdots \\ a_{2t} \end{pmatrix}=a_{2t+1}-a_{2t+1}'。 \tag{2.4}$$

方程(2.4)的解$\begin{pmatrix} a_2 \\ a_4 \\ \vdots \\ a_{2t} \end{pmatrix}$与方程组(2.2)的解

$$(a_2,a_4,\ldots,a_{2t},a_1a_2+a_3a_4+\cdots+a_{2t-1}a_{2t}-a_{2t+1})$$

一一对应。所以我们只需确定方程(2.4)的解的个数。

线性代数中有下述定理。

定理2.11. *设A为$m\times n$的矩阵。方程$AX=0$所有的解构成一个维数为$n-\mathrm{rank}(A)$的线性空间。*

定理2.12. *设A为$m\times n$的矩阵，b为$m\times 1$的矩阵。方程$AX=b$有解当且仅当*

$$\mathrm{rank}(A)=\mathrm{rank}\begin{pmatrix} A & b \end{pmatrix}。$$

一旦$AX=b$有一个解X_0，那么所有的解都可以写成$X=X_0+X_1$的形式，其中X_1为方程$AX=0$的任意解。

由定理2.11和定理2.12可知方程(2.4)有解当且仅当

$$\begin{aligned} &\mathrm{rank}\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' \end{pmatrix} \\ =&\mathrm{rank}\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' & a_{2t+1}-a_{2t+1}' \end{pmatrix}, \end{aligned} \tag{2.5}$$

并且若方程(2.4)有解，则解$\begin{pmatrix} a_2 \\ a_4 \\ \vdots \\ a_{2t} \end{pmatrix}$的个数等于$q^{(tn-k)n}$，其中$k$是矩阵

$$\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' \end{pmatrix}$$

的秩，因为$\begin{pmatrix} a_2 \\ a_4 \\ \vdots \\ a_{2t} \end{pmatrix}$的每一列都有$q^{tn-k}$种选择。

若$k=\operatorname{rank}\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' \end{pmatrix}=0$，那么$a_{2t+1}-a_{2t+1}'$必须等于0才能保证

$$\begin{aligned} &\operatorname{rank}\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' \end{pmatrix} \\ =&\operatorname{rank}\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' & a_{2t+1}-a_{2t+1}' \end{pmatrix}。 \end{aligned} \tag{2.6}$$

此时对所有的$i=1,3,\ldots,2t-1,2t+1$都有$a_i=a_i'$。这与$(a_1,a_3,\ldots,a_{2t-1},a_{2t+1})$和$(a_1',a_3',\ldots,a_{2t-1}',a_{2t+1}')$不同矛盾。所以当

$$k=\operatorname{rank}\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' \end{pmatrix}=0$$

时方程(2.4)无解。

对于$1\le k\le n$，记E_k为图G_k的邻接矩阵，其中G_k的顶点集为$(M_n(\mathbb{F}_q))^{t+1}$，$G_k$的两个顶点$(a_1,a_3,\ldots,a_{2t-1},a_{2t+1})$和$(a_1',a_3',\ldots,a_{2t-1}',a_{2t+1}')$之间有一条边当且仅当

$$\begin{aligned} k=&\operatorname{rank}\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' \end{pmatrix} \\ =&\operatorname{rank}\begin{pmatrix} a_1-a_1' & a_3-a_3' & \cdots & a_{2t-1}-a_{2t-1}' & a_{2t+1}-a_{2t+1}' \end{pmatrix}。 \end{aligned} \tag{2.7}$$

若$(0,0,\ldots,0,0)$与$(a_1,a_3,\ldots,a_{2t-1},a_{2t+1})$相邻，则$(a_1',a_3',\ldots,a_{2t-1}',a_{2t+1}')$ 与$(a_1+a_1',a_3+a_3',\ldots,a_{2t-1}+a_{2t-1}',a_{2t+1}+a_{2t+1}')$相邻，反之亦然。所以$G_k$是正则的。我们计算$(0,0,\ldots,0,0)$的度数，即具有以下性质的$(a_1,a_3,\ldots,a_{2t-1},a_{2t+1})$的数目，

$$\operatorname{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix}=\operatorname{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} & a_{2t+1} \end{pmatrix}=k。$$

我们首先选择$\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix}$，使得$\text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix} = k$。我们有以下定理。

定理2.13 ([45]). $\mathbb{F}_q$上秩为k的$m \times n$矩阵的数目为$\frac{Q_k(q^m)Q_k(q^n)}{Q_k(q^k)}$，其中$Q_k(q^m) = (q^m - 1)(q^m - q)\cdots(q^m - q^{k-1})$。

因为$\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix}$是$n \times tn$的矩阵，由定理2.13可知

$$\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix}$$

共有$\frac{Q_k(q^{tn})Q_k(q^n)}{Q_k(q^k)}$种选择。接下来我们选$a_{2t+1}$，因为

$$\text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix} = \text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} & a_{2t+1} \end{pmatrix} = k,$$

所以a_{2t+1}的每一列都在矩阵$\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix}$的列空间中，从而$a_{2t+1}$的每一列都有$q^k$种选择。综上，我们知道满足

$$\text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix} = \text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} & a_{2t+1} \end{pmatrix} = k$$

的$(a_1, a_3, \ldots, a_{2t-1}, a_{2t+1})$的个数为

$$\frac{Q_k(q^{tn})Q_k(q^n)}{Q_k(q^k)}q^{nk} \sim q^{tnk+2nk-k^2}。$$

对于$0 \le k \le n-1$，记F_k为图H_k的邻接矩阵，其中H_k的顶点集为$(M_n(\mathbb{F}_q))^{t+1}$，$H_k$的两个顶点$(a_1, a_3, \ldots, a_{2t-1}, a_{2t+1})$和$(a_1', a_3', \ldots, a_{2t-1}', a_{2t+1}')$之间有一条边当且仅当

$$\begin{aligned} k =& \text{rank}\begin{pmatrix} a_1 - a_1' & a_3 - a_3' & \cdots & a_{2t-1} - a_{2t-1}' \end{pmatrix} \\ <& \text{rank}\begin{pmatrix} a_1 - a_1' & a_3 - a_3' & \cdots & a_{2t-1} - a_{2t-1}' & a_{2t+1} - a_{2t+1}' \end{pmatrix}。 \end{aligned} \tag{2.8}$$

若$(0, 0, \ldots, 0, 0)$与$(a_1, a_3, \ldots, a_{2t-1}, a_{2t+1})$相邻，则$(a_1', a_3', \ldots, a_{2t-1}', a_{2t+1}')$ 与$(a_1 + a_1', a_3 + a_3', \ldots, a_{2t-1} + a_{2t-1}', a_{2t+1} + a_{2t+1}')$相邻，反之亦然。所以$H_k$是正则的。我们计算$(0, 0, \ldots, 0, 0)$的度数，即具有以下性质的$(a_1, a_3, \ldots, a_{2t-1}, a_{2t+1})$的数目，

$$\text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix} = k < \text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} & a_{2t+1} \end{pmatrix}。$$

我们首先选择$\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix}$，使得$\text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix} = k$。根据前面的计算，$\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix}$共有$\frac{Q_k(q^{tn})Q_k(q^n)}{Q_k(q^k)}$种选择。接下来我们选$a_{2t+1}$。因为满足

$$\text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix} = k = \text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} & a_{2t+1} \end{pmatrix}$$

的a_{2t+1}的数目为q^{nk}，所以满足

$$\text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix} = k < \text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} & a_{2t+1} \end{pmatrix}$$

的a_{2t+1}的数目为$q^{n^2} - q^{nk}$。因此满足

$$\text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} \end{pmatrix} = k < \text{rank}\begin{pmatrix} a_1 & a_3 & \cdots & a_{2t-1} & a_{2t+1} \end{pmatrix}$$

的$(a_1, a_3, \ldots, a_{2t-1}, a_{2t+1})$的数目是

$$\frac{Q_k(q^{tn})Q_k(q^n)}{Q_k(q^k)}(q^{n^2} - q^{nk}) \sim q^{n^2+tnk+nk-k^2}。$$

令N为$|U| \times |V|$的矩阵，其中$N_{ij} = 1$若i和j之间有一条边，否则$N_{ij} = 0$。所以$(NN^T)_{i_1i_2}$就是i_1和i_2的公共邻点数，其中i_1和i_2是U中不同的点，并且$(NN^T)_{ii}$是i的度数。我们按如下方式来构造NN^T。首先，令J是$|U|\times|U|$的全1矩阵。乘$q^{(t-1)n^2}$之后我们得到元素均为$q^{(t-1)n^2}$的$|U| \times |U|$的矩阵。接着，加上$(\deg(U) - q^{(t-1)n^2})I$，这样的话，对角线上的元素变为$\deg(U)$。然后，加上$\sum_{k=1}^{n}(q^{tn^2-nk} - q^{(t-1)n^2})E_k$，这样的话，$(i_1, i_2)$位置上的元素变为$i_1$和$i_2$的公共邻点数（若它们有公共邻点）。最后，减去$\sum_{k=0}^{n-1} q^{(t-1)n^2}F_k$，这样的话，$(i_1, i_2)$位置上的元素变为0（若它们没有公共邻点）。基于上述计算，我们有

$$\begin{aligned} &NN^T \\ =&q^{(t-1)n^2}J + \left(\deg(U) - q^{(t-1)n^2}\right)I + \sum_{k=1}^{n}\left(q^{tn^2-nk} - q^{(t-1)n^2}\right)E_k - \sum_{k=0}^{n-1} q^{(t-1)n^2}F_k \\ =&q^{(t-1)n^2}J + \left(\deg(U) - q^{(t-1)n^2}\right)I + \sum_{k=1}^{n-1}\left(q^{tn^2-nk} - q^{(t-1)n^2}\right)E_k - \sum_{k=0}^{n-1} q^{(t-1)n^2}F_k, \end{aligned} \tag{2.9}$$

其中I是单位矩阵。

记

$$E_{total1}=\sum_{k=1}^{n-1}\left(q^{tn^2-nk}-q^{(t-1)n^2}\right)E_k-\sum_{k=0}^{n-1}q^{(t-1)n^2}F_k。$$

设$v^3=(u_1,\ldots,u_{|U|},v_1,\ldots,v_{|V|})^T$为$A_G$的属于特征值$\lambda_3$的一个特征向量。由引理2.2可知$(u_1,\ldots,u_{|U|})^T$是$NN^T$的属于特征值$\lambda_3^2$的一个特征向量。由方程(2.9)得

$$\left(\lambda_3^2-\deg(U)+q^{(t-1)n^2}\right)(u_1,\ldots,u_{|U|})^T=E_{total1}(u_1,\ldots,u_{|U|})^T。\tag{2.10}$$

因此，$(u_1,\ldots,u_{|U|})^T$是E_{total1}的属于特征值$\lambda_3^2-\deg(U)+q^{(t-1)n^2}$的一个特征向量。

因为G_k是正则的，它的邻接矩阵的最大特征值等于顶点的度，即$\sim q^{tnk+2nk-k^2}$。所以，对于E_k的任意特征值λ，都有$|\lambda|\lesssim q^{tnk+2nk-k^2}$。类似地，因为$H_k$是正则的，对于$F_k$的任意特征值$\lambda$，都有$|\lambda|\lesssim q^{n^2+tnk+nk-k^2}$。所以若$\lambda$是$E_{total1}$的一个特征值，那么

$$\begin{aligned}|\lambda|&\lesssim\sum_{k=1}^{n-1}\left(q^{tn^2-nk}-q^{(t-1)n^2}\right)q^{2nk+tnk-k^2}+\sum_{k=0}^{n-1}q^{(t-1)n^2}q^{n^2+nk+tnk-k^2}\\&\le\sum_{k=1}^{n-1}q^{tn^2-nk}q^{2nk+tnk-k^2}+\sum_{k=0}^{n-1}q^{(t-1)n^2}q^{n^2+nk+tnk-k^2}\\&\lesssim\sum_{k=0}^{n-1}q^{tn^2+(t+1)nk-k^2}。\end{aligned}\tag{2.11}$$

注意到函数$f(k)=tn^2+(t+1)nk-k^2$在$k\le(t+1)n/2$时递增，所以它的最大值在$k=n-1$时取到，此时$tn^2+(t+1)nk-k^2\le tn^2+(t+1)n(n-1)-(n-1)^2=2tn^2-(t-1)n-1$。所以$E_{total1}$的特征值$\lambda_3^2-\deg(U)+q^{(t-1)n^2}$满足

$$|\lambda_3^2-\deg(U)+q^{(t-1)n^2}|\lesssim q^{2tn^2-(t-1)n-1}。$$

因为$\deg(U)=q^{tn^2}$，所以有

$$|\lambda_3|\lesssim q^{tn^2-\frac{(t-1)n+1}{2}}。$$

现在若$A_1,A_2,\ldots,A_{2t},A_{2t+1},A_{2t+2}\subseteq M_n(\mathbb{F}_q)$，那么我们可以将$A_1\times A_3\times\cdots\times A_{2t-1}\times A_{2t+1}$和$A_2\times A_4\times\cdots\times A_{2t}\times A_{2t+2}$分别看作$U$和$V$的子集，$N(A_1,A_2,\ldots,A_{2t+2})$就等于$e(A_1\times A_3\times\cdots\times A_{2t-1}\times A_{2t+1},A_2\times A_4\times\cdots\times A_{2t}\times A_{2t+2})$。所以由引理2.1可

得

$$\begin{aligned} & N(A_1, A_2, \ldots, A_{2t+2}) \\ \leq\ & \tfrac{\deg(U)}{|V|}|A_1 \times A_3 \times \cdots \times A_{2t+1}||A_2 \times A_4 \times \cdots \times A_{2t+2}| \\ & +|\lambda_3|\sqrt{|A_1 \times A_3 \times \cdots \times A_{2t+1}||A_2 \times A_4 \times \cdots \times A_{2t+2}|} \\ \leq\ & C(n)\left(\tfrac{\prod_{i=1}^{2t+2}|A_i|}{q^{n^2}} + q^{tn^2-\frac{(t-1)n+1}{2}}\sqrt{\prod_{i=1}^{2t+2}|A_i|}\right)。 \end{aligned}$$

□

注记2.4. *Nguyen*和*Vinh*在文献*[54]*中也得到了相似的结论。

特别地，令$t=2$，我们得到以下推论。

推论2.4.

$$N(A_1, A_2, \ldots, A_6) \leq C(n)\left(\frac{\prod_{i=1}^{6}|A_i|}{q^{n^2}} + q^{2n^2-\frac{n+1}{2}}\sqrt{\prod_{i=1}^{6}|A_i|}\right)。$$

§ 2.4 定理2.5和2.6的证明

在这一节，我们证明定理2.5和定理2.6。我们首先证明定理2.5。

定理2.5的证明. 对于$\lambda \in A+BC$，令

$$t(\lambda) = |\{(a,b,c) \in A \times B \times C : a+bc = \lambda\}|。$$

由Cauchy-Schwarz不等式，我们有

$$(|A||B||C|)^2 = \left(\sum_{\lambda \in A+BC} t(\lambda)\right)^2 \leq |A+BC| \sum_{\lambda \in A+BC} t(\lambda)^2。$$

注意到

$$\sum_{\lambda \in A+BC} t(\lambda)^2 = N(B, C, A, -A, -B, C)。$$

由推论2.4可得

$$\frac{(|A||B||C|)^2}{|A+BC|} \leq N(B,C,A,-A,-B,C) \lesssim \frac{|A|^2|B|^2|C|^2}{q^{n^2}} + q^{2n^2-\frac{n+1}{2}}|A||B||C|。$$

所以

$$\frac{(|A||B||C|)^2}{|A+BC|} \lesssim \frac{|A|^2|B|^2|C|^2}{q^{n^2}}$$

或

$$\frac{(|A||B||C|)^2}{|A+BC|} \lesssim q^{2n^2-\frac{n+1}{2}}|A||B||C|。$$

从而我们得出结论

$$|A+BC| \gtrsim \min\left\{q^{n^2}, \frac{|A||B||C|}{q^{2n^2-\frac{n+1}{2}}}\right\}。$$

□

在证明定理2.6之前，我们需要一个关于加法能量的估计。

对于$A, B \subseteq M_n(\mathbb{F}_q)$，定义

$$E_+(A,B) = |\{(a_1,a_2,b_1,b_2) \in A^2 \times B^2 : a_1+b_1 = a_2+b_2\}|。$$

引理2.3. 设$A, B \subseteq M_n(\mathbb{F}_q)$，$C \subseteq GL_n(\mathbb{F}_q)$。我们有

$$E_+(A,B) \lesssim \frac{|BC|^2|A|^2}{q^{n^2}} + q^{2n^2-\frac{n+1}{2}}\frac{|BC||A|}{|C|}。$$

证明. 根据定义，我们有

$$\begin{aligned}
&E_+(A,B)\\
=&|\{(a_1,a_2,b_1,b_2) \in A^2 \times B^2 : a_1+b_1 = a_2+b_2\}|\\
=&|\{(a_1,a_2,b_1,b_2,c_1,c_2) \in A^2 \times B^2 \times C^2 : a_1+b_1c_1c_1^{-1} = a_2+b_2c_2c_2^{-1}\}| \cdot |C|^{-2}\\
\leq&|\{(a_1,a_2,s_1,s_2,t_1,t_2) \in A^2 \times (BC)^2 \times (C^{-1})^2 : a_1+s_1t_1 = a_2+s_2t_2\}| \cdot |C|^{-2}\\
=&|C|^{-2}N(BC,C^{-1},A,-A,BC,C^{-1})。
\end{aligned} \tag{2.12}$$

由推论2.4可得

$$\begin{aligned}
E_+(A,B) &\leq |C|^{-2}N(BC,C^{-1},A,-A,BC,C^{-1})\\
&\lesssim |C|^{-2}\left(\frac{|BC|^2|C|^2|A|^2}{q^{n^2}} + q^{2n^2-\frac{n+1}{2}}|BC||C||A|\right)\\
&= \frac{|BC|^2|A|^2}{q^{n^2}} + q^{2n^2-\frac{n+1}{2}}\frac{|BC||A|}{|C|}。
\end{aligned} \tag{2.13}$$

□

对于$\lambda \in A+B$，定义

$$t_{A+B}(\lambda) = |\{(a,b) \in A \times B : a+b=\lambda\}|。$$

由Cauchy-Schwarz不等式，我们有

$$(|A||B|)^2 = \left(\sum_{\lambda \in A+B} t_{A+B}(\lambda)\right)^2 \leq |A+B| \sum_{\lambda \in A+B} t_{A+B}(\lambda)^2 = |A+B|E_+(A,B)。 \tag{2.14}$$

现在我们可以证明定理2.6。

定理2.6的证明. 因为$|A| \geq C(n)q^{n^2-1}$且$|Z_n(\mathbb{F}_q)| \sim q^{n^2-1}$，我们可以选$C(n)$使得$|A| > 2|Z_n(\mathbb{F}_q)|$。从而$|A \cap GL_n(\mathbb{F}_q)| \geq |A|/2$。因此我们可以假设$A \subseteq GL_n(\mathbb{F}_q)$。在引理2.3中令$A=C$，我们有

$$\begin{aligned} \frac{(|A||B|)^2}{|A+B|} &\leq E_+(A,B) \\ &\lesssim \frac{|BA|^2|A|^2}{q^{n^2}} + q^{2n^2-\frac{n+1}{2}}|BA|。 \end{aligned} \tag{2.15}$$

所以

$$\max\{|A+B|,|BA|\} \gtrsim \min\left\{\frac{|A||B|}{q^{n^2-\frac{n+1}{4}}}, q^{n^2/3}|B|^{2/3}\right\}。$$

$$\max\{|A+B|,|AB|\} \gtrsim \min\left\{\frac{|A||B|}{q^{n^2-\frac{n+1}{4}}}, q^{n^2/3}|B|^{2/3}\right\}$$

的证明也是类似的。 □

此外，我们还有另外一个定理，它推广了[51]中的结果。

定理2.14. 令$A,B,C,D \subseteq M_n(\mathbb{F}_q)$。记$N$为下列方程的解的数目，

$$a+b=cd,\ (a,b,c,d) \in A \times B \times C \times D。$$

那么我们有

$$N \lesssim \frac{|A||B|^{\frac{1}{2}}|C||D|}{q^{\frac{n^2}{2}}} + q^{n^2-\frac{n+1}{4}}(|A||C||D||B|)^{\frac{1}{2}}。$$

证明. 对任意$b \in B$，令

$$r(b) = |\{(a,c,d) \in A \times C \times D : -a + cd = b\}|。$$

根据定义，我们有$N = \sum_{b\in B} r(b)$。由Cauchy-Schwarz不等式可得

$$N^2 = \left(\sum_{b\in B} r(b)\right)^2 \leq |B| \sum_{b\in B} r(b)^2。$$

注意到

$$\begin{aligned}
&\sum_{b\in B} r(b)^2 \\
=&|\{(a_1,c_1,d_1,a_2,c_2,d_2) \in (A\times C\times D)^2 : -a_1 + c_1d_1 = -a_2 + c_2d_2 \in B\}| \\
\leq&|\{(a_1,c_1,d_1,a_2,c_2,d_2) \in (A\times C\times D)^2 : -a_1 + c_1d_1 = -a_2 + c_2d_2\}| \\
=&N(C,D,A,-A,-C,D) \\
\lesssim&\frac{|A|^2|C|^2|D|^2}{q^{n^2}} + q^{2n^2-\frac{n+1}{2}}|A||C||D|。
\end{aligned}$$

所以

$$N \lesssim \frac{|A||B|^{\frac{1}{2}}|C||D|}{q^{\frac{n^2}{2}}} + q^{n^2-\frac{n+1}{4}}(|A||C||D||B|)^{\frac{1}{2}}。$$

□

§ 2.5 定理2.4的证明

在这一节，我们给出定理2.4的一个新的证明。

我们构造一个二部图$G' = (U' \cup V', E')$，其中$U' = V' = (M_n(\mathbb{F}_q))^3$。$(a,e,c) \in U$与$(b,f,d) \in V$相邻当且仅当$ba + ef = c + d$。我们仍然有

$$|U'| = |V'| = (|M_n(\mathbb{F}_q)|)^3 = q^{3n^2}，\ \deg(U') = q^{2n^2}，\text{以及}\frac{\deg(U')}{|V'|} = \frac{1}{q^{n^2}}。$$

对于U'中任意两个不同的点(a_1,e_1,c_1)和(a_2,e_2,c_2)，我们计算它们的公共邻点个数，即下列方程的解(b,f,d)的个数

$$ba_1 + e_1f = c_1 + d，\ ba_2 + e_2f = c_2 + d。 \tag{2.16}$$

我们有

$$b(a_1-a_2)+(e_1-e_2)f=c_1-c_2。\tag{2.17}$$

方程(2.17)的解(b,f)与方程组(2.16)的解$(b,f,ba_1+e_1f-c_1)$一一对应。所以我们只需确定方程(2.17)的解的个数。

令$k_1=\mathrm{rank}(e_1-e_2)$，$k_2=\mathrm{rank}(a_1-a_2)$。存在$P_1,Q_1,P_2,Q_2\in GL_n(\mathbb{F}_q)$使得$P_1(e_1-e_2)Q_1=\begin{pmatrix} I_{k_1} & 0\\ 0 & 0\end{pmatrix}$，且$P_2(a_1-a_2)Q_2=\begin{pmatrix} I_{k_2} & 0\\ 0 & 0\end{pmatrix}$。方程(2.17)化为

$$P_1bP_2^{-1}P_2(a_1-a_2)Q_2+P_1(e_1-e_2)Q_1Q_1^{-1}fQ_2=P_1(c_1-c_2)Q_2,\tag{2.18}$$

即

$$P_1bP_2^{-1}\begin{pmatrix} I_{k_2} & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix} I_{k_1} & 0\\ 0 & 0\end{pmatrix}Q_1^{-1}fQ_2=P_1(c_1-c_2)Q_2。\tag{2.19}$$

如果我们记$b'=P_1bP_2^{-1}$，$f'=Q_1^{-1}fQ_2$，那么方程(2.17)的解(b,f)与方程

$$b'\begin{pmatrix} I_{k_2} & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix} I_{k_1} & 0\\ 0 & 0\end{pmatrix}f'=P_1(c_1-c_2)Q_2\tag{2.20}$$

的解(b',f')一一对应。所以方程(2.17)的解(b,f)的个数等于方程(2.20)的解(b',f')的个数。进一步记$b'=(b_{ij})_{1\le i,j\le n}$，$f'=(f_{ij})_{1\le i,j\le n}$，以及$P_1(c_1-c_2)Q_2=(c_{ij})_{1\le i,j\le n}$，那么方程(2.20)化为

$$\begin{cases} b_{ij}+f_{ij}=c_{ij}, & 若1\le i\le k_1且1\le j\le k_2;\\ f_{ij}=c_{ij}, & 若1\le i\le k_1且k_2+1\le j\le n;\\ b_{ij}=c_{ij}, & 若k_1+1\le i\le n且1\le j\le k_2;\\ c_{ij}=0, & 若k_1+1\le i\le n且k_2+1\le j\le n。\end{cases}\tag{2.21}$$

因此，方程(2.17)有解当且仅当对于$k_1+1\le i\le n$和$k_2+1\le j\le n$，有$c_{ij}=0$。并且一旦方程(2.17)有解，不难计算出解的个数为

$$q^{2n^2-k_1n-k_2n+k_1k_2}。$$

若$k_1=k_2=0$，则对于$1\le i\le n$和$1\le j\le n$，有$c_{ij}=0$，即$P_1(c_1-c_2)Q_2=0$。因为$k_1=\mathrm{rank}(e_1-e_2)$，$k_2=\mathrm{rank}(a_1-a_2)$，所以$a_1=a_2$，$e_1=e_2$，$c_1=$

c_2，这与(a_1, e_1, c_1)和(a_2, e_2, c_2)不同矛盾。所以当$k_1 = k_2 = 0$时方程(2.17)无解。如果k_1或k_2中的某个等于n，不妨假设$k_1 = n$，则方程(2.17)总会有一个解(b, f)，其中$f = (e_1 - e_2)^{-1}(c_1 - c_2 - b(a_1 - a_2))$。

若$0 \leq k_1, k_2 \leq n$（k_1和k_2不同时为0），记E_{k_1,k_2}为图G_{k_1,k_2}的邻接矩阵，其中G_{k_1,k_2}的顶点集为$(M_n(\mathbb{F}_q))^3$，G_{k_1,k_2}中的两个顶点(a_1, e_1, c_1)和(a_2, e_2, c_2)之间有一条边当且仅当$\mathrm{rank}(e_1 - e_2) = k_1$，$\mathrm{rank}(a_1 - a_2) = k_2$，以及方程(2.17)有解。如果$(0, 0, 0)$与$(a, e, c)$相邻，则$(a', e', c')$ 与$(a+a', e+e', c+c')$相邻，反之亦然。故G_{k_1,k_2}是正则的。我们计算$(0, 0, 0)$的度数，即具有以下性质的(a, e, c)的数目，$\mathrm{rank}(e) = k_1$，$\mathrm{rank}(a) = k_2$，并且$ba + ef = c$有解。

我们首先选择a和e使得$\mathrm{rank}(e) = k_1$，$\mathrm{rank}(a) = k_2$。由定理2.13可知(a, e)共有$\frac{Q_{k_2}(q^n)Q_{k_2}(q^n)}{Q_{k_2}(q^{k_2})}\frac{Q_{k_1}(q^n)Q_{k_1}(q^n)}{Q_{k_1}(q^{k_1})}$种选择。接下来选$c$。给定$a$和$e$满足$\mathrm{rank}(e) = k_1$以及$\mathrm{rank}(a) = k_2$，存在$P_1, Q_1, P_2, Q_2 \in GL_n(\mathbb{F}_q)$，使得$P_1eQ_1 = \begin{pmatrix} I_{k_1} & 0 \\ 0 & 0 \end{pmatrix}$，$P_2aQ_2 = \begin{pmatrix} I_{k_2} & 0 \\ 0 & 0 \end{pmatrix}$。方程(2.21)说明对$c$的唯一的限制是当$k_1+1 \leq i \leq n$和$k_2+1 \leq j \leq n$时，必须有$(P_1cQ_2)_{ij} = 0$。那么对于$P_1cQ_2$，有$q^{n^2-(n-k_1)(n-k_2)} = q^{nk_1+nk_2-k_1k_2}$种选择。所以$c$也有$q^{nk_1+nk_2-k_1k_2}$种选择。因此，满足条件$\mathrm{rank}(e) = k_1$，$\mathrm{rank}(a) = k_2$，并且$ba + ef = c$有解的$(a, e, c)$的数目是

$$\frac{Q_{k_2}(q^n)Q_{k_2}(q^n)}{Q_{k_2}(q^{k_2})}\frac{Q_{k_1}(q^n)Q_{k_1}(q^n)}{Q_{k_1}(q^{k_1})}q^{nk_1+nk_2-k_1k_2} \sim q^{3nk_1+3nk_2-k_1^2-k_2^2-k_1k_2}。$$

若$0 \leq k_1, k_2 \leq n-1$，记F_{k_1,k_2}为图H_{k_1,k_2}的邻接矩阵，其中H_{k_1,k_2}的顶点集为$(M_n(\mathbb{F}_q))^3$，H_{k_1,k_2}的顶点(a_1, e_1, c_1)和(a_2, e_2, c_2)之间有一条边当且仅当$\mathrm{rank}(e_1 - e_2) = k_1$，$\mathrm{rank}(a_1 - a_2) = k_2$，并且方程(2.17)无解。如果$(0, 0, 0)$与$(a, e, c)$相邻，那么$(a', e', c')$与$(a + a', e + e', c + c')$相邻，反之亦然。所以$H_{k_1,k_2}$是正则的。我们计算$(0, 0, 0)$的度数，即具有以下性质的$(a, e, c)$的数目，$\mathrm{rank}(e) = k_1$，$\mathrm{rank}(a) = k_2$，并且$ba + ef = c$无解。

我们首先选择a和e使得$\mathrm{rank}(e) = k_1$，$\mathrm{rank}(a) = k_2$。由定理2.13可知(a, e)共有$\frac{Q_{k_2}(q^n)Q_{k_2}(q^n)}{Q_{k_2}(q^{k_2})}\frac{Q_{k_1}(q^n)Q_{k_1}(q^n)}{Q_{k_1}(q^{k_1})}$种选择。接下来我们选$c$。根据以上论述，我们知道$c$共有$q^{n^2} - q^{nk_1+nk_2-k_1k_2}$种选择。所以满足条件$\mathrm{rank}(e) = k_1$，$\mathrm{rank}(a) = k_2$，并且$ba+ef =$

c无解的(a,e,c)的数目是

$$\frac{Q_{k_2}(q^n)Q_{k_2}(q^n)}{Q_{k_2}(q^{k_2})}\frac{Q_{k_1}(q^n)Q_{k_1}(q^n)}{Q_{k_1}(q^{k_1})}(q^{n^2}-q^{nk_1+nk_2-k_1k_2})\sim q^{n^2+2nk_1+2nk_2-k_1^2-k_2^2}。$$

令N为$|U'|\times|V'|$的矩阵，其中$N_{ij}=1$若i和j之间有一条边，否则$N_{ij}=0$。所以$(NN^T)_{i_1i_2}$就是i_1和i_2的公共邻点数，其中i_1和i_2是U'中不同的点，且$(NN^T)_{ii}$是i的度数。我们按如下方式来构造NN^T。首先，令J是$|U'|\times|U'|$的全1矩阵。乘q^{n^2}之后我们得到元素均为q^{n^2}的$|U'|\times|U'|$的矩阵。接着，加上$(\deg(U')-q^{n^2})I$，这样的话，对角线上的元素变为$\deg(U')$。然后，加上$\sum_{k_2=1}^{n}(q^{2n^2-k_2n}-q^{n^2})E_{0,k_2}$和

$$\sum_{k_2=0}^{n}\sum_{k_1=1}^{n}(q^{2n^2-k_1n-k_2n+k_1k_2}-q^{n^2})E_{k_1,k_2},$$

这样的话，(i_1,i_2)位置上的元素变为i_1和i_2的公共邻点数（若它们有公共邻点）。最后，减去$\sum_{k_1,k_2=0}^{n-1}q^{n^2}F_{k_1,k_2}$，这样的话，$(i_1,i_2)$位置上的元素变为0（若它们没有公共邻点）。基于上述计算，我们有

$$\begin{aligned}NN^T=&q^{n^2}J+(\deg(U')-q^{n^2})I+\sum_{k_2=1}^{n}(q^{2n^2-k_2n}-q^{n^2})E_{0,k_2}\\&+\sum_{k_2=0}^{n}\sum_{k_1=1}^{n}(q^{2n^2-k_1n-k_2n+k_1k_2}-q^{n^2})E_{k_1,k_2}-\sum_{k_1,k_2=0}^{n-1}q^{n^2}F_{k_1,k_2}\\=&q^{n^2}J+(\deg(U')-q^{n^2})I+\sum_{k_2=1}^{n-1}(q^{2n^2-k_2n}-q^{n^2})E_{0,k_2}\\&+\sum_{k_2=0}^{n-1}\sum_{k_1=1}^{n-1}(q^{2n^2-k_1n-k_2n+k_1k_2}-q^{n^2})E_{k_1,k_2}-\sum_{k_1,k_2=0}^{n-1}q^{n^2}F_{k_1,k_2}。\end{aligned}\tag{2.22}$$

记

$$\begin{aligned}E_{total2}=&\sum_{k_2=1}^{n-1}(q^{2n^2-k_2n}-q^{n^2})E_{0,k_2}+\sum_{k_2=0}^{n-1}\sum_{k_1=1}^{n-1}(q^{2n^2-k_1n-k_2n+k_1k_2}-q^{n^2})E_{k_1,k_2}\\&-\sum_{k_1,k_2=0}^{n-1}q^{n^2}F_{k_1,k_2}。\end{aligned}\tag{2.23}$$

设$v^3=(u_1,\ldots,u_{|U'|},v_1,\ldots,v_{|V'|})^T$为$A_{G'}$的属于特征值$\lambda_3$的一个特征向量。由引理2.2可得$(u_1,\ldots,u_{|U'|})^T$是$NN^T$的属于特征值$\lambda_3^2$的一个特征向量。由方程(2.22)得

$$\left(\lambda_3^2-\deg(U')+q^{n^2}\right)(u_1,\ldots,u_{|U'|})^T=E_{total2}(u_1,\ldots,u_{|U'|})^T。\tag{2.24}$$

因此，$(u_1,\ldots,u_{|U'|})^T$是E_{total2}的属于特征值$\lambda_3^2-\deg(U')+q^{n^2}$的一个特征向量。

因为G_{k_1,k_2}是正则的，它的最大特征值等于顶点的度，即$\sim q^{3nk_1+3nk_2-k_1^2-k_2^2-k_1k_2}$。所以，对于$E_{k_1,k_2}$的任意特征值$\lambda$，都有$|\lambda|\lesssim q^{3nk_1+3nk_2-k_1^2-k_2^2-k_1k_2}$。类似地，因为$H_{k_1,k_2}$是正则的，对于$F_{k_1,k_2}$的任意特征值$\lambda$，都有$|\lambda|\lesssim q^{n^2+2nk_1+2nk_2-k_1^2-k_2^2}$。所以若$\lambda$是$E_{total2}$的一个特征值，那么

$$\begin{aligned}
&|\lambda|\\
\lesssim&\sum_{k_2=1}^{n-1}(q^{2n^2-k_2n}-q^{n^2})q^{3nk_2-k_2^2}+\sum_{k_2=0}^{n-1}\sum_{k_1=1}^{n-1}(q^{2n^2-k_1n-k_2n+k_1k_2}-q^{n^2})q^{3nk_1+3nk_2-k_1^2-k_2^2-k_1k_2}\\
&+\sum_{k_1,k_2=0}^{n-1}q^{n^2}q^{n^2+2nk_1+2nk_2-k_1^2-k_2^2}\\
\le&\sum_{k_2=1}^{n-1}q^{2n^2+2nk_2-k_2^2}+\sum_{k_2=0}^{n-1}\sum_{k_1=1}^{n-1}q^{2n^2+2nk_1+2nk_2-k_1^2-k_2^2}+\sum_{k_1,k_2=0}^{n-1}q^{2n^2+2nk_1+2nk_2-k_1^2-k_2^2}\\
\lesssim&\sum_{k_1,k_2=0}^{n-1}q^{2n^2+2nk_1+2nk_2-k_1^2-k_2^2}。
\end{aligned}\tag{2.25}$$

给定k_1和n，注意到函数$g(k_2)=2n^2+2nk_1+2nk_2-k_1^2-k_2^2$在$k_2\le n$时递增，所以它的最大值在$k_2=n-1$时取到，且$2n^2+2nk_1+2nk_2-k_1^2-k_2^2\le 2n^2+2nk_1+2n(n-1)-k_1^2-(n-1)^2=3n^2+2nk_1-k_1^2-1$。类似地，$3n^2+2nk_1-k_1^2-1$在$k_1=n-1$时取到最大值。所以$3n^2+2nk_1-k_1^2-1\le 3n^2+2n(n-1)-(n-1)^2-1=4n^2-2$。因此，$E_{total2}$的特征值$\lambda_3^2-\deg(U')+q^{n^2}$满足

$$|\lambda_3^2-\deg(U')+q^{n^2}|\lesssim q^{4n^2-2}。$$

由于$\deg(U')=q^{2n^2}$，所以

$$|\lambda_3|\lesssim q^{2n^2-1}。$$

现在若$A\subseteq GL_n(\mathbb{F}_q)$，$B,C\subseteq M_n(\mathbb{F}_q)$，那么我们可以取$X=\{(b_1,a_2,a_2c_2):a_2\in A,b_1\in B,c_2\in C\}\subseteq U'$且$Y=\{(a_1,-b_2,-a_1c_1):a_1\in A,b_2\in B,c_1\in C\}\subseteq V'$。因为$A\subseteq GL_n(\mathbb{F}_q)$，我们有$|X|=|Y|=|A||B||C|$。注意到$X$和$Y$之间的边数恰好等于

$$|\{(a_1,b_1,c_1,a_2,b_2,c_2)\in A\times B\times C\times A\times B\times C:a_1(b_1+c_1)=a_2(b_2+c_2)\}|。$$

与定理2.5的证明类似，我们有

$$\begin{aligned}
&\frac{|A|^2|B|^2|C|^2}{|A(B+C)|}\\
\leq&|\{(a_1,b_1,c_1,a_2,b_2,c_2)\in(A\times B\times C)^2 : a_1(b_1+c_1)=a_2(b_2+c_2)\}|\\
=&e(X,Y)\\
\lesssim&\frac{\deg(U')}{|V'|}|X||Y|+|\lambda_3|\sqrt{|X||Y|}\\
\lesssim&\frac{|A|^2|B|^2|C|^2}{q^{n^2}}+q^{2n^2-1}|A||B||C|。
\end{aligned}$$

