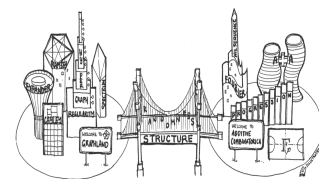




# GRAPH THEORY AND ADDITIVE COMBINATORICS

作者: Yufei Zhao

时间: July 13, 2021



## 特别声明

凭爱好翻译。

Chenghua Liu

July 13, 2021

# 目录

<b>1</b>	<b>绪论</b>	<b>1</b>
1.1	Schur 定理	1
1.2	加性组合的亮点	2
1.3	然后呢?	4
	<b>第一部分 图论</b>	<b>5</b>
<b>2</b>	<b>禁止子图</b>	<b>6</b>
2.1	Mantel 定理: 禁止三角形	6
2.2	Turán 定理: 禁止团	6
2.3	超图上的 Turán 问题	8
2.4	Erdős–Stone–Simonovits 定理: 禁止一般子图	9
2.5	Kovári–Sós–Turán 定理: 禁止完全二分图	10
2.6	下界: 随机构造	12
2.7	下界: 代数构造	14
2.8	下界: 随机代数构造	17
2.9	禁止稀疏二分图	19
<b>3</b>	<b>Szemerédi 正则性引理</b>	<b>24</b>
3.1	定理陈述和证明	24
3.2	三角形记数和删除引理	27
3.3	Roth 定理	30
3.4	构造没有三项等差数列的集合	31
3.5	图嵌入、计数和删除引理	33
3.6	导出子图的删除引理	35
3.7	属性检测 (property testing)	38
3.8	超图的删除引理	39
3.9	超图的正则性	39
3.10	Szemerédi 正则性引理的谱证明	41
<b>4</b>	<b>伪随机图</b>	<b>43</b>
4.1	拟随机图	43
4.2	Expander mixing 引理	47
4.3	拟随机凯莱图	49
4.4	Alon–Boppana 界	50
4.5	Ramanujan 图	52
4.6	稀疏图正则性和 Green–Tao 定理	52
<b>5</b>	<b>图极限</b>	<b>54</b>
5.1	主要结论的介绍和说明	54
5.2	W-随机图	57
5.3	正则性和计数引理	57

5.4	Graphon 空间的紧致性	60
5.5	紧致性的应用	62
5.6	子图密度间的不等式	64
<b>第二部分 加性组合</b>		<b>71</b>
<b>6</b>	<b>Roth 定理</b>	<b>72</b>
6.1	有限域 Roth 定理	72
6.2	Roth 对整数 Roth 定理的证明	76
6.3	有限域 Roth 定理的多项式证明	80
6.4	Roth 定理与流行公差	83
<b>7</b>	<b>集合的加性结构</b>	<b>86</b>
7.1	Small doubling set 结构	86
7.2	Plünnecke–Ruzsa 不等式	88
7.3	有限域上的 Freiman 定理	90
7.4	Freiman 同态	92
7.5	建模引理	92
7.6	Bogolyubov 引理	94
7.7	几何数论	96
7.8	Freiman 定理的证明	98
7.9	一般阿贝尔群的 Freiman 定理	99
7.10	非阿贝尔群中的 Freiman 问题	100
7.11	多项式 Freiman–Ruzsa 猜想	101
7.12	加性能量和 Balog–Szémeredi–Gowers 定理	102
<b>8</b>	<b>Sum-Product 问题</b>	<b>107</b>
8.1	交叉数不等式	107
8.2	重合几何	108
8.3	从积性能量看 Sum-product 问题	109

# 第1章 绪论

## 1.1 Schur 定理

1910 年左右, Schur 试图通过将方程  $X^n + Y^n = Z^n$  模掉素数  $p$  来解决费马大定理<sup>1</sup>, 但是他没有成功。事实上, 对于每一个正整数  $n$ , 该方程对于所有足够大的素数  $p$  都有非平凡解  $\text{mod } p$ , Schur 通过证明以下经典结果建立了这一点。

### 定理 1.1 (Schur 定理)

如果把正整数集用有限多种颜色着色, 那么  $x + y = z$  总是有一个单色解。即,  $x, y, z$  都具有相同的颜色。

我们将很快证明 Schur 定理, 但首先我们将展示如何使用 Schur 定理推导出  $X^n + Y^n \equiv Z^n \pmod{p}$  的解的存在性。

以上是 Schur 定理的“无限”版本, 它等价于以下的“有限”版本。我们定义记号  $[N] := \{1, 2, \dots, N\}$ 。

### 定理 1.2 (有限版本 Schur 定理)

对于每个正整数  $r$ , 存在一个正整数  $N = N(r)$  使得如果将  $[N]$  用  $r$  种颜色着色, 则存在一个单色解  $x + y = z$ , 其中  $x, y, z \in [N]$ 。

对于有限版本, 我们还可以提出定量问题, 例如关于  $r$  的函数  $N(r)$  是怎样的。对于大多数此类问题, 我们不知道答案, 甚至不知道近似结果。下面让我们证明定理 1.1 和定理 1.2 是等价的。很明显, Schur 定理的无限版本蕴含了它的有限版本。下面用反证法说明如何从有限版本推出无限版本, 固定  $r$ , 并假设对于每个  $N$  有着色方案  $\phi_N : [N] \rightarrow [r]$ , 并且该方案使得  $x + y = z$  没有单色解。我们可以取一个  $(\phi_N)$  的一个无限子序列, 使得对于每一个  $k \in \mathbb{N}$ ,  $\phi_N(k)$  的值随着  $N$  沿着子序列的增加而稳定。然后  $\phi_N$  沿着这个子序列逐点收敛到某种着色  $\phi : \mathbb{N} \rightarrow [r]$ , 使得该着色没有单色解  $x + y = z$ 。显然这与定理 1.2 矛盾。

接下来, 让我们来证明 Schur 这个关于  $X^n + Y^n \equiv Z^n \pmod{p}$  存在非平凡解的断言。

### 定理 1.3

$n$  为正整数, 对于所有足够大的素数  $p$ , 存在  $X, Y, Z \in \{1, \dots, p-1\}$  满足  $X^n + Y^n \equiv Z^n \pmod{p}$ 。

**证明** [定理 1.3] 我们先默认 Schur 定理 (定理 1.2) 成立。然后用  $(\mathbb{Z}/p\mathbb{Z})^\times$  来表示乘法下模掉  $p$  后的非零元素组成的群, 令  $H$  表示  $(\mathbb{Z}/p\mathbb{Z})^\times$  的所有元素的  $n$  次幂构成的子群。  $(\mathbb{Z}/p\mathbb{Z})^\times$  中, 子群  $H$  的指数<sup>2</sup>最多为  $n$ 。所以  $H$  的陪集最多将  $\{1, 2, \dots, p-1\}$  划分为  $n$  个集合。根据有限版本 Schur 定理, 对于足够大的  $p$ , 存在一个解

$$x + y = z \quad \text{in } \mathbb{Z}$$

使得  $x, y, z$  属于其中的同一个集合。假设他们属于陪集  $aH$  (其中  $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ )。注意到  $H$  由  $n$  次幂组成, 从而一定存在  $X, Y, Z \in (\mathbb{Z}/p\mathbb{Z})^\times$ , 使得  $x = aX^n, y = aY^n, z = aZ^n$  因此

$$aX^n + aY^n \equiv aZ^n \pmod{p}$$

于是存在  $X, Y, Z \in \{1, \dots, p-1\}$  满足

$$X^n + Y^n \equiv Z^n \pmod{p}$$

现在我们准备借助对完全图进行边着色来证明定理 1.2。下面给出的结果是 Ramsey 定理的一个特例。

<sup>1</sup>Fermat's Last Theorem: 当整数  $n > 2$  时, 不定方程  $X^n + Y^n = Z^n$  无正整数解 (Wiles 1995)

<sup>2</sup>群  $G$  中子群  $H$  的指数是  $G$  中  $H$  的左陪集数, 或等效地,  $G$  中  $H$  的右陪集数。(译者注: 这里  $H$  的指数至多为  $n$ , 是由于数论中的拉格朗日定理, 定义在  $(\mathbb{Z}/p\mathbb{Z})^\times$  上映射  $x \rightarrow x^n$  的核 (kernel) 最大为  $n$ 。)



**定理 1.4**

对于每一个正整数  $r$ ，都存在整数  $N = N(r)$ ，使得无论如何对完全图  $K_N$  的边用  $r$  种颜色着色，总是存在一个单色三角形。

**证明** [定理 1.4]

我们对  $r$  进行归纳。显然  $N(1) = 3$  可以使得  $r = 1$  的情况成立。令  $r \geq 2$  并假设  $r - 1$  种颜色的情况下，命题对  $N = N'$  成立，我们将证明在  $r$  种颜色的情况下，取  $N = r(N' - 1) + 2$  可以使命题成立。

假设我们使用  $r$  种颜色为  $r(N' - 1) + 2$  个顶点的完全图的边着色。任意选取一个顶点  $v$ ，考虑与  $v$  相连的  $r(N' - 1) + 1$  条边，根据鸽巢原理，至少  $N'$  条与  $v$  相连的边具有相同的颜色，比如说是红色。令  $V_0$  是通过红色边连到  $v$  的顶点集。如果  $V_0$  内的顶点间有红色边，我们将获得红色三角形。否则， $V_0$  中最多出现  $r - 1$  种颜色，但顶点数  $|V_0| \geq N'$ ，根据归纳法，还是存在一个单色三角形。

我们现在就要构造一个图，使得该图的单色三角形对应于  $x + y = z$  的单色解，从而允许我们将上述结果应用到到整数上（来证明 Schur 定理）。

**证明** [定理 1.2]

令  $\phi: [N] \rightarrow [r]$  是一种对  $[N]$  的着色方案。我们通过给满足  $i < j$  的无向边  $\{i, j\}$  上色  $\phi(j - i)$ ，来为顶点集  $\{1, \dots, N + 1\}$  的完全图的边着色。根据定理 1.4，如果  $N$  足够大，则存在一个单色三角形。假设它的顶点是  $i < j < k$ ，我们一定有  $\phi(j - i) = \phi(k - j) = \phi(k - i)$ ，取  $x = j - i$ 、 $y = k - j$ 、 $z = k - i$ ，那么我们发现  $\phi(x) = \phi(y) = \phi(z)$  并且  $x + y = z$ ，这正是我们想要的。