所以

$$|A(B+C)|\gtrsim\min\left\{q^{n^2},\frac{|A||B||C|}{q^{2n^2-1}}\right\}。$$

§2.6 定理2.7和定理2.8的证明

我们首先介绍一个递归过程。固定t为2的幂。设$A_1,A_2,\ldots,A_t,A_{t+1},A_{t+2}\subseteq M_n(\mathbb{F}_q)$。我们利用命题2.1来计算方程

$$a_1a_2+a_3a_4+\cdots+a_{t-1}a_t=a_{t+1}+a_{t+2}，\ a_i\in A_i, 1\leq i\leq t+2$$

的解的个数$N(A_1,\ldots,A_{t+2})$。

对任意$a_{t+1}\in A_{t+1}$，令

$$\begin{aligned}
r(a_{t+1})=&|\{(a_1,a_2,\ldots,a_t,a_{t+2})\in A_1\times A_2\times\cdots\times A_t\times A_{t+2}:\\
&a_1a_2+a_3a_4+\cdots+a_{t-1}a_t-a_{t+2}=a_{t+1}\}|。
\end{aligned}\tag{2.26}$$

根据定义，我们有$N(A_1,\ldots,A_{t+2})=\sum_{a_{t+1}\in A_{t+1}}r(a_{t+1})$。由Cauchy-Schwarz不等式得

$$N(A_1,\ldots,A_{t+2})^2=\left(\sum_{a_{t+1}\in A_{t+1}}r(a_{t+1})\right)^2\leq|A_{t+1}|\sum_{a_{t+1}\in A_{t+1}}r(a_{t+1})^2。$$

注意到

$$\begin{aligned}
&\sum_{a_{t+1}\in A_{t+1}} r(a_{t+1})^2\\
=&|\{(a_1,\dots,a_t,a_{t+2},a_1',\dots,a_t',a_{t+2}')\in(A_1\times\cdots\times A_t\times A_{t+2})^2:\\
&a_1a_2+\cdots+a_{t-1}a_t-a_{t+2}=a_1'a_2'+\cdots+a_{t-1}'a_t'-a_{t+2}'\in A_{t+1}\}|\\
\le&|\{(a_1,\dots,a_t,a_{t+2},a_1',\dots,a_t',a_{t+2}')\in(A_1\times\cdots\times A_t\times A_{t+2})^2:\\
&a_1a_2+\cdots+a_{t-1}a_t-a_{t+2}=a_1'a_2'+\cdots+a_{t-1}'a_t'-a_{t+2}'\}|\\
=&N(A_1,A_2,\dots,A_{t-1},A_t,-A_1,A_2,\dots,-A_{t-1},A_t,-A_{t+2},A_{t+2})\\
\le&C(n)\left(\frac{(|A_{t+2}|\prod_{i=1}^t|A_i|)^2}{q^{n^2}}+q^{tn^2-\frac{(t-1)n+1}{2}}|A_{t+2}|\prod_{i=1}^t|A_i|\right)。
\end{aligned}$$

其中最后一个不等号由命题2.1得到。所以

$$N(A_1,\dots,A_{t+2})\le C(n)^{1/2}\left(\frac{|A_{t+1}|^{1/2}|A_{t+2}|\prod_{i=1}^t|A_i|}{q^{\frac{n^2}{2}}}+q^{\frac{t}{2}n^2-\frac{(t-1)n+1}{4}}\sqrt{\prod_{i=1}^{t+2}|A_i|}\right)。\tag{2.27}$$

继续这个过程。对于$A_1,A_2,\dots,A_{\frac{t}{2}},A_{\frac{t}{2}+1},A_{\frac{t}{2}+2}\subseteq M_n(\mathbb{F}_q)$，若$N(A_1,\dots,A_{\frac{t}{2}+2})$是方程

$$a_1a_2+a_3a_4+\cdots+a_{\frac{t}{2}-1}a_{\frac{t}{2}}=a_{\frac{t}{2}+1}+a_{\frac{t}{2}+2},\ a_i\in A_i,1\le i\le\frac{t}{2}+2$$

的解的个数，那么

$$\begin{aligned}
&N(A_1,\dots,A_{\frac{t}{2}+2})\\
\le&C(n)^{1/4}\left(\frac{|A_{\frac{t}{2}+1}|^{1/2}|A_{\frac{t}{2}+2}|^{3/4}\prod_{i=1}^{t/2}|A_i|}{q^{\frac{n^2}{4}}}+q^{\frac{t}{4}n^2-\frac{(t-1)n+1}{8}}\sqrt{\prod_{i=1}^{\frac{t}{2}+2}|A_i|}\right)。
\end{aligned}\tag{2.28}$$

最终，我们得到下列命题。

命题2.2. *令$C(n)$是命题2.1中的常数。设$A_1,A_2,\dots,A_6\subseteq M_n(\mathbb{F}_q)$。若*

$$N(A_1,A_2,A_3,A_4,A_5,A_6)$$

是方程

$$a_1a_2+a_3a_4=a_5+a_6,\ a_i\in A_i,1\le i\le6$$

的解的个数，那么

$$\begin{aligned}&N(A_1,A_2,A_3,A_4,A_5,A_6)\\ \leq& C(n)^{2/t}\left(\frac{|A_1||A_2||A_3||A_4||A_5|^{\frac{1}{2}}|A_6|^{\frac{t+4}{2t}}}{q^{\frac{2n^2}{t}}}+q^{2n^2-\frac{(t-1)n+1}{t}}\sqrt{\prod_{i=1}^{6}|A_i|}\right)。\end{aligned}\tag{2.29}$$

关于加法能量，我们也有新的估计。

引理2.4. 设$A,B\subseteq M_n(\mathbb{F}_q)$，$C\subseteq GL_n(\mathbb{F}_q)$。我们有

$$E_+(A,B)\lesssim\frac{|BC|^2|A|^{1+\frac{2}{t}}}{q^{\frac{2n^2}{t}}}+q^{2n^2-\frac{(t-1)n+1}{t}}\frac{|BC||A|}{|C|}。$$

证明. 根据定义，我们有

$$\begin{aligned}&E_+(A,B)\\ =&|\{(a_1,a_2,b_1,b_2)\in A^2\times B^2:a_1+b_1=a_2+b_2\}|\\ =&|\{(a_1,a_2,b_1,b_2,c_1,c_2)\in A^2\times B^2\times C^2:a_1+b_1c_1c_1^{-1}=a_2+b_2c_2c_2^{-1}\}|\cdot|C|^{-2}\\ \leq&|\{(a_1,a_2,s_1,s_2,t_1,t_2)\in A^2\times (BC)^2\times (C^{-1})^2:a_1+s_1t_1=a_2+s_2t_2\}|\cdot|C|^{-2}\\ =&|C|^{-2}N(BC,C^{-1},-BC,C^{-1},A,-A)。\end{aligned}\tag{2.30}$$

由命题2.2可得

$$\begin{aligned}&E_+(A,B)\\ \leq&|C|^{-2}N(BC,C^{-1},-BC,C^{-1},A,-A)\\ \leq&|C|^{-2}C(n)^{2/t}\left(\frac{|BC|^2|C|^2|A|^{1+\frac{2}{t}}}{q^{\frac{2n^2}{t}}}+q^{2n^2-\frac{(t-1)n+1}{t}}|BC||C||A|\right)\\ =&C(n)^{2/t}\left(\frac{|BC|^2|A|^{1+\frac{2}{t}}}{q^{\frac{2n^2}{t}}}+q^{2n^2-\frac{(t-1)n+1}{t}}\frac{|BC||A|}{|C|}\right)。\end{aligned}\tag{2.31}$$

□

我们有下列定理。

定理2.15. 对任意正整数n，令$C(n)$是命题*2.1*中的常数。存在$C_1(n)$使得下述命题成立。如果$A,B\subseteq M_n(\mathbb{F}_q)$满足$|A|\geq C_1(n)q^{n^2-1}$，那么我们有

$$\max\{|A+B|,|BA|\}\gtrsim \max_{t是2的幂}\left\{\min\left\{\frac{|A||B|}{C(n)^{\frac{1}{t}}q^{n^2-\frac{(t-1)n+1}{2t}}},\frac{q^{\frac{2n^2}{3t}}|A|^{\frac{t-2}{3t}}|B|^{\frac{2}{3}}}{C(n)^{\frac{2}{3t}}}\right\}\right\},\tag{2.32}$$

和

$$\max\{|A+B|,|AB|\}\gtrsim \max_{t是2的幂}\left\{\min\left\{\frac{|A||B|}{C(n)^{\frac{1}{t}}q^{n^2-\frac{(t-1)n+1}{2t}}},\frac{q^{\frac{2n^2}{3t}}|A|^{\frac{t-2}{3t}}|B|^{\frac{2}{3}}}{C(n)^{\frac{2}{3t}}}\right\}\right\}。\tag{2.33}$$

证明. 因为$|A|\geq C_1(n)q^{n^2-1}$且$|Z_n(\mathbb{F}_q)|\sim q^{n^2-1}$，我们可以选取$C_1(n)$使得$|A|>2|Z_n(\mathbb{F}_q)|$。从而$|A\cap GL_n(\mathbb{F}_q)|\geq |A|/2$。因此我们可以假设$A\subseteq GL_n(\mathbb{F}_q)$。在引理2.4中令$A=C$，我们有

$$\begin{aligned}\frac{(|A||B|)^2}{|A+B|}&\leq E_+(A,B)\\&\lesssim C(n)^{2/t}\left(\frac{|BA|^2|A|^{1+\frac{2}{t}}}{q^{\frac{2n^2}{t}}}+q^{2n^2-\frac{(t-1)n+1}{t}}|BA|\right)。\end{aligned}\tag{2.34}$$

所以

$$\max\{|A+B|,|BA|\}\gtrsim \min\left\{\frac{|A||B|}{C(n)^{\frac{1}{t}}q^{n^2-\frac{(t-1)n+1}{2t}}},\frac{q^{\frac{2n^2}{3t}}|A|^{\frac{t-2}{3t}}|B|^{\frac{2}{3}}}{C(n)^{\frac{2}{3t}}}\right\}。$$

这对任意t都成立，只要t是2的幂。所以不等式(2.32)成立。

不等式(2.33)的证明也是类似的。 □

我们总是可以假设$C(n)\geq 1$并且我们不关心这个常数。简单起见，我们只考虑不等式(2.32)。它可以写成

$$\max\{|A+B|,|BA|\}\geq C_2(n)\cdot \max_{t是2的幂}\left\{\min\left\{\frac{|A||B|}{q^{n^2-\frac{(t-1)n+1}{2t}}},q^{\frac{2n^2}{3t}}|A|^{\frac{t-2}{3t}}|B|^{\frac{2}{3}}\right\}\right\},\tag{2.35}$$

其中$C_2(n)$是只与n有关的常数。

作为t的函数，$\frac{|A||B|}{q^{n^2-\frac{(t-1)n+1}{2t}}}$递增，$q^{\frac{2n^2}{3t}}|A|^{\frac{t-2}{3t}}|B|^{\frac{2}{3}}$递减。所以

$$\min\left\{\frac{|A||B|}{q^{n^2-\frac{(t-1)n+1}{2t}}},q^{\frac{2n^2}{3t}}|A|^{\frac{t-2}{3t}}|B|^{\frac{2}{3}}\right\}$$

的最大值在t_0处取到，其中t_0满足

$$\frac{|A||B|}{q^{n^2-\frac{(t_0-1)n+1}{2t_0}}}=q^{\frac{2n^2}{3t_0}}|A|^{\frac{t_0-2}{3t_0}}|B|^{\frac{2}{3}}。$$

此时我们有

$$|A|^{2+\frac{2}{t_0}}|B|=q^{3n^2-\frac{3((t_0-1)n+1)}{2t_0}+\frac{2n^2}{t_0}}。$$

接下来我们考虑$n=2$和$n=3$的情况。

当$n=2$时，不等式(2.35)化为

$$\max\{|A+B|,|BA|\}\geq C_2(2)\cdot\max_{t是2的幂}\left\{\min\left\{\frac{|A||B|}{q^{4-\frac{2t-1}{2t}}},q^{\frac{8}{3t}}|A|^{\frac{t-2}{3t}}|B|^{\frac{2}{3}}\right\}\right\}。$$

- 若$q^{\frac{55}{4}}\lesssim|A|^3|B|\lesssim q^{16}$，那么

$$\max\{|A+B|,|BA|\}\gtrsim q^{\frac{4}{3}}|B|^{\frac{2}{3}},$$

其中$q^{\frac{4}{3}}|B|^{\frac{2}{3}}$来自$\min\left\{\frac{|A||B|}{q^{4-\frac{2\cdot2-1}{2\cdot2}}},q^{\frac{8}{3\cdot2}}|A|^{\frac{2-2}{3\cdot2}}|B|^{\frac{2}{3}}\right\}$。

- 若对于某个$\delta>0$有$|A|^3|B|\lesssim q^{\frac{55}{4}}$且$|A|^2|B|\gtrsim q^{9+\delta}$，那么存在2的幂$t_0\geq2$，使得$|A|^{2+\frac{2}{t_0}}|B|\lesssim q^{9+\frac{19}{2t_0}}$ and $|A|^{2+\frac{1}{t_0}}|B|\gtrsim q^{9+\frac{19}{4t_0}}$。所以

$$\max\{|A+B|,|BA|\}\gtrsim\max\left\{\frac{|A||B|}{q^{4-\frac{2t_0-1}{2t_0}}},q^{\frac{4}{3t_0}}|A|^{\frac{2t_0-2}{6t_0}}|B|^{\frac{2}{3}}\right\},$$

其中$\frac{|A||B|}{q^{4-\frac{2t_0-1}{2t_0}}}$来自$\min\left\{\frac{|A||B|}{q^{4-\frac{2t_0-1}{2t_0}}},q^{\frac{8}{3t_0}}|A|^{\frac{t_0-2}{3t_0}}|B|^{\frac{2}{3}}\right\}$，$q^{\frac{4}{3t_0}}|A|^{\frac{2t_0-2}{6t_0}}|B|^{\frac{2}{3}}$来自$\min\left\{\frac{|A||B|}{q^{4-\frac{2\cdot2t_0-1}{2\cdot2t_0}}},q^{\frac{8}{3\cdot2t_0}}|A|^{\frac{2t_0-2}{3\cdot2t_0}}|B|^{\frac{2}{3}}\right\}$。

- 若$|A|^2|B|\lesssim q^9$，那么令$t\to\infty$，我们得到

$$\max\{|A+B|,|BA|\}\gtrsim\frac{|A||B|}{q^{3+\epsilon}},$$

其中$\epsilon>0$。这个界是平凡的。

令$A=B$，我们得到下面的结果。

- 若$q^{\frac{55}{16}} \lesssim |A| \lesssim q^4$，那么

$$\max\{|A+A|, |AA|\} \gtrsim q^{\frac{4}{3}}|A|^{\frac{2}{3}}。$$

- 若对于某个$\delta > 0$有$q^{3+\delta} \lesssim |A| \lesssim q^{\frac{55}{16}}$，那么存在2的幂$t_0 \geq 2$，使得$q^{\frac{36t_0+19}{12t_0+4}} \lesssim |A| \lesssim q^{\frac{18t_0+19}{6t_0+4}}$。所以

$$\max\{|A+A|, |AA|\} \gtrsim \max\left\{\frac{|A|^2}{q^{4-\frac{2t_0-1}{2t_0}}}, q^{\frac{4}{3t_0}}|A|^{1-\frac{1}{3t_0}}\right\}。$$

这证明了推论2.2。

当$n=3$时，不等式(2.35)化为

$$\max\{|A+B|, |BA|\} \geq C_2(3) \cdot \max_{t\text{是2的幂}}\left\{\min\left\{\frac{|A||B|}{q^{9-\frac{3t-2}{2t}}}, q^{\frac{6}{t}}|A|^{\frac{t-2}{3t}}|B|^{\frac{2}{3}}\right\}\right\}。$$

- 若$q^{33} \lesssim |A|^3|B| \lesssim q^{36}$，那么

$$\max\{|A+B|, |BA|\} \gtrsim q^3|B|^{\frac{2}{3}},$$

其中$q^3|B|^{\frac{2}{3}}$来自$\min\left\{\frac{|A||B|}{q^{9-\frac{3\cdot2-2}{2\cdot2}}}, q^{\frac{6}{2}}|A|^{\frac{2-2}{3\cdot2}}|B|^{\frac{2}{3}}\right\}$。

- 若$|A|^3|B| \lesssim q^{33}$且$|A|^{10}|B|^4 \gtrsim q^{111}$，那么

$$\max\{|A+B|, |BA|\} \gtrsim \max\left\{\frac{|A||B|}{q^8}, q^{\frac{3}{2}}|A|^{\frac{1}{6}}|B|^{\frac{2}{3}}\right\},$$

其中$\frac{|A||B|}{q^8}$来自$\min\left\{\frac{|A||B|}{q^{9-\frac{3\cdot2-2}{2\cdot2}}}, q^{\frac{6}{2}}|A|^{\frac{2-2}{3\cdot2}}|B|^{\frac{2}{3}}\right\}$，$q^{\frac{3}{2}}|A|^{\frac{1}{6}}|B|^{\frac{2}{3}}$来自$\min\left\{\frac{|A||B|}{q^{9-\frac{3\cdot4-2}{2\cdot4}}}, q^{\frac{6}{4}}|A|^{\frac{4-2}{3\cdot4}}|B|^{\frac{2}{3}}\right\}$。

令$A=B$，我们得到下面的结果。

- 若$q^{\frac{33}{4}} \lesssim |A| \lesssim q^9$，那么

$$\max\{|A+A|, |AA|\} \gtrsim q^3|A|^{\frac{2}{3}}。$$

- 若$q^8 \lesssim |A| \lesssim q^{\frac{33}{4}}$，那么

$$\max\{|A+A|, |AA|\} \gtrsim \max\left\{\frac{|A|^2}{q^8}, q^{\frac{3}{2}}|A|^{\frac{5}{6}}\right\}。$$

这证明了推论2.3。

注记2.5. 对于其他的n，我们的这个方法无法改进定理*2.6*的结果。

§2.7 定理2.9的证明

在这一节，我们证明定理2.9。

定理2.9的证明. 对于$\lambda \in A+BC$，令

$$t(\lambda) = |\{(a,b,c) \in A \times B \times C : a+bc = \lambda\}|。$$

由Cauchy-Schwarz不等式，我们有

$$(|A||B||C|)^2 = \left(\sum_{\lambda \in A+BC} t(\lambda)\right)^2 \leq |A+BC| \sum_{\lambda \in A+BC} t(\lambda)^2。$$

注意到

$$\sum_{\lambda \in A+BC} t(\lambda)^2 = N(B,C,-B,C,A,-A)。$$

由命题2.2可得

$$\begin{aligned} \frac{(|A||B||C|)^2}{|A+BC|} \leq & N(B,C,-B,C,A,-A) \\ \leq & C(n)^{2/t}\left(\frac{|A|^{1+\frac{2}{t}}|B|^2|C|^2}{q^{\frac{2n^2}{t}}} + q^{2n^2-\frac{(t-1)n+1}{t}}|A||B||C|\right)。 \end{aligned} \tag{2.36}$$

所以

$$\frac{(|A||B||C|)^2}{|A+BC|} \leq 2C(n)^{2/t}\frac{|A|^{1+\frac{2}{t}}|B|^2|C|^2}{q^{\frac{2n^2}{t}}}$$

或

$$\frac{(|A||B||C|)^2}{|A+BC|} \leq 2C(n)^{2/t}q^{2n^2-\frac{(t-1)n+1}{t}}|A||B||C|。$$

这对于任意t均成立（只要t是2的幂）。所以

$$|A+BC| \geq \max_{t\text{是2的幂}}\left\{\min\left\{\frac{q^{\frac{2n^2}{t}}|A|^{1-\frac{2}{t}}}{2C(n)^{\frac{2}{t}}}, \frac{|A||B||C|}{2C(n)^{\frac{2}{t}}q^{2n^2-\frac{(t-1)n+1}{t}}}\right\}\right\}。$$

与不等式(2.35)类似，我们有

$$|A+BC| \geq C_3(n)\cdot\max_{t\text{是2的幂}}\left\{\min\left\{q^{\frac{2n^2}{t}}|A|^{1-\frac{2}{t}}, \frac{|A||B||C|}{q^{2n^2-\frac{(t-1)n+1}{t}}}\right\}\right\},$$

其中$C_3(n)$是某个只与n有关的常数。 □

- 若$|A||B||C| \gtrsim q^{3n^2-\frac{n+1}{2}}$，那么

$$|A+BC| \gtrsim q^{n^2},$$

其中q^{n^2}来自$\min\left\{q^{\frac{2n^2}{2}}|A|^{1-\frac{2}{2}}, \frac{|A||B||C|}{q^{2n^2-\frac{(2-1)n+1}{2}}}\right\}$。

- 若$|A|^{\frac{2}{t_0}}|B||C| \lesssim q^{2n^2+\frac{2n^2}{t_0}-\frac{(t_0-1)n+1}{t_0}}$ 且对于2的某个幂t_0有

$$|A|^{\frac{1}{t_0}}|B||C| \gtrsim q^{2n^2+\frac{n^2}{t_0}-\frac{(2t_0-1)n+1}{2t_0}},$$

那么

$$|A+BC| \gtrsim \max\left\{\frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}, q^{\frac{n^2}{t_0}}|A|^{1-\frac{1}{t_0}}\right\},$$

其中$\frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}$来自$\min\left\{\frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}, q^{\frac{2n^2}{t_0}}|A|^{1-\frac{2}{t_0}}\right\}$，$q^{\frac{n^2}{t_0}}|A|^{1-\frac{1}{t_0}}$来自$\min\left\{\frac{|A||B||C|}{q^{2n^2-\frac{(2t_0-1)n+1}{2t_0}}}, q^{\frac{2n^2}{2t_0}}|A|^{1-\frac{2}{2t_0}}\right\}$。

- 若$|B||C| \lesssim q^{2n^2-n}$，那么令$t \to \infty$，我们得到

$$|A+BC| \gtrsim \frac{|A||B||C|}{q^{2n^2-n+\epsilon}},$$

其中$\epsilon > 0$。这个界是平凡的。

§2.8 定理2.10的证明

在证明定理2.10之前，我们需要下面的定理，它改进了定理2.14的结果。

定理2.16. 令$C(n)$是命题*2.4*中的常数。设$A_1, A_2, A_3, A_4 \subseteq M_n(\mathbb{F}_q)$。记

$$N(A_1, A_2, A_3, A_4)$$

为下列方程的解的数目，

$$a_1a_2 = a_3 + a_4,\ (a_1, a_2, a_3, a_4) \in A_1 \times A_2 \times A_3 \times A_4。$$

那么我们有

$$\begin{aligned} &N(A_1, A_2, A_3, A_4) \\ \leq &C(n)^{1/t}\left(\frac{|A_1||A_2||A_3|^{\frac{1}{2}}|A_4|^{\frac{t+2}{2t}}}{q^{\frac{n^2}{t}}} + q^{n^2-\frac{(t-1)n+1}{2t}}(|A_1||A_2||A_3||A_4|)^{\frac{1}{2}}\right) \end{aligned} \tag{2.37}$$

对2的任意幂t都成立。

证明. 该定理的证明与命题2.2及其证明类似，故这里不再赘述。 □

现在我们可以证明定理2.10。

定理*2.10*的证明. 设$A \subseteq GL_n(\mathbb{F}_q)$，$B, C \subseteq M_n(\mathbb{F}_q)$。不失一般性，假设$|B| \gtrsim |C|$。再令$A_1 = A^{-1}, A_2 = A(B+C), A_3 = B, A_4 = C$。由定理2.16，我们有

$$\begin{aligned} &N(A^{-1}, A(B+C), B, C) \\ \leq &C(n)^{\frac{1}{t}} \left(\frac{|A||A(B+C)||B|^{\frac{1}{2}}|C|^{\frac{t+2}{2t}}}{q^{\frac{n^2}{t}}} + q^{n^2 - \frac{(t-1)n+1}{2t}} (|A||A(B+C)||B||C|)^{\frac{1}{2}} \right)。 \end{aligned} \tag{2.38}$$

这对于任意t均成立（只要t是2的幂）。另一方面，对任意$a \in A, b \in B, c \in C$，$a_1 = a^{-1}, a_2 = a(b+c), a_3 = b, a_4 = c$以下方程的解

$$a_1 a_2 = a_3 + a_4，(a_1, a_2, a_3, a_4) \in A_1 \times A_2 \times A_3 \times A_4。$$

所以

$$N(A^{-1}, A(B+C), B, C) \geq |A||B||C|。 \tag{2.39}$$

综合不等式(2.38)和(2.39)，我们有

$$\begin{aligned} &|A||B||C| \\ \leq &C(n)^{\frac{1}{t}} \left(\frac{|A||A(B+C)||B|^{\frac{1}{2}}|C|^{\frac{t+2}{2t}}}{q^{\frac{n^2}{t}}} + q^{n^2 - \frac{(t-1)n+1}{2t}} (|A||A(B+C)||B||C|)^{\frac{1}{2}} \right)。 \end{aligned} \tag{2.40}$$

这对于2的任意幂t均成立。所以我们有

$$|A(B+C)| \geq C_4(n) \cdot \max_{t\text{是2的幂}} \left\{ \min \left\{ q^{\frac{n^2}{t}} |B|^{\frac{1}{2}} |C|^{\frac{1}{2}-\frac{1}{t}}, \frac{|A||B||C|}{q^{2n^2 - \frac{(t-1)n+1}{t}}} \right\} \right\},$$

其中$C_4(n)$是某个只与n有关的常数。 □

注意到$\frac{|A||B||C|}{q^{2n^2 - \frac{(t-1)n+1}{t}}} \geq \frac{|A||B||C|}{q^{2n^2-1}}$且$q^{\frac{n^2}{t}} |B|^{\frac{1}{2}} |C|^{\frac{1}{2}-\frac{1}{t}} \leq q^{n^2}$。若对于某个$t$有

$$q^{\frac{n^2}{t}} B|^{\frac{1}{2}} |C|^{\frac{1}{2}-\frac{1}{t}} \gtrsim \frac{|A||B||C|}{q^{2n^2-1}},$$

即

$$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}+\frac{1}{t}} \lesssim q^{2n^2+\frac{n^2}{t}-1},$$

那么定理2.10的结果比定理2.4更好。

- 若$|A||B|^{\frac{1}{2}}|C| \gtrsim q^{\frac{5n^2-n-1}{2}}$，那么

  $$|A(B+C)| \gtrsim q^{\frac{n^2}{2}}|B|^{\frac{1}{2}},$$

  其中$q^{\frac{n^2}{2}}|B|^{\frac{1}{2}}$来自$\min\left\{q^{\frac{n^2}{2}}|B|^{\frac{1}{2}}|C|^{\frac{1}{2}-\frac{1}{2}}, \frac{|A||B||C|}{q^{2n^2-\frac{(2-1)n+1}{2}}}\right\}$。

- 若$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}+\frac{1}{t_0}} \lesssim q^{2n^2+\frac{n^2}{t_0}-\frac{(t_0-1)n+1}{t_0}}$且存在2的某个幂$t_0$使得$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}+\frac{1}{2t_0}} \gtrsim q^{2n^2+\frac{n^2}{2t_0}-\frac{(2t_0-1)n+1}{2t_0}}$那么

  $$|A(B+C)| \gtrsim \max\left\{\frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}, q^{\frac{n^2}{2t_0}}|B|^{\frac{1}{2}}|C|^{\frac{1}{2}-\frac{1}{2t_0}}\right\},$$

  其中$\frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}$来自$\min\left\{\frac{|A||B||C|}{q^{2n^2-\frac{(t_0-1)n+1}{t_0}}}, q^{\frac{n^2}{t_0}}|B|^{\frac{1}{2}}|C|^{\frac{1}{2}-\frac{1}{t_0}}\right\}$，$q^{\frac{n^2}{2t_0}}|B|^{\frac{1}{2}}|C|^{\frac{1}{2}-\frac{1}{2t_0}}$来自$\min\left\{\frac{|A||B||C|}{q^{2n^2-\frac{(2t_0-1)n+1}{2t_0}}}, q^{\frac{n^2}{2t_0}}|B|^{\frac{1}{2}}|C|^{\frac{1}{2}-\frac{1}{2t_0}}\right\}$。

- 若$|A||B|^{\frac{1}{2}}|C|^{\frac{1}{2}} \lesssim q^{2n^2-n}$，那么令$t \to \infty$，我们有

  $$|A(B+C)| \gtrsim \frac{|A||B||C|}{q^{2n^2-n+\epsilon}},$$

  其中$\epsilon > 0$。这个界的平凡的。

第 3 章 高维超球堆积密度的下界

§3.1 简介

球堆积（sphere packing）问题指的是如何在空间$\mathbb{R}^n$中最紧密地堆积相同大小的球。这个离散几何问题既古老又困难。这个问题目前已知的确切结果只有1维，2维，3维，8维，以及24维。

- 在1维的时候，这个问题是平凡的，因为1维的球就是线段。
- 在2维的时候，最大堆积密度是$\pi/\sqrt{12}$，堆积方式为六边形格。
- 在3维的时候，这个问题就是著名的开普勒猜想，由Hales[27]解决。此时的最大堆积密度是$\pi/\sqrt{18}$，堆积方式为六方最密堆积（hexagonal closest packed，简称HCP）和面心立方最密堆积（face-centered cubic，简称FCC）。
- 在8维的时候，这个问题由Viazovska[81]解决。此时的最大堆积密度是$\pi^4/384$，堆积方式为E_8格。
- 在24维的时候，这个问题由Cohn等人[8]解决。此时的最大堆积密度是$\pi^{12}/12!$，堆积方式为Leech格。

值得一提的是，Cohn和Elkies[7]通过线性规划的方法，给出了球堆积密度的上界。他们的结果为解决8维和24维球堆积问题奠定了基础。

令$\Delta_2(n)$为欧几里得空间$\mathbb{R}^n$中相同大小的球的最大平移堆积密度。在高维的情况，$\Delta_2(n)$的最佳上界由Kabatjanskiĭ和Levenšteĭn[36]得到：$\Delta_2(n) \leq 2^{(-0.599...+o(1))n}$。Cohn和Zhao[9]以及Sardari和Zargar[70]进一步改进了常数因子。下界方面，$\Delta_2(n) \geq 2^{-n}$是平凡的，因为当球堆积得最密的时候，将半径变为双倍就可以覆盖整个空

间。Rogers[60]将下界改进为$n2^{-n}$。Ball[1]构造了一个密度为$2(n-1)2^{-n}\zeta(n)$的格球堆积。目前已知最佳的下界由Venkatesh[80]得出，为$(65963+o(1))n2^{-n}$。

我们考虑超球的堆积密度。设$k\in\mathbb{N}$，$p\geq 1$为实数。记$\|\cdot\|_2$为ℓ_2范数，即

$$\|(x_1,x_2,\ldots,x_k)\|_2=\sqrt{x_1^2+x_2^2+\cdots+x_k^2}。$$

再令$\boldsymbol{k}=(k_1,k_2,\ldots,k_{m+1})$满足$0=k_1<k_2<\cdots<k_{m+1}=n$。我们用

$$B^n_{p,\boldsymbol{k}}(\boldsymbol{x},r)=\left\{\boldsymbol{y}:\left(\sum_{j=1}^{m}\left\|\left(x_{k_j+1}-y_{k_j+1},x_{k_j+2}-y_{k_j+2},\ldots,x_{k_{j+1}}-y_{k_{j+1}}\right)\right\|_2^p\right)^{\frac{1}{p}}\leq r\right\}$$

表示$\mathbb{R}^n$中半径为r、球心为$\boldsymbol{x}$的超球，其中$\boldsymbol{x}=(x_1,x_2,\ldots,x_n)$，$\boldsymbol{y}=(y_1,y_2,\ldots,y_n)$。如果超球的球心为原点$\mathbf{0}$，那么我们简记为$B^n_{p,\boldsymbol{k}}(r)=B^n_{p,\boldsymbol{k}}(\mathbf{0},r)$。这里，$\boldsymbol{k}$的作用是切割$\mathbb{R}^n$中的向量。$\boldsymbol{k}$将$\mathbb{R}^n$中的向量$\boldsymbol{x}$和$\boldsymbol{y}$分别切成短向量$\boldsymbol{x}_j:=\left(x_{k_j+1},x_{k_j+2},\ldots,x_{k_{j+1}}\right)$和$\boldsymbol{y}_j:=\left(y_{k_j+1},y_{k_j+2},\ldots,y_{k_{j+1}}\right)$。我们首先计算$\boldsymbol{x}_j$和$\boldsymbol{y}_j$之间的$\ell_2$距离，然后将这些距离$\|\boldsymbol{x}_j-\boldsymbol{y}_j\|_2$列成一个新的向量，再计算这个新的向量的$\ell_p$范数。

在本章中，我们总是假设用于堆积的超球的体积为1，并用$r_{p,\boldsymbol{k},n}$表示体积为1的超球的半径。我们用$\Delta_{p,\boldsymbol{k}}(n)$表示体积为1的超球的最大平移堆积密度，即

$$\Delta_{p,\boldsymbol{k}}(n)=\limsup_{R\to\infty}\sup_{\mathcal{P}}\frac{\mathrm{vol}(\mathcal{P}\cap B^n_{p,\boldsymbol{k}}(R))}{\mathrm{vol}(B^n_{p,\boldsymbol{k}}(R))},$$

其中$\mathrm{vol}(\mathcal{P}\cap B^n_{p,\boldsymbol{k}}(R))$是$B^n_{p,\boldsymbol{k}}(R)$中的被体积为1、球心在$\mathcal{P}$的超球所覆盖的体积，上确界取遍所有的点集$\mathcal{P}\subseteq\mathbb{R}^n$，只要球心在$\mathcal{P}$的超球互不重叠。

特别地，取$\boldsymbol{k}=\boldsymbol{k}_n:=(0,1,2,\ldots,n)$。此时，

$$B^n_{p,\boldsymbol{k}_n}(\boldsymbol{x},r)=\left\{\boldsymbol{y}\in\mathbb{R}^n:\left(\sum_{j=1}^{n}|x_j-y_j|^p\right)^{1/p}\leq r\right\}$$

是$\mathbb{R}^n$中的ℓ_p球。令$\Delta_p(n):=\Delta_{p,\boldsymbol{k}_n}(n)$为$\ell_p$球的最大堆积密度。$\Delta_p(n)$的上界首先由van der Corput和Schaake[79]得到：当$p\geq 2$时，$\Delta_p(n)\leq\frac{1+n/p}{2^{n/p}}$；当$1\leq p\leq 2$时，$\Delta_p(n)\leq\frac{1+(1-1/p)n}{2^{n/p}}$。当$p\geq 1.494\ldots$时，Sah等人[69]做了指数型的改进。Minkowski-Hlawka定理[30]给出了下界$\Delta_{p,\boldsymbol{k}}(n)\geq\zeta(n)2^{-n+1}$，其中$\zeta(n)$是黎曼$\zeta$函数。在$p\geq 3$的情况下，Rush和Sloane[68]改进了$\ell_p$球的Minkowski-Hlawka界，如$\Delta_3(n)\geq 2^{-0.8226\ldots n+o(n)}$。对关于坐标平面对称的任意凸体，Rush[64]构造了密度为$2^{-n+o(n)}$的格堆积。后来，

在$p>2$的情况下，Elkies等人[17]对超球的Minkowski-Hlawka界做了指数型的改进。事实上他们的结果也适用于更一般的凸体。Rush[65–67]以及Liu和Xing[50]还尝试用纠错码来构造下界。

我们主要关注$1<p\le 2$时的下界。在这种情况下，Minkowski-Hlawka界仍然没有指数型的改进。Rogers[61]得到了$\Omega(\sqrt{n}/2^n)$的下界。Schmidt[71]得到了$\Omega(n/2^n)$的下界。后来，Rogers[62]以及Schmidt[72]分别对常数因子做了改进。目前最佳的结果由Schmidt[73]得到，其中的常数因子为$\log\sqrt{2}\approx 0.346$。我们对$\ell_p$球的堆积密度的下界$\Omega(n/2^n)$给出了两个新的证明。

定理3.1. *对任意$1<p\le 2$，存在常数$c_p\in(0,2)$使得*

$$\Delta_p(n)\ge(1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}。$$

事实上，我们的结论对上述定义的超球的堆积密度$\Delta_{p,\boldsymbol{k}}(n)$均成立。

定理3.2. *对任意$p\in(1,2]$，存在常数$c_p\in(0,2)$使得下述命题成立。对任意$\boldsymbol{k}=(k_1,k_2,\dots,k_{m+1})$满足$k_j\in\mathbb{N}\cup\{0\}$且$0=k_1<k_2<\cdots<k_{m+1}=n$，我们有*

$$\Delta_{p,\boldsymbol{k}}(n)\ge(1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}。$$

只要取$\boldsymbol{k}=(0,1,2,\dots,n)$，定理3.1可以直接由定理3.2推出。

定理3.2中的下界与$\boldsymbol{k}$无关。当$\boldsymbol{k}$取不同值的时候，用于堆积的凸体也不同。所以这个结论的意思是，只要给定$1<p\le 2$，再让n取得比较大，那么对于任意的$\boldsymbol{k}=(k_1,k_2,\dots,k_{m+1})$，只要$k_j\in\mathbb{N}\cup\{0\}$且$0=k_1<k_2<\cdots<k_{m+1}=n$，$B^n_{p,\boldsymbol{k}}(\mathbf{0},r_{p,\boldsymbol{k},n})$的平移堆积密度总是渐进大于$\frac{\log(2/c_p)n}{2^n}$。在这一章中，$p$和$\boldsymbol{k}$会出现在许多符号的下标位置，因为那些符号与$p$和$\boldsymbol{k}$有关。不过，我们总是假设$p$是一个取定的数，并且我们的界与$\boldsymbol{k}$无关（例如定理3.2，定理3.4，定理3.5，以及定理3.6）。所以简单起见，下标中的p和$\boldsymbol{k}$可以忽略。

对$p>2$的情况，我们的方法也可以给出下界$\Omega_p(n/2^n)$。但是这个界不如文献[17]的结果。

我们将用两种方法证明定理3.2。在§ 3.3中，我们给出第一个证明。我们的方法叫做刚性超球模型（hard superball model）。这个方法由统计物理发展而来。Jenssen等人用该方法证明了接触数的下界[33]和欧几里得球体的堆积密度的下界[34]。在他

们的文章中，该方法被分别称为刚性球盖模型（hard cap model）和刚性球面模型（hard sphere model）。最近，Fernández等人[22]将这个方法稍作修改，改进了文献[33]和文献[34]的结果中的常数因子。在§ 3.4中，我们给出第二个证明。第二个证明用到图的独立数。我们也会用到一致凸性的概念来克服非欧球体所带来的困难。