请注意我们是如何通过转移到图论的方式来解决数论问题的。定理 1.4 中的类似 Ramsey 定理的论证很难直接在整数内部进行。因此，我们通过考虑图从而获得了更大的灵活性。稍后我们将看到这个想法的其他更复杂的例子，在这些例子中，将数论问题带到图论领域会给我们一个新的视角。

## 1.2 加性组合的亮点

上面的 Schur 定理是现在被称为加性组合的领域最早的例子之一，加性组合该术语由 Terry Tao 在 2000 年代初期提出，用于描述关于加法的简单陈述问题和整数的乘法这一快速发展的数学方向。加性组合中的问题和方法是深刻而深远的，连接了许多不同的数学领域，如图论、调和分析、遍历理论、离散几何和模型论。本节的其余部分重点介绍了过去一个世纪加性组合学的一些重要发展。

在 1920 年代，van der Waerden 证明了以下关于整数中单色等差数列的结果。

**定理 1.5 (van der Waerden 定理)**

如果整数用有限多种颜色着色，则其中一个颜色类别必须包含任意长的等差数列。



**笔记** 具有任意长的等差数列与具有无限长的等差数列非常不同。作为练习，请证明可以只使用两种颜色为整数着色可以不会有无限长的单色等差数列。

在 1930 年代，Erdős 和 Turán 猜想一个更强的结论成立，即密度为正的整数的任何子集都包含任意长的等差数列。准确地说，我们说  $A \subseteq \mathbb{Z}$  具有正的上密度，如果

$$\limsup_{N \rightarrow \infty} \frac{|A \cap \{-N, \dots, N\}|}{2N + 1} > 0$$

(这个定义有几种变体——确切的表述并不重要。)

在 1950 年代，Roth 使用傅立叶分析方法证明了 3 项算术级数的猜想。在 1970 年代，Szemerédi 使用组合技术完全解决了这个猜想。这些是该领域的里程碑式定理。我们将讨论的大部分内容都是由这些结果及与其相关的发展所推动的。

**定理 1.6 (Roth 定理)**

整数每个具有正上密度的子集都包含一个长度为 3 的等差数列。

**定理 1.7 (Szemerédi 定理)**

整数每个具有正上密度的子集都包含任意长的等差数列。



Szemerédi 的定理是深刻而复杂的。这项工作导致了加法组合学的许多后续发展。此后，人们发现了 Szemerédi 定理的几种不同证明，其中一些已经发展成为数学研究的丰富领域。以下是 Szemerédi 定理的一些最具影响力的现代证明（按历史顺序）：

- 遍历理论方法 (Furstenberg 1977)
- 高阶傅立叶分析 (Gowers 2001)
- 超图正则性引理 (Rödl et al. 2005/Gowers 2007)

Szemerédi 定理的另一个现代证明来自密度 Hales-Jewett 定理，该定理最初由 Furstenberg 和 Katznelson 使用遍历理论证明 (1991)，随后在第一个成功的 Polymath 项目中发现了新的组合证明 (2012)。Polymath 项目是由 Gowers 发起的在线协作项目。这些不同方法之间的关系尚未完全理解，并且存在许多未解决的问题，尤其是定量的具体上下界。Szemerédi 定理的所有已知方法背后，都有一个统一主题，那就是结构和伪随机性之间的二分法<sup>3</sup>。以后会看到在图论和数论的不同背景下，这种二分法的具体内容。

以下是 Szemerédi 定理的其他一些重要后续发展。

我们不考虑整数的子集，而是考虑更高维点阵  $\mathbb{Z}^d$  的子集。我们说  $A \subset \mathbb{Z}^d$  具有正的上密度，如果

$$\limsup_{N \rightarrow \infty} \frac{|A \cap [-N, N]^d|}{(2N+1)^d} > 0$$

(和之前一样，其他类似的定义也可以，具体是哪个定义并不重要)。如果对于每个有限集  $F \subset \mathbb{Z}^d$ ，存在  $a \in \mathbb{Z}^d$  和  $t \in \mathbb{Z}_{>0}$ ，使得  $a + t \cdot F = \{a + tx : x \in F\}$  包含在  $A$  中，则我们称  $A$  包含任意“星座”，换句话说， $A$  包含每个有限模式（也就是“星座”），每个模式都由允许扩张和平移的整数网格的某个有限子集组成。Furstenberg 和 Katznelson 最初使用遍历理论证明了 Szemerédi 定理的以下多维推广 (1978)，尽管后来由前面提到的超图正则性方法可以得到一个组合证明。

**定理 1.8 (多维 Szemerédi 定理)**

$\mathbb{Z}^d$  正上密度的每个子集都包含任意星座。



例如，该定理意味着  $\mathbb{Z}^d$  的每个正上密度的子集都包含  $10 \times 10$  的一组点，这些点形成了一个轴对齐的方形网格。Szemerédi 定理还有一个多项式扩展。让我们首先陈述一个它的特例。这个特例最初由 Lovász 猜想并由 Furstenberg (1977) 和 Sárközy (1978) 独立证明。

**定理 1.9**

具有正上密度的整数的任何子集都包含差是完全平方数的两个数字。



换句话说，对于某  $x \in \mathbb{Z}$  和  $y \in \mathbb{Z}_{>0}$ ，该集合总是包含  $\{x, x + y^2\}$ 。其他多项式形式呢？Bergelson 和 Leibman 证明了以下多项式推广 (1996)。

**定理 1.10 (多项式 Szemerédi 定理)**

假设  $A \subset \mathbb{Z}$  具有正的上密度。如果  $P_1, \dots, P_k \in \mathbb{Z}[X]$  是多项式，其中  $P_1(0) = \dots = P_k(0) = 0$ ，则存在  $x \in \mathbb{Z}$  和  $y \in \mathbb{Z}_{>0}$  使得  $x + P_1(y), \dots, x + P_k(y) \in A$ 。



<sup>3</sup>译者注：即 Structure vs Randomness，也就是为了证明我们的结论，将某个数学对象分为两种情况。一种情况下它有特殊的结构，可以用结构的性质来证明我们的结论。另一种情况下，它和随机的情形相似，可以用伪随机性来证明我们想要的结论。从而结合起来，即可证明我们的结论在任意情况下成立。

我们把表述两个定理的共同扩展留作练习（即多维多项式 Szemerédi 定理），这个定理也被 Bergelson 和 Leibman 证明过了。

我们不会介绍定理 1.8 和 1.10 的证明。事实上，目前唯一已知的多项式 Szemerédi 定理的一般证明需要使用遍历理论，尽管如此，最近在特殊情形下有一些令人兴奋的发展。

基于 Szemerédi 定理以及数论的其他重要发展，Green 和 Tao 证明了他们著名的定理（2008），该定理解决了关于素数口耳相传的古老猜想。他们的定理被认为是本世纪最著名的数学成果之一。

#### 定理 1.11 (Green-Tao 定理)

素数包含任意长度的等差数列。



我们将讨论 Green-Tao 定理证明背后的许多核心思想。请参阅参考资料 (Conlon, Fox, and Zhao 2014)，来了解 Green-Tao 定理从图论观点的现代阐述，以及自原始工作以来发现的一些证明上的简化。

## 1.3 然后呢?

我们的目标之一是理解 Roth 定理的两种不同证明，Roth 定理可以改写为：

#### 定理 1.12 (Roth 定理)

$[N]$  中不包含长度为 3 的等差数列的子集的大小一定为  $o(N)$ 。



Roth 最初使用傅立叶分析技术证明了他的结果，我们将在本书的后半部分看到。1978 年，在 Szemerédi 证明其具有里程碑意义的结果之前，Szemerédi 提出了一个称为图正则性引理的重要工具。Ruzsa 和 Szemerédi 使用图正则性引理给出了 Roth 定理的新图论证明（1978）。我们的首要目标之一是理解这个图论证明。正如在 Schur 定理的证明中一样，我们将构造一个图论问题，解决了该问题就意味着解决了 Roth 定理。这一话题应当称为组合学领域中的极值图论，极值图论的起源（历史上和教学上）是以下问题：

**问题 1.1**  $n$  顶点的 triangle-free 图最多可以有多少条边？

这个问题相对简单，Mantel 在 20 世纪早期回答了这个问题（后来被 Turán 重新发现和概括）。这将是我们要解决的第一个问题。然而，尽管听起来与 Roth 定理相似，但它不能用于推导出 Roth 定理。稍后，我们将构建一个对应于 Roth 定理的图，正确的问题是：

**问题 1.2** 每条边都包含在一个唯一三角形中的  $n$  顶点图的最大边数是多少？

这个看似简单的问题竟然是不可思议的神秘。我们离了解真相还很远。我们稍后将使用 Szemerédi 的正则性引理证明，任何这样的图都必须有  $o(n^2)$  边，然后我们将从这个图论断言中推导出 Roth 定理。



# 第一部分

## 图论

## 第2章 禁止子图

### 2.1 Mantel 定理：禁止三角形

我们从以下基本问题开始讨论极值图论。

**问题 2.1** 不包含三角形 (triangle-free) 的  $n$  个点的图中，最多有多少条边？

注意二分图总是 triangle-free 的，而一个完全二分图最多有  $\lfloor n^2/4 \rfloor$  条边（这个完全二分图两侧的点数相同或至多相差一个点）。Mantel 定理指出，triangle-free 的图不能有比这更多的边。