我们还研究了球堆积的熵密度和压力。我们会在§ 3.5中给出定义。这些指标衡量了球堆积的丰富程度。

§ 3.2 一致凸空间

在本章中，我们总是假设$\boldsymbol{k}$是一列严格递增的非负整数序列（可以是有限的，也可以是无限的）。令$p \geq 1$。对于$\boldsymbol{k} = (k_1, k_2, \ldots, k_{m+1})$满足$0 = k_1 < k_2 < \cdots < k_{m+1} = n$，以及$\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$，我们定义

$$\|\boldsymbol{x}\|_{p,\boldsymbol{k},n} = \left(\sum_{j=1}^{m} \left\|\left(x_{k_j+1}, x_{k_j+2}, \ldots, x_{k_{j+1}}\right)\right\|_2^p\right)^{1/p} = \left(\sum_{j=1}^{m} \|\boldsymbol{x}_j\|_2^p\right)^{1/p},$$

其中$\boldsymbol{x}_j = (x_{k_j+1}, x_{k_j+2}, \ldots, x_{k_{j+1}})$。对于$\boldsymbol{k} = (k_1, k_2, \ldots, k_{m+1}, \ldots)$满足$0 = k_1 < k_2 < \cdots < k_{m+1} < \cdots$（此时显然有$\lim_{j\to\infty} k_j = \infty$，因为$k_j$都是非负整数），以及$\boldsymbol{x} = (x_1, x_2, x_3, \ldots)$，我们定义

$$\|\boldsymbol{x}\|_{p,\boldsymbol{k}} = \left(\sum_{j=1}^{\infty} \left\|\left(x_{k_j+1}, x_{k_j+2}, \ldots, x_{k_{j+1}}\right)\right\|_2^p\right)^{1/p} = \left(\sum_{j=1}^{\infty} \|\boldsymbol{x}_j\|_2^p\right)^{1/p},$$

其中$\boldsymbol{x}_j = (x_{k_j+1}, x_{k_j+2}, \ldots, x_{k_{j+1}})$。记由所有满足$\|\boldsymbol{x}\|_{p,\boldsymbol{k}} < \infty$的$\boldsymbol{x}$构成的集合为$\ell_{p,\boldsymbol{k}}$。

命题3.1. *对任意$\boldsymbol{k} = (k_1, k_2, \ldots, k_{m+1}, \ldots)$满足$0 = k_1 < k_2 < \cdots < k_{m+1} < \cdots$，以及任意$p \geq 1$，$\ell_{p,\boldsymbol{k}}$是一个赋范线性空间，其中范数为$\|\cdot\|_{p,\boldsymbol{k}}$。*

证明. 任取$\boldsymbol{x} = (x_1, x_2, \ldots), \boldsymbol{y} = (y_1, y_2, \ldots) \in \ell_{p,\boldsymbol{k}}$和$a \in \mathbb{R}$，令

$$\boldsymbol{x}_j = (x_{k_j+1}, x_{k_j+2}, \ldots, x_{k_{j+1}}),$$

$$\boldsymbol{y}_j = (y_{k_j+1}, y_{k_j+2}, \ldots, y_{k_{j+1}})。$$

我们有

$$\begin{aligned}\|\boldsymbol{x}+\boldsymbol{y}\|_{p,\boldsymbol{k}} =& \left(\sum_{j=1}^{\infty}\|\boldsymbol{x}_j+\boldsymbol{y}_j\|_2^p\right)^{1/p}\\ \leq& \left(\sum_{j=1}^{\infty}(\|\boldsymbol{x}_j\|_2+\|\boldsymbol{y}_j\|_2)^p\right)^{1/p}\\ \leq& \left(\sum_{j=1}^{\infty}\|\boldsymbol{x}_j\|_2^p\right)^{1/p}+\left(\sum_{j=1}^{\infty}\|\boldsymbol{y}_j\|_2^p\right)^{1/p}\\ =&\|\boldsymbol{x}\|_{p,\boldsymbol{k}}+\|\boldsymbol{y}\|_{p,\boldsymbol{k}}<\infty,\end{aligned} \tag{3.1}$$

其中第一个不等号是因为ℓ_2范数具有三角不等式，第二个不等号是因为Minkowski不等式

$$\left(\sum_{j=1}^{\infty}(A_j+B_j)^s\right)^{1/s}\leq\left(\sum_{j=1}^{\infty}A_j^s\right)^{1/s}+\left(\sum_{j=1}^{\infty}B_j^s\right)^{1/s}, \tag{3.2}$$

其中$(A_j)_{j\in\mathbb{N}}$和$(B_j)_{j\in\mathbb{N}}$是非负实数序列，$s\geq 1$（若$0<s\leq 1$，那么将不等式(3.2)的不等号变换方向，不等式仍然成立）。另一方面，

$$\begin{aligned}\|a\boldsymbol{x}\|_{p,\boldsymbol{k}} =& \left(\sum_{j=1}^{\infty}\|a\boldsymbol{x}_j\|_2^p\right)^{1/p}\\ =& \left(\sum_{j=1}^{\infty}a^p\|\boldsymbol{x}_j\|_2^p\right)^{1/p}\\ =&|a|\left(\sum_{j=1}^{\infty}\|\boldsymbol{x}_j\|_2^p\right)^{1/p}<\infty。\end{aligned} \tag{3.3}$$

所以在通常的加法和数乘下，$\ell_{p,\boldsymbol{k}}$是一个线性空间，

显然，对任意$\boldsymbol{x}\in\ell_{p,\boldsymbol{k}}$，我们有$\|\boldsymbol{x}\|_{p,\boldsymbol{k}}\geq 0$，并且如果$\|\boldsymbol{x}\|_{p,\boldsymbol{k}}=0$，那么对任意$j$，均有$\boldsymbol{x}_j=\boldsymbol{0}$，即$\boldsymbol{x}=\boldsymbol{0}$。我们已经证明了$\|\cdot\|_{p,\boldsymbol{k}}$具有正齐次性（等式(3.3)）和次可加性（不等式(3.1)）。所以$\|\cdot\|_{p,\boldsymbol{k}}$确实是一个范数。 □

类似地，$\|\boldsymbol{x}\|_{p,\boldsymbol{k},n}$是$\mathbb{R}^n$中的范数。对于$\boldsymbol{x},\boldsymbol{y}\in\mathbb{R}^n$，定义$d_{p,\boldsymbol{k},n}(\boldsymbol{x},\boldsymbol{y}):=\|\boldsymbol{y}-\boldsymbol{x}\|_{p,\boldsymbol{k},n}$为$\mathbb{R}^n$中$\boldsymbol{x}$和$\boldsymbol{y}$之间的$\ell_{p,\boldsymbol{k}}$距离。对于无限序列$\boldsymbol{x},\boldsymbol{y}\in\ell_{p,\boldsymbol{k}}$，定义$d_{p,\boldsymbol{k}}(\boldsymbol{x},\boldsymbol{y}):=\|\boldsymbol{y}-\boldsymbol{x}\|_{p,\boldsymbol{k}}$为$\ell_{p,\boldsymbol{k}}$中的$\boldsymbol{x}$和$\boldsymbol{y}$之间的$\ell_{p,\boldsymbol{k}}$距离。

定义3.1. 我们称一个具有范数$\|\cdot\|$的赋范线性空间是一致凸的（*uniformly convex*），如果对于每一个$\epsilon \in (0,2]$，都有常数$\delta(\epsilon)>0$，使得若$\|x\|=\|y\|=1$和$\|x-y\|\geq\epsilon$，则$\left\|\frac{x+y}{2}\right\|\leq 1-\delta(\epsilon)$。

如果我们记$\boldsymbol{k}_\infty=(0,1,2,3,\ldots)$，那么$\ell_{p,\boldsymbol{k}_\infty}$就是通常的$\ell^p$空间。文献[6]给出了以下定理。

定理3.3 ([6]). 对任意$p>1$，$\ell_{p,\boldsymbol{k}_\infty}$是一致凸的。若$1<p\leq 2$，设$\delta_{p,\boldsymbol{k}_\infty}(\epsilon)$对应定义*3.1*中的常数，那么我们可以取$\delta_{p,\boldsymbol{k}_\infty}(\epsilon)=1-\left(1-\left(\frac{\epsilon}{2}\right)^q\right)^{1/q}$，其中$q=p/(p-1)$是共轭指数。

定理3.3可以作如下推广。

命题3.2. 对任意$\boldsymbol{k}=(k_1,k_2,\ldots,k_{m+1},\ldots)$满足$0=k_1<k_2<\cdots<k_{m+1}<\cdots$，以及对任意$p>1$，$\ell_{p,\boldsymbol{k}}$空间是一致凸的。若$1<p\leq 2$，设$\delta_p(\epsilon)$对应定义*3.1*中的常数，那么我们可以取$\delta_p(\epsilon)=1-\left(1-\left(\frac{\epsilon}{2}\right)^q\right)^{1/q}$，其中$q=p/(p-1)$是共轭指数。

注记3.1. $\delta_p(\epsilon)$的选取与$\boldsymbol{k}$无关。

命题3.2的证明与定理3.3在文献[6]中的证明类似。因此我们首先给出以下引理。该引理是文献[6]中定理2的推广。

引理3.1. 对于如上定义的$\ell_{p,\boldsymbol{k}}$空间，若$p\geq 2$，那么对于任意元素$\boldsymbol{x}$和$\boldsymbol{y}$，我们有如下三个不等式（其中q是共轭指数，$q=p/(p-1)$）。

$$2\left(\|\boldsymbol{x}\|_{p,\boldsymbol{k}}^p+\|\boldsymbol{y}\|_{p,\boldsymbol{k}}^p\right)\leq\|\boldsymbol{x}+\boldsymbol{y}\|_{p,\boldsymbol{k}}^p+\|\boldsymbol{x}-\boldsymbol{y}\|_{p,\boldsymbol{k}}^p\leq 2^{p-1}\left(\|\boldsymbol{x}\|_{p,\boldsymbol{k}}^p+\|\boldsymbol{y}\|_{p,\boldsymbol{k}}^p\right);\tag{3.4}$$

$$2\left(\|\boldsymbol{x}\|_{p,\boldsymbol{k}}^p+\|\boldsymbol{y}\|_{p,\boldsymbol{k}}^p\right)^{q-1}\leq\|\boldsymbol{x}+\boldsymbol{y}\|_{p,\boldsymbol{k}}^q+\|\boldsymbol{x}-\boldsymbol{y}\|_{p,\boldsymbol{k}}^q;\tag{3.5}$$

$$\|\boldsymbol{x}+\boldsymbol{y}\|_{p,\boldsymbol{k}}^p+\|\boldsymbol{x}-\boldsymbol{y}\|_{p,\boldsymbol{k}}^p\leq 2\left(\|\boldsymbol{x}\|_{p,\boldsymbol{k}}^q+\|\boldsymbol{y}\|_{p,\boldsymbol{k}}^q\right)^{p-1}。\tag{3.6}$$

若$1<p\leq 2$，将以上不等式的不等号变换方向，不等式仍然成立。

证明. 简单起见，在该引理的证明中，我们记$\ell = \ell_{p,\boldsymbol{k}}$，$\|\cdot\| = \|\cdot\|_{p,\boldsymbol{k}}$。首先，注意到对于任意$p$，不等式(3.4)的第二个不等号与第一个不等号等价，不等式(3.5)与不等式(3.6)也等价。事实上，令$\boldsymbol{x}+\boldsymbol{y}=\boldsymbol{\xi}, \boldsymbol{x}-\boldsymbol{y}=\boldsymbol{\eta}$，我们有

$$\begin{aligned}
&\|\boldsymbol{x}+\boldsymbol{y}\|^p + \|\boldsymbol{x}-\boldsymbol{y}\|^p \le 2^{p-1}(\|\boldsymbol{x}\|^p + \|\boldsymbol{y}\|^p)\\
\Leftrightarrow &\|\boldsymbol{\xi}\|^p + \|\boldsymbol{\eta}\|^p \le 2^{p-1}(\|(\boldsymbol{\xi}+\boldsymbol{\eta})/2\|^p + \|(\boldsymbol{\xi}-\boldsymbol{\eta})/2\|^p)\\
\Leftrightarrow &\|\boldsymbol{\xi}\|^p + \|\boldsymbol{\eta}\|^p \le 2^{-1}(\|\boldsymbol{\xi}+\boldsymbol{\eta}\|^p + \|\boldsymbol{\xi}-\boldsymbol{\eta}\|^p)\\
\Leftrightarrow &2(\|\boldsymbol{\xi}\|^p + \|\boldsymbol{\eta}\|^p) \le \|\boldsymbol{\xi}+\boldsymbol{\eta}\|^p + \|\boldsymbol{\xi}-\boldsymbol{\eta}\|^p,
\end{aligned}$$

以及

$$\begin{aligned}
&2(\|\boldsymbol{x}\|^p + \|\boldsymbol{y}\|^p)^{q-1} \le \|\boldsymbol{x}+\boldsymbol{y}\|^q + \|\boldsymbol{x}-\boldsymbol{y}\|^q\\
\Leftrightarrow &2(\|(\boldsymbol{\xi}+\boldsymbol{\eta})/2\|^p + \|(\boldsymbol{\xi}-\boldsymbol{\eta})/2\|^p)^{q-1} \le \|\boldsymbol{\xi}\|^q + \|\boldsymbol{\eta}\|^q\\
\Leftrightarrow &2^{1-p(q-1)}(\|\boldsymbol{\xi}+\boldsymbol{\eta}\|^p + \|\boldsymbol{\xi}-\boldsymbol{\eta}\|^p)^{q-1} \le \|\boldsymbol{\xi}\|^q + \|\boldsymbol{\eta}\|^q\\
\Leftrightarrow &\|\boldsymbol{\xi}+\boldsymbol{\eta}\|^p + \|\boldsymbol{\xi}-\boldsymbol{\eta}\|^p \le 2(\|\boldsymbol{\xi}\|^q + \|\boldsymbol{\eta}\|^q)^{p-1}。
\end{aligned}$$

我们首先对$1 < p \le 2$的情况证明不等式(3.5)，即

$$2(\|\boldsymbol{x}\|^p + \|\boldsymbol{y}\|^p)^{q-1} \ge \|\boldsymbol{x}+\boldsymbol{y}\|^q + \|\boldsymbol{x}-\boldsymbol{y}\|^q。 \tag{3.7}$$

我们声明，对于$\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{R}^k$，有

$$2\left(\|\boldsymbol{\alpha}\|_2^p + \|\boldsymbol{\beta}\|_2^p\right)^{q-1} \ge \|\boldsymbol{\alpha}+\boldsymbol{\beta}\|_2^q + \|\boldsymbol{\alpha}-\boldsymbol{\beta}\|_2^q。 \tag{3.8}$$

如果$\boldsymbol{\alpha}$和$\boldsymbol{\beta}$中有一个是$\boldsymbol{0}$，那么不等式(3.8)显然成立。现假设$\|\boldsymbol{\alpha}\|_2 \ge \|\boldsymbol{\beta}\|_2 > 0$。在不等式(3.8)两边同时除以$\|\boldsymbol{\alpha}\|_2^q$，并利用范数的正齐次性，不等式(3.8)化为

$$2\left(\left\|\frac{\boldsymbol{\alpha}}{\|\boldsymbol{\alpha}\|_2}\right\|_2^p + \left\|\frac{\boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|_2}\right\|_2^p\right)^{q-1} \ge \left\|\frac{\boldsymbol{\alpha}}{\|\boldsymbol{\alpha}\|_2} + \frac{\boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|_2}\right\|_2^q + \left\|\frac{\boldsymbol{\alpha}}{\|\boldsymbol{\alpha}\|_2} - \frac{\boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|_2}\right\|_2^q。 \tag{3.9}$$

令$\boldsymbol{a} = \frac{\boldsymbol{\alpha}}{\|\boldsymbol{\alpha}\|_2}$，$\boldsymbol{b} = \frac{\boldsymbol{\beta}}{\|\boldsymbol{\alpha}\|_2}$。那么$\|\boldsymbol{a}\|_2 = 1$且$\|\boldsymbol{b}\|_2 \le 1$，此时不等式(3.9)等价于

$$2\left(1 + \|\boldsymbol{b}\|_2^p\right)^{q-1} \ge \|\boldsymbol{a}+\boldsymbol{b}\|_2^q + \|\boldsymbol{a}-\boldsymbol{b}\|_2^q,$$

即

$$2\left(1 + \|\boldsymbol{b}\|_2^p\right)^{q-1} \ge \left(\|\boldsymbol{a}\|_2^2 + \|\boldsymbol{b}\|_2^2 + 2\boldsymbol{a}\cdot\boldsymbol{b}\right)^{q/2} + \left(\|\boldsymbol{a}\|_2^2 + \|\boldsymbol{b}\|_2^2 - 2\boldsymbol{a}\cdot\boldsymbol{b}\right)^{q/2},$$

即

$$2\left(1+\|\boldsymbol{b}\|_2^p\right)^{q-1} \geq \left(1+\|\boldsymbol{b}\|_2^2+2\boldsymbol{a}\cdot\boldsymbol{b}\right)^{q/2}+\left(1+\|\boldsymbol{b}\|_2^2-2\boldsymbol{a}\cdot\boldsymbol{b}\right)^{q/2},$$

其中$\boldsymbol{a}\cdot\boldsymbol{b}$为通常的内积。设$\|\boldsymbol{b}\|_2 = b \in [0,1]$，则

$$|\boldsymbol{a}\cdot\boldsymbol{b}| \leq \|\boldsymbol{a}\|_2 \|\boldsymbol{b}\|_2 = b。$$

不妨假设$\boldsymbol{a}\cdot\boldsymbol{b} \in [0,b]$。考虑函数

$$g(x) = (1+b^2+2x)^{q/2}+(1+b^2-2x)^{q/2},\ x \in [0,b]。$$

当$x \in [0,b]$时，因为$q \geq 2$，我们有$g'(x) = q(1+b^2+2x)^{q/2-1}-q(1+b^2-2x)^{q/2-1} \geq 0$。所以$\max g(x) = g(b) = (1+b^2+2b)^{q/2}+(1+b^2-2b)^{q/2} = (b+1)^q+(1-b)^q$。这样就只需证明

$$2\left(1+b^p\right)^{q-1} \geq (1+b)^q+(1-b)^q。 \tag{3.10}$$

文献[6]已经证明了不等式(3.10)（见文献[6]的定理2）。所以不等式(3.8)成立，

现在我们证明不等式(3.7)。设$\boldsymbol{x} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots) = (x_1, x_2, \ldots), \boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots) = (y_1, y_2, \ldots) \in \ell$，其中

$$\boldsymbol{x}_j = (x_{k_j+1}, x_{k_j+2}, \ldots, x_{k_{j+1}}),$$

$$\boldsymbol{y}_j = (y_{k_j+1}, y_{k_j+2}, \ldots, y_{k_{j+1}})。$$

不等式(3.7)指的是

$$2\left(\sum_{j=1}^{\infty}\left(\|\boldsymbol{x}_j\|_2^p+\|\boldsymbol{y}_j\|_2^p\right)\right)^{q-1} \geq \left(\sum_{j=1}^{\infty}\|\boldsymbol{x}_j+\boldsymbol{y}_j\|_2^p\right)^{\frac{q}{p}}+\left(\sum_{j=1}^{\infty}\|\boldsymbol{x}_j-\boldsymbol{y}_j\|_2^p\right)^{\frac{q}{p}}。 \tag{3.11}$$

在变换不等号方向后的Minkowski不等式(3.2)中，取$A_j = \|\boldsymbol{x}_j+\boldsymbol{y}_j\|_2^q$，$B_j = \|\boldsymbol{x}_j-\boldsymbol{y}_j\|_2^q$，$s = p/q \leq 1$。这样的话，不等式(3.11)的右边就是

$$\begin{aligned}
&\left(\sum_{j=1}^{\infty}A_j^s\right)^{1/s}+\left(\sum_{j=1}^{\infty}B_j^s\right)^{1/s} \\
\leq &\left(\sum_{j=1}^{\infty}(A_j+B_j)^s\right)^{1/s} \\
= &\left(\sum_{j=1}^{\infty}\left(\|\boldsymbol{x}_j+\boldsymbol{y}_j\|_2^q+\|\boldsymbol{x}_j-\boldsymbol{y}_j\|_2^q\right)^{p/q}\right)^{q/p},
\end{aligned} \tag{3.12}$$

而根据不等式(3.8)又有

$$\leq \left(\sum_{j=1}^{\infty} \left(2 \left(\|\boldsymbol{x}_j\|_2^p + \|\boldsymbol{y}_j\|_2^p \right)^{q-1} \right)^{p/q} \right)^{q/p} = 2 \left(\sum_{j=1}^{\infty} \left(\|\boldsymbol{x}_j\|_2^p + \|\boldsymbol{y}_j\|_2^p \right) \right)^{q/p} 。$$

因为$q/p = q - 1$，所以我们完成了不等式(3.5)在$1 < p \leq 2$时的证明。

现在我们在$p \geq 2$时证明不等式(3.5)。我们首先需要证明变换不等号方向后的不等式(3.11)，即

$$2 \left(\sum_{j=1}^{\infty} \left(\|\boldsymbol{x}_j\|_2^p + \|\boldsymbol{y}_j\|_2^p \right) \right)^{q-1} \leq \left(\sum_{j=1}^{\infty} \|\boldsymbol{x}_j + \boldsymbol{y}_j\|_2^p \right)^{q/p} + \left(\sum_{j=1}^{\infty} \|\boldsymbol{x}_j - \boldsymbol{y}_j\|_2^p \right)^{q/p} 。 \tag{3.13}$$

A_j，B_j和s仍取成与前面相同的值。再利用Minkowski不等式(3.2)，我们就知道不等式(3.13)的右边为

$$\begin{aligned} & \left(\sum_{j=1}^{\infty} A_j^s \right)^{1/s} + \left(\sum_{j=1}^{\infty} B_j^s \right)^{1/s} \\ \geq & \left(\sum_{j=1}^{\infty} \left(A_j + B_j \right)^s \right)^{1/s} \\ = & \left(\sum_{j=1}^{\infty} \left(\|\boldsymbol{x}_j + \boldsymbol{y}_j\|_2^q + \|\boldsymbol{x}_j - \boldsymbol{y}_j\|_2^q \right)^{p/q} \right)^{q/p} 。 \end{aligned} \tag{3.14}$$

我们已经对$1 < p \leq 2$的情况证明了不等式(3.8)，而它又等价于

$$\|\boldsymbol{\alpha} + \boldsymbol{\beta}\|_2^p + \|\boldsymbol{\alpha} - \boldsymbol{\beta}\|_2^p \geq 2 \left(\|\boldsymbol{\alpha}\|_2^q + \|\boldsymbol{\beta}\|_2^q \right)^{p-1} 。$$

交换p和q以后，我们有

$$\|\boldsymbol{\alpha} + \boldsymbol{\beta}\|_2^q + \|\boldsymbol{\alpha} - \boldsymbol{\beta}\|_2^q \geq 2 \left(\|\boldsymbol{\alpha}\|_2^p + \|\boldsymbol{\beta}\|_2^p \right)^{q-1} ,$$

对$p \geq 2$成立。所以不等式(3.14)

$$\geq \left(\sum_{j=1}^{\infty} \left(2 \left(\|\boldsymbol{x}_j\|_2^p + \|\boldsymbol{y}_j\|_2^p \right)^{q-1} \right)^{p/q} \right)^{q/p} = 2 \left(\sum_{j=1}^{\infty} \left(\|\boldsymbol{x}_j\|_2^p + \|\boldsymbol{y}_j\|_2^p \right) \right)^{q-1} 。$$

所以，我们完成了不等式(3.5)在$p \geq 2$时的证明。

最后，我们证明不等式(3.4)。令$p \geq 2$，考虑不等式(3.4)的第二个不等号。事实上，这可以由不等式(3.6)简单推出：对于$x, y \geq 0$，我们有

$$2(x^q + y^q)^{p-1} \leq 2^{p-1}(x^p + y^p)。 \tag{3.15}$$

文献[6]已经给出了不等式(3.15)的证明（见文献[6]中定理2的证明）。对于$1 < p \leq 2$的情况，由不等式(3.15)得

$$2(x^q + y^q)^{p-1} \geq 2^{p-1}(x^p + y^p)。 \tag{3.16}$$

不等式(3.4)的第二个不等号（需要变换方向，因为此时$1 < p \leq 2$）可以由不等式(3.6)（需要变换不等号方向）和不等式(3.16)推出。 □

现在我们可以证明命题3.2。

命题3.2的证明. 当$p \geq 2$时，在不等式(3.4)中令$\|\boldsymbol{x}\|_{p,\boldsymbol{k}} = \|\boldsymbol{y}\|_{p,\boldsymbol{k}} = 1$，我们有

$$\|\boldsymbol{x} + \boldsymbol{y}\|_{p,\boldsymbol{k}}^p + \|\boldsymbol{x} - \boldsymbol{y}\|_{p,\boldsymbol{k}}^p \leq 2^p。$$

若$\|\boldsymbol{x} - \boldsymbol{y}\|_{p,\boldsymbol{k}} \geq \epsilon$，则

$$\left\|\frac{\boldsymbol{x} + \boldsymbol{y}}{2}\right\|_{p,\boldsymbol{k}} \leq (1 - (\epsilon/2)^p)^{1/p}。$$

所以我们可以取$\delta(\epsilon) = 1 - (1 - (\epsilon/2)^p)^{1/p}$。类似地，当$1 < p \leq 2$时，根据不等式(3.5)，我们可以取$\delta(\epsilon) = 1 - (1 - (\epsilon/2)^q)^{1/q}$。 □

§3.3 刚性超球模型

给定$p > 1, n \in \mathbb{N}$，以及$\boldsymbol{k} = (k_1, k_2, \ldots, k_{m+1})$满足$0 = k_1 < k_2 < \cdots < k_{m+1} = n$，我们考虑$B_{p,\boldsymbol{k}}^n(\boldsymbol{0}, r_{p,\boldsymbol{k},n})$的平移堆积。对于一个有界的可测集$S \subseteq \mathbb{R}^n$，记

$$P_{t,p,\boldsymbol{k}}(S) = \{\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_t\} \subseteq S : d_{p,\boldsymbol{k},n}(\boldsymbol{x}_i, \boldsymbol{x}_j) \geq 2r_{p,\boldsymbol{k},n} \forall i \neq j\}$$

为S中所有可以构成堆积的无序t元组构成的集合。

S上t个球心的*典型刚性超球模型*（canonical hard superball model）为$P_{t,p,\boldsymbol{k}}(S)$中均匀随机选取的一个$t$元组$X_{t,p,\boldsymbol{k}}$。$S$上的典型刚性超球模型的配分函数（partition function）为

$$\hat{Z}_{S,p,\boldsymbol{k}}(t) = \frac{1}{t!}\int_{S^t} \mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)} d\boldsymbol{x}_1 d\boldsymbol{x}_2 \cdots d\boldsymbol{x}_t, \tag{3.17}$$

其中对于$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_t \in \mathbb{R}^n$，$\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_t)$表示事件

“对任意$i \neq j$，均有$d_{p,\boldsymbol{k},n}(\boldsymbol{x}_i, \boldsymbol{x}_j) \geq 2r_{p,\boldsymbol{k},n}$”。

S上逸度（fugacity）为λ的*总典型刚性超球模型*（grand canonical hard superball model）为一个随机无序点集X，其中X在事件

“对任意不同的$\boldsymbol{x}, \boldsymbol{y} \in X$，均有$d_{p,\boldsymbol{k},n}(\boldsymbol{x}, \boldsymbol{y}) \geq 2r_{p,\boldsymbol{k},n}$”

的条件下服从强度为λ的泊松分布。换句话说，我们首先从$\{0, 1, 2, \ldots\}$中以正比于$\lambda^t \hat{Z}_{S,p,\boldsymbol{k}}(t)$的概率选取$t$，然后我们从$P_{t,p,\boldsymbol{k}}(S)$中均匀地选取$X$。$S$上的总典型刚性超球模型的配分函数为

$$Z_{S,p,\boldsymbol{k}}(\lambda) = \sum_{t=0}^{\infty} \lambda^t \hat{Z}_{S,p,\boldsymbol{k}}(t), \tag{3.18}$$

其中我们取$\hat{Z}_{S,p,\boldsymbol{k}}(0) = 1$。如果$S$是有界的，那么$Z_{S,p,\boldsymbol{k}}(\lambda)$就是一个关于$\lambda$的多项式。

刚性超球模型的*期望堆积密度*$\alpha_{S,p,\boldsymbol{k}}(\lambda)$为$S$中的球心数目的期望，并由$S$的体积标准化，即

$$\alpha_{S,p,\boldsymbol{k}}(\lambda) = \frac{\mathbb{E}_{S,p,\boldsymbol{k},\lambda}|X|}{\mathrm{vol}(S)}。$$

此处以及本章后续的论述中，$\mathbb{P}_{S,p,\boldsymbol{k},\lambda}$和$\mathbb{E}_{S,p,\boldsymbol{k},\lambda}$分别对应$S$上逸度为$\lambda$的总典型刚性超球模型中的概率和期望。

期望堆积密度可以表示成标准化的对数配分函数的导数。

$$\begin{aligned}
\alpha_{S,p,\boldsymbol{k}}(\lambda) &= \frac{1}{\mathrm{vol}(S)} \sum_{t=1}^{\infty} t \cdot \mathbb{P}_{S,p,\boldsymbol{k},\lambda}(|X| = t) \\
&= \frac{1}{\mathrm{vol}(S)} \sum_{t=1}^{\infty} \frac{t \cdot \lambda^t \hat{Z}_{S,p,\boldsymbol{k}}(t)}{Z_{S,p,\boldsymbol{k}}(\lambda)} \\
&= \frac{1}{\mathrm{vol}(S)} \frac{\lambda \cdot (Z_{S,p,\boldsymbol{k}}(\lambda))'}{Z_{S,p,\boldsymbol{k}}(\lambda)} \\
&= \frac{\lambda}{\mathrm{vol}(S)} (\log Z_{S,p,\boldsymbol{k}}(\lambda))'。
\end{aligned} \tag{3.19}$$

此处以及本章后续的论述中，$\log x$总是表示x的自然对数。

引理3.2. *$B^n_{p,\boldsymbol{k}}(R) \subseteq \mathbb{R}^n$的渐进期望堆积密度是最大超球堆积密度的一个下界。也就是说，对任意$\lambda > 0$，我们有*

$$\Delta_{p,\boldsymbol{k}}(n) \geq \limsup_{R \to \infty} \alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lambda)。$$

证明. 根据$\Delta_{p,\boldsymbol{k}}(n)$的定义，有

$$\Delta_{p,\boldsymbol{k}}(n)=\limsup_{R\to\infty}\sup_{X\in\mathcal{P}}\frac{|X|}{(R/r_{p,\boldsymbol{k},n})^n},$$

其中$\mathcal{P}$为$B^n_{p,\boldsymbol{k}}(R)$中半径为$r=r_{p,\boldsymbol{k},n}$的超球形成的所有堆积构成的集合，$(R/r_{p,\boldsymbol{k},n})^n$是$B^n_{p,\boldsymbol{k}}(R)$的体积。在该模型中，一些球心可能会在$B^n_{p,\boldsymbol{k}}(R)$的边界处，这些球心不应算在堆积中。不过，我们可以将$B^n_{p,\boldsymbol{k}}(R)$的半径稍作扩大，使得这些球心仍能形成堆积。换句话说，如果X是从$B^n_{p,\boldsymbol{k}}(R)$上的模型中选出的点集，那么$X$是$B^n_{p,\boldsymbol{k}}(R+100)$中的一个堆积。此时

$$\begin{aligned}\Delta_{p,\boldsymbol{k}}(n)&\geq\limsup_{R\to\infty}\frac{\mathbb{E}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}(|X|)}{((R+100)/r_{p,\boldsymbol{k},n})^n}\\&=\limsup_{R\to\infty}\frac{\mathbb{E}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}(|X|)}{((R+100)/r_{p,\boldsymbol{k},n})^n}\cdot\frac{((R+100)/r_{p,\boldsymbol{k},n})^n}{(R/r_{p,\boldsymbol{k},n})^n}\\&=\limsup_{R\to\infty}\frac{\mathbb{E}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}(|X|)}{(R/r_{p,\boldsymbol{k},n})^n}\\&=\limsup_{R\to\infty}\alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lambda)。\end{aligned}$$

□

定理3.4. 对任意$p\in(1,2]$，存在常数$c_p\in(0,2)$使得下述命题成立。令$S\subseteq\mathbb{R}^n$为有界可测集，且体积为正，那么对任意$\boldsymbol{k}=(k_1,k_2,\ldots,k_{m+1})$满足$0=k_1<k_2<\cdots<k_{m+1}=n$，以及任意$\lambda\geq n^{-1}c_p^{-n}$，我们有

$$\alpha_{S,p,\boldsymbol{k}}(\lambda)\geq(1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}。$$

注记3.2. 定理*3.4*中的常数c_p与n和$\boldsymbol{k}$无关。

由引理3.2和定理3.4可以直接推出定理3.2。

引理3.3. 令$S\subseteq\mathbb{R}^n$为有界可测集，并且体积为正，期望堆积密度$\alpha_{S,p,\boldsymbol{k}}(\lambda)$随$\lambda$严格递增。

证明. 利用等式(3.19)，我们有

$$\begin{aligned}&\lambda\cdot\mathrm{vol}(S)\cdot\alpha'_{S,p,\boldsymbol{k}}(\lambda)\\=&\lambda\cdot\left(\frac{\lambda\cdot(Z_{S,p,\boldsymbol{k}}(\lambda))'}{Z_{S,p,\boldsymbol{k}}(\lambda)}\right)'\\=&\lambda\cdot\left(\frac{(Z_{S,p,\boldsymbol{k}}(\lambda))'+\lambda\cdot(Z_{S,p,\boldsymbol{k}}(\lambda))''}{Z_{S,p,\boldsymbol{k}}(\lambda)}-\frac{\lambda\cdot[(Z_{S,p,\boldsymbol{k}}(\lambda))']^2}{(Z_{S,p,\boldsymbol{k}}(\lambda))^2}\right)。\end{aligned}$$

因为

$$\lambda \cdot \frac{(Z_{S,p,\boldsymbol{k}}(\lambda))'}{Z_{S,p,\boldsymbol{k}}(\lambda)} = \mathrm{vol}(S) \cdot \alpha_{S,p,\boldsymbol{k}} = \mathbb{E}_{S,p,\boldsymbol{k},\lambda}|X|$$

且

$$\begin{aligned}
&\lambda \cdot \frac{\lambda \cdot (Z_{S,p,\boldsymbol{k}}(\lambda))''}{Z_{S,p,\boldsymbol{k}}(\lambda)} \\
=&\lambda^2 \cdot \frac{\sum_{t=2}^{\infty} t(t-1)\lambda^{t-2}\hat{Z}_{S,p,\boldsymbol{k}}(t)}{Z_{S,p,\boldsymbol{k}}(\lambda)} \\
=&\sum_{t=2}^{\infty} t(t-1)\mathbb{P}_{S,p,\boldsymbol{k},\lambda}(|X|=t) \\
=&\mathbb{E}_{S,p,\boldsymbol{k},\lambda}[|X|(|X|-1)],
\end{aligned}$$

所以

$$\begin{aligned}
&\lambda \cdot \mathrm{vol}(S) \cdot \alpha'_{S,p,\boldsymbol{k}}(\lambda) \\
=&\mathbb{E}_{S,p,\boldsymbol{k},\lambda}|X| + \mathbb{E}_{S,p,\boldsymbol{k},\lambda}[|X|(|X|-1)] - (\mathbb{E}_{S,p,\boldsymbol{k},\lambda}|X|)^2 \qquad (3.20)\\
=&\mathrm{Var}(|X|) > 0。
\end{aligned}$$

所以$\alpha_{S,p,\boldsymbol{k}}(\lambda)$严格递增。 □

我们用$\mathrm{FV}_{S,p,\boldsymbol{k}}(\lambda)$表示刚性超球模型的自由体积（free volume）的期望。换句话说，$\mathrm{FV}_{S,p,\boldsymbol{k}}(\lambda)$是$S$中与$X$的距离至少为$2r_{p,\boldsymbol{k},n}$的点所占的体积比的期望。

$$\mathrm{FV}_{S,p,\boldsymbol{k}}(\lambda) = \frac{\mathbb{E}_{S,p,\boldsymbol{k},\lambda}\left[\mathrm{vol}(\{\boldsymbol{y} \in S : d_{p,\boldsymbol{k},n}(\boldsymbol{y},\boldsymbol{x}) \geq 2r_{p,\boldsymbol{k},n} \forall \boldsymbol{x} \in X\})\right]}{\mathrm{vol}(S)}。$$

引理3.4. 令$S \subseteq \mathbb{R}^n$为有界可测集，并且体积为正。则

$$\alpha_{S,p,\boldsymbol{k}}(\lambda) = \lambda \cdot \mathrm{FV}_{S,p,\boldsymbol{k}}(\lambda)。$$

证明. 根据$\alpha_{S,p,\boldsymbol{k}}(\lambda)$和$\mathrm{FV}_{S,p,\boldsymbol{k}}(\lambda)$的定义，我们有

$$\begin{aligned}
&\alpha_{S,p,\boldsymbol{k}}(\lambda)\\
=&\frac{\mathbb{E}_{S,p,\boldsymbol{k},\lambda}|X|}{\mathrm{vol}(S)}\\
=&\frac{1}{\mathrm{vol}(S)}\sum_{t=0}^{\infty}(t+1)\cdot\mathbb{P}_{S,p,\boldsymbol{k},\lambda}(|X|=t+1)\\
=&\frac{t+1}{\mathrm{vol}(S)Z_{S,p,\boldsymbol{k}}(\lambda)}\sum_{t=0}^{\infty}\int_{S^{t+1}}\frac{\lambda^{t+1}}{(t+1)!}\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_0d\boldsymbol{x}_1\cdots d\boldsymbol{x}_t\\
=&\frac{\lambda}{\mathrm{vol}(S)Z_{S,p,\boldsymbol{k}}(\lambda)}\sum_{t=0}^{\infty}\int_{S^{t+1}}\frac{\lambda^{t}}{t!}\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_0d\boldsymbol{x}_1\cdots d\boldsymbol{x}_t\\
=&\frac{\lambda}{\mathrm{vol}(S)Z_{S,p,\boldsymbol{k}}(\lambda)}\sum_{t=0}^{\infty}\int_{S^{t}}\frac{\lambda^{t}}{t!}\left(\int_S\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_0\right)d\boldsymbol{x}_1\cdots d\boldsymbol{x}_t。
\end{aligned}$$

令$Y=\mathrm{vol}(\{\boldsymbol{y}\in S:d_{p,\boldsymbol{k},n}(\boldsymbol{y},\boldsymbol{x})\geq 2r_{p,\boldsymbol{k},n}\forall\boldsymbol{x}\in X\})$。则

$$\mathbb{E}_{S,p,\boldsymbol{k},\lambda}\left(Y|X=\{\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t\}\right)=\int_S\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_0。$$

所以

$$\begin{aligned}
&\lambda\cdot\mathrm{FV}_{S,p,\boldsymbol{k}}(\lambda)\\
=&\frac{\lambda}{\mathrm{vol}(S)}\cdot\mathbb{E}_{S,p,\boldsymbol{k},\lambda}\left(Y\right)\\
=&\frac{\lambda}{\mathrm{vol}(S)}\cdot\mathbb{E}_{S,p,\boldsymbol{k},\lambda}\left[\mathbb{E}_{S,p,\boldsymbol{k},\lambda}\left(Y|X=\{\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t\}\right)\right]\\
=&\frac{\lambda}{\mathrm{vol}(S)}\sum_{t=0}^{\infty}\frac{\lambda^t}{Z_{S,p,\boldsymbol{k}}(\lambda)}\frac{1}{t!}\int_{S^t}\int_S\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_0\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_1\cdots d\boldsymbol{x}_t\\
=&\frac{\lambda}{\mathrm{vol}(S)Z_{S,p,\boldsymbol{k}}(\lambda)}\sum_{t=0}^{\infty}\int_{S^t}\frac{\lambda^t}{t!}\left(\int_S\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_0\right)d\boldsymbol{x}_1\cdots d\boldsymbol{x}_t\\
=&\alpha_{S,p,\boldsymbol{k}}(\lambda),
\end{aligned}$$

其中当$t=0$时，$\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)}\equiv 1$（因为此时$\hat{Z}_{S,p,\boldsymbol{k}}(0)=1$）。 □

现在我们考虑下面这个二部试验：先从S上逸度为λ的刚性超球模型中选取一个点集X，再独立地从S中选一个点$\boldsymbol{v}$。我们定义一个随机集合

$$\mathrm{T}=\{\boldsymbol{x}\in B^n_{p,\boldsymbol{k}}(\boldsymbol{v},2r_{p,\boldsymbol{k},n})\cap S:d_{p,\boldsymbol{k},n}(\boldsymbol{x},\boldsymbol{y})\geq 2r_{p,\boldsymbol{k},n}\forall\boldsymbol{y}\in X\cap B^n_{p,\boldsymbol{k}}(\boldsymbol{v},2r_{p,\boldsymbol{k},n})^c\}。\tag{3.21}$$

换句话说，T由S中这样的点所构成：这些点在$B^n_{p,\boldsymbol{k}}(\boldsymbol{v}, 2r_{p,\boldsymbol{k},n})$中，并且没有被$B^n_{p,\boldsymbol{k}}(\boldsymbol{v}, 2r_{p,\boldsymbol{k},n})$外面的点阻止形成一个球心。

引理3.5. 令$S \subseteq \mathbb{R}^n$为有界可测集，并且体积为正。则

$$\alpha_{S,p,\boldsymbol{k}}(\lambda) = \lambda \cdot \mathbb{E}\left[\frac{1}{Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)}\right] \tag{3.22}$$

且

$$\alpha_{S,p,\boldsymbol{k}}(\lambda) \geq 2^{-n} \cdot \mathbb{E}\left[\frac{\lambda \cdot (Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda))'}{Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)}\right], \tag{3.23}$$

其中以上两个期望都是关于以上定义的二部试验。

证明. 利用引理3.4，我们有

$$\begin{aligned}
\alpha_{S,p,\boldsymbol{k}}(\lambda) &= \lambda \cdot \mathrm{FV}_{S,p,\boldsymbol{k}}(\lambda) \\
&= \frac{\lambda}{\mathrm{vol}(S)} \cdot \int_S \mathbb{P}[d_{p,\boldsymbol{k},n}(\boldsymbol{x}, \boldsymbol{y}) \geq 2r_{p,\boldsymbol{k},n}, \forall \boldsymbol{x} \in X] d\boldsymbol{y} \\
&= \lambda \cdot \mathbb{E}(\mathbf{1}_{\mathrm{T} \cap X = \emptyset}) \\
&= \lambda \cdot \mathbb{E}\left[\frac{1}{Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)}\right],
\end{aligned}$$

最后一个等号用到刚性超球模型的空间Markov性：在$X \cap B^n_{p,\boldsymbol{k}}(\boldsymbol{v}, 2r_{p,\boldsymbol{k},n})^c$的条件下，$X \cap B^n_{p,\boldsymbol{k}}(\boldsymbol{v}, 2r_{p,\boldsymbol{k},n})$的分布与T上的刚性超球模型相同。

对任意$\boldsymbol{x} \in S$，$\mathbb{P}(\boldsymbol{x} \in B^n_{p,\boldsymbol{k}}(\boldsymbol{v}, 2r_{p,\boldsymbol{k},n})) = \mathrm{vol}(B^n_{p,\boldsymbol{k}}(\boldsymbol{v}, 2r_{p,\boldsymbol{k},n}) \cap S)/\mathrm{vol}(S) \leq 2^n/\mathrm{vol}(S)$。所以

$$\begin{aligned}
\alpha_{S,p,\boldsymbol{k}}(\lambda) &= \frac{\mathbb{E}_{S,p,\boldsymbol{k},\lambda}|X|}{\mathrm{vol}(S)} \\
&\geq 2^{-n}\mathbb{E}(|X \cap B^n_{p,\boldsymbol{k}}(\boldsymbol{v}, 2r_{p,\boldsymbol{k},n})|) \\
&= 2^{-n}\mathbb{E}(\alpha_{\mathrm{T},p,\boldsymbol{k}}(\lambda) \cdot \mathrm{vol}(\mathrm{T})) \\
&= 2^{-n} \cdot \mathbb{E}\left[\frac{\lambda \cdot (Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda))'}{Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)}\right]。
\end{aligned}$$

□

引理3.6. 令$S \subseteq \mathbb{R}^n$为有界可测集。则

$$\log Z_{S,p,\boldsymbol{k}}(\lambda) \leq \lambda \cdot \mathrm{vol}(S)。 \tag{3.24}$$

进一步如果S的体积为正，则

$$\alpha_{S,p,\boldsymbol{k}}(\lambda) \geq \lambda \cdot e^{-\lambda \cdot \mathbb{E}[\mathrm{vol(T)}]}。 \tag{3.25}$$

证明. 根据$Z_{S,p,\boldsymbol{k}}(\lambda)$的定义，我们有

$$\begin{aligned} Z_{S,p,\boldsymbol{k}}(\lambda) &= \sum_{t=0}^{\infty} \lambda^t \hat{Z}_{S,p,\boldsymbol{k}}(t) \\ &= \sum_{t=0}^{\infty} \frac{\lambda^t}{t!} \int_{S^t} \mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)} d\boldsymbol{x}_1 d\boldsymbol{x}_2 \cdots d\boldsymbol{x}_t \\ &\leq \sum_{t=0}^{\infty} \frac{\lambda^t}{t!} \int_{S^t} d\boldsymbol{x}_1 d\boldsymbol{x}_2 \cdots d\boldsymbol{x}_t \\ &= \sum_{t=0}^{\infty} \frac{\lambda^t}{t!} (\mathrm{vol}(S))^t \\ &= e^{\lambda \cdot \mathrm{vol}(S)}。 \end{aligned}$$

取对数后我们得到不等式(3.24)。

对于不等式(3.25)，我们利用等式(3.22)和不等式(3.24)。所以

$$\begin{aligned} \alpha_{S,p,\boldsymbol{k}}(\lambda) &= \lambda \cdot \mathbb{E}\left[\frac{1}{Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)}\right] \\ &\geq \lambda \cdot \mathbb{E}\left[e^{-\lambda \cdot \mathrm{vol(T)}}\right] \\ &\geq \lambda \cdot e^{-\lambda \cdot \mathbb{E}[\mathrm{vol(T)}]}, \end{aligned}$$

其中最后一个不等号是因为Jensen不等式。 □

注记3.3. 在文献*[34]*中，引理*3.3-3.6*是针对欧几里得球而言的。事实上这些引理对我们这里定义的超球也适用。

考虑函数

$$h(x) = \left(\frac{x}{4} + \frac{1}{2} - \frac{1}{x}\right)^q + \left(\frac{x+2}{4}\right)^q - 1。$$

注意到当$x \geq 1.5$时，$h(x)$连续，且$h(2) = 1/2^q > 0$，所以存在$x_p \in (1.5, 2)$使得对任意$x \in [x_p, 2]$都有$h(x) > 1/3^q$。我们将在下面这个引理的证明中用到x_p。

引理3.7. 对任意$p \in (1, 2]$，存在一个常数$c_p \in (0, 2)$使得下述命题成立。对任意$n \in \mathbb{N}$和$\boldsymbol{k} = (k_1, k_2, \ldots, k_{m+1})$满足$0 = k_1 < k_2 < \cdots < k_{m+1} = n$，设$S \subseteq B^n_{p,\boldsymbol{k}}(2r_{p,\boldsymbol{k},n})$可测。那么

$$\mathbb{E}\left[\mathrm{vol}(B^n_{p,\boldsymbol{k}}(\boldsymbol{u}, 2r_{p,\boldsymbol{k},n}) \cap S)\right] \leq 2 \cdot c_p^n, \tag{3.26}$$

其中$\boldsymbol{u}$是S中均匀随机选取的点。特别地，

$$\alpha_{S,p,\boldsymbol{k}}(\lambda) \geq \lambda \cdot e^{-\lambda \cdot 2 \cdot c_p^n}。 \tag{3.27}$$

注记3.4. 定理*3.4*中的常数c_p即为这里的常数c_p。所以我们用同一个符号。

证明. 显然，我们可以假设S的体积为正。我们有

$$\begin{aligned}
&\mathbb{E}\left[\mathrm{vol}(B_{p,\boldsymbol{k}}^n(\boldsymbol{u}, 2r_{p,\boldsymbol{k},n}) \cap S)\right] \\
=&\frac{1}{\mathrm{vol}(S)} \int_S \int_S \mathbf{1}_{d_{p,\boldsymbol{k},n}(\boldsymbol{u},\boldsymbol{v}) \leq 2r_{p,\boldsymbol{k},n}} d\boldsymbol{v} d\boldsymbol{u} \\
=&\frac{2}{\mathrm{vol}(S)} \int_S \int_S \mathbf{1}_{d_{p,\boldsymbol{k},n}(\boldsymbol{u},\boldsymbol{v}) \leq 2r_{p,\boldsymbol{k},n}} \cdot \mathbf{1}_{\|v\|_{p,\boldsymbol{k},n} \leq \|u\|_{p,\boldsymbol{k},n}} d\boldsymbol{v} d\boldsymbol{u} \\
\leq&2 \max_{\boldsymbol{u} \in B_{p,\boldsymbol{k}}^n(2r_{p,\boldsymbol{k},n})} \int_S \mathbf{1}_{d_{p,\boldsymbol{k},n}(\boldsymbol{u},\boldsymbol{v}) \leq 2r_{p,\boldsymbol{k},n}} \cdot \mathbf{1}_{\|v\|_{p,\boldsymbol{k},n} \leq \|u\|_{p,\boldsymbol{k},n}} d\boldsymbol{v} \\
\leq&2 \max_{\boldsymbol{u} \in B_{p,\boldsymbol{k}}^n(2r_{p,\boldsymbol{k},n})} \mathrm{vol}\left(B_{p,\boldsymbol{k}}^n(\boldsymbol{u}, 2r_{p,\boldsymbol{k},n}) \cap B_{p,\boldsymbol{k}}^n(\boldsymbol{0}, \|\boldsymbol{u}\|_{p,\boldsymbol{k},n})\right)。
\end{aligned}$$

为了证明不等式(3.26)，只需证明存在常数$c_p \in (0,2)$使得对任意$n, \boldsymbol{k}$，以及对任意$\boldsymbol{u} \in B_{p,\boldsymbol{k}}^n(\boldsymbol{0}, 2r_{p,\boldsymbol{k},n})$，我们有

$$\mathrm{vol}\left(B_{p,\boldsymbol{k}}^n(\boldsymbol{u}, 2r_{p,\boldsymbol{k},n}) \cap B_{p,\boldsymbol{k}}^n(\boldsymbol{0}, \|\boldsymbol{u}\|_{p,\boldsymbol{k},n})\right) \leq c_p^n。$$

对任意$n, \boldsymbol{k}$，以及任意$\boldsymbol{u} \in B_{p,\boldsymbol{k}}^n(\boldsymbol{0}, 2r_{p,\boldsymbol{k},n})$，若$\|\boldsymbol{u}\|_{p,\boldsymbol{k},n} \leq x_p \cdot r_{p,\boldsymbol{k},n}$，则

$$\mathrm{vol}\left(B_{p,\boldsymbol{k}}^n(\boldsymbol{u}, 2r_{p,\boldsymbol{k},n}) \cap B_{p,\boldsymbol{k}}^n(\boldsymbol{0}, \|\boldsymbol{u}\|_{p,\boldsymbol{k},n})\right) \leq \mathrm{vol}\left(B_{p,\boldsymbol{k}}^n(\boldsymbol{0}, \|\boldsymbol{u}\|_{p,\boldsymbol{k},n})\right) \leq x_p^n。$$

再考虑$\|\boldsymbol{u}\|_{p,\boldsymbol{k},n} \geq x_p \cdot r_{p,\boldsymbol{k},n}$的情况。对任意$\boldsymbol{x} \in B_{p,\boldsymbol{k}}^n(\boldsymbol{u}, 2r_{p,\boldsymbol{k},n}) \cap B_{p,\boldsymbol{k}}^n(\boldsymbol{0}, \|\boldsymbol{u}\|_{p,\boldsymbol{k},n})$，我们有$\|\boldsymbol{x} - \boldsymbol{u}\|_{p,\boldsymbol{k},n} \leq 2r_{p,\boldsymbol{k},n}$且$\|\boldsymbol{x}\|_{p,\boldsymbol{k},n} \leq \|\boldsymbol{u}\|_{p,\boldsymbol{k},n} \leq 2r_{p,\boldsymbol{k},n}$。若$\|\boldsymbol{x} - \boldsymbol{u}\|_{p,\boldsymbol{k},n} \leq x_p \cdot r_{p,\boldsymbol{k},n}$或$\|\boldsymbol{x}\|_{p,\boldsymbol{k},n} \leq x_p \cdot r_{p,\boldsymbol{k},n}$，根据范数的正齐次性和次可加性，我们有

$$\left\|\boldsymbol{x} - \frac{1}{2}\boldsymbol{u}\right\|_{p,\boldsymbol{k},n} = \frac{1}{2}\|2\boldsymbol{x} - \boldsymbol{u}\|_{p,\boldsymbol{k},n} \leq \frac{1}{2}\left(\|\boldsymbol{x} - \boldsymbol{u}\|_{p,\boldsymbol{k},n} + \|\boldsymbol{x}\|_{p,\boldsymbol{k},n}\right) \leq \frac{x_p + 2}{2} r_{p,\boldsymbol{k},n}。 \tag{3.28}$$

现在假设$\|\boldsymbol{x} - \boldsymbol{u}\|_{p,\boldsymbol{k},n} \geq x_p \cdot r_{p,\boldsymbol{k},n}$且$\|\boldsymbol{x}\|_{p,\boldsymbol{k},n} \geq x_p \cdot r_{p,\boldsymbol{k},n}$。固定$1 < p \leq 2$。令$\delta_p(\epsilon) = 1 - \left(1 - \left(\frac{\epsilon}{2}\right)^q\right)^{1/q}$。根据命题3.2，对任意$\boldsymbol{k} = (k_1, k_2, \ldots)$和任意$\boldsymbol{x}, \boldsymbol{y} \in \ell_{p,\boldsymbol{k}}$，若$\|\boldsymbol{x}\|_{p,\boldsymbol{k}} = \|\boldsymbol{y}\|_{p,\boldsymbol{k}} = 1$且$\|\boldsymbol{x} - \boldsymbol{y}\|_{p,\boldsymbol{k}} \geq \epsilon$，那么$\left\|\frac{\boldsymbol{x}+\boldsymbol{y}}{2}\right\|_{p,\boldsymbol{k}} \leq 1 - \delta_p(\epsilon)$。对任意$n \in$

$\mathbb{N}$和$\boldsymbol{k}=(k_1,k_2,\ldots,k_{m+1})$满足$0=k_1<k_2<\cdots<k_{m+1}=n$，通过在第$n$个坐标后添上0，我们可以将$\mathbb{R}^n$中的点$\boldsymbol{x}$看成是$\ell_{p,\tilde{\boldsymbol{k}}}$中的点，这里$\tilde{\boldsymbol{k}}=(k_1,k_2,\ldots,k_{m+1},n+1,n+2,\ldots)$。此时$\|\boldsymbol{x}\|_{p,\boldsymbol{k},n}=\|\boldsymbol{x}\|_{p,\tilde{\boldsymbol{k}}}$。在接下来的证明中，我们将用范数$\|\cdot\|_{p,\boldsymbol{k}}$来替代范数$\|\cdot\|_{p,\boldsymbol{k},n}$。

记$\|\boldsymbol{x}-\boldsymbol{u}\|_{p,\boldsymbol{k}}=a$，$\|\boldsymbol{x}\|_{p,\boldsymbol{k}}=b$，$\|\boldsymbol{u}\|_{p,\boldsymbol{k}}=c$。我们已经假设$x_p\cdot r_{p,\boldsymbol{k},n}\le a\le 2r_{p,\boldsymbol{k},n}$且$x_p\cdot r_{p,\boldsymbol{k},n}\le b\le c\le 2r_{p,\boldsymbol{k},n}$。因为$\left\|\frac{\boldsymbol{x}-\boldsymbol{u}}{a}\right\|_{p,\boldsymbol{k}}=\left\|\frac{\boldsymbol{x}}{b}\right\|_{p,\boldsymbol{k}}=1$，并且

$$\begin{aligned}\left\|\frac{\boldsymbol{x}-\boldsymbol{u}}{a}-\frac{\boldsymbol{x}}{b}\right\|_{p,\boldsymbol{k}}=&\left\|\frac{-\boldsymbol{u}}{a}+\left(\frac{1}{a}-\frac{1}{b}\right)\boldsymbol{x}\right\|_{p,\boldsymbol{k}}\\ \ge&\left\|\frac{-\boldsymbol{u}}{a}\right\|_{p,\boldsymbol{k}}-\left\|\left(\frac{1}{a}-\frac{1}{b}\right)\boldsymbol{x}\right\|_{p,\boldsymbol{k}}\\ =&\frac{c}{a}-\left|\frac{b-a}{a}\right|\\ \ge&\frac{x_p}{2}-\frac{|b-a|}{a},\end{aligned}\tag{3.29}$$

所以由$\ell_{p,\boldsymbol{k}}$的一致凸性可得

$$\left\|\frac{\frac{\boldsymbol{x}-\boldsymbol{u}}{a}+\frac{\boldsymbol{x}}{b}}{2}\right\|_{p,\boldsymbol{k}}\le 1-\delta_p(\epsilon_p),\tag{3.30}$$

其中$\epsilon_p:=\frac{x_p}{2}-\frac{|b-a|}{a}\ge\frac{x_p}{2}-\frac{2-x_p}{x_p}=1+\frac{x_p}{2}-\frac{2}{x_p}$。故$\delta_p(\epsilon_p)\ge\delta_p\left(1+\frac{x_p}{2}-\frac{2}{x_p}\right)$。在不等式(3.30)两端同时乘$a$，整理后得到

$$\left\|\frac{1+\frac{a}{b}}{2}\boldsymbol{x}-\frac{1}{2}\boldsymbol{u}\right\|_{p,\boldsymbol{k}}\le a(1-\delta_p(\epsilon_p))。$$

因此，

$$\begin{aligned}\left\|\boldsymbol{x}-\frac{1}{2}\boldsymbol{u}\right\|_{p,\boldsymbol{k}}=&\left\|\frac{1+\frac{a}{b}}{2}\boldsymbol{x}-\frac{1}{2}\boldsymbol{u}+\frac{1-\frac{a}{b}}{2}\boldsymbol{x}\right\|_{p,\boldsymbol{k}}\\ \le&\left\|\frac{1+\frac{a}{b}}{2}\boldsymbol{x}-\frac{1}{2}\boldsymbol{u}\right\|_{p,\boldsymbol{k}}+\left\|\frac{1-\frac{a}{b}}{2}\boldsymbol{x}\right\|_{p,\boldsymbol{k}}\\ \le&a(1-\delta_p(\epsilon_p))+\frac{|b-a|}{2}\\ \le&\left(2(1-\delta_p(\epsilon_p))+\frac{2-x_p}{2}\right)r_{p,\boldsymbol{k},n}\\ =&\left[2-\left(2\delta_p(\epsilon_p)-\frac{2-x_p}{2}\right)\right]r_{p,\boldsymbol{k},n}。\end{aligned}\tag{3.31}$$

因为

$$\begin{aligned}2\delta_p\left(\epsilon_p\right)-\frac{2-x_p}{2}&=2\left[1-\left(1-\left(\frac{\epsilon_p}{2}\right)^q\right)^{1/q}\right]-1+\frac{x_p}{2}\\&=1-2\left(1-\left(\frac{\epsilon_p}{2}\right)^q\right)^{1/q}+\frac{x_p}{2}\\&\geq 1-2\left(1-\left(\frac{1+\frac{x_p}{2}-\frac{2}{x_p}}{2}\right)^q\right)^{1/q}+\frac{x_p}{2}\\&=1-2\left(1-\left(\frac{1}{2}+\frac{x_p}{4}-\frac{1}{x_p}\right)^q\right)^{1/q}+\frac{x_p}{2},\end{aligned}$$

并根据x_p的定义

$$1-\left(\frac{1}{2}+\frac{x_p}{4}-\frac{1}{x_p}\right)^q\leq\left(\frac{x_p+2}{4}\right)^q-\frac{1}{3^q},$$

所以

$$\begin{aligned}2\delta_p\left(\epsilon_p\right)-\frac{2-x_p}{2}&\geq 1-2\left(1-\left(\frac{1}{2}+\frac{x_p}{4}-\frac{1}{x_p}\right)^q\right)^{1/q}+\frac{x_p}{2}\\&\geq 1+\frac{x_p}{2}-\left(\left(1+\frac{x_p}{2}\right)^q-\frac{2^q}{3^q}\right)^{1/q}\\&>0。\end{aligned}\tag{3.32}$$

令$c_p'=\max\left\{\frac{x_p+2}{2},2-\left(2\delta_p(\epsilon_p)-\frac{2-x_p}{2}\right)\right\}$。根据不等式(3.32)，我们知道$c_p'<2$。根据不等式(3.28)和不等式(3.31)，我们知道

$$B^n_{p,\boldsymbol{k}}(\boldsymbol{u},2r_{p,\boldsymbol{k},n})\cap B^n_{p,\boldsymbol{k}}(\mathbf{0},\|\boldsymbol{u}\|_{p,\boldsymbol{k},n})\subseteq B^n_{p,\boldsymbol{k}}(\boldsymbol{u}/2,c_p'r_{p,\boldsymbol{k},n})。$$

所以

$$\mathrm{vol}\left(B^n_{p,\boldsymbol{k}}(\boldsymbol{u},2r_{p,\boldsymbol{k},n})\cap B^n_{p,\boldsymbol{k}}(\mathbf{0},\|\boldsymbol{u}\|_{p,\boldsymbol{k},n})\right)\leq\mathrm{vol}\left(B^n_{p,\boldsymbol{k}}(\boldsymbol{u}/2,c_p'r_{p,\boldsymbol{k},n})\right)=(c_p')^n。$$

令$c_p=\max\{x_p,c_p'\}$，我们就完成了证明。

由不等式(3.25)和不等式(3.26)可以得到等式(3.27)。 □

现在我们可以证明定理3.4。

定理3.4的证明. 令$S\subseteq\mathbb{R}^n$为有界可测集，并且体积为正。令c_p为引理3.7中的常数，以及$\alpha=\alpha_{S,p,\boldsymbol{k}}(\lambda)$。由Jensen不等式有

$$\alpha=\lambda\cdot\mathbb{E}\left[\frac{1}{Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)}\right]\geq\lambda\cdot e^{-\mathbb{E}\log Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)},$$

这里的期望是关于前面定义的二部试验的，并且第一个等号是由于等式(3.22)。

另一方面，我们有

$$\begin{aligned}\alpha &\geq 2^{-n}\cdot\mathbb{E}\left[\frac{\lambda\cdot Z'_{\mathrm{T},p,\boldsymbol{k}}(\lambda)}{Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)}\right]\\ &= 2^{-n}\cdot\mathbb{E}\left[\mathrm{vol}(\mathrm{T})\cdot\alpha_{\mathrm{T},p,\boldsymbol{k}}(\lambda)\right]\\ &\geq 2^{-n}\cdot\mathbb{E}\left[\lambda\cdot\mathrm{vol}(\mathrm{T})\cdot e^{-\lambda\cdot 2\cdot c_p^n}\right]\\ &\geq 2^{-n}\cdot\mathbb{E}\left[\log Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)\cdot e^{-\lambda\cdot 2\cdot c_p^n}\right]\\ &= 2^{-n}\cdot e^{-\lambda\cdot 2\cdot c_p^n}\cdot\mathbb{E}\left[\log Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)\right]。\end{aligned}$$

将这两个下界结合起来，并令$z=\mathbb{E}\left[\log Z_{\mathrm{T},p,\boldsymbol{k}}(\lambda)\right]$，我们有

$$\alpha\geq\inf_z\max\left\{\lambda\cdot e^{-z},2^{-n}\cdot e^{-\lambda\cdot 2\cdot c_p^n}\cdot z\right\}。$$

因为$\lambda\cdot e^{-z}$随z递减，$2^{-n}\cdot e^{-\lambda\cdot 2\cdot c_p^n}\cdot z$随$z$递增，它们的最大值的下确界在它们相等的时候取到，即$\alpha\geq\lambda e^{-z^*}$，其中$z^*$是方程

$$\lambda\cdot e^{-z}=2^{-n}\cdot e^{-\lambda\cdot 2\cdot c_p^n}\cdot z$$

的解。换句话说，

$$z^*=W(\lambda 2^n e^{2\lambda c_p^n}),\tag{3.33}$$

其中$W(x)$是Lambert-W函数。对于$x>0$，$w=W(x)$定义为方程$we^w=x$的唯一解。所以

$$w=\log x-\log(\log x-\log w)=\log x-\log\log x-\log\left(1-\frac{\log w}{\log x}\right)。$$

当$x\to\infty$时，

$$W(x)=\log x-\log\log x+O\left(\frac{\log\log x}{\log x}\right)。$$

我们取$\lambda=n^{-1}c_p^{-n}$。所以当$n\to\infty$时，$\lambda 2^n e^{2\lambda c_p^n}=\frac{1}{n}\left(\frac{2}{c_p}\right)^n e^{2/n}\to\infty$。等式(3.33)化为

$$\begin{aligned}z^*&=W(\lambda 2^n e^{2/n})\\ &=\log\lambda+n\log 2-\log n-\log\log(2/c_p)+O(\log(\log n/n))。\end{aligned}\tag{3.34}$$

所以

$$\alpha \geq \lambda e^{-z^*} = (1 + O(\log n/n)) \frac{\log(2/c_p) \cdot n}{2^n}。$$

因为α随λ递增，这个界对所有$\lambda \geq n^{-1}c_p^{-n}$均成立。这就完成了证明。 □

在上述证明中，如果我们取$\lambda = n^{-1}c^{-n}$，其中$c \in [c_p, 2)$，那么我们有

$$\alpha_{S,p,\boldsymbol{k}}(e^{-n\log c}) = \alpha_{S,p,\boldsymbol{k}}(c^{-n}) \geq \alpha_{S,p,\boldsymbol{k}}(n^{-1}c^{-n}) \geq (1 + o_n(1)) \frac{(\log 2 - \log c) \cdot n}{2^n},$$

即

$$\alpha_{S,p,\boldsymbol{k}}(e^{-nt}) \geq (1 + o_n(1)) \frac{(\log 2 - t) \cdot n}{2^n}, \tag{3.35}$$

其中$t \in [\log c_p, \log 2)$。

§ 3.4 定理3.2的另一种证明

在这一节，我们不使用刚性超球模型，给出定理3.2的另一种证明。证明思想来自于文献[42]的6.1节。我们固定$p \in (1, 2]$和$\boldsymbol{k}$，并令n是一个充分大的数。方便起见，在这一节，我们简化一些符号：$B^n(R) = B^n(\mathbf{0}, R) := B^n_{p,\boldsymbol{k}}(R) = B^n_{p,\boldsymbol{k}}(\mathbf{0}, R)$，$r_n := r_{p,\boldsymbol{k},n}$，$B^n(\boldsymbol{x}, r_n) := B^n_{p,\boldsymbol{k}}(\boldsymbol{x}, r_{p,\boldsymbol{k},n})$，$\|\cdot\| := \|\cdot\|_{p,\boldsymbol{k},n}$，$d(\cdot,\cdot) := d_{p,\boldsymbol{k},n}(\cdot,\cdot)$。

令$B^n(R)$是球心在$\mathbf{0}$、半径为R的超球。考虑在$B^n(R)$中堆积$B^n(\boldsymbol{x}, r_n)$的问题。令ϵ是一个小的正实数（我们将在后面确定ϵ），$\mathrm{C}_\epsilon := [0, \epsilon]^n$是一个立方体，以及$\tilde{L}_\epsilon := (\epsilon\mathbb{Z})^n$是一个格。$\mathrm{C}_\epsilon + \tilde{L}_\epsilon$铺砌了全空间，所以它也划分了$B^n(R)$。令$L_\epsilon = \{\boldsymbol{x} \in \tilde{L}_\epsilon : \mathrm{C}_\epsilon + \boldsymbol{x} \subseteq B^n(R)\}$。我们有下面这个引理。

引理3.8. *$\{\mathrm{C}_\epsilon + \boldsymbol{x} : \boldsymbol{x} \in L_\epsilon\}$覆盖了$B^n(R - 2n^{\frac{p+2}{2p}}\epsilon)$。*

证明. 假设结论不对，那么存在$\tilde{\boldsymbol{y}} = (y_1, y_2, \ldots, y_n) \in B^n(R - 2n^{\frac{p+2}{2p}}\epsilon)$使得对任意$\boldsymbol{x} \in L_\epsilon$，都有$\boldsymbol{y} \notin \mathrm{C}_\epsilon + \boldsymbol{x}$。令$\tilde{\boldsymbol{x}} = (x_1, x_2, \ldots, x_n) \in \tilde{L}_\epsilon$使得对任意$1 \leq i \leq n$，都有$0 \leq y_i - x_i \leq \epsilon$。换句话说，$\tilde{\boldsymbol{y}} \in \mathrm{C}_\epsilon + \tilde{\boldsymbol{x}}$。根据$\tilde{\boldsymbol{y}}$的选取，我们知道$\mathrm{C}_\epsilon + \tilde{\boldsymbol{x}} \nsubseteq B^n(R)$。另一方面，对任意$\boldsymbol{z} \in \mathrm{C}_\epsilon + \tilde{\boldsymbol{x}}$，我们有

$$\|\boldsymbol{z}\| \leq \|\boldsymbol{z} - \boldsymbol{y}\| + \|\boldsymbol{y}\| \leq \left(\sum_{j=1}^{m} \|(\epsilon, \epsilon, \ldots, \epsilon)\|_2^p\right)^{1/p} + R - 2n^{\frac{p+2}{2p}}\epsilon。$$

注意到$\|(\epsilon,\epsilon,\ldots,\epsilon)\|_2^p = (\epsilon^2+\epsilon^2+\cdots+\epsilon^2)^{p/2} \leq n^{p/2}\epsilon^p$，因为最多有$n$个$\epsilon$。并且$\sum_{j=1}^m \|(\epsilon,\epsilon,\ldots,\epsilon)\|_2^p \leq n^{(p+2)/2}\epsilon^p$，因为$m \leq n$。所以

$$\|\boldsymbol{z}\| \leq \left(\sum_{j=1}^m \|(\epsilon,\epsilon,\ldots,\epsilon)\|_2^p\right)^{1/p} + R - 2n^{\frac{p+2}{2p}}\epsilon \leq R - 2n^{\frac{p+2}{2p}}\epsilon + n^{\frac{p+2}{2p}}\epsilon < R。$$

这对于所有$\boldsymbol{z} \in \mathrm{C}_\epsilon + \tilde{\boldsymbol{x}}$均成立。所以$\mathrm{C}_\epsilon + \tilde{\boldsymbol{x}} \subseteq B^n(R)$，矛盾！因此原结论成立。 □

如果我们记$N := |L_\epsilon|$，那么我们可以通过引理3.8来估计N的大小，即

$$\mathrm{vol}\left(B^n(R-2n^{\frac{p+2}{2p}}\epsilon)\right) \leq N \cdot \mathrm{vol}(\mathrm{C}_\epsilon) \leq \mathrm{vol}\left(B^n(R)\right),$$

等价地，

$$\left(\frac{R-2n^{\frac{p+2}{2p}}\epsilon}{\epsilon r_n}\right)^n \leq N \leq \left(\frac{R}{\epsilon r_n}\right)^n。$$

所以$N = (1-o_R(1))\left(\frac{R}{\epsilon r_n}\right)^n$。

设$\{\mathrm{C}_\epsilon + \boldsymbol{x} : \boldsymbol{x} \in L_\epsilon\} = \{C_1, C_2, \ldots, C_N\}$。我们从每一个$C_i$中任意选取一个点$\boldsymbol{v}_i$，并构造一个辅助图$G$。在图$G$中，$V(G) = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_N\}$，$\boldsymbol{v}_i$和$\boldsymbol{v}_j$之间有一条边当且仅当$d(\boldsymbol{v}_i, \boldsymbol{v}_j) < 2r_n$。所以如果我们在$B^n(R)$中尽可能多地堆积半径为$r_n$的超球，那么这些超球的数量会大于等于$\alpha(G)$，其中$\alpha(G)$是$G$的独立数。换句话说，

$$\Delta_{p,\boldsymbol{k}}(n) \geq \lim_{R\to\infty} \frac{\alpha(G)}{(R/r_n)^n}。 \tag{3.36}$$

利用引理3.2的证明中的小技巧，我们在这里同样可以忽略那些在$B^n(R)$的边界附近的点所带来的影响。

引理3.9. *G中任意一个顶点的度数最多为$\frac{1+o_n(1)}{1-o_R(1)}\left(\frac{2r_n}{R}\right)^n N$。*

证明. 我们用$N[\boldsymbol{x}] = N(\boldsymbol{x}) \cup \{\boldsymbol{x}\}$表示$\boldsymbol{x}$的闭邻域（由$\boldsymbol{x}$和$\boldsymbol{x}$的邻点构成的集合）。我们声明，对任意$\boldsymbol{x} \in V(G)$，有

$$B^n(\boldsymbol{x}, 2r_n - 2n^{\frac{p+2}{2p}}\epsilon) \cap B^n(\boldsymbol{0}, R-2n^{\frac{p+2}{2p}}\epsilon) \subseteq \bigcup_{\boldsymbol{v}_i \in N[\boldsymbol{x}]} C_i \subseteq B^n(\boldsymbol{x}, 2r_n + 2n^{\frac{p+2}{2p}}\epsilon)。 \tag{3.37}$$

对于第一个包含关系，设$\boldsymbol{y} \in B^n(\boldsymbol{x}, 2r_n - 2n^{\frac{p+2}{2p}}\epsilon) \cap B^n(\boldsymbol{0}, R-2n^{\frac{p+2}{2p}}\epsilon)$。由引理3.8，存在一个指标$i$使得$\boldsymbol{y} \in C_i$。所以$d(\boldsymbol{y}, \boldsymbol{v}_i) \leq n^{\frac{p+2}{2p}}\epsilon$。因为$d(\boldsymbol{x}, \boldsymbol{y}) \leq 2r_n - 2n^{\frac{p+2}{2p}}\epsilon$，所

以$d(\boldsymbol{x},\boldsymbol{v}_i)\le 2r_n-2n^{\frac{p+2}{2p}}\epsilon+n^{\frac{p+2}{2p}}\epsilon<2r_n$，即$\boldsymbol{v}_i\in N[\boldsymbol{x}]$。对于第二个包含关系，对于满足$\boldsymbol{v}_i\in N[\boldsymbol{x}]$的指标$i$，设$\boldsymbol{y}\in C_i$。我们有$d(\boldsymbol{y},\boldsymbol{v}_i)\le n^{\frac{p+2}{2p}}\epsilon$且$d(\boldsymbol{x},\boldsymbol{v}_i)<2r_{p,\boldsymbol{k},n}$。所以$d(\boldsymbol{y},\boldsymbol{x})\le 2r_{p,\boldsymbol{k},n}+2n^{\frac{p+2}{2p}}\epsilon$。这就完成了声明的证明。

因为C_i之间互不重叠，根据以上的声明，我们有

$$\mathrm{vol}\left(\bigcup_{\boldsymbol{v}_i\in N[\boldsymbol{x}]}C_i\right)=|N[\boldsymbol{x}]|\epsilon^n\le\mathrm{vol}(B^n(\boldsymbol{x},2r_n+2n^{\frac{p+2}{2p}}\epsilon))=\left(\frac{2r_n+2n^{\frac{p+2}{2p}}\epsilon}{r_n}\right)^n,\tag{3.38}$$

即

$$|N[\boldsymbol{x}]|\le\left(\frac{1}{\epsilon r_n}\right)^n(2r_n+2n^{\frac{p+2}{2p}}\epsilon)^n=\frac{1+o_n(1)}{1-o_R(1)}\left(\frac{2r_n}{R}\right)^n N,$$

其中我们选取ϵ满足$n^{\frac{p+2}{2p}}\epsilon/r_n<n^{-2}$。 □

记$D:=\frac{1+o_n(1)}{1-o_R(1)}\left(\frac{2r_n}{R}\right)^n N$，$K:=\frac{1}{10}\left(\frac{2}{c_p}\right)^n$，其中$c_p$是引理3.7中的常数。用$G[N(\boldsymbol{x})]$表示$G$的由$N(\boldsymbol{x})$导出的子图。我们有以下引理。

引理3.10. 设R和n都充分大。对任意$\boldsymbol{x}\in V(G)$，$G[N(\boldsymbol{x})]$的平均度至多是$\frac{D}{K}$。

证明. 首先，$\frac{D}{K}=10(1+o_n(1))\left(\frac{c_p}{\epsilon}\right)^n$。设$S'=\bigcup_{\boldsymbol{v}_i\in N(\boldsymbol{x})}C_i$，$N(\boldsymbol{x})=\{\boldsymbol{x}_1,\boldsymbol{x}_2,\dots,\boldsymbol{x}_t\}$，其中$t=|N(\boldsymbol{x})|$。所以$\mathrm{vol}(S')=t\epsilon^n$。根据定义，$G[N(\boldsymbol{x})]$的平均度至多是

$$\frac{1}{t}\sum_{i,j=1}^{t}\mathbf{1}_{d(\boldsymbol{x}_i,\boldsymbol{x}_j)\le 2r_n}=\frac{\epsilon^n}{\mathrm{vol}(S')}\sum_{i,j=1}^{t}\mathbf{1}_{d(\boldsymbol{x}_i,\boldsymbol{x}_j)\le 2r_n}。\tag{3.39}$$

根据积分的定义，我们有

$$\lim_{\epsilon\to 0}\epsilon^{2n}\sum_{i,j=1}^{t}\mathbf{1}_{d(\boldsymbol{x}_i,\boldsymbol{x}_j)\le 2r_n}=\int_{S'}\int_{S'}\mathbf{1}_{d(\boldsymbol{u},\boldsymbol{v})\le 2r_n}d\boldsymbol{u}d\boldsymbol{v},$$