#### 定理 2.1 (Mantel 1907)

任意  $n$  顶点 triangle-free 图最多有  $\lfloor n^2/4 \rfloor$  条边。

我们将给出定理 2.1 的两个不同版本的证明。

**证明** [版本 1] 令  $G = (V, E)$  表示一个具有  $n$  个顶点和  $m$  条边的 triangle-free 图。观察到如果两个点  $x, y \in V$  之间有边  $xy \in E$ ，那么  $x$  和  $y$  不能和同一个点相邻。因此， $d(x) + d(y) \leq n$ ，这意味着

$$\sum_{x \in V} d(x)^2 = \sum_{xy \in E} (d(x) + d(y)) \leq mn$$

第一个等号成立是因为每个顶点对等式右边的贡献也是该顶点度数的平方。另一方面，根据握手引理<sup>1</sup>， $\sum_{x \in V} d(x) = 2m$ 。根据 Cauchy-Schwarz 不等式和上面的方程可以得到

$$4m^2 = \left( \sum_{x \in V} d(x) \right)^2 \leq n \left( \sum_{x \in V} d(x)^2 \right) \leq mn^2$$

因此  $m \leq n^2/4$ 。由于  $m$  是一个整数，所以我们有  $m \leq \lfloor n^2/4 \rfloor$ 。

**证明** [版本 2] 令  $G = (V, E)$  和上面一样。由于  $G$  是 triangle-free 的，所以每个顶点  $x \in V$  的所有邻点  $N(x)$  是一个独立集<sup>2</sup>。

令  $A \subseteq V$  是最大独立集。然后对所有  $x \in V$ ，我们有  $d(x) \leq |A|$ 。令  $B = V \setminus A$ 。由于  $A$  的顶点之间无连边， $G$  的每条边都与  $B$  中的顶点相连，所以，

$$\begin{aligned} e(G) &\leq \sum_{x \in B} d(x) \leq |A||B| \\ &\leq_{\text{AM-GM}} \left\lfloor \left( \frac{|A| + |B|}{2} \right)^2 \right\rfloor = \left\lfloor \frac{n^2}{4} \right\rfloor \end{aligned}$$



**笔记** 为了使 Mantel 定理中的等号成立，在上面的证明中，我们必须有

- $e(G) = \sum_{x \in B} d(x)$ ，这意味着没有两端点都在  $B$  中的边。
- $\sum_{x \in B} d(x) = |A||B|$ ，这（与上一条一起）意味着  $B$  中的每个顶点与都与  $A$  中所有顶点相连。
- AM-GM 中的相等情况必须成立（或几乎成立，也就是当  $n$  为奇数时的情况），因此  $\left| |A| - |B| \right| \leq 1$ 。

因此， $n$  顶点上的 triangle-free 图恰好具有  $\lfloor n^2/4 \rfloor$  边当且仅当它是完全二分图  $K_{\lfloor n/2 \rfloor, \lfloor n/2 \rfloor}$ 。

### 2.2 Turán 定理：禁止团<sup>3</sup>

受定理 2.1 的启发，我们转向以下更一般性的问题。

**问题 2.2** 不包含  $K_{r+1}$  ( $K_{r+1}$ -free，这里  $K_{r+1}$  是指  $r+1$  个点的团) 的  $n$  个点的图中，最多能有多少条边？

<sup>1</sup>handshake lemma: 任意无向图  $G$  的所有顶点的度数之和等于两倍边的数目。

<sup>2</sup>独立集是指图  $G$  中两两互不相邻的顶点构成的集合。

<sup>3</sup>无向图中满足两两之间有边连接的顶点的集合，称为该无向图中的团 (clique)。

扩展之前的二分图（二部图）结构，我们容易看到  $r$  部图不包含  $K_{r+1}$ 。

### 定义 2.1

我们定义 Turán 图  $T_{n,r}$  是  $n$  个顶点的完全  $r$  部图，其中每个部分的顶点数都为  $\lfloor \frac{n}{r} \rfloor$  或  $\lceil \frac{n}{r} \rceil$ 。

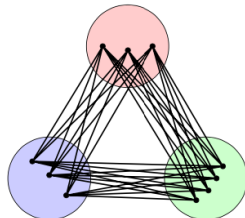


图 2.1: Turán 图  $T_{10,3}$

在本节我们将证明  $T_{n,r}$  确实最大化了  $K_{r+1}$ -free 图中的边数：

### 定理 2.2 (Turán)

如果  $G$  是  $n$  个顶点的  $K_{r+1}$ -free 图，则  $e(G) \leq e(T_{n,r})$ 。

当  $r = 2$  时，这就是定理 2.1。我们现在给出定理 2.2 的三个证明，其中前两个与 Mantel 定理（定理 2.1）的证明思路相同。

#### 证明 [版本 1]

固定  $r$ ，我们对  $n$  进行归纳。注意到如果  $n \leq r$ ，命题是不言自明的（因为  $K_n$  是  $K_{r+1}$ -free 的）。现在我们假设  $n > r$  并且 Turán 定理对于所有少于  $n$  个顶点的图都成立。令  $G$  是一个  $n$  个顶点的  $K_{r+1}$ -free 图，并且具有尽可能最多的边数。请注意， $G$  必须包含子图  $K_r$ ，否则我们可以在  $G$  中添加任意一条边使其仍然是  $K_{r+1}$ -free 的。令  $A$  是  $G$  中  $r$ -clique（大小为  $r$  的团）的顶点集，令  $B := V \setminus A$ 。由于  $G$  是  $K_{r+1}$ -free 的，每个  $v \in B$  在  $A$  中至多有  $r - 1$  个邻点。所以

$$\begin{aligned} e(G) &\leq \binom{r}{2} + (r-1)|B| + e(B) \\ &\leq \binom{r}{2} + (r-1)(n-r) + e(T_{n-r,r}) \\ &= e(T_{n,r}) \end{aligned}$$

第一个不等式来自计算  $AB$  的边以及它们之间的所有边的数量。第二个不等式来自归纳假设。最后一个等式成立是因为如果从  $T_{n,r}$  的  $r$  个部分中每个删去一个顶点，总共将会删去和这些点相连的  $\binom{r}{2} + (r-1)(n-r)$  条边。

#### 证明 [版本 2, Zykov symmetrization]

和之前一样，令  $G$  是一个  $n$  个顶点， $K_{r+1}$ -free 且尽可能边数最大的图。我们断言  $G$  的“非边”形成等价关系：也就是说，如果  $xy, yz \notin E$ ，那么  $xz \notin E$ 。对称性和自反性很容易检验。为了检查传递性，考虑反面，假设存在  $x, y, z \in V$  其中  $xy, yz \notin E$  但  $xz \in E$ 。

如果  $d(y) < d(x)$ ，我们可以用  $x$  的“克隆”替换  $y$ 。也就是说，我们删除  $y$  并添加一个新顶点  $x'$ ，它的邻点集正好是  $x$  的邻点集（并且  $x$  和  $x'$  之间没有边），如下图。

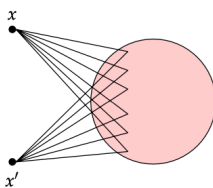


图 2.2:  $x$  和它的“克隆” $x'$

显然, 替换后得到的图  $G'$  也是  $K_{r+1}$ -free 的。另一方面, (因为  $xy \notin E$ )  $G'$  比  $G$  有更多的边, 这与  $G$  的边数尽可能最大的前提矛盾。

因此, 对于所有的  $xy \notin E$ , 我们有  $d(y) \geq d(x)$ 。类似地, 因为  $yz \notin E$ , 我们有  $d(y) \geq d(z)$ 。现在, 用  $y$  的“克隆”替换  $x$  和  $z$  得到新的图  $G'$  是  $K_{r+1}$ -free 的 (因为  $y$  不在任何子图  $K_{r+1}$  中)。而且有

$$e(G') = e(G) - (d(x) + d(z) - 1) + 2d(y) > e(G)$$

与  $e(G)$  是最大值相矛盾。因此这样的三元组  $(x, y, z)$  在  $G$  中不存在, 传递性成立。

这种等价关系表明  $G$  的补集是由若干个团组成的。因此  $G$  是一个完全多部图, 从而最多包含  $r$  个部分。容易验证, 增加部的数量会增加  $G$  中的边数。类似地, 如果两个部分的顶点数相差超过 1, 将一个顶点从较大部分移动到较小部分会增加  $G$  中的边数。由此可知, 达到最大边数的图为  $T_{n,r}$ 。

我们的第三个也是最后一个证明使用了一种叫做概率方法 (probabilistic method) 的技术。在这种方法中, 人们以一种巧妙的方式将随机性引入确定性问题来得到一个确定性的结果。

**证明** [版本 3] 令  $G = (V, E)$  是一个  $n$  顶点  $K_{r+1}$ -free 图。考虑一个均匀随机的顶点排列  $\sigma$ 。令

$$X = \{v \in V : v \text{ 与 } \sigma \text{ 中所有早于 } v \text{ 出现的顶点相邻}\}$$

观察到  $X$  中的顶点集形成一个团。由于排列是均匀随机选择的, 我们有

$$\mathbb{P}(v \in X) = \mathbb{P}(v \text{ 出现在其所有不相邻顶点之前}) = \frac{1}{n - d(v)}$$

所以,

$$r \geq \mathbb{E}[|X|] = \sum_{v \in V} \mathbb{P}(v \in X) = \sum_{v \in V} \frac{1}{n - d(v)} \stackrel{\text{convexity}}{\geq} \frac{n}{n - 2m/n}$$

整理得到  $m \leq \left(1 - \frac{1}{r}\right) \frac{n^2}{2}$  (一个已经适用于大多数情况的的上界)。请注意, 当  $n$  可以被  $r$  整除时, 这个不等式立即给出了 Turán 定理的证明。当  $n$  不能被  $r$  整除时, 我们需要借助凸性做更多的工作来论证  $d(v)$  应该尽可能接近  $\frac{2m}{n}$ , 我们省略相关细节。

## 2.3 超图<sup>4</sup>上的 Turán 问题

前几节给出的简短证明使极值图论中的问题看似简单。实际上, 我们刚才讨论许多的内容的一般性版本仍然是开放性问题。在这里, 我们叙述一个以困难而著称的开放性问题, 即 Mantel/Turán 的超图版本。

我们定义一个  $r$ -uniform 的超图由一个顶点集  $V$  和一个边集  $E$  组成, 其中  $E$  里的每条边现在都是  $V$  的  $r$  个元素构成的子集。普通的图就对应了 2-uniform 的超图。