换句话说，对任意$\delta>0$，存在$\epsilon_0(\delta)$，只要$\epsilon<\epsilon_0(\delta)$，那么我们就有

$$\epsilon^{2n}\sum_{i,j=1}^{t}\mathbf{1}_{d(\boldsymbol{x}_i,\boldsymbol{x}_j)\le 2r_n}\le\int_{S'}\int_{S'}\mathbf{1}_{d(\boldsymbol{u},\boldsymbol{v})\le 2r_n}d\boldsymbol{u}d\boldsymbol{v}+\delta。\tag{3.40}$$

在引理3.9的证明中，我们知道$S'\subseteq B^n(\boldsymbol{x},2r_n+2n^{\frac{p+2}{2p}}\epsilon)$。设$S=\frac{2r_n}{2r_n+2n^{\frac{p+2}{2p}}\epsilon}S'$。

则$S \subseteq B^n(\boldsymbol{x}, 2r_n)$，并且

$$\begin{aligned}
&\int_{S'}\int_{S'} \mathbf{1}_{d(\boldsymbol{u},\boldsymbol{v})\le 2r_n} d\boldsymbol{u}d\boldsymbol{v} \\
=&\left(\frac{2r_n + 2n^{\frac{p+2}{2p}}\epsilon}{2r_n}\right)^{2n} \int_S\int_S \mathbf{1}_{d(\boldsymbol{u},\boldsymbol{v})\le 2r_n\cdot 2r_n/(2r_n+2n^{\frac{p+2}{2p}}\epsilon)} d\boldsymbol{u}d\boldsymbol{v} \\
\le&\left(\frac{2r_n + 2n^{\frac{p+2}{2p}}\epsilon}{2r_n}\right)^{n} \frac{\mathrm{vol}(S')}{\mathrm{vol}(S)} \int_S\int_S \mathbf{1}_{d(\boldsymbol{u},\boldsymbol{v})\le 2r_n} d\boldsymbol{u}d\boldsymbol{v} \\
=&(1+o_n(1))\frac{\mathrm{vol}(S')}{\mathrm{vol}(S)} \int_S\int_S \mathbf{1}_{d(\boldsymbol{u},\boldsymbol{v})\le 2r_n} d\boldsymbol{u}d\boldsymbol{v},
\end{aligned} \tag{3.41}$$

其中我们选取ϵ充分小，使得$\left(\frac{2r_n+2n^{\frac{p+2}{2p}}\epsilon}{2r_n}\right)^n = 1+o_n(1)$。例如，如果我们取$\epsilon$满足$n^{\frac{p+2}{2p}}\epsilon/r_n < n^{-2}$，那么$\left(\frac{2r_n+2n^{\frac{p+2}{2p}}\epsilon}{2r_n}\right)^n < \left(1+\frac{1}{n^2}\right)^n < e^{1/n} = 1+o_n(1)$。

在引理3.7的证明中，我们有

$$\int_S\int_S \mathbf{1}_{d(\boldsymbol{u},\boldsymbol{v})\le 2r_n} d\boldsymbol{u}d\boldsymbol{v} \le 2\mathrm{vol}(S)c_p^n。 \tag{3.42}$$

综合等式(3.39)和不等式(3.40)-(3.42)，$G[N(\boldsymbol{x})]$的平均度至多是

$$\begin{aligned}
&\frac{\epsilon^n}{\mathrm{vol}(S')}\sum_{i,j=1}^{t} \mathbf{1}_{d(\boldsymbol{x}_i,\boldsymbol{x}_j)\le 2r_n} \\
\le&\frac{1}{\mathrm{vol}(S')\epsilon^n}\left(\int_{S'}\int_{S'} \mathbf{1}_{d(\boldsymbol{u},\boldsymbol{v})\le 2r_n} d\boldsymbol{u}d\boldsymbol{v} + \delta\right) \\
\le&\frac{1}{\mathrm{vol}(S')\epsilon^n}\left((1+o_n(1))\frac{\mathrm{vol}(S')}{\mathrm{vol}(S)}\int_S\int_S \mathbf{1}_{d(\boldsymbol{u},\boldsymbol{v})\le 2r_n} d\boldsymbol{u}d\boldsymbol{v} + \delta\right) \\
\le&\frac{1}{\mathrm{vol}(S')\epsilon^n}\left((1+o_n(1))\cdot 2c_p^n\mathrm{vol}(S') + \delta\right) \\
=&(1+o_n(1))\cdot 2\left(\frac{c_p}{\epsilon}\right)^n + \frac{\delta}{\mathrm{vol}(S')\epsilon^n}。
\end{aligned} \tag{3.43}$$

接下来我们给出$\mathrm{vol}(S')$的一个下界。在包含关系(3.37)中，我们有

$$\bigcup_{\boldsymbol{v}_i\in N[\boldsymbol{x}]} C_i \supseteq B^n(\boldsymbol{x}, 2r_n - 2n^{\frac{p+2}{2p}}\epsilon) \cap B^n(\mathbf{0}, R - 2n^{\frac{p+2}{2p}}\epsilon)。$$

记$V_{\text{lower}} := \mathrm{vol}\left(B^n(\boldsymbol{x}, 2r_n - 2n^{\frac{p+2}{2p}}\epsilon) \cap B^n(\mathbf{0}, R - 2n^{\frac{p+2}{2p}}\epsilon)\right)$。若$B^n(\boldsymbol{x}, 2r_n - 2n^{\frac{p+2}{2p}}\epsilon) \subseteq B^n(\mathbf{0}, R - 2n^{\frac{p+2}{2p}}\epsilon)$，则

$$V_{\text{lower}} \ge \mathrm{vol}\left(B^n(\boldsymbol{x}, 2r_n - 2n^{\frac{p+2}{2p}}\epsilon)\right) = \left(\frac{2r_n - 2n^{\frac{p+2}{2p}}\epsilon}{r_n}\right)^n = (1-o_n(1))2^n。$$

若$B^n(\boldsymbol{x}, 2r_n - 2n^{\frac{p+2}{2p}}\epsilon) \nsubseteq B^n(\mathbf{0}, R - 2n^{\frac{p+2}{2p}}\epsilon)$，那么我们有

$$B^n(\boldsymbol{x}, 2r_n - 2n^{\frac{p+2}{2p}}\epsilon) \cap B^n(\mathbf{0}, R - 2n^{\frac{p+2}{2p}}\epsilon) \supseteq B^n\left(\boldsymbol{y}, r_n - 2n^{\frac{p+2}{2p}}\epsilon\right),$$

其中$\boldsymbol{y} := \left(1 - \frac{r_n}{\|\boldsymbol{x}\|}\right)\boldsymbol{x}$。为了证明这个，我们任取$\boldsymbol{z} \in B^n\left(\boldsymbol{y}, r_n - 2n^{\frac{p+2}{2p}}\epsilon\right)$，有$d(\boldsymbol{z}, \boldsymbol{y}) \leq r_n - 2n^{\frac{p+2}{2p}}\epsilon$。所以

$$d(\boldsymbol{x}, \boldsymbol{z}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z}) \leq r_n + r_n - 2n^{\frac{p+2}{2p}}\epsilon = 2r_n - 2n^{\frac{p+2}{2p}}\epsilon。$$

并且

$$d(\mathbf{0}, \boldsymbol{z}) \leq d(\mathbf{0}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z}) \leq \|\boldsymbol{x}\| - r_n + r_n - 2n^{\frac{p+2}{2p}}\epsilon \leq R - 2n^{\frac{p+2}{2p}}\epsilon,$$

因为$\boldsymbol{x} \in B^n(\mathbf{0}, R)$。因此

$$V_{\text{lower}} \geq \text{vol}\left(B^n\left(\boldsymbol{y}, r_n - 2n^{\frac{p+2}{2p}}\epsilon\right)\right) = \left(\frac{r_n - 2n^{\frac{p+2}{2p}}\epsilon}{r_n}\right)^n = 1 - o_n(1)。$$

综上，我们有

$$\text{vol}(S') = \text{vol}\left(\bigcup_{\boldsymbol{v}_i \in N[\boldsymbol{x}]} C_i\right) - \epsilon^n \geq V_{\text{lower}} - \epsilon^n \geq 1 - o_n(1)。$$

所以，如果我们取$\delta = c_p^n$，$\epsilon \leq \min\{\epsilon_0(c_p^n), r_n/n^{2+\frac{p+2}{2p}}\}$，那么由不等式(3.43)，我们知道$G[N(\boldsymbol{x})]$的平均度至多是

$$\begin{aligned}
&(1 + o_n(1)) \cdot 2\left(\frac{c_p}{\epsilon}\right)^n + \frac{\delta}{\text{vol}(S')\epsilon^n} \\
\leq &(1 + o_n(1)) \cdot 2\left(\frac{c_p}{\epsilon}\right)^n + \frac{c_p^n}{(1 - o_n(1))\epsilon^n} \\
< &5\left(\frac{c_p}{\epsilon}\right)^n \\
< &\frac{D}{K},
\end{aligned} \tag{3.44}$$

其中n充分大。注意到这与$\boldsymbol{x}$的选取无关，这就完成了证明。 □

根据引理3.9和引理3.10，我们知道图G的最大度为D，并且每一个由某个点的邻点导出的子图的平均度都至多为D/K。我们称这样的图是局部稀疏（locally sparse）

的。根据Hurley和Pirot在文献[58]中的结果，G的染色数至多为$(1+o_K(1))\frac{D}{\log K}$。所以$G$的独立数$\alpha(G)$至少是

$$\begin{aligned}(1-o_K(1))\frac{N}{D}\log K =&(1-o_n(1))\frac{1-o_R(1)}{1+o_n(1)}\left(\frac{R}{2r_n}\right)^n\log\left(\frac{1}{10}\left(\frac{2}{c_p}\right)^n\right)\\ =&(1-o_n(1))(1-o_R(1))\left(\frac{R}{r_n}\right)^n\frac{\log(2/c_p)\cdot n}{2^n},\end{aligned}\tag{3.45}$$

以及

$$\Delta_{p,\boldsymbol{k}}(n)\geq\lim_{R\to\infty}\frac{\alpha(G)}{(R/r_n)^n}=(1-o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}。$$

这就完成了定理3.2的证明.

§3.5 熵密度和压力的下界

在这一节，我们研究堆积的熵密度和压力。

设$B^n_{p,\boldsymbol{k}}(R)$是堆积的区域，$V=\mathrm{vol}(B^n_{p,\boldsymbol{k}}(R))=(R/r_{p,\boldsymbol{k},n})^n$。定义

$$f_{p,\boldsymbol{k},n}(\alpha)=\lim_{V\to\infty}\frac{1}{\alpha V}\log\frac{\hat{Z}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lfloor\alpha V\rfloor)}{V^{\lfloor\alpha V\rfloor}/\lfloor\alpha V\rfloor!}$$

为堆积的熵密度（entropy density）。考虑在$B^n_{p,\boldsymbol{k}}(R)$中的密度为$\alpha$的随机堆积。用来堆积的超球的体积是1，所以共有$\lfloor\alpha V\rfloor$个球心。$V^{\lfloor\alpha V\rfloor}/\lfloor\alpha V\rfloor!$衡量了在$B^n_{p,\boldsymbol{k}}(R)$中选取$\lfloor\alpha V\rfloor$个无序点的所有可能性，$\hat{Z}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lfloor\alpha V\rfloor)$衡量了$\lfloor\alpha V\rfloor$个无序点可以构成堆积的所有可能性。除以$\alpha V$可以保证$f_{p,\boldsymbol{k},n}(\alpha)$与用来堆积的超球的体积无关。所以$f_{p,\boldsymbol{k},n}(\alpha)$衡量了密度为$\alpha$的堆积的丰富程度。我们再定义

$$g_{p,\boldsymbol{k},n}(\lambda)=\lim_{V\to\infty}\frac{1}{V}\log Z_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lambda)$$

为堆积的压力（pressure）。$g_{p,\boldsymbol{k},n}(\lambda)$衡量了逸度为$\lambda$的堆积的丰富程度。我们有下列定理。

定理3.5. *设c_p是定理3.4中的常数。当$\lambda\in(2^{-n},c_p^{-n}]$时，我们有*

$$g_{p,\boldsymbol{k},n}(\lambda)\geq\left(\frac{\left(\log 2+\frac{1}{n}\log\lambda\right)^2}{2}+o_n(1)\right)\frac{n^2}{2^n}。\tag{3.46}$$

在定理3.5中，$\log 2+\frac{1}{n}\log\lambda\in(0,\log 2-\log c_p]$。

定理3.6. 设c_p是定理*3.4*中的常数。存在$\alpha = (1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}$使得

$$f_{p,\boldsymbol{k},n}(\alpha) \geq -(1+o_n(1))\log(2/c_p)\cdot n。$$

定理3.5和定理3.6的证明分别与文献[34]的定理4和定理5类似。为了完整性，我们在这里依旧给出证明。

定理3.5的证明. 我们可以算出

$$\begin{aligned}\frac{1}{V}\log Z_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lambda) =& \lim_{\epsilon\to 0}\int_{\epsilon}^{\lambda}\frac{1}{V}\left(\log Z_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(x)\right)' dx\\ =& \lim_{\epsilon\to 0}\int_{\epsilon}^{\lambda}\frac{\alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(x)}{x}dx\\ \geq& \int_{2^{-n}}^{\lambda}\frac{\alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(x)}{x}dx,\end{aligned}$$

其中第二个等号利用了等式(3.19)，最后一个不等号利用了被积函数的非负性。取$x = e^{-nt}$。当$x=\lambda$时，$t=-\frac{1}{n}\log\lambda$；当$x=2^{-n}$时，$t=\log 2$。因为$\lambda\in(2^{-n},c_p^{-n}]$，所以$[-\frac{1}{n}\log\lambda,\log 2]\subseteq[\log c_p,\log 2]$。我们可以利用不等式(3.35)来估计$\alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(e^{-nt})$的下界。我们有

$$\begin{aligned}\int_{2^{-n}}^{\lambda}\frac{\alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(x)}{x}dx =& -n\int_{\log 2}^{-\frac{1}{n}\log\lambda}\alpha_{B^n_{p,\boldsymbol{k}}(\boldsymbol{0},R),p,\boldsymbol{k}}(e^{-nt})dt\\ =& n\int_{-\frac{1}{n}\log\lambda}^{\log 2}\alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(e^{-nt})dt\\ \geq& n\,(1+o(1))\int_{-\frac{1}{n}\log\lambda}^{\log 2}\frac{(\log 2-t)\cdot n}{2^n}dt\\ =& \left(\frac{\left(\log 2+\frac{1}{n}\log\lambda\right)^2}{2}+o_n(1)\right)\frac{n^2}{2^n}。\end{aligned}$$

令V趋于无穷，我们就得到了不等式等式(3.46)。 □

在证明定理3.6之前，我们先给出一个关于$f_{p,\boldsymbol{k},n}(\alpha)$的简单的事实：密度越大，这样的堆积就越少。

引理3.11. $f_{p,\boldsymbol{k},n}(\alpha)$随$\alpha$递减。

证明. 若$\alpha>\Delta_{p,\boldsymbol{k}}(n)$，则对较大的$V$，有$\hat{Z}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lfloor\alpha V\rfloor)=0$。所以当$\alpha>\Delta_{p,\boldsymbol{k}}(n)$时，$f_{p,\boldsymbol{k},n}(\alpha)=0$。

设$0 < \alpha_1 < \alpha_2 \leq \Delta_{p,\boldsymbol{k}}(n)$，令$V_1$和$V_2$满足$\alpha_1 V_1 = \alpha_2 V_2$（所以$V_1 > V_2$）。我们声明，

$$\frac{1}{\alpha_1 V_1}\log\frac{\hat{Z}_{B^n_{p,\boldsymbol{k}}(R_1),p,\boldsymbol{k}}(\lfloor\alpha_1 V_1\rfloor)}{V_1^{\lfloor\alpha_1 V_1\rfloor}/\lfloor\alpha_1 V_1\rfloor!} > \frac{1}{\alpha_2 V_2}\log\frac{\hat{Z}_{B^n_{p,\boldsymbol{k}}(R_2),p,\boldsymbol{k}}(\lfloor\alpha_2 V_2\rfloor)}{V_2^{\lfloor\alpha_2 V_2\rfloor}/\lfloor\alpha_2 V_2\rfloor!}, \tag{3.47}$$

其中$V_1 = (R_1/r_{p,\boldsymbol{k},n})^n$，$V_2 = (R_2/r_{p,\boldsymbol{k},n})^n$（所以$R_1 > R_2$）。为了证明不等式(3.47)，只需证明

$$\frac{\hat{Z}_{B^n_{p,\boldsymbol{k}}(R_1),p,\boldsymbol{k}}(\lfloor\alpha_1 V_1\rfloor)}{V_1^{\lfloor\alpha_1 V_1\rfloor}} > \frac{\hat{Z}_{B^n_{p,\boldsymbol{k}}(R_2),p,\boldsymbol{k}}(\lfloor\alpha_2 V_2\rfloor)}{V_2^{\lfloor\alpha_2 V_2\rfloor}}。$$

利用不等式(3.17)和$\hat{Z}_{S,p,\boldsymbol{k}}(t)$的定义，我们需要证明

$$\frac{\int_{B^n_{p,\boldsymbol{k}}(R_1)^t}\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_1 d\boldsymbol{x}_2\cdots d\boldsymbol{x}_t}{V_1^t} > \frac{\int_{B^n_{p,\boldsymbol{k}}(R_2)^t}\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_1 d\boldsymbol{x}_2\cdots d\boldsymbol{x}_t}{V_2^t}, \tag{3.48}$$

其中$t = \lfloor\alpha_1 V_1\rfloor = \lfloor\alpha_2 V_2\rfloor$。考虑不等式(3.48)的右边

$$\frac{\int_{B^n_{p,\boldsymbol{k}}(R_2)^t}\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_1 d\boldsymbol{x}_2\cdots d\boldsymbol{x}_t}{V_2^t}。$$

令$\boldsymbol{y}_i = (R_1/R_2)\boldsymbol{x}_i, i = 1,\ldots,t$。那么

$$\frac{\int_{B^n_{p,\boldsymbol{k}}(R_2)^t}\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)}d\boldsymbol{x}_1 d\boldsymbol{x}_2\cdots d\boldsymbol{x}_t}{V_2^t} = \frac{\int_{B^n_{p,\boldsymbol{k}}(R_1)^t}\mathbf{1}_{\mathcal{D}'_{p,\boldsymbol{k}}(\boldsymbol{y}_1,\boldsymbol{y}_2,\ldots,\boldsymbol{y}_t)}d\boldsymbol{y}_1 d\boldsymbol{y}_2\cdots d\boldsymbol{y}_t}{V_1^t}, \tag{3.49}$$

其中$\mathcal{D}'_{p,\boldsymbol{k}}(\boldsymbol{y}_1,\boldsymbol{y}_2,\ldots,\boldsymbol{y}_t)$表示事件“对任意$i \neq j$，都有$d_{p,\boldsymbol{k},n}(\boldsymbol{y}_i,\boldsymbol{y}_j) \geq \frac{R_1}{R_2}\cdot 2r_{p,\boldsymbol{k},n}$”。

不等式(3.48)的左边是事件“从$B^n_{p,\boldsymbol{k}}(R_1)$中均匀取出$t$个点，两两之间距离大于等于$2r_{p,\boldsymbol{k},n}$”的概率，而不等式(3.48)的右边是事件“从$B^n_{p,\boldsymbol{k}}(R_1)$中均匀取出$t$个点，两两之间距离大于等于$\frac{R_1}{R_2}\cdot 2r_{p,\boldsymbol{k},n}$”的概率。后者的事件包含前者的事件，即

$$\mathbf{1}_{\mathcal{D}_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)} \geq \mathbf{1}_{\mathcal{D}'_{p,\boldsymbol{k}}(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)}。$$

所以不等式(3.48)成立，声明得证。

在不等式(3.47)两边，令V_1趋于无穷，我们得到

$$f_{p,\boldsymbol{k},n}(\alpha_1) > f_{p,\boldsymbol{k},n}(\alpha_2)。$$

这就完成了证明。 □

最后，我们给出定理3.6的证明。

定理3.6的证明. 考虑$B^n_{p,\boldsymbol{k}}(R)$中的堆积。记$V=\mathrm{vol}(B^n_{p,\boldsymbol{k}}(R))=(R/r_{p,\boldsymbol{k},n})^n$。假设对任意$\lambda\in[c_p^{-n},2c_p^{-n}]$，都有$\mathrm{Var}(|X|)\geq V^{3/2}$。利用引理3.3的证明中的等式(3.20)，我们有

$$\begin{aligned}\alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(2c_p^{-n})&=\int_0^{2c_p^{-n}}\alpha'_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(x)dx\\&=\int_0^{2c_p^{-n}}\frac{\mathrm{Var}(|X|)}{xV}dx\\&\geq\int_{c_p^{-n}}^{2c_p^{-n}}\frac{\mathrm{Var}(|X|)}{xV}dx\\&\geq V^{1/2}(\log 2-1)>1。\end{aligned}$$

矛盾。所以存在$\lambda\in[c_p^{-n},2c_p^{-n}]$使得$\mathrm{Var}(|X|)<V^{3/2}$。

我们选取$\lambda\in[c_p^{-n},2c_p^{-n}]$使得$\mathrm{Var}(|X|)<V^{3/2}$。利用Chebyshev不等式，我们有

$$\mathbb{P}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}\left(\left||X|-\mathbb{E}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}(|X|)\right|\geq V^{4/5}\right)\leq\frac{\mathrm{Var}(|X|)}{V^{8/5}}<V^{-1/10}。$$

所以

$$\mathbb{P}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}\left(\left||X|-\mathbb{E}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}(|X|)\right|\leq V^{4/5}\right)\geq 1-V^{-1/10}。$$

注意到$|X|$是一个整数。平均来看，存在一个整数

$$t\in\left[\mathbb{E}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}(|X|)-V^{4/5},\mathbb{E}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}(|X|)+V^{4/5}\right]$$

使得

$$\mathbb{P}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}\left(|X|=t\right)\geq\frac{1-V^{-1/10}}{\lfloor 2V^{4/5}\rfloor}\geq\frac{1}{V},$$

其中V是比较大的数。回顾

$$\mathbb{P}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}\left(|X|=t\right)=\frac{\lambda^t\hat{Z}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(t)}{Z_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lambda)}。$$

所以

$$\hat{Z}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(t)\geq\frac{1}{V\lambda^t}Z_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lambda)\geq\frac{1}{V\lambda^t}。$$

另一方面，根据定理3.4和$\alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lambda)$的定义，我们有

$$\mathbb{E}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k},\lambda}(|X|)=\alpha_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lambda)\cdot V\geq(1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}\cdot V。$$

设ϵ是一个小的正数（我们在后面会选取ϵ与n有关，但与V无关），

$$\alpha = (1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n} - \epsilon。$$

所以对于比较大的V，我们有

$$\alpha \le (1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n} - V^{-1/5} \le \frac{t}{V}。$$

由引理3.11可得

$$f_{p,\boldsymbol{k},n}(\alpha) = \lim_{V\to\infty}\frac{1}{\alpha V}\log\frac{\hat{Z}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(\lfloor\alpha V\rfloor)}{V^{\lfloor\alpha V\rfloor}/\lfloor\alpha V\rfloor!} \ge \lim_{V\to\infty}\frac{1}{t}\log\frac{\hat{Z}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(t)}{V^t/t!}。$$

计算出

$$\begin{aligned}\lim_{V\to\infty}\frac{1}{t}\log\frac{\hat{Z}_{B^n_{p,\boldsymbol{k}}(R),p,\boldsymbol{k}}(t)}{V^t/t!} &\ge \lim_{V\to\infty}\frac{1}{t}\log\frac{t!}{V^{t+1}\lambda^t}\\ &= \lim_{V\to\infty}\frac{1}{t}\log\frac{t!}{V^{t+1}} - \log\lambda\\ &\ge \lim_{V\to\infty}\frac{1}{t}\log\frac{t!}{V^{t+1}} + n\log c_p - \log 2。\end{aligned}$$

当$V\to\infty$时，$t\to\infty$。所以由Stirling公式可得

$$\begin{aligned}\lim_{V\to\infty}\frac{1}{t}\log\frac{t!}{V^{t+1}} &= \lim_{V\to\infty}\frac{1}{t}\log\frac{\sqrt{2\pi t}(t/e)^t}{V^{t+1}}\\ &= \lim_{V\to\infty}\left(\frac{1}{t}\log\sqrt{2\pi t} + \log(t/V) - 1 - \frac{1}{t}\log(1/V)\right)\\ &= \lim_{V\to\infty}\log(t/V) - 1\\ &\ge \log\left((1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}\right) - 1\\ &= (-\log 2 + o_n(1))n。\end{aligned}$$

因此

$$f_{p,\boldsymbol{k},n}(\alpha) \ge (-\log 2 + o_n(1))n + n\log c_p - \log 2 = -(1+o_n(1))\log(2/c_p)\cdot n。$$

选取$\epsilon = o_n\left(\frac{\log(2/c_p)\cdot n}{2^n}\right)$使得$\alpha = (1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n} - \epsilon = (1+o_n(1))\frac{\log(2/c_p)\cdot n}{2^n}$即可。 □

第 4 章　高维ℓ_p球的接触数的下界

§4.1　简介

记S^{n-1}为$\mathbb{R}^n$中的单位球面。接触数（kissing number）的问题是指最多能有多少个互不重叠的平移$S^{n-1}+\boldsymbol{x}$同时与S^{n-1}相切。这是一个既古老又困难的离散几何问题。这个问题目前已知的确切结果只有1维，2维，3维，4维，8维，以及24维。

- 在1维和2维的时候，这个问题是平凡的，因为1维的球就是线段，2维的最大接触数为6。
- 在3维的时候，这个问题就是著名的Gregory-Newton问题，由Schütte和van der Waerden[74]解决（此外，文献[47]给出了另一种证明）。此时的最大接触数为12。
- 在4维的时候，这个问题由Musin[53]解决，他推广了Delsarte方法。此时的最大接触数为24。
- 在8维和24维的时候，这个问题由Levenšteĭn[48]，以及Odlyzko和Sloane[55]独立解决。最大接触数分别为240和196560。

用$K_2(n)$表示S^{n-1}的最大接触数。在高维时，$K_2(n)$的最佳上界由Kabatjanskiĭ和Levenšteĭn[36]得到：$K_2(n)\leq 2^{0.401n(1+o(1))}$。利用球面覆盖的方法，Shannon[75]和Wyner[84]得到了下界$K_2(n)\geq c\sqrt{n}(2/\sqrt{3})^n$。最近，Jenssen等人[33]将下界改进为$\Omega\left(n^{3/2}(2/\sqrt{3})^n\right)$。Fernández等人[22]又进一步改进了常数因子。

在这一章，我们考虑ℓ_p球的最大接触数。对于$p\geq 1$，记$S_p^{n-1}(R)$为$\mathbb{R}^n$中半径为R、球心为$\mathbf{0}$的ℓ_p球，即$S_p^{n-1}(R):=\{\boldsymbol{x}\in\mathbb{R}^n:\|\boldsymbol{x}\|_p=R\}$，其中$\ell_p$范数$\|\cdot\|_p$定义为$\|\boldsymbol{x}\|_p=(\sum_{i=1}^n|x_i|^p)^{1/p}$，$\boldsymbol{x}=(x_1,x_2,\ldots,x_n)$。在接触数问题上，我们不区分球

面和球体。我们简记$S_p^{n-1} = S_p^{n-1}(1)$。令$K_p(n)$为S_p^{n-1}的最大接触数。Minkowski-Hadwiger定理[26]给出了上界$K_p(n) \leq 3^n - 1$。在$p \geq 2$时，Sah等人[69]对这个界做了改进。当p在1到2之间时，已知的上界很少。

在下界方面，Larman和Zong[46]证明了$K_p(n) \geq (9/8)^{n(1+o(1))} = 2^{0.1699n(1+o(1))}$。Xu[85]改进了他们的结果，例如$K_3(n) \geq 2^{0.4564n(1+o(1))}$。我们的工作进一步改进了Xu的结果。因为我们的结果没有显式表达式，所以我们在这里列出一些数值结果：

$$K_1(n) \geq 2^{0.1247n(1+o(1))} + 2^{0.1825n(1+o(1))} + 2^{0.1554n(1+o(1))} + \cdots;$$

$$K_2(n) \geq 2^{0.2059n(1+o(1))} + 2^{0.1381n(1+o(1))} + 2^{0.0584n(1+o(1))} + \cdots;$$

$$K_3(n) \geq cn2^{0.4564n(1+o(1))} + 2^{0.1562n(1+o(1))} + 2^{0.0425n(1+o(1))} + \cdots。$$

我们对这些结果做出一些解释。在$K_2(n)$的下界中，$2^{0.2059n(1+o(1))}$项与Xu所得到的下界相同，所以我们的改进是添加了一些余项$2^{0.1381n(1+o(1))} + 2^{0.0584n(1+o(1))} + \cdots$。在$K_3(n)$的下界中，$2^{0.4564n(1+o(1))}$与Xu所得到的下界相同，所以我们的改进是在首项上乘了因子n并添加了一些余项。

我们的思路来源于编码理论。最大接触数$K_p(n)$与最小距离为1的ℓ_p球面码的最大基数相等（见引理4.1）。我们从S_p^{n-1}上选取一个离散的集合X。利用编码理论中的思想，我们可以找到X的一个比较大的子集，其中的点两两之间距离不小于1。这就给出了$K_p(n)$的一个下界。

§ 4.2 改进的Gilbert-Varshamov型界

记$A_p(n,d)$为S_p^{n-1}的子集的最大基数，其中的点两两之间的ℓ_p距离至少为$2d$。也就是说，

$$A_p(n,d) := \max\{|C| : C \subseteq S_p^{n-1} \text{并且} d_p(\boldsymbol{x},\boldsymbol{y}) \geq 2d, \forall \boldsymbol{x},\boldsymbol{y} \in C\},$$

其中$d_p(\boldsymbol{x},\boldsymbol{y}) := \|\boldsymbol{x}-\boldsymbol{y}\|_p$是$\boldsymbol{x}$和$\boldsymbol{y}$之间的$\ell_p$距离。换句话说，$A_p(n,d)$是最小距离为$2d$的$\ell_p$球面码（spherical code）的最大基数。我们有下面这个简单的引理。

引理4.1. S_p^{n-1}的最大接触数等于$A_p(n,1/2)$。

证明. 方便起见，记$k_1 = K_p(n)$，$k_2 = A_p(n, 1/2)$。

假设$S_p^{n-1}, S_p^{n-1} + \boldsymbol{x}_1, S_p^{n-1} + \boldsymbol{x}_2, \ldots, S_p^{n-1} + \boldsymbol{x}_{k_1}$形成一个接触数的构型。对任意$i$，如果$d_p(\mathbf{0}, \boldsymbol{x}_i) > 2$，那么$S_p^{n-1} + \boldsymbol{x}_i$和$S_p^{n-1}$就没有交点；如果$d_p(\mathbf{0}, \boldsymbol{x}_i) < 2$，那么$S_p^{n-1} + \boldsymbol{x}_i$和$S_p^{n-1}$就会重叠。所以，对任意$i$，都有$d_p(\mathbf{0}, \boldsymbol{x}_i) = 2$，此时$\frac{1}{2}\boldsymbol{x}_i \in S_p^{n-1}$。进一步，若$i \neq j$，那么$d_p(\boldsymbol{x}_i, \boldsymbol{x}_j) \geq 2$，即$d_p(\frac{1}{2}\boldsymbol{x}_i, \frac{1}{2}\boldsymbol{x}_j) \geq 1$。因此$\{\frac{1}{2}\boldsymbol{x}_1, \frac{1}{2}\boldsymbol{x}_2, \ldots, \frac{1}{2}\boldsymbol{x}_{k_1}\}$是一个最小距离为1的$\ell_p$球面码，即$k_2 \geq k_1$。

另一方面，假设$\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{k_2}\}$是一个最小距离为1的$\ell_p$球面码。那么$S_p^{n-1} + 2\boldsymbol{x}_1, S_p^{n-1} + 2\boldsymbol{x}_2, \ldots, S_p^{n-1} + 2\boldsymbol{x}_{k_2}$互不重叠，并且对任意$i$，$S_p^{n-1} + 2\boldsymbol{x}_i$与$S_p^{n-1}$在$\boldsymbol{x}_i$处相切。所以$k_1 \geq k_2$。引理得证。 □

对于正整数$m \leq n$（我们会在之后确定m的值），我们递归地定义$\mathbb{R}^n$的子集族$\mathcal{J}(m, n)$。定义$m_1 := m$，以及

$$J_1(m, n) := \left\{ \boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \{0, \pm 1\}^n : \sum_{i=1}^{n} |u_i|^p = m \right\}。$$

假设我们已经定义了m_i和$J_i(m, n)$。那么我们定义

$$m_{i+1} := \lfloor m_i / 2^p \rfloor \tag{4.1}$$

以及

$$J_{i+1}(m, n) := \left\{ \boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \{0, \pm (m/m_{i+1})^{1/p}\}^n : \sum_{i=1}^{n} |u_i|^p = m \right\}。$$

当进行到第r步，$m_r < 2^p$时，该过程停止。所以我们有$\{m_1 > m_2 > \ldots > m_r\}$和$\mathcal{J}(m, n) = \{J_1(m, n), J_2(m, n), \ldots, J_r(m, n)\}$。我们有下面这个命题。

命题4.1. 对于以上定义的$\mathcal{J}(m, n)$，我们有下面这些性质。

1. 若$i \neq j$，则$J_i(m, n) \cap J_j(m, n) = \emptyset$。

2. 对任意$1 \leq i \leq r$和任意$\boldsymbol{u} \in J_i(m, n)$，$\boldsymbol{u}$的坐标中恰好有$n - m_i$个0。

3. 对任意$1 \leq i \leq r$，

$$|J_i(m, n)| = \binom{n}{m_i} 2^{m_i}。 \tag{4.2}$$

4. 对任意$1 \le i \le r$和任意$\boldsymbol{u} \in J_i(m,n)$，$\boldsymbol{u}$的$\ell_p$范数是$m^{1/p}$。

5. 若$i \ne j$，那么对任意$\boldsymbol{u} \in J_i(m,n)$和$\boldsymbol{v} \in J_j(m,n)$，我们有$d_p(\boldsymbol{u},\boldsymbol{v}) \ge m^{1/p}$。

证明. 前四条性质是平凡的。

我们证明最后一条性质。设$\boldsymbol{u} = (u_1, u_2, \dots, u_n) \in J_i(m,n)$，$\boldsymbol{v} = (v_1, v_2, \dots, v_n) \in J_j(m,n)$，其中$1 \le i < j \le r$。不失一般性，假设$u_1 = u_2 = \cdots = u_{m_i} = (m/m_i)^{1/p}$，$u_{m_i+1} = u_{m_i+2} = \cdots = u_n = 0$。换句话说，$\boldsymbol{u} = (m/m_i)^{1/p} \cdot 1^{m_i} 0^{n-m_i}$。对于$1 \le k \le m_i$，我们有$v_k \in \{0, \pm(m/m_j)^{1/p}\}$，以及

$$\begin{aligned}
&|u_k - v_k|^p \\
\ge& \min\left\{|(m/m_i)^{1/p} - 0|^p, |(m/m_i)^{1/p} - (m/m_j)^{1/p}|^p, |(m/m_i)^{1/p} + (m/m_j)^{1/p}|^p\right\} \\
=& \min\left\{|(m/m_i)^{1/p} - 0|^p, |(m/m_i)^{1/p} - (m/m_j)^{1/p}|^p\right\} \\
=& \min\left\{\frac{m}{m_i}, \frac{m}{m_i} \cdot |1 - (m_i/m_j)^{1/p}|^p\right\} \\
=& \frac{m}{m_i} \min\left\{1, |1 - (m_i/m_j)^{1/p}|^p\right\}。
\end{aligned}$$

因为$j > i$，所以$m_j \le m_{i+1} = \lfloor \frac{m_i}{2^p} \rfloor \le \frac{m_i}{2^p}$。所以$m_i/m_j \ge 2^p$，并且

$$\begin{aligned}
|u_k - v_k|^p \ge& \frac{m}{m_i} \min\left\{1, |1 - (m_i/m_j)^{1/p}|^p\right\} \\
\ge& \frac{m}{m_i} \min\left\{1, |1 - (2^p)^{1/p}|^p\right\} \\
=& \frac{m}{m_i}。
\end{aligned}$$

从而

$$d_p(\boldsymbol{u},\boldsymbol{v})^p = \sum_{k=1}^{n} |u_k - v_k|^p \ge \sum_{k=1}^{m_i} |u_k - v_k|^p \ge \sum_{k=1}^{m_i} \frac{m}{m_i} = m。$$

这就完成了证明。 □

对任意i，记$J_i'(m,n)$是$J_i(m,n)$的满足性质

“对任意$\boldsymbol{u},\boldsymbol{v} \in J_i'(m,n)$，都有$d_p(\boldsymbol{u},\boldsymbol{v}) \ge m^{1/p}$”

的一个最大子集。因为我们已经证明当$i \ne j$时，若$\boldsymbol{u} \in J_i'(m,n) \subseteq J_i(m,n)$，$\boldsymbol{v} \in J_j'(m,n) \subseteq J_j(m,n)$，则$d_p(\boldsymbol{u},\boldsymbol{v}) \ge m^{1/p}$，所以

$$\frac{1}{m^{1/p}} \bigcup_{i=1}^{r} J_i'(m,n) := \left\{\boldsymbol{x} \in \mathbb{R}^n : m^{1/p}\boldsymbol{x} \in \bigcup_{i=1}^{r} J_i'(m,n)\right\}$$

是一个最小距离为1的ℓ_p球面码。因此

$$A_p(n,1/2) \geq \left| \frac{1}{m^{1/p}} \bigcup_{i=1}^{r} J_i'(m,n) \right| = \left| \bigcup_{i=1}^{r} J_i'(m,n) \right| = \sum_{i=1}^{r} |J_i'(m,n)| \text{。} \tag{4.3}$$

对于$1 \leq i \leq r$和$\boldsymbol{u} \in J_i(m,n)$，定义

$$B_{i,n}(\boldsymbol{u},m) := \left\{ \boldsymbol{v} \in J_i(m,n) : d_p(\boldsymbol{u},\boldsymbol{v}) < m^{1/p} \right\}$$

为度量空间$(J_i(m,n), \|\cdot\|_p)$中的半径为$m^{1/p}$、球心为$\boldsymbol{u}$的开ℓ_p球。注意到$B_{i,n}(\boldsymbol{u},m)$的基数与球心$\boldsymbol{u}$无关。如果我们用$B_{i,n}(m)$来表示$B_{i,n}(\boldsymbol{u},m)$的基数，那么

$$B_{i,n}(m) = \sum_{2t+2^p x < m_i} \binom{m_i}{t} \binom{n-m_i}{t} \binom{m_i - t}{x} 2^t \text{。} \tag{4.4}$$

利用上述符号，我们有下面这个定理。它是$|J_i'(m,n)|$的Gilbert-Varshamov型界。

定理4.1. *对任意$1 \leq i \leq r$，我们有*

$$|J_i'(m,n)| \geq \left\lceil \frac{|J_i(m,n)|}{B_{i,n}(m)} \right\rceil = \left\lceil \frac{\binom{n}{m_i} 2^{m_i}}{B_{i,n}(m)} \right\rceil \text{。} \tag{4.5}$$

我们立刻可以得到下面这个推论，并且它是我们的主要结果。

推论4.1.

$$A_p(n,1/2) \geq \max_{1 \leq m \leq n} \sum_{i=1}^{r} \left\lceil \frac{\binom{n}{m_i} 2^{m_i}}{B_{i,n}(m)} \right\rceil \text{。} \tag{4.6}$$

注记4.1. *在文献[85]的引理2.1中，$A_p(n,1/2)$的下界是*

$$\max_{1 \leq m \leq n} \left\lceil \frac{\binom{n}{m_1} 2^{m_1}}{B_{1,n}(m)} \right\rceil \text{。}$$

所以推论4.1做了改进。

定理4.1的证明. 给定i，记$J = \left\lceil \frac{|J_i(m,n)|}{B_{i,n}(m)} \right\rceil$。我们从$J_i(m,n)$递归地选点。首先，我们从$J_i(m,n)$任选一点$\boldsymbol{u}_1$。假设我们已经选了$\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$，其中$k < J$。集合

$$J_i(m,n) \setminus \left(\bigcup_{j=1}^{k} B_{i,n}(\boldsymbol{u}_j, m) \right)$$

的基数至少是

$$|J_i(m,n)| - \sum_{j=1}^{k} |B_{i,n}(\boldsymbol{u}_j, m)| = |J_i(m,n)| - kB_{i,n}(m) > 0。$$

所以我们可以从$J_i(m,n) \setminus \left(\bigcup_{j=1}^{k} B_{i,n}(\boldsymbol{u}_j, m)\right)$中选出一点$\boldsymbol{u}_{k+1}$，使得对任意$1 \le j \le k$，都有$d_p(\boldsymbol{u}_{k+1}, \boldsymbol{u}_j) \ge m^{1/p}$。只要$k < J$，这个过程就可以一直持续下去。最终，我们得到了$J_i(m,n)$的一个子集$\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_J\}$，其中的点两两之间的$\ell_p$距离至少是$m^{1/p}$。所以$|J_i'(m,n)| \ge J$。 □

§ 4.3 当p比较小时的数值结果

对于推论4.1的下界，似乎没有一个显式表达式。因此，在这一节，我们给出p比较小的时候的数值结果。在文献[85]中，Xu给出了

$$\max_{1 \le m \le n} \left\lceil \frac{\binom{n}{m_1} 2^{m_1}}{B_{1,n}(m)} \right\rceil$$

的下界。不过我们仍然需要估计不等式(4.6)右边的余项。

定义

$$F_p(\sigma) = \frac{\binom{n}{\lfloor \sigma n \rfloor} 2^{\lfloor \sigma n \rfloor}}{\sum_{2t+2^p x < \lfloor \sigma n \rfloor} \binom{\lfloor \sigma n \rfloor}{t} \binom{n-\lfloor \sigma n \rfloor}{t} \binom{\lfloor \sigma n \rfloor - t}{x} 2^t}, \sigma \in (0,1)。$$

由等式(4.1)-(4.4)和不等式(4.6)，我们有

$$A_p(n, 1/2) \ge \max_{0<\sigma<1} \sum_{i=1}^{r} F_p\left(\frac{\sigma}{2^{(i-1)p}}\right)。$$

4.3.1 r的值

我们首先估计r的大小。假设对于某个k，有$m = \lceil 2^{kp} + 2^{(k-1)p} + \cdots + 2^p \rceil$。那么

$$\begin{aligned} m_1 = m &= \lceil 2^{kp} + 2^{(k-1)p} + \cdots + 2^p \rceil \\ &\in \left[2^{kp} + 2^{(k-1)p} + \cdots + 2^p, 2^{kp} + 2^{(k-1)p} + \cdots + 2^p + 1\right]。 \end{aligned}$$

计算得

$$\begin{aligned} m_2 = \left\lfloor \frac{m_1}{2^p} \right\rfloor &\in \left[\lfloor 2^{(k-1)p} + 2^{(k-2)p} + \cdots + 1 \rfloor, \lfloor 2^{(k-1)p} + 2^{(k-2)p} + \cdots + 1 + 2^{-p} \rfloor\right] \\ &\subseteq \left[2^{(k-1)p} + 2^{(k-2)p} + \cdots + 2^p, 2^{(k-1)p} + 2^{(k-2)p} + \cdots + 1 + 2^{-p}\right], \end{aligned}$$

以及

$$m_3 = \left\lfloor \frac{m_2}{2^p} \right\rfloor \in \left[\lfloor 2^{(k-2)p} + 2^{(k-3)p} + \cdots + 1 \rfloor, \lfloor 2^{(k-2)p} + 2^{(k-3)p} + \cdots + 2^{-p} + 2^{-2p} \rfloor \right]$$
$$\subseteq \left[2^{(k-2)p} + 2^{(k-3)p} + \cdots + 2^p, 2^{(k-2)p} + 2^{(k-3)p} + \cdots + 2^{-p} + 2^{-2p} \right] 。$$

所以

$$m_k \in \left[2^p, 2^p + 1 + 2^{-p} + \cdots + 2^{-(k-1)p} \right] ,$$

并且

$$m_{k+1} \in \left[1, 1 + 2^{-p} + 2^{-2p} + \cdots + 2^{-kp} \right] \subseteq [1, 2)。$$

所以若$m = \lceil 2^{kp} + 2^{(k-1)p} + \cdots + 2^p \rceil$，则$m_{k+1} = 1$，$r = k+1$。注意到$\lceil 2^{kp} + 2^{(k-1)p} + \cdots + 2^p \rceil \in [2^{kp}, 2^{(k+1)p})$。另一方面，若$m \in [2^{kp}, \lceil 2^{kp} + 2^{(k-1)p} + \cdots + 2^p \rceil)$，那么$m_k$可能会比$2^p$小。综上，我们知道$r = \lfloor \log_{2^p} m \rfloor + 1$或$r = \lfloor \log_{2^p} m \rfloor$。

4.3.2 $F_p(\sigma)$的渐进行为

在这一子节，我们研究$F_p(\sigma)$的渐进行为。

定义$H(\sigma)$为熵函数，

$$H(\sigma) = \begin{cases} 0, & 若\sigma = 0或\sigma = 1; \\ -\sigma \log_2 \sigma - (1-\sigma) \log_2 (1-\sigma), & 若0 < \sigma < 1。 \end{cases}$$

我们有下面的定理。

定理4.2 ([85]).

$$\lim_{n \to \infty} \frac{1}{n} \log_2 F_p(\sigma) \geq \min_{0 \leq y \leq \min\{\sigma/2, 1-\sigma\}} f_p(\sigma, y),$$

其中

$$\begin{aligned} & f_p(\sigma, y) \\ =& (\sigma - y) \left(1 - H\left(\frac{\sigma - 2y}{2^p(\sigma - y)} \right) \right) + H(\sigma) - \sigma H\left(\frac{y}{\sigma} \right) - (1-\sigma) H\left(\frac{y}{1-\sigma} \right) 。 \end{aligned}$$

4.3.3 对于特定的p的数值结果

记$g_p(\sigma)=\min_{0\le y\le \min\{\sigma/2,1-\sigma\}} f_p(\sigma,y)$。我们列出一些特定的$p$的数值结果。

当$p=1$时，$g_1(\sigma)$在$\sigma_0=0.2605$时取到最大值0.1825。所以

$$\begin{aligned}
A_1(n,1/2) &\ge \max_{0\le\sigma\le 1}\sum_{i=1}^{r} F_1\left(\frac{\sigma}{2^{i-1}}\right)\\
&\ge \sum_{i=1}^{r} F_1\left(\frac{2\sigma_0}{2^{i-1}}\right)\\
&\ge F_1(2\sigma_0)+F_1(\sigma_0)+F_1\left(\frac{\sigma_0}{2}\right)+\cdots\\
&\ge 2^{g_1(2\sigma_0)\cdot n(1+o(1))}+2^{g_1(\sigma_0)\cdot n(1+o(1))}+2^{g_1(\sigma_0/2)\cdot n(1+o(1))}+\cdots\\
&= 2^{0.1247n(1+o(1))}+2^{0.1825n(1+o(1))}+2^{0.1554n(1+o(1))}+\cdots。
\end{aligned}$$

尽管$2^{0.1247n(1+o(1))}+2^{0.1554n(1+o(1))}+\cdots=o(2^{0.1825n(1+o(1))})$，我们仍然保留这些项，因为它们改进了以前的结果。

注记4.2. *在文献[77]中，Talata也得到了*$A_1(n,1/2)\ge 2^{0.1825n(1+o(1))}$。

当$p=2$时，$g_2(\sigma)$在$\sigma_0=0.3881$时取到最大值0.2059。所以

$$\begin{aligned}
A_2(n,1/2) &\ge \max_{0\le\sigma\le 1}\sum_{i=1}^{r} F_2\left(\frac{\sigma}{2^{2(i-1)}}\right)\\
&\ge \sum_{i=1}^{r} F_2\left(\frac{\sigma_0}{4^{i-1}}\right)\\
&\ge F_2(\sigma_0)+F_2\left(\frac{\sigma_0}{4}\right)+F_2\left(\frac{\sigma_0}{4^2}\right)+\cdots\\
&\ge 2^{g_2(\sigma_0)\cdot n(1+o(1))}+2^{g_2(\sigma_0/4)\cdot n(1+o(1))}+2^{g_2(\sigma_0/16)\cdot n(1+o(1))}+\cdots\\
&= 2^{0.2059n(1+o(1))}+2^{0.1381n(1+o(1))}+2^{0.0584n(1+o(1))}+\cdots。
\end{aligned}$$

在数值结果中，我们仍然保留$2^{0.1381n(1+o(1))}+2^{0.0584n(1+o(1))}+\cdots$这些项。

当$p=2.1$时，$g_{2.1}(\sigma)$在$\sigma_0=0.9998$时取到最大值0.2163。所以

$$\begin{aligned}
&A_{2.1}(n,1/2)\\
\geq&\max_{0\leq\sigma\leq1}\sum_{i=1}^{r}F_{2.1}\left(\frac{\sigma}{2^{2.1(i-1)}}\right)\\
\geq&\sum_{i=1}^{r}F_{2.1}\left(\frac{\sigma_0}{4.2871^{i-1}}\right)\\
\geq&F_{2.1}\left(\sigma_0\right)+F_{2.1}\left(\frac{\sigma_0}{4.2871}\right)+F_{2.1}\left(\frac{\sigma_0}{4.2871^2}\right)+\cdots\\
\geq&2^{g_{2.1}(\sigma_0)\cdot n(1+o(1))}+2^{g_{2.1}(\sigma_0/4.2871)\cdot n(1+o(1))}+2^{g_{2.1}(\sigma_0/18.3792)\cdot n(1+o(1))}+\cdots\\
=&2^{0.2163n(1+o(1))}+2^{0.1944n(1+o(1))}+2^{0.0995n(1+o(1))}+\cdots。
\end{aligned}$$

我们仍然保留$2^{0.1944n(1+o(1))}+2^{0.0995n(1+o(1))}+\cdots$这些项。

§ 4.4 当p比较大时的数值结果

存在一个临界值$p_0\approx2.1$（这里我们并不关心p_0的确切值），使得当$p>p_0$时，$F_p(\sigma)$在$\sigma=1$时取到最大值。当$\sigma=1$时，$m=n$，我们将给出另一个下界。

令$m=n$。回顾不等式(4.3)和不等式(4.5)，我们有

$$\begin{aligned}
A_p(n,1/2)&\geq\sum_{i=1}^{r}|J_i'(n,n)|\\
&=|J_1'(n,n)|+\sum_{i=2}^{r}|J_i'(n,n)|\\
&\geq|J_1'(n,n)|+\sum_{i=2}^{r}\left\lceil\frac{\binom{n}{m_i}2^{m_i}}{B_{i,n}(n)}\right\rceil\\
&=|J_1'(n,n)|+\sum_{i=2}^{r}F_p\left(\frac{1}{2^{p(i-1)}}\right)。
\end{aligned}$$

事实上，我们可以适当改进$|J_1'(n,n)|$的下界。

4.4.1 $|J_1'(n,n)|$的改进下界

回顾$J_1(n,n)$和$J_1'(n,n)$的定义。$J_1(n,n)=\{\pm1\}^n$，并且$J_1'(n,n)$是$\{\pm1\}^n$的最大子集，其中的点两两之间的ℓ_p距离至少是$n^{1/p}$。对于$\boldsymbol{u},\boldsymbol{v}\in\{\pm1\}^n$，令$d_H(\boldsymbol{u},\boldsymbol{v}):=|\{i:u_i\neq v_i\}|$为它们之间的Hamming距离。我们有下面这个简单的引理。

引理4.2. *对任意$\boldsymbol{u},\boldsymbol{v}\in\{\pm1\}^n$，我们有*

$$(d_p(\boldsymbol{u},\boldsymbol{v}))^p = 2^p\cdot d_H(\boldsymbol{u},\boldsymbol{v})。$$

因此，我们只需找到$\{\pm1\}^n$的一个最大的子集，其中的点两两之间的Hamming距离至少为$\lceil n/2^p\rceil$。回顾$B_{1,n}(\boldsymbol{u},n)$的定义，我们有

$$\begin{aligned}B_{1,n}(\boldsymbol{u},n) &= \left\{\boldsymbol{v}\in\{\pm1\}^n : d_p(\boldsymbol{u},\boldsymbol{v})<n^{1/p}\right\}\\ &= \{\boldsymbol{v}\in\{\pm1\}^n : 2^p\cdot d_H(\boldsymbol{u},\boldsymbol{v})<n\}\\ &= \{\boldsymbol{v}\in\{\pm1\}^n : d_H(\boldsymbol{u},\boldsymbol{v})\le\lceil n/2^p\rceil-1\}。\end{aligned}$$

所以$B_{1,n}(n)=|B_{1,n}(\boldsymbol{u},n)|=\sum_{k=0}^{\lceil n/2^p\rceil-1}\binom{n}{k}$。下面这个定理给出了$|J_1'(n,n)|$的一个更好的下界。

定理4.3 ([35]). *存在一个正常数c使得*

$$|J_1'(n,n)|\ge c\frac{2^n}{B_{1,n}(n)}\log_2 B_{1,n}(n)。$$

注意到，由Stirling公式，我们有

$$\lim_{n\to\infty}\frac{1}{n}\log_2 B_{1,n}(n)=H\left(\frac{1}{2^p}\right)。$$

所以

$$|J_1'(n,n)|\ge c\frac{n2^n}{B_{1,n}(n)}=cn2^{n(1-H(2^{-p})+o(1))},$$

其中c是某个常数（可能与p有关，但与n无关）。

4.4.2 对于特定的p的数值结果

跟之前一样，令$g_p(\sigma)=\min_{0\le y\le\min\{\sigma/2,1-\sigma\}}f_p(\sigma,y)$。我们在这里列出一些特定的$p$的数值结果。

当$p=2.2$时，我们有

$$\begin{aligned}
&A_{2.2}(n,1/2)\\
\geq&|J_1'(n,n)|+\sum_{i=2}^{r}F_{2.2}\left(\frac{1}{2^{2.2(i-1)}}\right)\\
\geq&cn2^{n(1-H(2^{-2.2})+o(1))}+F_{2.2}\left(0.2176\right)+F_{2.2}\left(0.0474\right)+\cdots\\
\geq&cn2^{n(1-H(2^{-2.2})+o(1))}+2^{g_{2.2}(0.2176)\cdot n(1+o(1))}+2^{g_{2.2}(0.0474)\cdot n(1+o(1))}+\cdots\\
=&cn2^{0.2442n(1+o(1))}+2^{0.1913n(1+o(1))}+2^{0.0915n(1+o(1))}+\cdots。
\end{aligned}$$

当$p=3$时，我们有

$$\begin{aligned}
&A_3(n,1/2)\\
\geq&|J_1'(n,n)|+\sum_{i=2}^{r}F_3\left(\frac{1}{2^{3(i-1)}}\right)\\
\geq&cn2^{n(1-H(2^{-3})+o(1))}+F_3\left(0.1250\right)+F_3\left(0.0156\right)+\cdots\\
\geq&cn2^{n(1-H(2^{-3})+o(1))}+2^{g_3(0.1250)\cdot n(1+o(1))}+2^{g_3(0.0156)\cdot n(1+o(1))}+\cdots\\
=&cn2^{0.4564n(1+o(1))}+2^{0.1562n(1+o(1))}+2^{0.0425n(1+o(1))}+\cdots。
\end{aligned}$$

当$p=4$时，我们有

$$\begin{aligned}
&A_4(n,1/2)\\
\geq&|J_1'(n,n)|+\sum_{i=2}^{r}F_4\left(\frac{1}{2^{4(i-1)}}\right)\\
\geq&cn2^{n(1-H(2^{-4})+o(1))}+F_4\left(0.0625\right)+F_4\left(0.0039\right)+\cdots\\
\geq&cn2^{n(1-H(2^{-4})+o(1))}+2^{g_4(0.0625)\cdot n(1+o(1))}+2^{g_4(0.0039)\cdot n(1+o(1))}+\cdots\\
=&cn2^{0.6627n(1+o(1))}+2^{0.1083n(1+o(1))}+2^{0.0145n(1+o(1))}+\cdots。
\end{aligned}$$

§4.5 进一步的讨论

在文献[69]中，Sah等人得到了一个关于不同的ℓ_p球面码之间的不等式，即对任意$1\leq q\leq p$和$d\in(0,1]$，有$A_p(n,d)\leq A_q(n,d^{p/q})$。所以

$$A_2(n,d)\leq A_p(n,d^{2/p})，若1\leq p\leq 2，\tag{4.7}$$

且

$$A_p(n,d) \le A_2(n,d^{p/2})，若p \ge 2。 \tag{4.8}$$

Sah等人利用不等式(4.8)得到了$A_p(n,d)$的上界（$p \ge 2$）。

另一方面，Swanepoel[76]利用不等式(4.7)得到了$A_p(n,1/2)$的下界（$1.62107 < p \le 2$）。在那之后，$A_2(n,d)$的最佳下界有所改进，所以我们在这里更新这一类下界。我们有下述定理，它是目前已知$A_2(n,d)$（$d \in (0,1)$）的最佳下界。

定理4.4 ([22])**.** 给定$\theta \in (0,\pi/2)$，则

$$A_2(n,\sin(\theta/2)) \ge (1+o(1))\ln\frac{\sin\theta}{\sqrt{2}\sin(\theta/2)}\cdot n\cdot\frac{\sqrt{2\pi n}\cos\theta}{\sin^{n-1}\theta}。$$

当$1 < p \le 2$时，我们有

$$A_p(n,1/2) \ge A_2(n,(1/2)^{p/2})。$$

令$\sin(\theta/2) = 2^{-p/2}$。则$\cos(\theta/2) = \sqrt{1-2^{-p}}$，$\sin\theta = 2^{1-p/2}\sqrt{1-2^{-p}}$，$\cos\theta = 1-2^{1-p}$。所以

$$\begin{aligned} A_p(n,1/2) &\ge A_2(n,(1/2)^{p/2}) \\ &= A_2(n,\sin(\theta/2)) \\ &\ge (1+o(1))\ln\sqrt{2-2^{1-p}}\cdot n\cdot\frac{\sqrt{2\pi n}(1-2^{1-p})}{(2^{1-p/2}\sqrt{1-2^{-p}})^{n-1}}。 \end{aligned} \tag{4.9}$$

经过数值计算，当$p \in (1.9948,2]$时，不等式(4.9)给出的下界比不等式(4.6)给出的下界更好。

第 5 章 有限域上的相似图形

§ 5.1 简介

离散几何中的许多问题都问一个集合的最小基数，使得这个集合中必定会有某种给定的结构。Falconer猜想便是其中之一。Falconer猜想指的是如果$\mathbb{R}^d$的一个子集$\mathcal{E}$的Hausdorff维数严格大于$d/2$，那么$\mathcal{E}$中任意两点之间的距离构成的集合具有正Lebesgue测度。目前已知最佳的结果可以参考文献[14, 15, 24]。

设$\mathbb{F}_q$为q个元素的域。在有限域中，Erdős-Falconer距离问题问的是$\mathbb{F}_q^d$的子集$\mathcal{E}$的最小基数，使得距离集合

$$\Delta(\mathcal{E}) := \{\|\boldsymbol{x}-\boldsymbol{y}\| : \boldsymbol{x},\boldsymbol{y} \in \mathcal{E}\}$$

占$\mathbb{F}_q$的正比例，其中对于$\boldsymbol{x} = (x_1, x_2, \ldots, x_d) \in \mathbb{F}_q^d$，$\|\boldsymbol{x}\| := x_1^2 + x_2^2 + \cdots + x_d^2$。在文献[32]中，Iosevich和Rudnev证明了存在一个常数C，如果$|\mathcal{E}| \geq Cq^{(d+1)/2}$，那么$\Delta(\mathcal{E}) = \mathbb{F}_q$。同时他们也证明在一般情况下，$|\mathcal{E}| \geq Cq^{d/2}$是一个必要条件。Hart等人[28]证明了在奇数维数时，$(d+1)/2$是最佳的指数。在文献[5]中，Chapman等人证明了如果$\mathcal{E} \subseteq \mathbb{F}_q^2$，$q \equiv 3 \pmod 4$，且$|\mathcal{E}| \geq q^{4/3}$，那么$|\Delta(\mathcal{E})| \geq cq$。这个结果改进了2维时的指数$(d+1)/2$。Bennett等人[2]接着将这个结论推广到任意域上的2维线性空间。在一般的偶数维数时，指数$d/2$是否充分，仍然有待研究。

Iosevich等人[31]考察了距离集的商集

$$\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})} := \left\{\frac{a}{b} : a \in \Delta(\mathcal{E}), b \in \Delta(\mathcal{E}) \setminus \{0\}\right\},$$

并得到如下定理。

定理5.1 ([31]). 设$\mathcal{E} \subseteq \mathbb{F}_q^d$，且$d$是大于等于2的偶数。若$|\mathcal{E}| \geq 9q^{d/2}$，则

$$\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})} = \mathbb{F}_q。$$

定理5.2 ([31]). 设$\mathcal{E} \subseteq \mathbb{F}_q^d$，且$d$是大于等于3的奇数。若$|\mathcal{E}| \geq 6q^{d/2}$，则

$$\frac{\Delta(\mathcal{E})}{\Delta(\mathcal{E})} \supseteq \mathbb{F}_q^+ \cup \{0\},$$

其中$\mathbb{F}_q^+$表示$\mathbb{F}_q$中的非零二次剩余的集合。

定理5.1的结论意味着对任意$r \in \mathbb{F}_q^*$，存在$\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}', \boldsymbol{y}' \in \mathcal{E}$，使得$\|\boldsymbol{y}' - \boldsymbol{y}\| = r\|\boldsymbol{x}' - \boldsymbol{x}\| \neq 0$。换句话说，$K_{|\mathcal{E}|}$包含一对长度比为$r$的边。确切地说，我们有以下定义。

定义5.1. 设$G = (V, E)$是一个图，$V = \{1, 2, \ldots, n\}$，$E \subseteq \binom{V}{2}$。对于$\mathbb{F}_q^d$的一个子集$\mathcal{E}$，我们称$\mathcal{E}$包含一对相似比为r的图G，如果存在不同的$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in \mathcal{E}$和不同的$\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n \in \mathcal{E}$，使得对任意$\{i, j\} \in E$，都有$\|\boldsymbol{y}_i - \boldsymbol{y}_j\| = r\|\boldsymbol{x}_i - \boldsymbol{x}_j\| \neq 0$。

注记5.1. 当$d = 2$且-1不是$\mathbb{F}_q$的二次剩余时，由$\boldsymbol{x}_i \neq \boldsymbol{x}_j$可以推出$\|\boldsymbol{x}_i - \boldsymbol{x}_j\| \neq 0$。在其他情况，有可能会出现$\boldsymbol{x}_i \neq \boldsymbol{x}_j$且$\|\boldsymbol{x}_i - \boldsymbol{x}_j\| = 0$。为了避免平凡的情况，我们在定义*5.1*中加上了条件$\|\boldsymbol{x}_i - \boldsymbol{x}_j\| \neq 0$。

最近，Rakhmonov[59]针对特定的图G，考察了$\mathcal{E}$的最小基数条件。方便起见，我们给出一些图类的基本定义。对于一个自然数n，我们用$[n]$表示集合$\{1, 2, \ldots, n\}$。

定义5.2. 设$G = (V, E)$是一个图，其中$V = [n]$，$E \subseteq \binom{[n]}{2}$。

- 若$n = k + 1$且$E = \{\{1, 2\}, \{2, 3\}, \ldots, \{k, k + 1\}\}$，则称$G$是一条$k$长路径（*k-path*）。
- 若$n = k + 1$且$E = \{\{1, 2\}, \{1, 3\}, \ldots, \{1, k + 1\}\}$，则称$G$是一个$k$星（*k-star*）。
- 若$n = k$且$E = \{\{1, 2\}, \{2, 3\}, \ldots, \{k - 1, k\}, \{k, 1\}\}$，则称$G$是一个$k$圈（*k-cycle*）。

记$\mathbb{F}_q^*$为$\mathbb{F}_q$中的非零元素构成的集合。Rakhmonov得到了下列结论。

定理5.3 ([59]). 若$r \in \mathbb{F}_p^*$，p是一个素数且$p \equiv 3 \pmod 4$，$\mathcal{E} \subseteq \mathbb{F}_p^2$且$|\mathcal{E}| > (\sqrt{3} + 1)p$，则$\mathcal{E}$包含一对相似比为$r$的2长路径。

定理5.4 ([59]). 若$r \in \mathbb{F}_p^*$，p是一个素数且$p \equiv 3 \pmod 4$，$\mathcal{E} \subseteq \mathbb{F}_p^2$且$|\mathcal{E}| > 4\sqrt{3}p^{3/2}$，则$\mathcal{E}$包含一对相似比为$r$的4圈。

在这一章，我们关注k星和4长路径这两类情况。我们的主要结果是以下定理。

定理5.5. 设q是一个奇素数的幂，$\mathcal{E} \subseteq \mathbb{F}_q^d$，且$k \geq 2$为整数。

- 若$q \geq 5$，$d \geq 2$为偶数，$r \in \mathbb{F}_q^*$，且$\mathcal{E}$的基数至少是$\left(31 + 10\binom{k}{2}\right) q^{d/2}$，则$\mathcal{E}$包含一对相似比为$r$的$k$星。
- 若$d \geq 3$为奇数，$r \in \mathbb{F}_q^+$，且$\mathcal{E}$的基数至少是$\left(4 + \sqrt{3}\binom{k}{2}\right) q^{d/2}$，则则$\mathcal{E}$包含一对相似比为$r$的$k$星。

定理5.6. 设q是一个奇素数的幂，且$\mathcal{E} \subseteq \mathbb{F}_q^d$。

- 若$q \geq 5$，d为2或4，$r \in \mathbb{F}_q^*$，且$\mathcal{E}$的基数至少是$36q^{(2d+1)/3}$，则$\mathcal{E}$包含一对相似比为r的4长路径。
- 若$d = 3$，$r \in \mathbb{F}_q^+$，且$\mathcal{E}$的基数至少是$9q^{(2d+1)/3}$，则$\mathcal{E}$包含一对相似比为r的4长路径。
- 若$d = 5$，$r \in \mathbb{F}_q^+$，且$\mathcal{E}$的基数至少是$12q^3$，则$\mathcal{E}$包含一对相似比为r的4长路径。
- 若$q \geq 5$，$d \geq 6$为偶数，$r \in \mathbb{F}_q^*$，且$\mathcal{E}$的基数至少是$313q^{d/2}$，则$\mathcal{E}$包含一对相似比为r的4长路径。
- 若$d \geq 7$为奇数，$r \in \mathbb{F}_q^+$，且$\mathcal{E}$的基数至少是$313q^{d/2}$，则$\mathcal{E}$包含一对相似比为r的4长路径。

注记5.2. 定理*5.5*和定理*5.6*中的常数因子是为方便而取的，并不一定是最优的。

我们会在§ 5.2证明定理5.5，在§ 5.3证明定理5.6。

以下是我们的想法。回顾定义5.1，$\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$各不相同，$\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n$也各不相同。如果我们允许一些$\boldsymbol{x}_i$（或$\boldsymbol{y}_i$）相同，那么我们会得到一对退化的图。我们有

$$\text{非退化的图的数目} = \text{总数} - \text{退化的图的数目}。$$

当$\mathcal{E}$的基数比较大时，总数会比较多，并且退化的图会相对较少。这样的话$\mathcal{E}$就会包含一对相似比为r的图。证明过程中我们也用到一些图论工具。

§ 5.2 定理5.5的证明

在这一节，我们研究$\mathcal{E}$的最小基数，使得$\mathcal{E}$会包含一对相似比为r的k星，并证明定理5.5。

令

$$\begin{aligned} S_k(r) =&\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{k+1}, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{k+1}) \in \mathcal{E}^{2k+2} : \\ &\|\boldsymbol{y}_i - \boldsymbol{y}_1\| = r\|\boldsymbol{x}_i - \boldsymbol{x}_1\| \neq 0, i = 2, 3, \ldots, k+1\}。 \end{aligned}$$

记

$$A_{ij} = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{k+1}, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{k+1}) \in S_k(r) : \boldsymbol{x}_i = \boldsymbol{x}_j\},$$

$$A'_{ij} = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{k+1}, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{k+1}) \in S_k(r) : \boldsymbol{y}_i = \boldsymbol{y}_j\},$$

以及

$$\begin{aligned} B =&\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{k+1}, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{k+1}) \in S_k(r) : \\ &\boldsymbol{x}_i \neq \boldsymbol{x}_j, \boldsymbol{y}_i \neq \boldsymbol{y}_j, \forall 1 \leq i < j \leq k+1\}。 \end{aligned}$$

容易看出

$$S_k(r) = \left(\bigcup_{2 \leq i < j \leq k+1} (A_{ij} \cup A'_{ij}) \right) \bigcup B$$

且

$$|B| = |S_k(r)| - \left| \bigcup_{2 \leq i < j \leq k+1} (A_{ij} \cup A'_{ij}) \right|。$$

注意到

$$\left| \bigcup_{2 \leq i < j \leq k+1} (A_{ij} \cup A'_{ij}) \right| \leq \sum_{2 \leq i < j \leq k+1} \left| A_{ij} \cup A'_{ij} \right| = \binom{k}{2} \left| A_{k,k+1} \cup A'_{k,k+1} \right|$$

并且

$$\left| A_{k,k+1} \cup A'_{k,k+1} \right| = |A_{k,k+1}| + |A'_{k,k+1}| - \left| A_{k,k+1} \cap A'_{k,k+1} \right|。$$

经过计算，我们有

$$\begin{aligned}
&|A_{k,k+1}|\\
=&|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k,\boldsymbol{x}_{k+1},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_k,\boldsymbol{y}_{k+1})\in\mathcal{E}^{2k+2}:\boldsymbol{x}_k=\boldsymbol{x}_{k+1},\\
&\|\boldsymbol{y}_i-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_i-\boldsymbol{x}_1\|\neq 0,i=2,3,\ldots,k+1\}|\\
=&|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_k,\boldsymbol{y}_{k+1})\in\mathcal{E}^{2k+1}:\\
&\|\boldsymbol{y}_i-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_i-\boldsymbol{x}_1\|\neq 0,2\leq i\leq k,\|\boldsymbol{y}_{k+1}-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_k-\boldsymbol{x}_1\|\}|\\
\leq&|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_k)\in\mathcal{E}^{2k}:\|\boldsymbol{y}_i-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_i-\boldsymbol{x}_1\|\neq 0,2\leq i\leq k\}|\\
&\cdot|\{\boldsymbol{y}_{k+1}:\boldsymbol{y}_{k+1}\in\mathcal{E}\}|\\
=&|\mathcal{E}|\cdot|S_{k-1}(r)|。
\end{aligned}\tag{5.1}$$

类似地，$|A'_{k,k+1}|\leq|\mathcal{E}|\cdot|S_{k-1}(r)|$，$\left|A_{k,k+1}\cap A'_{k,k+1}\right|=|S_{k-1}(r)|$。所以我们有

$$\begin{aligned}
|B|=&|S_k(r)|-\left|\bigcup_{2\leq i<j\leq k+1}(A_{ij}\cup A'_{ij})\right|\\
\geq&|S_k(r)|-\binom{k}{2}\left|A_{k,k+1}\cup A'_{k,k+1}\right|\\
\geq&|S_k(r)|-\binom{k}{2}\left(2|\mathcal{E}|\cdot|S_{k-1}(r)|-|S_{k-1}(r)|\right)\\
=&|S_k(r)|-\binom{k}{2}\left(2|\mathcal{E}|-1\right)|S_{k-1}(r)|。
\end{aligned}\tag{5.2}$$

我们构造一个辅助图$\mathcal{G}$，其中$V(\mathcal{G})=\mathcal{E}\times\mathcal{E}=\{(\boldsymbol{x},\boldsymbol{y}):\boldsymbol{x},\boldsymbol{y}\in\mathcal{E}\}$。$V(\mathcal{G})$中的两个点$(\boldsymbol{x},\boldsymbol{y})$和$(\boldsymbol{x}',\boldsymbol{y}')$之间有一条边相连当且仅当$\|\boldsymbol{y}'-\boldsymbol{y}\|=r\|\boldsymbol{x}'-\boldsymbol{x}\|\neq 0$。不难看出$\mathcal{G}$是良好定义的，并且$|E(\mathcal{G})|=|S_1(r)|/2$。进一步，我们有

$$\begin{aligned}
|S_k(r)|=&|\{(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_{k+1},\boldsymbol{y}_1,\boldsymbol{y}_2,\ldots,\boldsymbol{y}_{k+1})\in\mathcal{E}^{2k+2}:\\
&\|\boldsymbol{y}_i-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_i-\boldsymbol{x}_1\|\neq 0,i=2,3,\ldots,k+1\}|\\
=&|\{(\boldsymbol{x}_1,\boldsymbol{y}_1,\boldsymbol{x}_2,\boldsymbol{y}_2,\ldots,\boldsymbol{x}_{k+1},\boldsymbol{y}_{k+1})\in V(\mathcal{G})^{k+1}:\\
&(\boldsymbol{x}_1,\boldsymbol{y}_1)\text{与}(\boldsymbol{x}_i,\boldsymbol{y}_i)\text{相邻},i=2,3,\ldots,k+1\}|\\
=&\sum_{(\boldsymbol{x}_1,\boldsymbol{y}_1)\in V(\mathcal{G})}(\deg(\boldsymbol{x}_1,\boldsymbol{y}_1))^k。
\end{aligned}\tag{5.3}$$

回顾Hölder不等式$(\sum_{i=1}^n a_i^\alpha)^{1/\alpha}(\sum_{i=1}^n b_i^\beta)^{1/\beta}\geq\sum_{i=1}^n a_ib_i$。在Hölder不等式中，令$a_i=$

$(\deg(\boldsymbol{x},\boldsymbol{y}))^{k-1}$，$b_i=1$，$n=|V(\mathcal{G})|$，以及$\alpha=k/(k-1)$，我们得到

$$|S_k(r)|^{(k-1)/k}|V(\mathcal{G})|^{1/k}\geq|S_{k-1}(r)|,$$

即

$$|S_k(r)|\geq\frac{1}{|V(\mathcal{G})|^{1/(k-1)}}|S_{k-1}(r)|^{k/(k-1)}=\frac{1}{|\mathcal{E}|^{2/(k-1)}}|S_{k-1}(r)|^{k/(k-1)}。$$

在Hölder不等式中，令$a_i=\deg(\boldsymbol{x},\boldsymbol{y})$，$b_i=1$，$n=|V(\mathcal{G})|$，以及$\alpha=k-1$，我们得到

$$|S_{k-1}(r)|^{1/(k-1)}|V(\mathcal{G})|^{(k-2)/(k-1)}\geq|S_1(r)|,$$

即

$$|S_{k-1}(r)|^{1/(k-1)}\geq|\mathcal{E}|^{(4-2k)/(k-1)}|S_1(r)|。$$

所以不等式(5.2)化为

$$\begin{aligned}|B|\geq&|S_k(r)|-\binom{k}{2}(2|\mathcal{E}|-1)\,|S_{k-1}(r)|\\ \geq&|S_{k-1}(r)|\cdot\left(\frac{1}{|\mathcal{E}|^{2/(k-1)}}|S_{k-1}(r)|^{1/(k-1)}-2\binom{k}{2}|\mathcal{E}|+\binom{k}{2}\right)\\ \geq&|\mathcal{E}|^{-2}|S_{k-1}(r)|\cdot\left(|S_1(r)|-2\binom{k}{2}|\mathcal{E}|^3+\binom{k}{2}|\mathcal{E}|^2\right)。\end{aligned}\tag{5.4}$$

若$|S_1(r)|-2\binom{k}{2}|\mathcal{E}|^3\geq0$，即$|S_1(r)|\geq2\binom{k}{2}|\mathcal{E}|^3$，则$|S_{k-1}(r)|>0$（因为$|S_1(r)|>0$）且$|B|\geq\binom{k}{2}|S_{k-1}(r)|>0$。这意味着$\mathcal{E}$包含一对相似比为$r$的$k$星。

在完成定理5.5的证明之前，我们还需要以下定理。它可以由文献[31]的(2-7)，(2-9)，(3-2)，以及(3-3)得到。

定理5.7 ([31]). 设$\mathcal{E}\subseteq\mathbb{F}_q^d$，$|\mathcal{E}|\geq q^{d/2}$，$S_1(r)$如上定义。

- 若$d\geq2$为偶数且$r\in\mathbb{F}_q^*$，则

$$|S_1(r)|\geq q^{-1}|\mathcal{E}|^4-2|\mathcal{E}|^3-q^{d-1}|\mathcal{E}|^2-4q^{-2}|\mathcal{E}|^4-4q^{(d-2)/2}|\mathcal{E}|^3。$$

- 若$d\geq3$为奇数且$r\in\mathbb{F}_q^+$，则

$$|S_1(r)|\geq q^{-1}|\mathcal{E}|^4-2|\mathcal{E}|^3-2q^{d-1}|\mathcal{E}|^2-q^{-2}|\mathcal{E}|^4-2q^{(d-3)/2}|\mathcal{E}|^3。$$