**问题 2.3** 没有四面体<sup>5</sup>的  $n$  个顶点的 3-uniform 超图中, 最多有多少条边 (也就是  $E$  中的三元组个数)?

Turán 提出了以下构造, 并推测它是最优的。

### 命题 2.1 (Turán)

令  $V$  是一组  $n$  个顶点集。将  $V$  分成 3 个 (大致) 相等的集合  $V_1, V_2, V_3$ 。添加一个三元组  $\{x, y, z\}$  到  $e(G)$  如果它满足以下四个条件之一:

- $x, y, z$  在不同的分区
- $x, y \in V_1$  且  $z \in V_2$
- $x, y \in V_2$  且  $z \in V_3$
- $x, y \in V_3$  且  $z \in V_1$

请读者自行检验所构建的 3-uniform 超图是否无四面体, 并且边密度<sup>6</sup>为  $5/9$ 。

<sup>4</sup>超图 (Hypergraph) 是图的推广, 超图一个边可以连接任意数量的顶点。相比之下, 在普通的图中, 一条边正好连接两个顶点。

<sup>5</sup>译者注: 即四个点, 他们之间连了  $\binom{4}{3}$  条超图的边

<sup>6</sup>译者注: 边密度是指  $\lim_{n \rightarrow \infty} m(n)/\binom{n}{3}$ 。这里  $n$  是点数,  $m(n)$  是所构造的  $n$  个点的图中的边数。

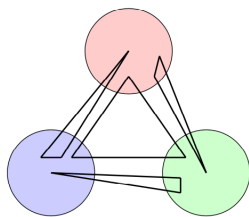


图 2.3: Turán 构造的四面体-free 3-uniform 超图

另一方面，最著名的密度上限约为 0.562，这是最近使用旗代数（Flag Algebras）技术得到的。

## 2.4 Erdős-Stone-Simonovits 定理：禁止一般子图

（除了超图以外）人们可能还想知道，如果定理 2.2 中的  $K_{r+1}$  被替换为任意图  $H$  会发生什么：

**问题 2.4** 固定图  $H$ 。如果  $G$  是一个  $n$  顶点图，并且  $H$  不在其中作为子图出现，那么  $G$  最多有多少条边？

### 定义 2.2

对于图  $H$  和  $n \in \mathbb{N}$ ，将  $\text{ex}(n, H)$  定义为  $n$  顶点  $H$ -free 图的最大边数。

例如，定理 2.2 告诉我们对于任何给定的  $r$ ，

$$\text{ex}(n, K_{r+1}) = e(T_{n,r}) = \left(1 - \frac{1}{r} + o(1)\right) \binom{n}{2}$$

乍一看，人们可能不会期望问题 2.4 有一个明确的答案。实际上，该解决方案似乎取决于  $H$  的各种特征（例如，其直径<sup>7</sup>或最大度数）。令人惊讶的是，一个单一的参数—— $H$  的色数，控制着  $\text{ex}(n, H)$  的增长。

### 定义 2.3

图  $G$  的色数  $\chi(G)$ ，是给  $G$  的顶点着色所需的最小颜色数。其中，一个着色方案必须满足任意两个相邻的顶点具有不同的颜色。

轻而易见的， $\chi(K_{r+1}) = r + 1$  和  $\chi(T_{n,r}) = r$ 。

可以观察到，如果  $H \subseteq G$ ，则  $\chi(H) \leq \chi(G)$ 。实际上，当  $H \subseteq G$ ， $G$  的任意正确着色都是  $H$  的一个正确着色（也就是说如果  $\chi(H) > \chi(G)$ ，则  $H \not\subseteq G$ ）。由此，我们得出如果  $\chi(H) = r + 1$ ，则  $T_{n,r}$  是  $H$ -free 的。所以，

$$\text{ex}(n, H) \geq e(T_{n,r}) = \left(1 - \frac{1}{r} + o(1)\right) \binom{n}{2}$$

这是我们能做的最好的结果吗？答案是肯定的。

### 定理 2.3 (Erdős-Stone-Simonovits 1966)

对于任意图  $H$ ，我们有

$$\lim_{n \rightarrow \infty} \frac{\text{ex}(n, H)}{\binom{n}{2}} = 1 - \frac{1}{\chi(H) - 1}$$

我们暂时跳过证明。

**笔记** 在本书的后面，我们将展示如何使用 Szemerédi 正则性引理从定理 2.2 推导出定理 2.3。

当  $H = K_3$  时，定理 2.3 告诉我们

$$\lim_{n \rightarrow \infty} \frac{\text{ex}(n, H)}{\binom{n}{2}} = \frac{1}{2}$$

<sup>7</sup>顶点  $v$  的偏心率 (eccentricity)，用来表示连接图  $G$  中的顶点  $v$  到图  $G$  中其它顶点之间的最大距离，用符号  $\epsilon_G(v)$  表示。图的直径 (diameter)，表示取遍图的所有顶点，得到的偏心率的最大值，记作  $\text{diam}(G)$ 。



符合定理 2.2。当  $H = K_4$  时，我们得到

$$\lim_{n \rightarrow \infty} \frac{\text{ex}(n, H)}{\binom{n}{2}} = \frac{2}{3}$$

也符合定理 2.2。当  $H$  是 Peterson 图（图 2.4）时，定理 2.3 告诉我们

$$\lim_{n \rightarrow \infty} \frac{\text{ex}(n, H)}{\binom{n}{2}} = \frac{1}{2}$$

这与  $H = K_3$  的答案相同！这令人惊讶，因为 Peterson 图似乎比三角形复杂得多。

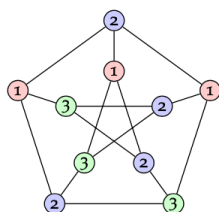


图 2.4: 一个 Peterson 图的 3-着色方案

## 2.5 Kovári-Sós-Turán 定理：禁止完全二分图

Erdős-Stone-Simonovits 定理（定理 2.3）给出了当  $\chi(H) > 2$  时  $\text{ex}(n, H)$  的一阶近似。不幸的是，定理 2.3 还并不完整。例如当  $\chi(H) = 2$  时，也就是  $H$  是二分图时，定理 2.3 告诉我们  $\text{ex}(n, H) = o(n^2)$ ，这就迫使我们询问是否可以获得更精确的界限？如果我们将  $\text{ex}(n, H)$  写成  $n$  的函数，它相对于  $n$  的增长是怎样的？对于大多数二分图（例如， $K_{4,4}$ ）这是一个未完全解决的问题，也是本章其余部分的重点。

令  $K_{s,t}$  是完全二分图，其中二分图的两部分分别有  $s$  个点和  $t$  个点。在本节中，我们考虑  $\text{ex}(n, K_{s,t})$ ，并试图回答以下主要问题：

**问题 2.5 (Zarankiewicz)** 对于  $s, t \geq 1$ ，不包含子图  $K_{s,t}$  的  $n$  顶点图的最大边数是多少？

每个二分图  $H$  都是某个完全二分图  $K_{s,t}$  的子图。如果  $H \subseteq K_{s,t}$ ，那么  $\text{ex}(n, H) \leq \text{ex}(n, K_{s,t})$ 。因此，如果得到了禁止完全二分图的极值的上界，那么它也是禁止一般二分图的极值的一个上界。稍后我们将给出几个禁止特定二分图的改进上界。Kövari、Sós 和 Turán 给出了禁止  $K_{s,t}$  时的上限：

### 定理 2.4 (Kövari-Sós-Turán 1954)

对于任意整数  $1 \leq s \leq t$ ，都存在常数  $C$ ，使得

$$\text{ex}(n, K_{s,t}) \leq Cn^{2-\frac{1}{s}}$$

**证明** 令  $G$  是一个  $K_{s,t}$ -free 的  $n$  顶点  $m$  边图。

首先，我们删除所有  $d(v) < s-1$  的顶点  $v \in V(G)$ 。由于我们以这种方式最多只删除  $(s-2)n$  条边（阶数为 1，小于  $2 - \frac{1}{s}$ ），因此假设所有顶点的度数至少为  $s-1$  对该命题没有影响。

我们将  $G$  中  $K_{s,1}$  的数量记作  $\#K_{s,1}$ 。我们用算两次的方法，以两个方式分别给出  $\#K_{s,1}$  的上界和下界，然后结合上界和下界得到  $m$  的上界。<sup>8</sup>

由于  $K_{s,1}$  是一个完整的二分图，我们可以将有  $s$  个顶点的一侧称为“左侧”，将有 1 个顶点的一侧称为“右侧”。

一方面，我们可以通过枚举“左侧”计算  $\#K_{s,1}$ 。对于任何  $s$  个顶点的子集，以这  $s$  个顶点作为“左侧”的  $K_{s,1}$  的数量正是这  $s$  个顶点的公共邻点的数量。由于  $G$  是  $K_{s,t}$ -free 的， $s$  个顶点的任何子集的公共邻点数最多

<sup>8</sup>译者注：证明的思想如下，我们希望证明图中的边数不会太多，如果边数太多那么每个点度数都会比较大，从而会有很多子图  $K_{s,1}$  以这个点作为“右侧”。而因为禁止了  $K_{s,t}$ ， $G$  中的子图  $K_{s,1}$  不能太多，这是因为以任意  $s$  个点作为“左侧”，都最多会有  $t-1$  个这样的子图。从而就证明了图中的边数不能太多。

为  $t-1$ 。因此，我们有  $\#K_{s,1} \leq \binom{n}{s}(t-1)$ 。

另一方面，对于每个“右侧”顶点  $v \in V(G)$ ， $K_{s,1}$  的数量正好是  $\binom{d(v)}{s}$ 。因此

$$\#K_{s,1} = \sum_{v \in V(G)} \binom{d(v)}{s} \geq n \binom{\frac{1}{n} \sum_{v \in V(G)} d(v)}{s} = n \binom{2m/n}{s}$$

其中不等号成立是因为  $x \mapsto \binom{x}{s}$  在  $[s-1, +\infty)$  上的凸性。结合  $\#K_{s,1}$  的上界和下界，我们得到  $n \binom{2m/n}{s} \leq \binom{n}{s}(t-1)$ 。

对于常量  $s$ ，我们可以使用  $\binom{x}{s} = (1+o(1))\frac{x^s}{s!}$ ，从而得到  $n \left(\frac{2m}{n}\right)^s \leq (1+o(1))n^s(t-1)$ 。该不等式简化为

$$m \leq \left(\frac{1}{2} + o(1)\right) (t-1)^{1/s} n^{2-\frac{1}{s}}$$

现在让我们讨论定理 2.4 在几何上的应用。

**问题 2.6(单位距离问题)**  $\mathbb{R}^2$  上的  $n$  个点中，最多有多少点对之间距离为 1？

给定  $n$  个点，我们将距离为 1 的点对个数称为单位距离数。

当  $n$  取较小的值，我们精确地知道单位距离问题的答案。图 2.5 列出了最佳方案。可以将这些结构中的一些推广到任意  $n$ 。

- 直线图<sup>9</sup>的单位距离数是  $(n-1)$ 。
- 对于  $n \geq 3$ ，三角形链的单位距离数是  $(2n-3)$ （图 2.5 中  $n=3$ 、 $n=5$ ）。
- 我们还有一个递归构造。给定  $n/2$  个点的方案  $P$  具有  $f(n/2)$  单位距离，我们可以复制  $P$  得到  $P'$  并用单位向量与其连接。方案  $P \cup P'$  至少有  $2f(n/2) + n/2$  对单位距离。我们可以求解递归得到  $f(n) = \Omega(n \log n)$ 。

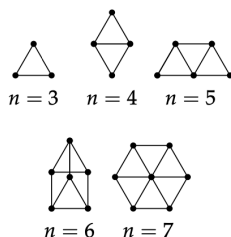


图 2.5: 注：除了  $n=6$ ，这些构造在同构前是唯一的

Erdős 给出了已知最大单位距离数的最佳下界（1946）。

### 命题 2.2

在  $\mathbb{R}^2$  中存在一组点 ( $n$  个)，对于某个常数  $c$ ，它们的单位距离数是  $n^{1+c/\log \log n}$ 。

### 证明 [概要]

考虑具有  $\lfloor \sqrt{n} \rfloor \times \lfloor \sqrt{n} \rfloor$  顶点的单位方形网格。对于任意整数  $r$ ，我们可以都把图形缩小  $\sqrt{r}$  倍，所以我们只要最大化距离为  $\sqrt{r}$  的点对数量即可。由勾股定理，我们应该选择可以多种不同的方式表示为两个平方的和的  $r$ 。 $r$  的一个合适候选是许多模 4 余 1 的素数的乘积。我们可以使用一些数论定理来分析最佳的  $r$ ，并得到下界  $n^{1+c/\log \log n}$ 。

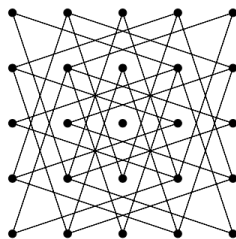


图 2.6: An example grid graph where  $n=25$  and  $r=10$ .

<sup>9</sup>即第  $i$  个点的坐标是  $(i, 0)$

定理2.4 可用于证明单位距离数的上限。

### 定理 2.5

$\mathbb{R}^2$  中的每组点 ( $n$  个) 单位距离数最多为  $O(n^{3/2})$ 。

**证明** 给定任意一组点  $S \subset \mathbb{R}^2$ ，我们可以创建单位距离图  $G$  如下：

- $G$  的顶点集是  $S$ 。
- 对于任意  $d(p, q) = 1$  的点  $p, q$ ，我们在  $p$  和  $q$  之间添加一条边。

因为对于每对点  $p, q$ ，至多有 2 个点与它们都有单位距离（见图 2.7），所以图  $G$  是  $K_{2,3}$ -free 的。通过应用定理2.4，我们得到  $e(G) = O(n^{3/2})$

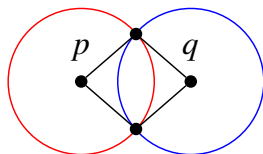


图 2.7: 单位距离图中顶点  $p, q$  最多有两个共同邻点

**笔记** 最著名的单位距离数上界是  $O(n^{4/3})$  (Spencer, Szemerédi and Trotter 1984)。

下面是另一个与单位距离问题密切相关的问题：

**问题 2.7(不同距离问题)** 由  $\mathbb{R}^2$  中的  $n$  个点形成的不同距离的最少有多少种？

**例题 2.1** 考虑  $x$  轴上的  $n$  个点，其中第  $i$  个点的坐标为  $(i, 0)$ ，这些点的不同距离的数量是  $n - 1$ 。

目前最小不同距离的最佳构造也是由网格图给出的。考虑具有  $\lfloor \sqrt{n} \rfloor \times \lfloor \sqrt{n} \rfloor$  顶点的方形网格。两个顶点之间可能的距离是可以表示为两个最多为  $\lfloor \sqrt{n} \rfloor$  的数的平方和。借助数论的知识，我们可以得到不同距离数是  $\Theta(n/\sqrt{\log n})$  的。注意到，不同距离数和单位距离数之间有以下关系：

$$\text{\#distinct distances} \geq \frac{\binom{n}{2}}{\max \text{\#unit distances}}$$

如果我们将定理2.5应用于上述不等式，我们立即得到不同距离数的下界  $\Omega(n^{0.5})$ 。许多数学家在七年的时间里相继改进了这个下界的指数。最近，Guth 和 Katz 给出了下面这个著名的定理，它几乎与上界相匹配（仅相差  $O(\sqrt{\log n})$ ）。

### 定理 2.6 (Guth-Katz 2015)

$\mathbb{R}^2$  中的任意组点 ( $n$  个)，对于某些常数  $c$ ，至少有  $cn/\log n$  个不同的距离。

定理2.6 的证明非常复杂，它使用了包括多项式方法、代数几何等各种工具，我们不会在本书中介绍它<sup>10</sup>。

## 2.6 下界：随机构造

我们推测定理2.4的上界是紧的。换句话说， $\text{ex}(n, K_{s,t}) = \Theta(n^{2-1/s})$ 。尽管对于任意的  $K_{s,t}$  问题仍然是开放的，但它已经在一些  $t$  远大于  $s$  的案例中得到了证明。在本节和接下来的两节中，我们将展示构造  $H$ -free 图的技术。以下是我们将介绍的三种主要结构类型：

- 随机构造。这种方法强大且通用，但引入随机性意味着构造得到的界通常是不紧的。
- 代数构造。这种方法使用数论或代数中的工具来辅助构造。它给出了更紧的结果，但它们通常是“奇妙的”并且只适用于一小部分情况。
- 随机代数构造。这种方法是上述两种方法的混合，结合了两者的优点。

<sup>10</sup>译者注：Terry Tao 有一篇博客介绍了这个证明的基本思路。

<https://terrytao.wordpress.com/2010/11/20/the-guth-katz-bound-on-the-erdos-distance-problem/>

本节将重点介绍随机结构。我们从极值的一般下界开始。

### 定理 2.7

对于任何至少有 2 条边的图  $H$ ，令  $e(H)$  为  $H$  的边数， $v(H)$  为  $H$  的点数，存在一个常数  $c > 0$ ，使得对于任意  $n \in \mathbb{N}$ ，存在具有至少  $cn^{2-\frac{v(H)-2}{e(H)-1}}$  条边的  $n$  顶点  $H$ -free 图。换句话说，

$$\text{ex}(n, H) \geq cn^{2-\frac{v(H)-1}{e(H)-2}}$$

♡

**证明** 证明的想法是使用 **alteration method**：我们可以构建一个图使其与  $H$  同构的子图很少，然后我们在每个这样的子图中删除一条边，从而消除其中所有  $H$ 。

令  $G = G(n, p)$  为  $n$  顶点的随机图，其中任意两点间存在边的概率为  $p$  ( $p$  待定)<sup>11</sup>。令  $\#H$  为  $G$  中与  $H$  同构的子图个数。然后，

$$\mathbb{E}[\#H] = \frac{n(n-1) \cdots (n-v(H)+1)}{|\text{Aut}(H)|} p^{e(H)} \leq p^{e(H)} n^{v(H)}$$

其中  $\text{Aut}(H)$  是图  $H$  的自同构群<sup>12</sup>，并且

$$\mathbb{E}[e(G)] = p \binom{n}{2}$$


令  $p = \frac{1}{2} n^{-\frac{v(H)-2}{e(H)-1}}$ ，此时满足

$$\mathbb{E}[\#H] \leq \frac{1}{2} \mathbb{E}[e(G)]$$

进一步有

$$\mathbb{E}[e(G) - \#H] \geq \frac{1}{2} p \binom{n}{2} \geq \frac{1}{16} n^{2-\frac{v(H)-2}{e(H)-1}}$$

因此，存在一个图  $G$ ，使得  $(e(G) - \#H)$  的值至少是期望值。从  $G$  中  $H$  的每个副本中删除一条边，我们得到一个满足条件的  $H$ -free 图。

 **笔记** 例如，如果  $H$  是下图

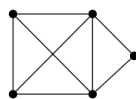


图 2.8

根据定理 2.7 我们有

$$\text{ex}(n, H) \gtrsim n^{11/7}$$

但是，如果我们禁止  $H$  的子图  $K_4$ （禁止  $H$  的子图将自动禁止图  $H$ ），定理 2.7 实际上给了我们一个更好的下界：

$$\text{ex}(n, H) \geq \text{ex}(n, K_4) \gtrsim n^{8/5}$$

对于一般的  $H$ ，我们将定理 2.7 应用于使  $(e-1)/(v-2)$  取值最大的子图。为此，我们定义  $H$  的 2-密度

$$m_2(H) := \max_{\substack{H' \subset H \\ v(H') \geq 3}} \frac{e(H') - 1}{v(H') - 2}$$