现在我们可以完成定理5.5的证明。

定理5.5的证明. 根据不等式(5.4)，我们只需证明$|S_1(r)| - 2\binom{k}{2}|\mathcal{E}|^3 \geq 0$。

情况1： $q \geq 5$，$d \geq 2$为偶数，且$r \in \mathbb{F}_q^*$。

设$|\mathcal{E}| = tq^{d/2}$，其中$t \geq 31 + 10\binom{k}{2}$。由定理5.7，我们有

$$\begin{aligned}
&|S_1(r)| - 2\binom{k}{2}|\mathcal{E}|^3 \\
\geq& q^{2d-1}t^4 - 2t^3q^{3d/2} - q^{2d-1}t^2 - 4q^{2d-2}t^4 - 4q^{2d-1}t^3 - 2\binom{k}{2}t^3q^{3d/2} \\
\geq& t^2q^d\left(t^2q^{d-1} - 2tq^{d/2} - q^{d-1} - \frac{4}{5}q^{d-1}t^2 - 4q^{d-1}t - 2\binom{k}{2}tq^{d/2}\right) \\
=& \frac{1}{5}t^2q^{3d/2}\left(\left(t^2 - 20t - 5\right)q^{(d-2)/2} - 10t - 10\binom{k}{2}t\right) \\
\geq& \frac{1}{5}t^2q^{3d/2}\left(\left(t^2 - 21t\right)q^{(2-2)/2} - 10t - 10\binom{k}{2}t\right) \\
\geq& \frac{1}{5}t^2q^{3d/2}\left(t^2 - 31t - 10\binom{k}{2}t\right) \geq 0。
\end{aligned} \tag{5.5}$$

情况2： $d \geq 3$为奇数，且$r \in \mathbb{F}_q^+$。

设$|\mathcal{E}| = tq^{d/2}$，其中$t \geq 4 + \sqrt{3}\binom{k}{2}$。由定理5.7，我们有

$$\begin{aligned}
&|S_1(r)| - 2\binom{k}{2}|\mathcal{E}|^3 \\
\geq& q^{2d-1}t^4 - 2t^3q^{3d/2} - 2q^{2d-1}t^2 - q^{2d-2}t^4 - 2q^{(4d-3)/2}t^3 - 2\binom{k}{2}t^3q^{3d/2} \\
=& t^2q^{2d-1}\left(t^2 - 2tq^{(2-d)/2} - 2 - q^{-1}t^2 - 2q^{-1/2}t - 2\binom{k}{2}tq^{(2-d)/2}\right) \\
\geq& t^2q^{2d-1}\left(t^2 - 2t\cdot 3^{(2-3)/2} - 2 - 3^{-1}t^2 - 2\cdot 3^{-1/2}t - 2\binom{k}{2}t\cdot 3^{(2-3)/2}\right) \\
=& \frac{2}{3}t^2q^{2d-1}\left(t^2 - \sqrt{3}t - 3 - \sqrt{3}t - \sqrt{3}\binom{k}{2}t\right) \\
=& \frac{2}{3}t^2q^{2d-1}\left(\left(t - 2\sqrt{3} - \sqrt{3}\binom{k}{2}\right)t - 3\right) \\
\geq& \frac{2}{3}t^2q^{2d-1}\left(\left(4 - 2\sqrt{3}\right)\left(4 + \sqrt{3}\right) - 3\right) > 0。
\end{aligned} \tag{5.6}$$

□

§ 5.3 定理5.6的证明

在这一节，我们研究$\mathcal{E}$的最小基数，使得$\mathcal{E}$能包含一对相似比为r的4长路径，并

证明定理5.6。

令

$$\begin{aligned}P_k(r) =&\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{k+1}, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{k+1}) \in \mathcal{E}^{2k+2} : \\ &\|\boldsymbol{y}_{i+1} - \boldsymbol{y}_i\| = r\|\boldsymbol{x}_{i+1} - \boldsymbol{x}_i\| \neq 0, i = 1, 2, \ldots, k\}。\end{aligned}$$

我们考察$k = 4$的情况。记

$$A_1 = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{x}_1 = \boldsymbol{x}_3\},$$

$$A_1' = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{y}_1 = \boldsymbol{y}_3\},$$

$$A_2 = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{x}_1 = \boldsymbol{x}_4\},$$

$$A_2' = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{y}_1 = \boldsymbol{y}_4\},$$

$$A_3 = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{x}_1 = \boldsymbol{x}_5\},$$

$$A_3' = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{y}_1 = \boldsymbol{y}_5\},$$

$$A_4 = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{x}_3 = \boldsymbol{x}_5\},$$

$$A_4' = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{y}_3 = \boldsymbol{y}_5\},$$

$$A_5 = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{x}_2 = \boldsymbol{x}_5\},$$

$$A_5' = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{y}_2 = \boldsymbol{y}_5\},$$

$$A_6 = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{x}_2 = \boldsymbol{x}_4\},$$

$$A_6' = \{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{y}_2 = \boldsymbol{y}_4\},$$

以及

$$C =\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_5) \in P_4(r) : \boldsymbol{x}_i \neq \boldsymbol{x}_j, \boldsymbol{y}_i \neq \boldsymbol{y}_j, \forall 1 \leq i < j \leq 5\}。$$

容易看出

$$P_4(r) = \left(\bigcup_{i=1}^{6}(A_i \cup A_i')\right) \bigcup C$$

且

$$|C| = |P_4(r)| - \left|\bigcup_{i=1}^{6}(A_i \cup A_i')\right| \geq |P_4(r)| - \sum_{i=1}^{6}|A_i \cup A_i'|。$$

经过计算，我们有

$$\begin{aligned}
|A_1| =&|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in\mathcal{E}^{10}:\\
&\|\boldsymbol{y}_{i+1}-\boldsymbol{y}_i\|=r\|\boldsymbol{x}_{i+1}-\boldsymbol{x}_i\|\neq 0, i=1,2,3,4, \boldsymbol{x}_1=\boldsymbol{x}_3\}|\\
=&|\{(\boldsymbol{x}_2,\ldots,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in\mathcal{E}^{9}:\|\boldsymbol{y}_2-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_2-\boldsymbol{x}_3\|,\\
&\|\boldsymbol{y}_{i+1}-\boldsymbol{y}_i\|=r\|\boldsymbol{x}_{i+1}-\boldsymbol{x}_i\|\neq 0, i=2,3,4\}|\\
\leq&|\{\boldsymbol{y}_1:\boldsymbol{y}_1\in\mathcal{E}\}|\cdot|\{(\boldsymbol{x}_2,\ldots,\boldsymbol{x}_5,\boldsymbol{y}_2,\ldots,\boldsymbol{y}_5)\in\mathcal{E}^{8}:\\
&\|\boldsymbol{y}_{i+1}-\boldsymbol{y}_i\|=r\|\boldsymbol{x}_{i+1}-\boldsymbol{x}_i\|\neq 0, i=2,3,4\}|\\
=&|\mathcal{E}|\cdot|P_3(r)|。
\end{aligned}\tag{5.7}$$

类似地，对于$i=1,2,\ldots,5$，都有$|A_i|,|A_i'|\leq|\mathcal{E}|\cdot|P_3(r)|$。另一方面，我们有

$$\begin{aligned}
&|A_6\cup A_6'|\\
=&|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in P_4(r):\boldsymbol{x}_2=\boldsymbol{x}_4\text{或}\boldsymbol{y}_2=\boldsymbol{y}_4\}|\\
=&|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in P_4(r):\boldsymbol{x}_2=\boldsymbol{x}_4\text{且}\boldsymbol{y}_2\neq\boldsymbol{y}_4\}|\\
&+|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in P_4(r):\boldsymbol{x}_2\neq\boldsymbol{x}_4\text{且}\boldsymbol{y}_2=\boldsymbol{y}_4\}|\\
&+|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in P_4(r):\boldsymbol{x}_2=\boldsymbol{x}_4\text{且}\boldsymbol{y}_2=\boldsymbol{y}_4\}|\\
:=&I+II+III。
\end{aligned}\tag{5.8}$$

计算得到

$$\begin{aligned}
I =&|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in\mathcal{E}^{10}:\\
&\|\boldsymbol{y}_{i+1}-\boldsymbol{y}_i\|=r\|\boldsymbol{x}_{i+1}-\boldsymbol{x}_i\|\neq 0, i=1,2,3,4, \boldsymbol{x}_2=\boldsymbol{x}_4, \boldsymbol{y}_2\neq\boldsymbol{y}_4\}|\\
=&|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in\mathcal{E}^{10}:\boldsymbol{x}_2=\boldsymbol{x}_4,\boldsymbol{y}_2\neq\boldsymbol{y}_4,\\
&\|\boldsymbol{y}_{i+1}-\boldsymbol{y}_i\|=r\|\boldsymbol{x}_{i+1}-\boldsymbol{x}_i\|\neq 0, i=1,2,4, \|\boldsymbol{y}_4-\boldsymbol{y}_3\|=r\|\boldsymbol{x}_2-\boldsymbol{x}_3\|\}|\\
\leq&|\{(\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_4,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in\mathcal{E}^{9}:\boldsymbol{x}_2=\boldsymbol{x}_4,\boldsymbol{y}_2\neq\boldsymbol{y}_4,\\
&\|\boldsymbol{y}_2-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_2-\boldsymbol{x}_1\|\neq 0, \|\boldsymbol{y}_3-\boldsymbol{y}_2\|=\|\boldsymbol{y}_4-\boldsymbol{y}_3\|\neq 0,\\
&\|\boldsymbol{y}_5-\boldsymbol{y}_4\|=r\|\boldsymbol{x}_5-\boldsymbol{x}_4\|\neq 0\}|\cdot|\{\boldsymbol{x}_3:\boldsymbol{x}_3\in\mathcal{E}\}|\\
=&|\{(\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_4,\boldsymbol{x}_5,\boldsymbol{y}_1,\ldots,\boldsymbol{y}_5)\in\mathcal{E}^{9}:\boldsymbol{x}_2=\boldsymbol{x}_4,\boldsymbol{y}_2\neq\boldsymbol{y}_4,\\
&\|\boldsymbol{y}_2-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_2-\boldsymbol{x}_1\|\neq 0, \|\boldsymbol{y}_3-\boldsymbol{y}_2\|=\|\boldsymbol{y}_4-\boldsymbol{y}_3\|\neq 0,\\
&\|\boldsymbol{y}_5-\boldsymbol{y}_4\|=r\|\boldsymbol{x}_5-\boldsymbol{x}_4\|\neq 0\}|\cdot|\mathcal{E}|。
\end{aligned}\tag{5.9}$$

如果我们记$\boldsymbol{y}_2 = (u_1, u_2, \ldots, u_d)$，$\boldsymbol{y}_3 = (v_1, v_2, \ldots, v_d)$，$\boldsymbol{y}_4 = (w_1, w_2, \ldots, w_d)$，其中$(u_1, u_2, \ldots, u_d) \neq (w_1, w_2, \ldots, w_d)$，那么$\|\boldsymbol{y}_3 - \boldsymbol{y}_2\| = \|\boldsymbol{y}_4 - \boldsymbol{y}_3\|$化为

$$\begin{aligned}&(v_1 - u_1)^2 + (v_2 - u_2)^2 + \cdots + (v_d - u_d)^2\\ =&(v_1 - w_1)^2 + (v_2 - w_2)^2 + \cdots + (v_d - w_d)^2,\end{aligned}$$

即

$$2(w_1 - u_1)v_1 + 2(w_2 - u_2)v_2 + \cdots + 2(w_d - u_d)v_d = \sum_{i=1}^{d} w_i^2 - \sum_{i=1}^{d} u_i^2。 \tag{5.10}$$

只要$\boldsymbol{y}_2 \neq \boldsymbol{y}_4$，方程(5.10)关于$\boldsymbol{y}_3$的解总是至多有$q^{d-1}$个。另一方面，$\boldsymbol{y}_3 \in \mathcal{E}$。所以

$$\begin{aligned}&|\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_4, \boldsymbol{x}_5, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_5) \in \mathcal{E}^9 : \boldsymbol{x}_2 = \boldsymbol{x}_4, \boldsymbol{y}_2 \neq \boldsymbol{y}_4,\\ &\|\boldsymbol{y}_2 - \boldsymbol{y}_1\| = r\|\boldsymbol{x}_2 - \boldsymbol{x}_1\| \neq 0, \|\boldsymbol{y}_3 - \boldsymbol{y}_2\| = \|\boldsymbol{y}_4 - \boldsymbol{y}_3\| \neq 0,\\ &\|\boldsymbol{y}_5 - \boldsymbol{y}_4\| = r\|\boldsymbol{x}_5 - \boldsymbol{x}_4\| \neq 0\}|\\ \leq&|\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_4, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_4, \boldsymbol{y}_5) \in \mathcal{E}^8 : \boldsymbol{x}_2 = \boldsymbol{x}_4, \boldsymbol{y}_2 \neq \boldsymbol{y}_4,\\ &\|\boldsymbol{y}_2 - \boldsymbol{y}_1\| = r\|\boldsymbol{x}_2 - \boldsymbol{x}_1\| \neq 0, \|\boldsymbol{y}_5 - \boldsymbol{y}_4\| = r\|\boldsymbol{x}_5 - \boldsymbol{x}_4\| \neq 0\}|\\ &\cdot \min\left\{q^{d-1}, |\mathcal{E}|\right\}\\ =&|\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_4, \boldsymbol{y}_5) \in \mathcal{E}^7 : \boldsymbol{y}_2 \neq \boldsymbol{y}_4,\\ &\|\boldsymbol{y}_2 - \boldsymbol{y}_1\| = r\|\boldsymbol{x}_2 - \boldsymbol{x}_1\| \neq 0, \|\boldsymbol{y}_5 - \boldsymbol{y}_4\| = r\|\boldsymbol{x}_5 - \boldsymbol{x}_2\| \neq 0\}|\\ &\cdot \min\left\{q^{d-1}, |\mathcal{E}|\right\}\\ \leq&|\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_4, \boldsymbol{y}_5) \in \mathcal{E}^7 : \|\boldsymbol{y}_2 - \boldsymbol{y}_1\| = r\|\boldsymbol{x}_2 - \boldsymbol{x}_1\| \neq 0,\\ &\|\boldsymbol{y}_5 - \boldsymbol{y}_4\| = r\|\boldsymbol{x}_5 - \boldsymbol{x}_2\| \neq 0\}| \cdot \min\left\{q^{d-1}, |\mathcal{E}|\right\}。\end{aligned} \tag{5.11}$$

为了得到集合

$$\begin{aligned}&\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_5, \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_4, \boldsymbol{y}_5) \in \mathcal{E}^7 : \|\boldsymbol{y}_2 - \boldsymbol{y}_1\| = r\|\boldsymbol{x}_2 - \boldsymbol{x}_1\| \neq 0,\\ &\|\boldsymbol{y}_5 - \boldsymbol{y}_4\| = r\|\boldsymbol{x}_5 - \boldsymbol{x}_2\| \neq 0\}\end{aligned}$$

的基数的上界，我们首先选取$(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{y}_2) \in \mathcal{E}^4$，使得$\|\boldsymbol{y}_2 - \boldsymbol{y}_1\| = r\|\boldsymbol{x}_2 - \boldsymbol{x}_1\| \neq 0$，所以$(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{y}_2)$共有$|P_1(r)|$种选择。然后，我们从$\mathcal{E}$中选$\boldsymbol{x}_5$和$\boldsymbol{y}_4$，使得$\|\boldsymbol{x}_5 - \boldsymbol{x}_2\| \neq 0$，至多有$|\mathcal{E}|^2$种选择。最后，我们选$\boldsymbol{y}_5 \in \mathcal{E}$使得$\|\boldsymbol{y}_5 - \boldsymbol{y}_4\| = r\|\boldsymbol{x}_5 - \boldsymbol{x}_2\|$。如果我们用$S(\boldsymbol{x}, t)$来表示球心为$\boldsymbol{x}$、半径为$t$的球面，即$S(\boldsymbol{x}, t) := \{\boldsymbol{y} \in \mathbb{F}_q^d : \|\boldsymbol{y} - \boldsymbol{x}\| = t\}$，

那么$\boldsymbol{y}_5 \in S(\boldsymbol{y}_4, r\|\boldsymbol{x}_5 - \boldsymbol{x}_2\|)$。下面这个定理给出了$|S(\boldsymbol{x},t)|$的确切值，它可以从文献[49]的定理6.26和定理6.27得出。

定理5.8 ([49]). 设$S(\boldsymbol{x},t)$是$\mathbb{F}_q^d$中球心为$\boldsymbol{x}$、半径为t的球面。

- 若d是偶数，则

$$|S(\boldsymbol{x},t)| = q^{d-1} + \mu(t) q^{(d-2)/2} \psi\left((-1)^{d/2}\right),$$

  其中$\mu(t) = q-1$若$t=0$，$\mu(t) = -1$若$t \in \mathbb{F}_q^*$，以及ψ是$\mathbb{F}_q$的二次特征。

- 若$d \geq 3$为奇数，则

$$|S(\boldsymbol{x},t)| = q^{d-1} + q^{(d-1)/2} \eta\left((-1)^{(d-1)/2} t\right),$$

  其中η是$\mathbb{F}_q^*$的二次特征，且$\eta(0) = 0$。

若$d=2$，在定理5.8中令$\boldsymbol{x} = \boldsymbol{y}_4$，$t = r\|\boldsymbol{x}_5 - \boldsymbol{x}_2\| \neq 0$，我们知道$\boldsymbol{y}_5$至多有$q^{d-1} + q^{(d-2)/2}$种选择。此时$q^{d-1} + q^{(d-2)/2} = q^{d-1}\left(1 + q^{-d/2}\right) \leq q^{d-1}\left(1 + \frac{1}{3}\right) \leq 1.5q^{d-1}$。若$d \geq 3$，在定理5.8中令$\boldsymbol{x} = \boldsymbol{y}_4$，$t = r\|\boldsymbol{x}_5 - \boldsymbol{x}_2\| \neq 0$，我们知道$\boldsymbol{y}_5$至多有$q^{d-1} + q^{(d-1)/2}$种选择。此时$q^{d-1} + q^{(d-1)/2} = q^{d-1}\left(1 + q^{(1-d)/2}\right) \leq q^{d-1}\left(1 + \frac{1}{3}\right) \leq 1.5q^{d-1}$。所以$\boldsymbol{y}_5$的选择总是至多有$1.5q^{d-1}$种。另一方面，由于$\boldsymbol{y}_5 \in \mathcal{E}$，所以$\boldsymbol{y}_5$的选择至多有$|\mathcal{E}|$种。综上，我们有

$$\begin{aligned} I \leq & |\mathcal{E}| \cdot \min\left\{q^{d-1}, |\mathcal{E}|\right\} \cdot |P_1(r)| \cdot |\mathcal{E}|^2 \cdot \min\left\{1.5q^{d-1}, |\mathcal{E}|\right\} \\ = & |\mathcal{E}|^3 \cdot |P_1(r)| \cdot \min\left\{q^{d-1}, |\mathcal{E}|\right\} \cdot \min\left\{1.5q^{d-1}, |\mathcal{E}|\right\}。 \end{aligned} \tag{5.12}$$

当$2 \leq d \leq 4$时，$\min\left\{q^{d-1}, |\mathcal{E}|\right\} \cdot \min\left\{1.5q^{d-1}, |\mathcal{E}|\right\} \leq q^{d-1} \cdot 1.5q^{d-1} = 1.5q^{2d-2}$。当$d \geq 5$时，$\min\left\{q^{d-1}, |\mathcal{E}|\right\} \cdot \min\left\{1.5q^{d-1}, |\mathcal{E}|\right\} \leq |\mathcal{E}| \cdot |\mathcal{E}| = |\mathcal{E}|^2$。所以

$$I \leq \begin{cases} 1.5|\mathcal{E}|^3 \cdot q^{2d-2} \cdot |P_1(r)|, & 若2 \leq d \leq 4; \\ |\mathcal{E}|^5 \cdot |P_1(r)|, & 若d \geq 5。 \end{cases} \tag{5.13}$$

类似地，

$$II \leq \begin{cases} 1.5|\mathcal{E}|^3 \cdot q^{2d-2} \cdot |P_1(r)|, & 若2 \leq d \leq 4; \\ |\mathcal{E}|^5 \cdot |P_1(r)|, & 若d \geq 5。 \end{cases} \tag{5.14}$$

最后，我们计算

$$\begin{aligned} III =&|\{(\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3,\boldsymbol{x}_5,\boldsymbol{y}_1,\boldsymbol{y}_2,\boldsymbol{y}_3,\boldsymbol{y}_5)\in\mathcal{E}^8:\|\boldsymbol{y}_2-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_2-\boldsymbol{x}_1\|\neq 0,\\ &\|\boldsymbol{y}_3-\boldsymbol{y}_2\|=r\|\boldsymbol{x}_3-\boldsymbol{x}_2\|\neq 0,\|\boldsymbol{y}_5-\boldsymbol{y}_2\|=r\|\boldsymbol{x}_5-\boldsymbol{x}_2\|\neq 0\}|\\ \leq&|\{(\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_5,\boldsymbol{y}_1,\boldsymbol{y}_2,\boldsymbol{y}_5)\in\mathcal{E}^6:\|\boldsymbol{y}_2-\boldsymbol{y}_1\|=r\|\boldsymbol{x}_2-\boldsymbol{x}_1\|\neq 0,\\ &\|\boldsymbol{y}_5-\boldsymbol{y}_2\|=r\|\boldsymbol{x}_5-\boldsymbol{x}_2\|\neq 0\}|\cdot|\{\boldsymbol{x}_3:\boldsymbol{x}_3\in\mathcal{E}\}|\cdot|\{\boldsymbol{y}_3:\boldsymbol{y}_3\in\mathcal{E}\}|\\ =&|\mathcal{E}|^2\cdot|P_2(r)|。 \end{aligned} \tag{5.15}$$

将等式(5.8)，不等式(5.13)-(5.15)结合起来，我们得到

$$|A_6\cup A_6'|\leq\begin{cases} 3|\mathcal{E}|^3\cdot q^{2d-2}\cdot|P_1(r)|+|\mathcal{E}|^2\cdot|P_2(r)|, & 若2\leq d\leq 4;\\ 2|\mathcal{E}|^5\cdot|P_1(r)|+|\mathcal{E}|^2\cdot|P_2(r)|, & 若d\geq 5。 \end{cases} \tag{5.16}$$

所以

$$\begin{aligned} &|C|\\ \geq&|P_4(r)|-\sum_{i=1}^{6}|A_i\cup A_i'|\\ \geq&|P_4(r)|-\sum_{i=1}^{5}(|A_i|+|A_i'|)-|A_6\cup A_6'|\\ \geq&\begin{cases} |P_4(r)|-10|\mathcal{E}|\cdot|P_3(r)|-3|\mathcal{E}|^3\cdot q^{2d-2}\cdot|P_1(r)|-|\mathcal{E}|^2\cdot|P_2(r)|, & 若2\leq d\leq 4;\\ |P_4(r)|-10|\mathcal{E}|\cdot|P_3(r)|-2|\mathcal{E}|^5\cdot|P_1(r)|-|\mathcal{E}|^2\cdot|P_2(r)|, & 若d\geq 5。 \end{cases} \end{aligned} \tag{5.17}$$

我们构造一个辅助图$\mathcal{G}$，其中$V(\mathcal{G})=\mathcal{E}\times\mathcal{E}=\{(\boldsymbol{x},\boldsymbol{y}):\boldsymbol{x},\boldsymbol{y}\in\mathcal{E}\}$。两个点$(\boldsymbol{x},\boldsymbol{y})$和$(\boldsymbol{x}',\boldsymbol{y}')$之间有一条边相连当且仅当$\|\boldsymbol{y}'-\boldsymbol{y}\|=r\|\boldsymbol{x}'-\boldsymbol{x}\|\neq 0$。我们有

$$\begin{aligned} |P_k(r)|=&|\{(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{k+1},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{k+1})\in\mathcal{E}^{2k+2}:\\ &\|\boldsymbol{y}_{i+1}-\boldsymbol{y}_i\|=r\|\boldsymbol{x}_{i+1}-\boldsymbol{x}_i\|\neq 0,1\leq i\leq k\}|\\ =&|\{(\boldsymbol{x}_1,\boldsymbol{y}_1,\boldsymbol{x}_2,\boldsymbol{y}_2,\ldots,\boldsymbol{x}_{k+1},\boldsymbol{y}_{k+1})\in V(\mathcal{G})^{k+1}:\\ &(\boldsymbol{x}_i,\boldsymbol{y}_i)与(\boldsymbol{x}_{i+1},\boldsymbol{y}_{i+1})相邻,1\leq i\leq k\}|\\ :=&w_k(\mathcal{G}), \end{aligned} \tag{5.18}$$

其中我们用$w_k(\mathcal{G})$表示$\mathcal{G}$中长为k的通路（walk）。以下两个定理给出了不同的$w_k(\mathcal{G})$之间的关系，它们分别由文献[3]和文献[44]得出。

定理5.9 ([3]). 对于图G和正整数k，我们有

$$w_1(G)^k \leq w_0(G)^{k-1} \cdot w_k(G)。 \tag{5.19}$$

定理5.10 ([44]). 对于图G和非负整数a和b，我们有

$$w_{2a+b}(G) \cdot w_b(G) \leq w_0(G) \cdot w_{2(a+b)}(G)。 \tag{5.20}$$

在不等式(5.19)中取$k=4$，我们得到$|P_1(r)|^4 \leq |P_0(r)|^3 \cdot |P_4(r)|$。在不等式(5.19)中取$k=2$，我们得到$|P_1(r)|^2 \leq |P_0(r)| \cdot |P_2(r)|$。在不等式(5.20)中取$a=b=1$，我们得到$|P_3(r)| \cdot |P_1(r)| \leq |P_0(r)| \cdot |P_4(r)|$。在不等式(5.20)中取$a=0$和$b=2$，我们得到$|P_2(r)|^2 \leq |P_0(r)| \cdot |P_4(r)|$。注意到$|P_0(r)|$恰好是$\mathcal{G}$的顶点数。所以

$$|P_4(r)| \geq |\mathcal{E}|^{-6}|P_1(r)|^4, \tag{5.21}$$

$$|P_2(r)| \geq |\mathcal{E}|^{-2}|P_1(r)|^2, \tag{5.22}$$

$$|P_4(r)| \geq |\mathcal{E}|^{-2}|P_3(r)| \cdot |P_1(r)|, \tag{5.23}$$

以及

$$|P_4(r)| \geq |\mathcal{E}|^{-2}|P_2(r)|^2。 \tag{5.24}$$

5.3.1 $2 \leq d \leq 4$的情况

当$2 \leq d \leq 4$时，不等式(5.17)化为

$$\begin{aligned}
|C| \geq & |P_4(r)| - 10|\mathcal{E}| \cdot |P_3(r)| - 3|\mathcal{E}|^3 \cdot q^{2d-2} \cdot |P_1(r)| - |\mathcal{E}|^2 \cdot |P_2(r)| \\
\geq & (0.96536|P_4(r)| - 10|\mathcal{E}| \cdot |P_3(r)|) + \left(0.02357|P_4(r)| - 3|\mathcal{E}|^3 \cdot q^{2d-2} \cdot |P_1(r)|\right) \\
& + \left(0.01105|P_4(r)| - |\mathcal{E}|^2 \cdot |P_2(r)|\right) \\
:= & I' + II' + III'。
\end{aligned} \tag{5.25}$$

根据不等式(5.23)，我们有

$$\begin{aligned}
I' = & 0.96536|P_4(r)| - 10|\mathcal{E}| \cdot |P_3(r)| \\
\geq & |\mathcal{E}|^{-2}|P_3(r)| \left(0.96536|P_1(r)| - 10|\mathcal{E}|^3\right)。
\end{aligned} \tag{5.26}$$

根据不等式(5.21)，我们有

$$\begin{aligned} II' =&0.02357|P_4(r)| - 3|\mathcal{E}|^3 \cdot q^{2d-2} \cdot |P_1(r)| \\ \geq&|\mathcal{E}|^{-6}|P_1(r)| \left(0.02357|P_1(r)|^3 - 3q^{2d-2}|\mathcal{E}|^9\right)。 \end{aligned} \tag{5.27}$$

根据不等式(5.24)和(5.22)，我们有

$$\begin{aligned} III' =&0.01105|P_4(r)| - |\mathcal{E}|^2 \cdot |P_2(r)| \\ \geq&|\mathcal{E}|^{-2}|P_2(r)| \left(0.01105|P_2(r)| - |\mathcal{E}|^4\right) \\ \geq&|\mathcal{E}|^{-4}|P_2(r)| \left(0.01105|P_1(r)|^2 - |\mathcal{E}|^6\right)。 \end{aligned} \tag{5.28}$$

假设$|P_1(r)| > 5.03023q^{(2d-2)/3}|\mathcal{E}|^3$。则$0.02357|P_1(r)|^3 - 3q^{2d-2}|\mathcal{E}|^9 > 0$，所以在不等式(5.27)中，$II' > 0$。另外，

$$\begin{aligned} &0.96536|P_1(r)| - 10|\mathcal{E}|^3 \\ >&0.96536 \cdot 5.03023q^{(2d-2)/3}|\mathcal{E}|^3 - 10|\mathcal{E}|^3 \\ \geq&0.96536 \cdot 5.03023 \cdot 3^{(2\cdot 2-2)/3}|\mathcal{E}|^3 - 10|\mathcal{E}|^3 \\ >&0.1|\mathcal{E}|^3 > 0。 \end{aligned} \tag{5.29}$$

所以在不等式(5.26)中，$I' > 0$。

$$\begin{aligned} &\sqrt{0.01105}|P_1(r)| - |\mathcal{E}|^3 \\ >&\sqrt{0.01105} \cdot 5.03023q^{(2d-2)/3}|\mathcal{E}|^3 - |\mathcal{E}|^3 \\ \geq&\sqrt{0.01105} \cdot 5.03023 \cdot 3^{(2\cdot 2-2)/3}|\mathcal{E}|^3 - |\mathcal{E}|^3 \\ >&0.09|\mathcal{E}|^3 > 0。 \end{aligned} \tag{5.30}$$

所以在不等式(5.28)中，$III' > 0$。

5.3.2 $d = 5$的情况

当$d = 5$时，不等式(5.17)化为

$$\begin{aligned} |C| \geq&|P_4(r)| - 10|\mathcal{E}| \cdot |P_3(r)| - 2|\mathcal{E}|^5 \cdot |P_1(r)| - |\mathcal{E}|^2 \cdot |P_2(r)| \\ \geq&\left(0.16|P_4(r)| - 10|\mathcal{E}| \cdot |P_3(r)|\right) + \left(0.82|P_4(r)| - 2|\mathcal{E}|^5 \cdot |P_1(r)|\right) \\ &+ \left(0.01|P_4(r)| - |\mathcal{E}|^2 \cdot |P_2(r)|\right) \\ :=&I'' + II'' + III''。 \end{aligned} \tag{5.31}$$

与子节5.3.1类似，我们有

$$\begin{aligned} I'' =&0.16|P_4(r)| - 10|\mathcal{E}| \cdot |P_3(r)| \\ \geq&|\mathcal{E}|^{-2}|P_3(r)| \left(0.16|P_1(r)| - 10|\mathcal{E}|^3\right), \end{aligned} \tag{5.32}$$

$$\begin{aligned} II'' =&0.82|P_4(r)| - 2|\mathcal{E}|^5 \cdot |P_1(r)| \\ \geq&|\mathcal{E}|^{-6}|P_1(r)| \left(0.82|P_1(r)|^3 - 2|\mathcal{E}|^{11}\right), \end{aligned} \tag{5.33}$$

以及

$$\begin{aligned} III'' =&0.01|P_4(r)| - |\mathcal{E}|^2 \cdot |P_2(r)| \\ \geq&|\mathcal{E}|^{-2}|P_2(r)| \left(0.01|P_2(r)| - |\mathcal{E}|^4\right) \\ \geq&|\mathcal{E}|^{-4}|P_2(r)| \left(0.01|P_1(r)|^2 - |\mathcal{E}|^6\right)。 \end{aligned} \tag{5.34}$$

假设$|P_1(r)| > 1.34609|\mathcal{E}|^{11/3}$，且$|\mathcal{E}| \geq 12q^3$。那么$0.82|P_1(r)|^3 - 2|\mathcal{E}|^{11} > 0$，此时在不等式(5.33)中，$II'' > 0$。另外，$|P_1(r)| \geq 1.34609 \cdot (12q^3)^{2/3} |\mathcal{E}|^3 \geq 63.49|\mathcal{E}|^3$。所以

$$\begin{aligned} &0.16|P_1(r)| - 10|\mathcal{E}|^3 \\ >&0.16 \cdot 63.49|\mathcal{E}|^3 - 10|\mathcal{E}|^3 \\ >&0.15|\mathcal{E}|^3 > 0, \end{aligned} \tag{5.35}$$

从而在不等式(5.32)中，$I'' > 0$。

$$\begin{aligned} &\sqrt{0.01}|P_1(r)| - |\mathcal{E}|^3 \\ >&\sqrt{0.01} \cdot 63.49|\mathcal{E}|^3 - |\mathcal{E}|^3 \\ >&5|\mathcal{E}|^3 > 0, \end{aligned} \tag{5.36}$$

从而在不等式(5.34)中，$III'' > 0$。

5.3.3 $d \geq 6$的情况

当$d \geq 6$时，不等式(5.17)化为

$$\begin{aligned} |C| \geq&|P_4(r)| - 10|\mathcal{E}| \cdot |P_3(r)| - 2|\mathcal{E}|^5 \cdot |P_1(r)| - |\mathcal{E}|^2 \cdot |P_2(r)| \\ \geq&\left(0.0191|P_4(r)| - 10|\mathcal{E}| \cdot |P_3(r)|\right) + \left(0.98|P_4(r)| - 2|\mathcal{E}|^5 \cdot |P_1(r)|\right) \\ &+ \left(0.0009|P_4(r)| - |\mathcal{E}|^2 \cdot |P_2(r)|\right) \\ :=&I''' + II''' + III'''。 \end{aligned} \tag{5.37}$$

与子节5.3.1类似，我们有

$$\begin{aligned} I''' =&0.0191|P_4(r)| - 10|\mathcal{E}| \cdot |P_3(r)| \\ \geq&|\mathcal{E}|^{-2}|P_3(r)| \left(0.0191|P_1(r)| - 10|\mathcal{E}|^3\right), \end{aligned} \tag{5.38}$$

$$\begin{aligned} II''' =&0.98|P_4(r)| - 2|\mathcal{E}|^5 \cdot |P_1(r)| \\ \geq&|\mathcal{E}|^{-6}|P_1(r)| \left(0.98|P_1(r)|^3 - 2|\mathcal{E}|^{11}\right), \end{aligned} \tag{5.39}$$

以及

$$\begin{aligned} III''' =&0.0009|P_4(r)| - |\mathcal{E}|^2 \cdot |P_2(r)| \\ \geq&|\mathcal{E}|^{-2}|P_2(r)| \left(0.0009|P_2(r)| - |\mathcal{E}|^4\right) \\ \geq&|\mathcal{E}|^{-4}|P_2(r)| \left(0.0009|P_1(r)|^2 - |\mathcal{E}|^6\right)。 \end{aligned} \tag{5.40}$$

假设$|P_1(r)| > 1.26844|\mathcal{E}|^{11/3}$且$|\mathcal{E}| \geq 313q^{d/2}$。那么$0.98|P_1(r)|^3 - 2|\mathcal{E}|^{11} > 0$，此时在不等式(5.39)中，$II''' > 0$。另外，$|P_1(r)| \geq 1.26844 \cdot (313q^3)^{2/3} |\mathcal{E}|^3 \geq 526.27|\mathcal{E}|^3$。所以

$$\begin{aligned} &0.0191|P_1(r)| - 10|\mathcal{E}|^3 \\ >&0.0191 \cdot 526.27|\mathcal{E}|^3 - 10|\mathcal{E}|^3 \\ >&0.05|\mathcal{E}|^3 > 0, \end{aligned} \tag{5.41}$$

从而在不等式(5.38)中，$I''' > 0$。

$$\begin{aligned} &\sqrt{0.0009}|P_1(r)| - |\mathcal{E}|^3 \\ >&\sqrt{0.0009} \cdot 526.27|\mathcal{E}|^3 - |\mathcal{E}|^3 \\ >&10|\mathcal{E}|^3 > 0, \end{aligned} \tag{5.42}$$

从而在不等式(5.40)中，$III''' > 0$。

5.3.4 完成定理5.6的证明

现在我们可以完成定理5.6的证明。

定理5.6的证明. **情况1**：$q \geq 5$，d为2或4，且$r \in \mathbb{F}_q^*$。

正如子节5.3.1中所说，我们只需证明$|P_1(r)| > 5.03023q^{(2d-2)/3}|\mathcal{E}|^3$。这样的话，$|C| \geq I' + II' + III' > 0$，所以$\mathcal{E}$包含一对相似比为$r$的4长路径。

设$|\mathcal{E}| = tq^{(2d+1)/3}$，其中$t \geq 36$。注意到$P_1(r) = S_1(r)$。所以我们可以用定理5.7，计算得

$$
\begin{aligned}
&|P_1(r)| - 5.03023q^{(2d-2)/3}|\mathcal{E}|^3 \\
\geq& q^{-1}|\mathcal{E}|^4 - 2|\mathcal{E}|^3 - q^{d-1}|\mathcal{E}|^2 - 4q^{-2}|\mathcal{E}|^4 - 4q^{(d-2)/2}|\mathcal{E}|^3 - 5.03023q^{(2d-2)/3}|\mathcal{E}|^3 \\
\geq& t^4q^{(8d+1)/3} - 2t^3q^{2d+1} - t^2q^{(7d-1)/3} - 4t^4q^{(8d-2)/3} - 4t^3q^{5d/2} - 5.03023t^3q^{(8d+1)/3} \\
=& t^2q^{(8d+1)/3} \cdot \left(t^2 - 2tq^{(-2d+2)/3} - q^{(-d-2)/3} - 4t^2q^{-1} - 4tq^{(-d-2)/6} - 5.03023t\right) \\
\geq& t^2q^{(8d+1)/3} \cdot \left(t^2 - 2t \cdot 5^{(-2\cdot 2+2)/3} - 5^{(-2-2)/3} - 4t^2 \cdot 5^{-1} - 4t \cdot 5^{(-2-2)/6} - 5.03023t\right) \\
\geq& t^2q^{(8d+1)/3}\left(0.2t^2 - 7.1t - 0.2\right) \\
\geq& t^2q^{(8d+1)/3}\left((0.2 \cdot 36 - 7.1) \cdot 36 - 0.2\right) > 0。
\end{aligned}
\tag{5.43}
$$