我们有以下推论。

### 推论 2.1

对于任何具有至少两条边的图  $H$ ，存在常数  $c = c_H > 0$  使得

$$\text{ex}(n, H) \geq cn^{2-1/m_2(H)}$$

♡

<sup>11</sup> $G(n, p)$  对应的随机图模型叫做 *Erdős-Rényi random graph*。

<sup>12</sup>一个图的自同构，是顶点的一个置换，使得边与非边保持不变：两个顶点若有边连接，则在置换下这两顶点的像有边连接，反之亦然。

**例题 2.2** 我们将上述下界与 KőváriSós-Turán 定理（定理 2.4）的上界结合，得到：对于任意的  $2 \leq s \leq t$ ,

$$n^{2-\frac{s+t-2}{st-1}} \lesssim \text{ex}(n, K_{s,t}) \lesssim n^{2-1/s}$$

当  $t$  远大于  $s$  时，上述两个边界中的指数彼此接近（但永远不会相等）。当  $t = s$  时，有不等式

$$n^{2-\frac{2}{s+1}} \lesssim n^{2-\frac{s+t-2}{st-1}} \lesssim n^{2-1/s}$$

特别地，对于  $s = 2$ ，我们得到

$$n^{4/3} \lesssim \text{ex}(n, K_{2,2}) \lesssim n^{3/2}$$

事实上，这里的上界是比较紧的，接下来我们将展示一个基于代数方法的  $K_{2,2}$ -free 图构造。

## 2.7 下界：代数构造

在本节中，我们使用代数构造来寻找  $K_{s,t}$ -free 图，对于  $(s, t)$  的各种取值，这些构造都达到了 KőváriSós-Turán 定理（定理 2.4）中的上界（仅相差常数因子）。这种代数构造的最简单例子是下面关于  $K_{2,2}$ -free 图的构造。

### 定理 2.8 (Erdős-Rényi-Sós 1966)

$$\text{ex}(n, K_{2,2}) \geq \left(\frac{1}{2} - o(1)\right) n^{3/2}$$

**证明** 假设  $n = p^2 - 1$  其中  $p$  是素数。考虑下面的图  $G$ （称为 polarity 图）：

- $V(G) = \mathbb{F}_p^2 \setminus \{(0, 0)\}$
- $E(G) = \{(x, y) \sim (a, b) \mid ax + by = 1 \text{ in } \mathbb{F}_p\}$

对于任意两个不同的顶点  $(a, b) \neq (a', b') \in V(G)$ ，最多有一个解（公共邻点） $(x, y) \in V(G)$  满足  $ax + by = 1$  和  $a'x + b'y = 1$ 。因此， $G$  是  $K_{2,2}$ -free 的。

此外，每个顶点都有度数  $p$  或  $p - 1$ ，所以边的总数

$$e(G) = \left(\frac{1}{2} - o(1)\right) p^3 = \left(\frac{1}{2} - o(1)\right) n^{3/2}$$

这就完成了证明。如果对于某个素数  $n$  不具有  $p^2 - 1$  形式，那么我们让  $p$  是满足  $p^2 - 1 \leq n$  条件下最大的素数。我们有  $p = (1 - o(1)) n^{1/2}$ ，构造相同的图  $G_{p^2-1}$  并添加  $n - p^2 + 1$  个孤立顶点。

**笔记** 为什么叫作 polarity 图？您可以从下面二分图的角度考虑：其中一个顶点集是  $\mathbb{F}_p$  平面上（投影得到）的点集，另一个顶点集是同一平面中的线集。如果  $p \in \ell$ ，点  $p$  和线  $\ell$  之间有一条边。因为不存在两条线在两个不同的点相交的情况，所以该图是  $C_4$ -free 的。

定理 2.8 证明中的构造有一个用线当作点的顶点集。点和线之间的这种对偶配对在射影几何中被称作极性。

因为方程  $ax + by = 1$  正好有  $p$  个解  $(x, y)$ ，所以大多数顶点的度数为  $p$ 。有时我们必须减去 1，因为其中一个解可能是  $(a, b)$  本身，这导致了一个自环。

事实上，对于每个足够大的  $n$ ，在区间  $[n - n^{0.525}, n]$  中都存在一个素数<sup>13</sup>。

一个自然的问题是，上述构造是否可以推广。下一个例子为我们提供了  $K_{3,3}$ -free 图的构造。

### 定理 2.9 (Brown 1966)

$$\text{ex}(n, K_{3,3}) \geq \left(\frac{1}{2} - o(1)\right) n^{5/3}$$

**笔记** 定理 2.9 中的常数  $1/2$  是已知的最佳常数。

**证明** [概要] 令  $n = p^3$ ，其中  $p$  是素数。考虑如下图  $G$ ：

<sup>13</sup>译者注：您可以参考该著名结果的原文 Baker, Harman and Pintz: The difference between consecutive primes  
Terry Tao 博客有一篇讲述了相邻素数差的下界的研究进展：  
<https://terrytao.wordpress.com/2014/08/21/large-gaps-between-consecutive-prime-numbers/>



- $V(G) = \mathbb{F}_p^3$
- $E(G) = \{(x, y, z) \sim (a, b, c) \mid (ax)^2 + (by)^2 + (cz)^2 = u \text{ in } \mathbb{F}_p\}$ , 其中  $u$  是  $\mathbb{F}_p$  中精心挑选的固定非零元素。

我们需要检查是否可以选出使得上图为  $K_{3,3}$ -free 的  $u$ 。我们省略证明，但会给一些直观上的说明。如果我们使用  $\mathbb{R}^3$  上的点而不是  $\mathbb{F}_p^3$ ,  $K_{3,3}$ -free 等价于三个单位球至多有两个公共点。事实上，这个关于  $\mathbb{R}^3$  中单位球的陈述可以通过一些代数运算来严格证明。我们可以对  $\mathbb{F}_p$  进行类似的代数运算，验证上面的图中没有  $K_{3,3}$ 。

另外，每个顶点的度数大约为  $p^2$ ，因为  $(x, y, z) \in \mathbb{F}_p^3 \mapsto (ax)^2 + (by)^2 + (cz)^2$  在  $\mathbb{F}_p$  的取值上几乎是均匀随机的。因此我们预计大约有  $1/p$  占比的  $(x, y, z)$  满足  $(ax)^2 + (by)^2 + (cz)^2 = u$ ，我们再次省略相应细节。

尽管  $K_{2,2}$  和  $K_{3,3}$  的情况已经完全解决，但  $K_{4,4}$  的对应问题是极值图论中的核心开放问题。

**问题 2.8**  $ex(n, K_{4,4})$  的增长情况是怎么样的？是否与定理 2.4 中的上界相同 ( $\Theta(n^{7/4})$ )？

我们已经得到了 Kővári-Sós-Turán 定理具体到  $K_{2,2}$  和  $K_{3,3}$  的常数因子。现在我们提出一个与 Kővári-Sós-Turán 匹配的构造，但  $K_{s,t}$  中的  $t$  要远大于  $s$ 。

**定理 2.10 (Alon, Kollár, Rónyai, Szabó 1996 1999)**

如果  $t \geq (s-1)! + 1$ ，则

$$ex(n, K_{s,t}) = \Theta\left(n^{2-\frac{1}{s}}\right)$$

我们首先证明较弱版本： $t \geq s! + 1$ 。两者证明的思路是相似的，稍后我们将对证明细节进行调整从而得到我们之前想要的。取质数  $p$  和  $n = p^s$ ，其中  $s \geq 2$ 。考虑范数映射  $N: \mathbb{F}_{p^s} \rightarrow \mathbb{F}_p$

$$N(x) = x \cdot x^p \cdot x^{p^2} \cdots x^{p^{s-1}} = x^{\frac{p^s-1}{p-1}}$$

定义图  $\text{NormG}_{p,s} = (V, E)$

$$V = \mathbb{F}_{p^s}, \quad E = \{\{a, b\} \mid a \neq b, N(a+b) = 1\}$$

**命题 2.3**

$\text{NormG}_{p,s}$  的定义同上，顶点数为  $n = p^s$ ，

$$|E| \geq \frac{1}{2} n^{2-\frac{1}{s}}$$

**证明** 由于  $\mathbb{F}_{p^s}^\times$  是  $p^s - 1$  阶的循环群，我们有

$$\left| \{x \in \mathbb{F}_{p^s} \mid N(x) = 1\} \right| = \frac{p^s - 1}{p - 1}$$

因此，对于每个顶点  $x$  (减去一个顶点的自环  $N(x+x) = 1$ )

$$\deg(x) \geq \frac{p^s - 1}{p - 1} - 1 \geq p^{s-1} = n^{1-\frac{1}{s}}$$

我们得到了所需的边数的下界。

**命题 2.4**

$\text{NormG}_{p,s}$  是  $K_{s,s!+1}$ -free 图。

我们希望给出  $s$  个顶点的共同邻点数的上界。我们不加证明地引用下面的结论，该结论可以通过代数几何来证明。

**定理 2.11 (Kollár, Rónyai, and Szabó 1996)**

令  $\mathbb{F}$  是任意域,  $a_{ij}, b_i \in \mathbb{F}$  且对于所有  $i \neq i'$  满足  $a_{ij} \neq a_{i'j}$ 。则方程组

$$\begin{aligned}(x_1 - a_{11})(x_2 - a_{12}) \cdots (x_s - a_{1s}) &= b_1 \\(x_1 - a_{21})(x_2 - a_{22}) \cdots (x_s - a_{2s}) &= b_2 \\&\vdots \\(x_1 - a_{s1})(x_2 - a_{s2}) \cdots (x_s - a_{ss}) &= b_s\end{aligned}$$

在  $\mathbb{F}^s$  中至多有  $s!$  个解。



**笔记** 考虑所有  $b_i$  都是 0 的特殊情况。在这种情况下, 由于  $a_{ij}$  对于固定的  $j$  是不同的, 我们选择满足  $x_j = a_{ij}$  的  $i_j$ 。因为所有的  $i_j$  都是不同的, 这相当于在  $[s]$  上选择一个排列。因此, 正好有  $s!$  解决方案。

我们现在可以证明命题 2.4。

**证明** [命题 2.4] 考虑互不相同的  $y_1, y_2, \dots, y_s \in \mathbb{F}_{p^s}$ 。我们希望限制他们共同邻点  $x$  的数量。我们可以利用这样一个事实: 在具有特征  $p$  的域中, 我们有  $(x+y)^p = x^p + y^p$ , 从而对于所有  $1 \leq i \leq s$

$$\begin{aligned}1 &= N(x + y_i) = (x + y_i)(x + y_i)^p \cdots (x + y_i)^{p^{s-1}} \\&= (x + y_i)(x^p + y_i^p) \cdots (x^{p^{s-1}} + y_i^{p^{s-1}})\end{aligned}$$

根据定理 2.11, 这  $s$  个方程在  $x$  中最多有  $s!$  个解。之所以满足定理 2.11 的形式是因为在我们的域中  $y_i^p = y_j^p$  当且仅当  $y_i = y_j$ 。

现在我们进行调整来实现定理 2.10 中的  $t \geq (s-1)! + 1$ 。我们定义图  $\text{NormG}_{p,s} = (V, E)$ , 其中  $V = \mathbb{F}_{p^{s-1}} \times \mathbb{F}_p$  ( $s \geq 3$ )。易知  $n = (p-1)p^{s-1}$ 。定义两点之间边存在  $(X, x) \sim (Y, y)$  当且仅当

$$N(X + Y) = xy$$

**命题 2.5**

$\text{NormG}_{p,s}$  的定义同上, 顶点数为  $n$ , 显然  $n = (p-1)p^{s-1}$ , 则

$$|E| = \left(\frac{1}{2} - o(1)\right)n^{2-\frac{1}{s}}$$



**证明** 每个顶点  $(X, x)$  的邻点  $(Y, N(X+Y)/x)$  覆盖了  $\mathbb{F}_{p^{s-1}}$ 。减去自环后, 每个顶点的度数都为  $p^{s-1} - 1 = (1 - o(1))n^{1-1/s}$ 。

现在我们确定了边的数量, 我们只需要证明我们的图是  $K_{s, (s-1)!+1}$ -free 的。

**命题 2.6**

$\text{NormG}_{p,s}$  是  $K_{s, (s-1)!+1}$ -free 图。



**证明** 固定不同的  $(Y_i, y_i) \in V$ ,  $1 \leq i \leq s$ 。我们希望找到所有的共同邻点  $(X, x)$ 。考虑

$$N(X + Y_i) = xy_i$$

假设这个系统至少有一个解。如果  $Y_i = Y_j$  且  $i \neq j$ , 则必须有  $y_i = y_j$ 。因此, 所有  $Y_i$  都是不同的。对于每个  $i < s$  我们可以取  $N(X + Y_i) = xy_i$  并除以  $N(X + Y_s) = xy_s$  从而得到

$$N\left(\frac{X + Y_i}{X + Y_s}\right) = \frac{y_i}{y_s}$$

两边再除以  $N(Y_i - Y_s)$  ( $1 \leq i \leq s-1$ ) 得到

$$N\left(\frac{1}{X + Y_s} + \frac{1}{Y_i - Y_s}\right) = \frac{y_i}{N(Y_i - Y_s)y_s}$$

现在应用定理 2.11,  $X$  最多有  $(s-1)!$  个解, 这也意味着  $x = N(X + Y_1)/y_1$ 。因此, 至多有  $(s-1)!$  个共同的邻点。

最后, 我们来证明定理 2.10。

**证明** [定理2.10] 根据命题 2.5 和命题 2.6, 我们知道  $\text{NormG}_{p,s}$  是  $K_{s,(s-1)!+1}$ -free 并且有  $\left(\frac{1}{2} - o(1)\right)n^{2-\frac{1}{s}}$  条边。

## 2.8 下界：随机代数构造

到目前为止, 我们已经看到了使用随机图和代数结构的两种构造方法。在本节中, 我们将展示由 Bukh 提出的  $K_{s,t}$ -free 图的另一种构造 (2015), 对于某些函数  $t_0$ , 在  $t > t_0(s)$  条件下将有  $\Theta\left(n^{2-\frac{1}{s}}\right)$  条边。这是一个添加了一些随机性的代数结构。

首先, 固定  $s \geq 4$  并取一个素数  $q$ 。令  $d = s^2 - s + 2$ , 令  $f \in \mathbb{F}_q[x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_s]$  是一个在  $X = (x_1, x_2, \dots, x_s)$  和  $Y = (y_1, y_2, \dots, y_s)$  上所有阶数小于等于  $d$  的多项式中均匀随机选择一个多项式。将  $G$  的顶点集分为数量相等的两部分  $n = L = R = \mathbb{F}_q^s$ , 定义边关系为  $(X, Y) \in L \times R$  当且仅当  $f(X, Y) = 0$ 。

### 引理 2.1

对于所有  $u, v \in \mathbb{F}_q^s$  和如上所述随机选择的  $f$

$$\mathbb{P}[f(u, v) = 0] = \frac{1}{q}$$

**证明** 注意到如果  $g$  是  $\mathbb{F}_q$  上一个均匀随机选择的常数, 则  $f(u, v)$  和  $f(u, v) + g$  是同分布的。因此, 每个取值的概率都为  $1/q$ 。

现在边数的期望是我们想要的,  $\mathbb{E}[e(G)] = \frac{n^2}{q}$ 。我们还需要保证  $K_{s,t}$  的副本数较小。为此, 我们必须回答以下问题: 对于  $L$  中大小为  $s$  的一组顶点, 它可以有多少个共同的邻点?

### 引理 2.2

假设  $r, s \leq \min(\sqrt{q}, d)$ ,  $U, V \subset \mathbb{F}_q^s$  且  $|U| = s$  和  $|V| = r$ 。此外, 令  $f \in \mathbb{F}_q[x_1, x_2, \dots, x_s, y_1, y_2, \dots, y_s]$  是一个在  $X = (x_1, x_2, \dots, x_s)$  和  $Y = (y_1, y_2, \dots, y_s)$  上所有阶数小于等于  $d$  的多项式中均匀随机选出的一个多项式。则

$$\mathbb{P}[f(u, v) = 0 \text{ for all } u \in U, v \in V] = q^{-sr}$$

**证明** 首先让我们考虑  $U$  中所有点的第一个坐标都不同和  $V$  中所有点的第一个坐标都不同的特殊情况。定义

$$g(X_1, Y_1) = \sum_{\substack{0 \leq i \leq s-1 \\ 0 \leq j \leq r-1}} a_{ij} X_1^i Y_1^j$$

$a_{ij}$  是  $\mathbb{F}_q$  上独立同分布的均匀随机变量。我们要证明  $f$  和  $f+g$  具有相同的分布, 只需证明对于任意的  $b_{uv} \in \mathbb{F}_q$  ( $u \in U, v \in V$ ), 存在  $a_{ij}$  使得对于任意的  $u \in U, v \in V$  有  $g(u, v) = b_{uv}$ 。证明的思路是应用两次拉格朗日插值。首先, 任取一个  $u \in U$ , 我们可以找到一个阶数最多为  $r-1$  的单变量多项式  $g_u(Y_1)$  使得对于所有的  $v \in V$  有  $g_u(v) = b_{uv}$ 。然后我们可以将  $g(X_1, Y_1)$  看作  $Y_1$  的多项式, 其中系数是  $X_1$  中的多项式, 即,

$$g(X_1, Y_1) = \sum_{0 \leq j \leq r-1} a_j(X_1) Y_1^j$$

再次应用拉格朗日插值定理, 我们可以找到多项式  $a_0, a_1, \dots, a_{r-1}$  使得  $g(u, Y_1) = g_u(Y_1)$  对于所有的  $u \in U$  成立。

现在假设  $U$  中所有点的第一个坐标不一定都不同和  $V$  中所有点的第一个坐标不一定都不同。我们只需找到线性映射  $T, S: \mathbb{F}_q^s \rightarrow \mathbb{F}_q^s$  满足  $TU$  和  $SV$  像中所有点的第一个坐标都不同。下面让我们证明这样的映射  $T$  存在。如果我们找到一个线性映射  $T_1: \mathbb{F}_q^s \rightarrow \mathbb{F}_q^s$  将  $U$  的元素映射到不同的元素, 那么我们可以通过使用  $T_1$  作为第一个坐标将  $T_1$  扩展成  $T$ 。我们在所有线性映射中均匀随机的选择出  $T_1$ , 那么  $U$  中的每一对冲突的概率是  $\frac{1}{q}$ 。所以通过联合边界我们成功的概率至少是  $1 - \binom{|U|}{2} \frac{1}{q} > 0$ , 所以这样的映射  $T$  存在。同理存在映射  $S$ 。

固定  $|U| = s$ , 其中  $U \subset \mathbb{F}_q^s$ 。我们希望给出  $U$  的共同邻点的数量的上界。我们将使用矩方法实现这一点。令

$I(v)$  为指示变量, 当  $v$  是  $U$  的公共邻点时恰好为 1。令  $X$  为  $U$  的公共邻点的数量。借助引理 2.2,

$$\begin{aligned}\mathbb{E}[X^d] &= \mathbb{E}\left[\left(\sum_{v \in \mathbb{F}_q^s} I(v)\right)^d\right] = \sum_{v_1, \dots, v_d \in \mathbb{F}_q^s} \mathbb{E}[I(v_1) \cdots I(v_d)] \\ &= \sum_{r \leq d} \binom{q^s}{r} q^{-rs} M_r \leq \sum_{r \leq d} M_r = M\end{aligned}$$

其中  $M_r$  定义为从  $[d]$  到  $[r]$  的投影数<sup>14</sup>,  $M = \sum_{r \leq d} M_r$ 。使用马尔可夫不等式我们得到

$$\mathbb{P}(X \geq \lambda) \leq \frac{\mathbb{E}[X^d]}{\lambda^d} \leq \frac{M}{\lambda^d}$$

现在, 即使  $X$  的期望值很小, 我们也不能确定  $X$  很大的概率很小。例如, 如果我们采用带有  $p = n^{-\frac{1}{s}}$  的随机图, 那么  $X$  的期望值会很低, 但是会有一条长而平滑的衰减尾部。

事实证明, 代数几何理论帮助我们阻止了公共邻点  $X$  的数量可以取任意值。公共邻点由一组多项式方程的零点确定, 因此变成了一个代数问题。直觉告诉我们, 我们要么处于  $X$  非常小的“零维”情况, 要么处于  $X$  至少在  $q$  数量级的“正维”情况。