情况2： $d = 3$，且$r \in \mathbb{F}_q^+$。

正如子节5.3.1中所说，我们只需证明$|P_1(r)| > 5.03023q^{(2d-2)/3}|\mathcal{E}|^3$。

设$|\mathcal{E}| = tq^{(2d+1)/3}$，其中$t \geq 9$。根据定理5.7，我们有

$$
\begin{aligned}
&|P_1(r)| - 5.03023q^{(2d-2)/3}|\mathcal{E}|^3 \\
\geq& q^{-1}|\mathcal{E}|^4 - 2|\mathcal{E}|^3 - 2q^{d-1}|\mathcal{E}|^2 - q^{-2}|\mathcal{E}|^4 - 2q^{(d-3)/2}|\mathcal{E}|^3 - 5.03023q^{(2d-2)/3}|\mathcal{E}|^3 \\
\geq& t^4q^{(8d+1)/3} - 2t^3q^{2d+1} - 2t^2q^{(7d-1)/3} - t^4q^{(8d-2)/3} - 2t^3q^{(5d-1)/2} - 5.03023t^3q^{(8d+1)/3} \\
=& t^2q^{(8d+1)/3} \cdot \left(t^2 - 2tq^{(-2d+2)/3} - 2q^{(-d-2)/3} - t^2q^{-1} - 2tq^{(-d-5)/6} - 5.03023t\right) \\
\geq& t^2q^{(8d+1)/3} \cdot \left(t^2 - 2t \cdot 3^{(-2\cdot 3+2)/3} - 2 \cdot 3^{(-3-2)/3} - \frac{1}{3}t^2 - 2t \cdot 3^{(-3-5)/6} - 5.03023t\right) \\
\geq& t^2q^{(8d+1)/3}\left(\frac{2}{3}t^2 - 5.95479t - 0.3205\right) \\
\geq& t^2q^{(8d+1)/3}\left(\frac{2}{3} \cdot 81 - 5.95479 \cdot 9 - 0.3205\right) > 0。
\end{aligned}
\tag{5.44}
$$

情况3： $d = 5$，且$r \in \mathbb{F}_q^+$。

正如子节5.3.2中所说，只需证明$|\mathcal{E}| \geq 12q^3$可以推出$|P_1(r)| > 1.34609|\mathcal{E}|^{11/3}$。

设$|\mathcal{E}|=tq^3$，其中$t\geq 12$。根据定理5.7，我们有

$$\begin{aligned}
&|P_1(r)|-1.34609|\mathcal{E}|^{11/3}\\
\geq&q^{-1}|\mathcal{E}|^4-2|\mathcal{E}|^3-2q^{d-1}|\mathcal{E}|^2-q^{-2}|\mathcal{E}|^4-2q^{(d-3)/2}|\mathcal{E}|^3-1.34609|\mathcal{E}|^{11/3}\\
\geq&t^4q^{11}-2t^3q^9-2t^2q^{10}-t^4q^{10}-2t^3q^{10}-1.34609t^{11/3}q^{11}\\
=&t^2q^{11}\left(t^2-2tq^{-2}-2q^{-1}-t^2q^{-1}-2tq^{-1}-1.34609t^{5/3}\right)\\
\geq&t^2q^{11}\left(t^2-\frac{2}{9}t-\frac{2}{3}-\frac{t^2}{3}-\frac{2}{3}t-1.34609t^{5/3}\right)\\
=&t^2q^{11}\left(\frac{2}{3}t^2-\frac{8}{9}t-\frac{2}{3}-1.34609t^{5/3}\right)\\
\geq&t^2q^{11}\left(\frac{2}{3}t^2-\frac{17}{18}t-1.34609t^{5/3}\right)\\
\geq&t^3q^{11}\left(\frac{2}{3}t-\frac{17}{18}-1.34609t^{2/3}\right)\\
=&t^3q^{11}\left(t^{2/3}\left(\frac{2}{3}t^{1/3}-1.34609\right)-\frac{17}{18}\right)\\
\geq&t^3q^{11}\left(12^{2/3}\left(\frac{2}{3}\cdot 12^{1/3}-1.34609\right)-\frac{17}{18}\right)>0。
\end{aligned}\tag{5.45}$$

情况4： $q\geq 5$，d是大于等于6的偶数，且$r\in\mathbb{F}_q^*$。

正如子节5.3.3中所说，只需证明$|\mathcal{E}|\geq 313q^{d/2}$可以推出$|P_1(r)|>1.26844|\mathcal{E}|^{11/3}$。

设$|\mathcal{E}|=tq^{d/2}$，其中$t\geq 313$。根据定理5.7，我们有

$$\begin{aligned}
&|P_1(r)|-1.26844|\mathcal{E}|^{11/3}\\
\geq&q^{-1}|\mathcal{E}|^4-2|\mathcal{E}|^3-q^{d-1}|\mathcal{E}|^2-4q^{-2}|\mathcal{E}|^4-4q^{(d-2)/2}|\mathcal{E}|^3-1.26844|\mathcal{E}|^{11/3}\\
\geq&t^4q^{2d-1}-2t^3q^{3d/2}-t^2q^{2d-1}-4t^4q^{2d-2}-4t^3q^{2d-1}-1.26844t^{11/3}q^{11d/6}\\
=&t^2q^{2d-1}\left(t^2-2tq^{(2-d)/2}-1-4t^2q^{-1}-4t-1.26844t^{5/3}q^{(6-d)/6}\right)\\
\geq&t^2q^{2d-1}\left(t^2-2t\cdot 5^{(2-6)/2}-1-4t^2\cdot 5^{-1}-4t-1.26844t^{5/3}\cdot 5^{(6-6)/6}\right)\\
=&t^2q^{2d-1}\left(\frac{1}{5}t^2-\frac{102}{25}t-1-1.26844t^{5/3}\right)\\
\geq&t^2q^{2d-1}\left(\frac{1}{5}t^2-\frac{49}{12}t-1.26844t^{5/3}\right)\\
=&t^3q^{2d-1}\left(t^{2/3}\left(\frac{1}{5}t^{1/3}-1.26844\right)-\frac{49}{12}\right)\\
\geq&t^3q^{2d-1}\left(313^{2/3}\left(\frac{1}{5}\cdot 313^{1/3}-1.26844\right)-\frac{49}{12}\right)>0。
\end{aligned}\tag{5.46}$$

情况5：d是大于等于7的奇数，且$r \in \mathbb{F}_q^+$。

正如子节5.3.3中所说，只需证明$|\mathcal{E}| \geq 313q^{d/2}$可以推出$|P_1(r)| > 1.26844|\mathcal{E}|^{11/3}$。

设$|\mathcal{E}| = tq^{d/2}$，其中$t \geq 313$。根据定理5.7，我们有

$$
\begin{aligned}
&|P_1(r)| - 1.26844|\mathcal{E}|^{11/3} \\
\geq& q^{-1}|\mathcal{E}|^4 - 2|\mathcal{E}|^3 - 2q^{d-1}|\mathcal{E}|^2 - q^{-2}|\mathcal{E}|^4 - 2q^{(d-3)/2}|\mathcal{E}|^3 - 1.26844|\mathcal{E}|^{11/3} \\
\geq& t^4q^{2d-1} - 2t^3q^{3d/2} - 2t^2q^{2d-1} - t^4q^{2d-2} - 2t^3q^{(4d-3)/2} - 1.26844t^{11/3}q^{11d/6} \\
=& t^2q^{2d-1}\left(t^2 - 2tq^{(2-d)/2} - 2 - t^2q^{-1} - 2tq^{-1/2} - 1.26844t^{5/3}q^{(6-d)/6}\right) \\
\geq& t^2q^{2d-1}\left(t^2 - 2t\cdot 3^{(2-7)/2} - 2 - \frac{1}{3}t^2 - \frac{1}{\sqrt{3}}2t - 1.26844t^{5/3}\cdot 3^{(6-7)/6}\right) \qquad (5.47) \\
\geq& t^2q^{2d-1}\left(\frac{2}{3}t^2 - 1.2894t - 1.05621t^{5/3}\right) \\
=& t^3q^{2d-1}\left(t^{2/3}\left(\frac{2}{3}t^{1/3} - 1.05621\right) - 1.2894\right) \\
\geq& t^3q^{2d-1}\left(313^{2/3}\left(\frac{2}{3}\cdot 313^{1/3} - 1.05621\right) - 1.2894\right) > 0。
\end{aligned}
$$

□

§ 5.4 进一步的讨论

在文献[23]中，Greenleaf等人考察了$\mathbb{R}^d$中的相似图形的问题，并证明如果一个紧集$\mathcal{E}$的Hausdorff维数大于某个临界值$s_{k,d}$，那么就会存在许多对$(k+1)$个点的相似图形，其中相似比为r。Rakhmonov在文献[59]中也考虑了$\mathbb{F}_p^d$中的相似$(d+1)$单形。

根据定义，2星恰好是2长路径。所以关于相似的3长路径的问题仍有待解决。其中的一个难点是，我们无法找到一个合适的不等式来描述$w_3(G)$和$w_2(G)$的关系。

第 6 章 其他在研问题

本章将简要介绍本人在攻读博士学位期间的其他研究课题。其中部分课题仍处于研究阶段，尚未形成完整的研究成果。限于篇幅，我们对这些课题和目前的进展做简要介绍。

§ 6.1 Grassmannian覆盖码

本世纪以来，网络编码受到了大量的关注。在文献[43]中，Kötter和Kschischang建立了一种新的纠错码模型，称为常维码（constant-dimension code），其中的码字是有限域上的线性空间的k维子空间。对于子空间U和V，定义它们之间的距离为$d_s(U,V)=\dim(U+V)-\dim(U\cap V)=\dim(U)+\dim(V)-2\dim(U\cap V)$。

Etzion和Zhang[20]研究了线性空间子空间的堆积（packing）与覆盖（covering），并引入Grassmannian覆盖码（covering Grassmannian code）的概念。一个参数为α-$(n,k,\delta)_q^c$的Grassmannian覆盖码$\mathcal{C}$（简称α-$(n,k,\delta)_q^c$码）是$\mathbb{F}_q^n$的一些k维子空间构成的集合，其中任意α个码字都能张成一个维数至少为$k+\delta$的子空间。在$\alpha=2$的情况下，Grassmannian覆盖码就是常维码。我们用$B_q(n,k,\delta;\alpha)$表示α-$(n,k,\delta)_q^c$码的最大基数。一个参数为t-$(n,k,\lambda)_q$的子空间堆积$\mathcal{C}$是$\mathbb{F}_q^n$的一些k维子空间构成的集合，使得$\mathbb{F}_q^n$的任意t维子空间至多只包含在$\mathcal{C}$的λ个成员中。当$\lambda=1$时，子空间堆积就是常维码。我们用$A_q(n,k,t;\lambda)$表示参数为t-$(n,k,\lambda)_q$的子空间堆积的最大基数。文献[20]证明了子空间堆积和Grassmannian覆盖码的等价性：

$$B_q(n,k,\delta;\alpha)=A_q(n,n-k,n-k-\delta+1;\alpha-1)。$$

所以该问题转化为研究某些参数限制下$B_q(n,k,\delta;\alpha)$的上下界。

运用多种不同的工具，我们给出了在特殊参数下$B_q(n,k,\delta;\alpha)$的上下界。

- 我们建立起了超图与Grassmannian覆盖码之间的联系，并通过超图的方法给出了$B_q(n,k,\delta;\alpha)$的上界。

定理6.1. 设n，k，δ，以及α都是正整数，满足$\alpha \geq 2$以及$\delta \leq (\alpha-1)k$，则

$$B_q(n,k,\delta;\alpha) \leq (\alpha-1)\frac{\begin{bmatrix} n \\ h \end{bmatrix}_q}{\begin{bmatrix} k \\ h \end{bmatrix}_q},$$

其中$h = \lfloor k+1-\frac{\delta}{\alpha-1} \rfloor$。

定理6.2. $B_q(n,3,3;3) \leq \left(1+\frac{1}{2\begin{bmatrix} 3 \\ 2 \end{bmatrix}_q - 1}\right)\frac{\begin{bmatrix} n \\ 2 \end{bmatrix}_q}{\begin{bmatrix} 3 \\ 2 \end{bmatrix}_q}$。

定理6.3. $B_q(n,k,\delta;3) \leq \left(1+\frac{1}{2\begin{bmatrix} k \\ h \end{bmatrix}_q - 1}\right)\frac{\begin{bmatrix} n \\ h \end{bmatrix}_q}{\begin{bmatrix} k \\ h \end{bmatrix}_q}$，其中$h = \lfloor k+1-\frac{\delta}{2} \rfloor$。

定理6.4. 设n，k，δ，以及α都是正整数，满足$\alpha \geq 3$以及$\delta \geq (\alpha-1)(k-1)$，则

$$B_q(n,k,\delta;\alpha) = O\left(q^{\left(1+\frac{1}{\lfloor \alpha/2 \rfloor}\right)n}\right)。$$

定理6.5. 设n，k，δ，以及α都是正整数，满足$3 \leq \alpha \leq \begin{bmatrix} k \\ 1 \end{bmatrix}_q$以及$\delta \geq (\alpha-1)(k-1)+1$，则

$$B_q(n,k,\delta;\alpha) \leq (\alpha-1)\frac{\begin{bmatrix} n \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q + 1}。$$

定理6.6. $B_q(n,2,2;3) = o(q^{2n})$。

定理6.7. 设n，k，δ，以及α都是正整数，满足$\alpha \geq 3$以及$\delta > \alpha-2$，则

$$B_q(n,k,\delta;\alpha) = O\left(q^{\left(1+\frac{1}{\lfloor \alpha/2 \rfloor}\right)(k-1)n}\right)。$$

- 通过具体的构造，我们给出了$B_q(n,k,\delta;\alpha)$的下界。

定理6.8. 设n和k都是正整数，满足$k \geq 2$以及$n \geq 2k+1$，则$B_2(n,k,k+1;3) \geq 2^{n-2k+1}$。

定理6.9. 设n, k, 以及γ都是正整数, 满足$k \geq 3\lceil \frac{\gamma}{2} \rceil$以及$n \geq 2k+\gamma$, 则$B_2(n,k,k+\gamma;3) \geq 2^{\lfloor \frac{n-2k+1}{k+1} \rfloor \lfloor \frac{k}{\lceil \gamma/2 \rceil} \rfloor}$。

定理6.10. 设n，k，以及γ都是正整数，满足$\gamma+1 \leq k < 3\lceil \frac{\gamma}{2} \rceil$以及$n \geq 2k+\gamma$，则$B_2(n,k,k+\gamma;3) \geq 2^{2\lfloor \frac{n-2k+1}{k+1} \rfloor}$。

定理6.11. 设n和k都是正整数，满足$n \geq 3k$，则$B_2(n,k,2k;3) \geq 2^{\lfloor \frac{n-k}{k} \rfloor}$。

定理6.12. 设n，k，以及γ都是正整数，满足$n \geq 2k+\gamma$，则$B_q(n,k,k+\gamma;3) \geq q^{\lfloor \frac{n-2k+1}{k+1} \rfloor \lfloor \frac{k}{\gamma} \rfloor}$。

- 当n比较大时，通过概率方法，我们给出了$B_q(n,k,\delta;\alpha)$的下界。

定理6.13. 若$\alpha \geq 3$且$\gcd(\alpha-1,\delta-1)=1$，则$B_q(n,k,\delta;\alpha) = \Omega\left(q^{(k-\frac{\delta-1}{\alpha-1})n} n^{\frac{1}{\alpha-1}}\right)$。

这些结论改进了前人的结果。

这项工作即将发表在《IEEE Transactions on Information Theory》。

§6.2 有限域上的线性空间中的内积链

在有限域中，Erdős-Falconer距离问题问的是$\mathbb{F}_q^d$的子集$\mathcal{E}$的最小基数，使得距离集合

$$\Delta(\mathcal{E}) := \{\|\boldsymbol{x}-\boldsymbol{y}\| : \boldsymbol{x},\boldsymbol{y} \in \mathcal{E}\}$$

占$\mathbb{F}_q$的正比例，其中对于$\boldsymbol{x}=(x_1,x_2,\ldots,x_d) \in \mathbb{F}_q^d$，$\|\boldsymbol{x}\| := x_1^2+x_2^2+\cdots+x_d^2$。将距离换成其他的二元运算，我们仍然可以提出同样的问题。定义$\mathcal{E}$上的内积集合

$$\Pi(\mathcal{E}) := \{x \cdot y : x,y \in \mathcal{E}\}。$$

在文献[28]中，Hart等人证明了下列结果。

定理6.14. 设$\mathcal{E} \subseteq \mathbb{F}_q^d$，$t \in \mathbb{F}_q^*$，则

$$|\{(x,y) \in \mathcal{E}\times\mathcal{E} : x\cdot y = t\}| = \frac{|\mathcal{E}|^2}{q} + R(t),$$

其中$|R(t)| \leq |\mathcal{E}|q^{(d-1)/2}$。

推论6.1. 设$\mathcal{E} \subseteq \mathbb{F}_q^d$满足$|\mathcal{E}| \geq Cq^{(d+1)/2}$，其中$C$是常数，则

$$\Pi(\mathcal{E}) \supseteq \mathbb{F}_q^*。$$

这个问题可以与图结合起来。设$\mathcal{E} \subseteq \mathbb{F}_q^d$，我们可以得到一个完全图$K_{\mathcal{E}}$，其顶点集为$\mathcal{E}$。我们进一步给$K_{\mathcal{E}}$的每一条边赋权，即边$\{x, y\}$的权重为$x \cdot y$。因此，推论6.1就是说，只要$|\mathcal{E}| \geq Cq^{(d+1)/2}$，那么对任意$t \in \mathbb{F}_q^*$，我们都可以在$K_{\mathcal{E}}$中找到一条权重为$t$的边。定理6.14说明这样的边有$\frac{|\mathcal{E}|^2}{q}(1 + o(1))$条。我们可以将这个问题做一个自然的推广：给定某种构型，我们是否可以在$K_{\mathcal{E}}$中找到任意权重的相应构型？文献[10]给出了关于2路径的结论。

定理6.15. *设$\mathcal{E} \subseteq \mathbb{F}_q^d$，定义*

$$\Pi_{\alpha,\beta}(\mathcal{E}) := \{(x, y, z) \in \mathcal{E}^3 : x \cdot y = \alpha, y \cdot z = \beta\}。$$

若$d \geq 2$，$\mathcal{E} \geq q^{(d+1)/2}$，并且$\alpha, \beta \in \mathbb{F}_q^*$，则

$$|\Pi_{\alpha,\beta}(\mathcal{E})| = \frac{|\mathcal{E}|^3}{q^2}(1 + o(1))。$$

我们考虑更长的路径，称为内积链（dot product chain），并且我们允许元素来自不同的集合。确切地说，对于$A_1, A_2, \ldots, A_{k+1} \subseteq \mathbb{F}_q^d$，令

$$\Pi(A_1, A_2, \ldots, A_{k+1}) = \{(x_1 \cdot x_2, x_2 \cdot x_3, \ldots, x_k \cdot x_{k+1}) \in \mathbb{F}_q^k : x_i \in A_i, 1 \leq i \leq k+1\}。$$

我们有以下结果。

定理6.16. *设$d \geq 1$和$k \geq 2$均为整数，存在常数$C = C(k)$使得下述命题成立。若$A_1, A_2, \ldots, A_{k+1} \subseteq \mathbb{F}_q^d$满足$|A_i||A_{i+1}| \geq Cq^{d+k-1}$，则*

$$\Pi(A_1, A_2, \ldots, A_{k+1}) \supseteq (\mathbb{F}_q^*)^k。$$

我们也准备考虑树（tree）的情况。

这方面的工作仍在整理中。

§6.3 $(\mathbb{Z}/N\mathbb{Z})^n$上的Furstenberg集

Kakeya猜想由日本数学家Soichi Kakeya于1917年提出。$\mathbb{R}^n$中的一个Kakeya集包含任意方向上的单位线段。Kakeya猜想是指$\mathbb{R}^n$中的任意Kakeya集的Hausdorff维数和Minkowski维数均为n。这个猜想与调和分析有着密切联系。这方面的研究可以

参考文献[29, 38–41, 82]。Wolff[83]提出了有限域上的Kakeya问题。$\mathbb{F}_q^n$上的Kakeya集包含任意方向上的一条直线。Dvir[16]突破性地使用多项式方法解决了有限域上的Kakeya问题，证明了$\mathbb{F}_q^n$中的Kakeya集的基数至少为$C_n q^n$。最近，Dhar和Dvir[12]以及Dhar[11]运用推广后的多项式方法解决了$(\mathbb{Z}/N\mathbb{Z})^n$上的Kakeya问题。

对于整数$n > k \geq 1$和$m \geq 1$，我们称$S \subseteq \mathbb{F}_q^n$是一个$(k,m)$-Furstenberg集，如果对于$\mathbb{F}_q^n$的任意$k$维子空间$W$，都存在$W$的一个平移与$S$相交至少$m$个点。我们用$K(q,n,k,m)$表示$\mathbb{F}_q^n$上的$(k,m)$-Furstenberg集的最小基数。所以$(1,q)$-Furstenberg集就是Kakeya集，并且$K(q,n,1,q) \geq C_n q^n$。Ellenberg和Erman[18]证明了

$$K(q,n,k,m) \geq C_{n,k} m^{n/k}。$$

Dhar等人[13]利用多项式方法给出了另一种证明。

我们考察$(\mathbb{Z}/N\mathbb{Z})^n$的Furstenberg集，其中$N$无平方因子。设$K\left((\mathbb{Z}/N\mathbb{Z})^n, k, m\right)$是$(\mathbb{Z}/N\mathbb{Z})^n$上的$(k,m)$-Furstenberg集的最小基数。我们有以下结果

定理6.17. *设$N = p_1 p_2 \cdots p_r$，其中$p_1, p_2, \ldots, p_r$为互不相同的素数。则*

$$K\left((\mathbb{Z}/N\mathbb{Z})^n, k, N^k\right) \geq \frac{N^n}{\prod_{i=1}^r \left(1 + \frac{p_i - 1}{p_i^k}\right)^n}。$$

目前，这部分工作仍在整理中。

参考文献

[1] K. Ball. A lower bound for the optimal density of lattice packings. *Internat. Math. Res. Notices*, (10):217–221, 1992.

[2] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, and M. Rudnev. Group actions and geometric combinatorics in $\mathbb{F}_q^d$. *Forum Math.*, 29(1):91–110, 2017.

[3] G. R. Blakley and P. Roy. A Hölder type inequality for symmetric matrices with nonnegative entries. *Proc. Amer. Math. Soc.*, 16:1244–1245, 1965.

[4] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1):27–57, 2004.

[5] J. Chapman, M. B. Erdoğan, D. Hart, A. Iosevich, and D. Koh. Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates. *Math. Z.*, 271(1–2):6393, 2012.

[6] J. A. Clarkson. Uniformly convex spaces. *Trans. Amer. Math. Soc.*, 40(3):396–414, 1936.

[7] H. Cohn and N. Elkies. New upper bounds on sphere packings. I. *Ann. of Math. (2)*, 157(2):689–714, 2003.

[8] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska. The sphere packing problem in dimension 24. *Ann. of Math. (2)*, 185(3):1017–1033, 2017.

[9] H. Cohn and Y. Zhao. Sphere packing bounds via spherical codes. *Duke Math. J.*, 163(10):1965–2002, 2014.

[10] D. Covert and S. Senger. Pairs of dot products in finite fields and rings. In *Combinatorial and additive number theory. II*, volume 220 of *Springer Proc. Math. Stat.*, pages 129–138. Springer, Cham, 2017.

[11] M. Dhar. Maximal and (m, ϵ)-Kakeya bounds over $\mathbb{Z}/N\mathbb{Z}$ for general N. *arXiv e-prints*, page arXiv:2209.11443, Sept. 2022.

[12] M. Dhar and Z. Dvir. Proof of the Kakeya set conjecture over rings of integers modulo square-free N. *Comb. Theory*, 1:Paper No. 4, 21, 2021.

[13] M. Dhar, Z. Dvir, and B. Lund. Simple proofs for Furstenberg sets over finite fields. *Discrete Anal.*, pages Paper No. 22, 16, 2021.

[14] X. Du, L. Guth, Y. Ou, H. Wang, B. Wilson, and R. Zhang. Weighted restriction estimates and application to Falconer distance set problem. *Amer. J. Math.*, 143(1):175–211, 2021.

[15] X. Du, A. Iosevich, Y. Ou, H. Wang, and R. Zhang. An improved result for Falconer's distance set problem in even dimensions. *Math. Ann.*, 380(3-4):1215–1231, 2021.

[16] Z. Dvir. On the size of Kakeya sets in finite fields. *J. Amer. Math. Soc.*, 22(4):1093–1097, 2009.

[17] N. D. Elkies, A. M. Odlyzko, and J. A. Rush. On the packing densities of superballs and other bodies. *Invent. Math.*, 105(3):613–639, 1991.

[18] J. S. Ellenberg and D. Erman. Furstenberg sets and Furstenberg schemes over finite fields. *Algebra Number Theory*, 10(7):1415–1436, 2016.

[19] P. Erdős and E. Szemerédi. On sums and products of integers. In *Studies in Pure Mathematics*, pages 213–218, Birkhäuser, Basel, 1983.

[20] T. Etzion and H. Zhang. Grassmannian codes with new distance measures for network coding. *IEEE Trans. Inform. Theory*, 65(7):4131–4142, 2019.

[21] A. Eustis. *Hypergraph Independence Numbers*. ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–University of California, San Diego.

[22] I. G. Fernández, J. Kim, H. Liu, and O. Pikhurko. New lower bounds on kissing numbers and spherical codes in high dimensions. *arXiv e-prints*, page arXiv:2111.01255, Nov. 2021.

[23] A. Greenleaf, A. Iosevich, and S. Mkrtchyan. Existence of similar point configurations in thin subsets of $\mathbb{R}^d$. *Math. Z.*, 297(1-2):855–865, 2021.

[24] L. Guth, A. Iosevich, Y. Ou, and H. Wang. On Falconer's distance set problem in the plane. *Invent. Math.*, 219(3):779–830, 2020.

[25] D. M. Ha and H. T. Ngo. Expanders on matrices over a finite chain ring, I. *arXiv e-prints*, page arXiv:2207.08221, July 2022.

[26] H. Hadwiger. Über Treffanzahlen bei translationsgleichen Eikörpern. *Arch. Math.*, 8:212–213, 1957.

[27] T. C. Hales. A proof of the Kepler conjecture. *Ann. of Math. (2)*, 162(3):1065–1185, 2005.

[28] D. Hart, A. Iosevich, D. Koh, and M. Rudnev. Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture. *Trans. Amer. Math. Soc.*, 363(6):3255–3275, 2011.

[29] J. Hickman, K. M. Rogers, and R. Zhang. Improved bounds for the Kakeya maximal conjecture in higher dimensions. *Amer. J. Math.*, 144(6):1511–1560, 2022.

[30] E. Hlawka. Zur Geometrie der Zahlen. *Math. Z.*, 49:285–312, 1943.

[31] A. Iosevich, D. Koh, and H. Parshall. On the quotient set of the distance set. *Mosc. J. Comb. Number Theory*, 8(2):103–115, 2019.

[32] A. Iosevich and M. Rudnev. Erdős distance problem in vector spaces over finite fields. *Trans. Amer. Math. Soc.*, 359(12):6127–6142, 2007.

[33] M. Jenssen, F. Joos, and W. Perkins. On kissing numbers and spherical codes in high dimensions. *Adv. Math.*, 335:307–321, 2018.

[34] M. Jenssen, F. Joos, and W. Perkins. On the hard sphere model and sphere packings in high dimensions. *Forum Math. Sigma*, 7:Paper No. e1, 19, 2019.

[35] T. Jiang and A. Vardy. Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes. *IEEE Trans. Inform. Theory*, 50(8):1655–1664, 2004.

[36] G. A. Kabatjanskiĭ and V. I. Levenšteĭn. Bounds for packings on the sphere and in space. *Problemy Peredači Informacii*, 14(1):3–25, 1978.

[37] Y. D. Karabulut, D. Koh, T. Pham, C.-Y. Shen, and A. V. Le. Expanding phenomena over matrix rings. *Forum Math.*, 31(4):951–970, 2019.

[38] N. H. Katz, I. Łaba, and T. Tao. An improved bound on the Minkowski dimension of Besicovitch sets in $\mathbf{R}^3$. *Ann. of Math. (2)*, 152(2):383–446, 2000.

[39] N. H. Katz and T. Tao. New bounds for Kakeya problems. *J. Anal. Math.*, 87:231–263, 2002. Dedicated to the memory of Thomas H. Wolff.

[40] N. H. Katz and J. Zahl. An improved bound on the Hausdorff dimension of Besicovitch sets in $\mathbb{R}^3$. *J. Amer. Math. Soc.*, 32(1):195–259, 2019.

[41] N. H. Katz and J. Zahl. A Kakeya maximal function estimate in four dimensions using planebrushes. *Rev. Mat. Iberoam.*, 37(1):317–359, 2021.

[42] J. Kim, H. Liu, and T. Tran. Exponential decay of intersection volume with applications on list-decodability and Gilbert-Varshamov type bound. *IEEE Trans. Inform. Theory*, 2023.

[43] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, 2008.

[44] J. Lagarias, J. Mazo, L. Shepp, and B. McKay. An inequality for walks in a graph. *SIAM Review*, 25(3):403–403, 1983.

[45] G. Landsberg. Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe. *J. Reine Angew. Math.*, 111:87–88, 1893.

[46] D. G. Larman and C. Zong. On the kissing numbers of some special convex bodies. *Discrete Comput. Geom.*, 21(2):233–242, 1999.

[47] J. Leech. The problem of the thirteen spheres. *Math. Gaz.*, 40:22–23, 1956.

[48] V. I. Levenšteĭn. On bounds for packings in n-dimensional euclidean space. *Soviet Math. Dokl.*, 20:417–421, 1979.

[49] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[50] L. Liu and C. P. Xing. Packing superballs from codes and algebraic curves. *Acta Math. Sin. (Engl. Ser.)*, 24(1):1–6, 2008.

[51] A. Mohammadi, T. Pham, and Y. Wang. An energy decomposition theorem for matrices and related questions. *arXiv e-prints*, page arXiv:2106.07328, June 2021.

[52] A. Mohammadi and S. Stevens. Attaining the exponent 5/4 for the sum-product problem in finite fields. *arXiv e-prints*, page arXiv:2103.08252, Mar. 2021.

[53] O. R. Musin. The kissing number in four dimensions. *Ann. of Math. (2)*, 168(1):1–32, 2008.

[54] T. Nguyen and L. A. Vinh. A point-plane incidence theorem in matrix rings. *Discrete Appl. Math.*, 322:166–170, 2022.

[55] A. M. Odlyzko and N. J. A. Sloane. New bounds on the number of unit spheres that can touch a unit sphere in n dimensions. *J. Combin. Theory Ser. A*, 26(2):210–214, 1979.

[56] T. Pham. A sum-product theorem in matrix rings over finite fields. *C. R. Math. Acad. Sci. Paris*, 357(10):766–770, 2019.

[57] N. D. Phuong, T. Pham, and L. A. Vinh. Incidences between planes over finite fields. *Proc. Am. Math. Soc.*, 147(5):2185–2196, 2019.

[58] F. Pirot and E. Hurley. Colouring locally sparse graphs with the first moment method. *arXiv e-prints*, page arXiv:2109.15215, Sept. 2021.

[59] F. Rakhmonov. Distribution of similar configurations in subsets of $\mathbb{F}_q^d$. *arXiv e-prints*, page arXiv:2208.11579, Aug. 2022.

[60] C. A. Rogers. Existence theorems in the geometry of numbers. *Ann. of Math. (2)*, 48:994–1002, 1947.

[61] C. A. Rogers. The number of lattice points in a set. *Proc. London Math. Soc. (3)*, 6:305–320, 1956.

[62] C. A. Rogers. Lattice covering of space: The Minkowski-Hlawka theorem. *Proc. London Math. Soc. (3)*, 8:447–465, 1958.

[63] M. Rudnev and S. Stevens. An update on the sum-product problem. *Math. Proc. Cambridge Philos. Soc.*, 173(2):411–430, 2022.

[64] J. A. Rush. A lower bound on packing density. *Invent. Math.*, 98(3):499–509, 1989.

[65] J. A. Rush. Constructive packings of cross polytopes. *Mathematika*, 38(2):376–380 (1992), 1991.

[66] J. A. Rush. An indexed set of density bounds on lattice packings. *Geom. Dedicata*, 53(2):217–221, 1994.

[67] J. A. Rush. Lattice packing of nearly-Euclidean balls in spaces of even dimension. *Proc. Edinburgh Math. Soc. (2)*, 39(1):163–169, 1996.

[68] J. A. Rush and N. J. A. Sloane. An improvement to the Minkowski-Hlawka bound for packing superballs. *Mathematika*, 34(1):8–18, 1987.

[69] A. Sah, M. Sawhney, D. Stoner, and Y. Zhao. Exponential improvements for superball packing upper bounds. *Adv. Math.*, 365:107056, 9, 2020.

[70] N. T. Sardari and M. Zargar. New upper bounds for spherical codes and packings. *arXiv e-prints*, page arXiv:2001.00185, Jan. 2020.

[71] W. M. Schmidt. The measure of the set of admissible lattices. *Proc. Amer. Math. Soc.*, 9:390–403, 1958.

[72] W. M. Schmidt. Masstheorie in der Geometrie der Zahlen. *Acta Math.*, 102:159–224, 1959.

[73] W. M. Schmidt. On the Minkowski-Hlawka theorem. *Illinois J. Math.*, 7:18–23, 1963.

[74] K. Schütte and B. L. van der Waerden. Das problem der dreizehn kugeln. *Math. Ann.*, 125(1):325–334, 1952.

[75] C. E. Shannon. Probability of error for optimal codes in a Gaussian channel. *Bell System Tech. J.*, 38:611–656, 1959.

[76] K. J. Swanepoel. New lower bounds for the Hadwiger numbers of l_p balls for $p < 2$. *Appl. Math. Lett.*, 12(5):57–60, 1999.

[77] I. Talata. A lower bound for the translative kissing numbers of simplices. *Combinatorica*, 20(2):281–293, 2000.

[78] N. V. The and L. A. Vinh. Expanding phenomena over higher dimensional matrix rings. *J. Number Theory*, 216:174–191, 2020.

[79] J. van der Corput and G. Schaake. Anwendung einer blichfeldtschen beweismethode in der geometrie der zahlen. *Acta Arithmetica*, 2:152–160, 1936.

[80] A. Venkatesh. A note on sphere packings in high dimension. *Int. Math. Res. Not. IMRN*, (7):1628–1642, 2013.

[81] M. S. Viazovska. The sphere packing problem in dimension 8. *Ann. of Math. (2)*, 185(3):991–1015, 2017.

[82] T. Wolff. An improved bound for Kakeya type maximal functions. *Rev. Mat. Iberoamericana*, 11(3):651–674, 1995.

[83] T. Wolff. Recent work connected with the Kakeya problem. In *Prospects in mathematics (Princeton, NJ, 1996)*, pages 129–162. Amer. Math. Soc., Providence, RI, 1999. 11

[84] A. D. Wyner. Capabilities of bounded discrepancy decoding. *Bell System Tech. J.*, 44:1061–1122, 1965.

[85] L. Xu. A note on the kissing numbers of superballs. *Discrete Comput. Geom.*, 37(3):485–491, 2007.

致谢

回想2017年进入首都师范大学学习，我的研究生生涯即将结束。六年弹指一挥间，我过得很充实，走得很坚定，也遇见了许多人。在此，我想向我的老师、家人、朋友和同学表达我内心最真挚的感谢。正因为有了你们，我才能克服各种困难挫折，战胜各种风险挑战。

首先我要特别感谢我的导师葛根年教授。我的成长离不开葛老师的悉心教导。在学习上，葛老师指导我们打好数学基础，邀请外校专家为我们讲课，丰富了我的专业知识，开拓了我的学术视野。在科研上，葛老师严谨的治学态度与创新的思维令我受益匪浅，帮助我脚踏实地地走好科研的每一步。在生活上，葛老师为我们提供了良好的科研环境，为我们的科研提供了许多便利。在三年疫情期间，葛老师十分关心我们的身心健康。葛老师的优秀品格必将激励我在科研的道路上越走越远。

我还要感谢在我的学习与科研过程中帮助过我的专家学者们，特别是天津大学的宗传明教授和韩国基础科学研究院的刘鸿老师。宗老师在离散几何方面的远见卓识提升了我的学术眼界，刘老师对我的研究工作提出了许多有益的思路与建议。同时我也感谢首都师范大学的张利友老师和杜少飞老师，普林斯顿大学的Zeev Dvir老师，纽约城市大学的Adam Sheffer老师，麻省理工学院的Yufei Zhao老师，亚利桑那州立大学的姜子麟老师，山东大学的上官冲老师。在与他们的邮件来往中，我得以体会到科研的乐趣，也得以认识到自身的不足。

感谢一起在首师大学习生活的同门：汪馨师兄、张一炜师兄、张韬师兄、马景学师兄、丁报昆师兄、钱昺辰师兄、孔祥梁师兄、戚立波师兄、奚元霄师兄、余文俊师兄、叶左师兄、韩雪姣师姐、徐子翔师兄、兰昭君、徐民、魏歆、李好阳、孙钰博、刘欣、马鋆、于泉勇、王昊、李玉玲、李震洋、张仪轩、李济村、王运韬。特别感谢钱昺辰师兄，带领我走出了科研的第一步。同时我也感谢杭州团队的陈婷婷给予的帮助。

感谢我的朋友们：俞彬彬、傅炯怡、邵泽伟、吴奇栋。感谢他们在我低谷时给我带来的鼓励与欢乐。

最后，我要感谢我的父母。二十余年寒窗，他们一直在背后默默地关心与支持我，帮助我可以专心学习与科研。

攻读博士学位期间的研究成果

1. **Chengfei Xie** and Gennian Ge. Some sum-product estimates in matrix rings over finite fields. *Finite Fields Appl.*, 79:Paper No. 101997, 2022.

2. Bingchen Qian, **Chengfei Xie**, and Gennian Ge. On the minimal degree condition of graphs implying equality of the largest K_r-free subgraphs and $(r-1)$-partite subgraphs. *Discrete Math.*, 344(8):Paper No. 112453, 11, 2021.

3. Bingchen Qian, **Chengfei Xie**, and Gennian Ge. Some results on k-Turán-good graphs. *Discrete Math.*, 344(9):Paper No. 112509, 10, 2021.

4. Bingchen Qian, Xin Wang, **Chengfei Xie**, Gennian Ge. Covering Grassmannian Codes: Bounds and Constructions. To appear in *IEEE Transactions on Information Theory*, 2023.

5. **Chengfei Xie** and Gennian Ge. A graph theoretical approach to estimating packing densities of superballs in high dimensions. Submitted.

6. **Chengfei Xie** and Gennian Ge. Some results on similar configurations in subsets of $\mathbb{F}_q^d$. Submitted.

7. **Chengfei Xie** and Gennian Ge. Some improved sum-product estimates in $M_n(\mathbb{F}_q)$. In preparation.

8. **Chengfei Xie** and Gennian Ge. On the lower bound for kissing numbers of ℓ_p-spheres in high dimensions. In preparation.

9. **Chengfei Xie** and Gennian Ge. Dot product chains of large sets in finite fields. In preparation.

10. **Chengfei Xie** and Gennian Ge. On the size of Kakeya-type sets over $\mathbb{Z}/N\mathbb{Z}$ with square-free N. In preparation.