### 引理 2.3 (Bukh 2015)

对于所有  $s, d$ , 存在一个常数  $C$  使得如果  $f_1(Y), \dots, f_s(Y)$  是  $\mathbb{F}_q^s$  上阶数最大为  $d$  的多项式, 则

$$\{y \in \mathbb{F}_q^s \mid f_1(y) = \dots = f_s(y) = 0\}$$

集合的大小满足以下两者之一: 最大为  $C$  或者最少为  $q - C\sqrt{q}$ 。

引理 2.3 可以由代数几何重要结论 Lang-Weil 界<sup>15</sup>推导出来, 它说  $\mathbb{F}_q^s$  中  $r$  维代数簇<sup>16</sup>的点数大致为  $q^r$ , 只要满足某些不可约性假设即可。

### 定理 2.12 (Lang-Weil bound 1954)

如果  $V = \{y \in \mathbb{F}_q^s \mid g_1(y) = g_2(y) = \dots = g_m(y)\}$  是不可约且  $g_i$  的阶数至多为  $d$ , 则

$$|V \cap \mathbb{F}_q^s| = q^{\dim V} \left(1 + O_{s,m,d}\left(q^{-\frac{1}{2}}\right)\right)$$

现在我们可以使用马尔可夫不等式的界和引理 2.3。令引理 2.41 中的  $s$  个多项式  $f_1(Y), \dots, f_s(Y)$  为  $s$  个覆盖  $U$  中  $s$  个元素的关于  $u$  的多项式  $f(u, Y)$ 。对于足够大的  $q$ , 存在一个来自引理 2.3 的常数  $C$ , 使得  $X > C$ , 这告诉我们  $X \geq q - C\sqrt{q} > q/2$ , 所以

$$\mathbb{P}(X > C) = \mathbb{P}\left(X > \frac{q}{2}\right) \leq \frac{M}{(q/2)^d}$$

因此,  $L$  或  $R$  的大小为  $s$  且大于  $C$  个共同邻点的子集的数量至多为

$$2 \binom{n}{s} \frac{M}{(q/2)^d} = O\left(q^{s-2}\right)$$

我们从  $G$  中每个这样的子集中删除一个顶点来得到  $G'$ 。首先我们知道  $G'$  是  $K_{s,C+1}$ -free 的, 然后

$$\mathbb{E}[e(G')] \geq \frac{n^2}{q} - O\left(nq^{s-2}\right) = (1 - o(1)) \frac{n^2}{q} = (1 - o(1))n^{2-\frac{1}{s}}$$

且  $v(G') \leq 2n$ 。所以确实存在一个的实例  $G'$ , 它达到了所需的上界。

<sup>14</sup>包含  $m$  元素的集合到包含  $n$  元素的集合 ( $m > n$ ) 的投影数是  $\sum_{i=0}^n (-1)^i \binom{m}{i} (n-i)^m$

<sup>15</sup>Terry Tao 的博客中有一篇详细介绍了 Lang-Weil Bound:

<https://terrytao.wordpress.com/2012/08/31/the-lang-weil-bound/>

<sup>16</sup>代数簇, 亦作代数多形体, 是代数几何学上多项式集合的公共零点解的集合。

## 2.9 禁止稀疏二分图

对于任何二分图  $H$ ，它总是包含在某些  $K_{s,t}$  中。根据定理2.4，

$$\text{ex}(n, H) \leq \text{ex}(n, K_{s,t}) \lesssim n^{2-\frac{1}{s}}$$

当  $H$  是稀疏二分图时，第一个不等式一般不紧。在本节中，我们将看到一些给稀疏二分图  $H$  提供  $\text{ex}(n, H)$  更好上界的技术。

第一个结论给出了当  $H$  是二分图并且一个部分的顶点度数有上界时  $\text{ex}(n, H)$  的上界。

### 定理 2.13 (Füredi 1991)

令  $H$  为顶点集  $A \cup B$  的二分图，其中  $A$  中的每个顶点的度数至多为  $r$ 。那么存在一个常数  $C = C_H$  使得

$$\text{ex}(n, H) \leq Cn^{2-\frac{1}{r}}$$

为了证明这个结论，我们引入下面被称为“独立随机选择”的概率技术。这个引理的主要思想是：如果  $G$  有很多边，那么存在  $V(G)$  的一个大的子集  $U$ ，使得  $U$  中顶点的所有小子集都有许多共同的邻点。

### 引理 2.4 (Dependent random choice: Alon, Krivelevich and Sudakov 2003)

设  $u, n, r, m, t \in \mathbb{N}, \alpha > 0$  是满足下述不等式的数

$$n\alpha^t - \binom{n}{r} \left(\frac{m}{n}\right)^t \geq u$$

则每个至少有  $\alpha n^2/2$  条边的  $n$  顶点图  $G$  包含一个大小至少为  $u$  的顶点子集  $U$ ，且  $U$  的任意元素个数为  $r$  的子集  $S$  至少有  $m$  个共同邻点。

**证明** 令  $T$  是从  $V(G)$  中均匀随机选择的一个有  $t$  个顶点的序列（允许顶点重复）。令  $A$  是  $T$  的公共邻域。 $|A|$  的期望为

$$\begin{aligned} \mathbb{E}|A| &= \sum_{v \in V} \mathbb{P}(v \in A) = \sum_{v \in V} \mathbb{P}(T \subseteq N(v)) = \sum_{v \in V} \left(\frac{d(v)}{n}\right)^t \\ &\stackrel{\text{convexity}}{\geq} n \left(\frac{1}{n} \sum_{v \in V} \frac{d(v)}{n}\right)^t \geq n\alpha^t \end{aligned}$$

对于  $V$  的任意元素个数为  $r$  的子集  $S$ ，事件  $A$  包含  $S$  发生，当且仅当  $T$  包含在  $S$  的公共邻域中，该事件发生的概率为

$$\left(\frac{\#\text{ common neighbors of } S}{n}\right)^t$$

我们称公共邻点少于  $m$  的集合为坏集。则根据上面所得到的概率我们知道，所有由  $r$  个元素构成的坏子集  $S \subset V$  包含在  $A$  中的概率小于  $(m/n)^t$ 。由期望的线性性质，

$$\mathbb{E}[\text{the number bad } r\text{-element subset of } A] < \binom{n}{r} \left(\frac{m}{n}\right)^t$$

为了确保没有坏子集，我们可以去掉每个坏子集中的一个元素。剩余元素的个数至少为  $|A|$  减去  $A$  中元素个数为  $r$  的坏子集的数量，其期望值至少为

$$n\alpha^t - \binom{n}{r} \left(\frac{m}{n}\right)^t \geq u$$

因此，存在一个顶点序列  $T$ ，使得在去掉所有坏的  $r$  元素子集后， $A$  中至少还剩下  $u$  个元素。剩下的  $u$  个元素构成的集合  $U$  满足所需的属性。

将引理 2.4 的参数设置为证明定理 2.13 所需的参数，我们得到以下推论。



**推论 2.2**

对于任何顶点集为  $A \cup B$  的二分图  $H$ ，其中  $A$  中的每个顶点的度数最多为  $r$ ，存在  $C$  使得以下结果成立：每个至少有  $Cn^{2-\frac{1}{r}}$  条边的图包含一个顶点子集  $U$ ， $|U| = |B|$ ，且  $U$  中的每个元素个数为  $r$  的子集至少有  $|A| + |B|$  个共同邻点。



**证明** 根据引理 2.4， $u = |B|, m = |A| + |B|, t = r$ ，只需检查是否存在  $C$ ，使得

$$n \left( 2Cn^{-\frac{1}{r}} \right)^r - \binom{n}{r} \left( \frac{|A| + |B|}{n} \right)^r \geq |B|$$

第一项化简为  $(2C)^r$ ，第二项化简为  $O_H(1)$ 。因此我们可以选择足够大的  $C$  来使这个不等式成立。

现在我们准备证明定理 2.13。

**证明** [定理 2.13]

令  $G$  是一个至少有  $Cn^{2-\frac{1}{r}}$  条边的  $n$  顶点图，其中  $C$  是推论 2.2 的  $C$ 。首先，使用推论 2.2 中的  $U$  将  $B$  嵌入到  $V(G)$  中。我们计划将这种嵌入进一步扩展到  $A \cup B \hookrightarrow V(G)$ 。为此，假设我们已经有一个嵌入  $\phi: A' \cup B \hookrightarrow V(G)$ ，其中  $A' \subseteq A$ ，并且我们想要扩展  $\phi$  到任意  $v \in A \setminus A'$ 。我们必须确保  $\phi(v)$  是  $G$  中  $\phi(N(v))$  的公共邻点。注意到，根据假设， $|\phi(N(v))| = |N(v)| \leq r$ ，并且通过选择合适的  $B$ ，集合  $\phi(N(v))$  至少有  $|A| + |B|$  个共同邻点。 $\phi(v)$  可以是这些公共邻点中的任何一个，但不能与  $\phi(u)$  相同 ( $\forall u \in A' \cup B$ )。由于至少有  $|A| + |B|$  个顶点可供选择，我们可以通过将  $\phi(v)$  设置为其余可选顶点之一来扩展  $\phi$ 。通过这个过程，我们可以将嵌入扩展到  $A \cup B \hookrightarrow V(G)$ ，这说明  $G$  中存在  $H$  的副本。

定理 2.13 是可以应用于所有二分图的一般性结论。但是，对于某些特定的二分图  $H$ ，我们可能还有改进的余地。例如，通过这个定理我们知道的  $C_6$  与  $C_4$  的上界相同，即  $O(n^{3/2})$ 。但这个上界并不紧。

**定理 2.14 (Even cycles: Bondy and Simonovits 1974)**

对于所有整数  $k \geq 2$ ，存在一个常数  $C$  使得

$$\text{ex}(n, C_{2k}) \leq Cn^{1+\frac{1}{k}}$$



**笔记** 目前已知当  $k = 2, 3, 5$  时， $\text{ex}(n, C_{2k}) = \Theta(n^{1+1/k})$  (Benson 1966)。但是，对于  $k$  的其他值是否也是如此，这问题开放的。

我们准备证明这个定理而是关注一个弱一些的结论：

**定理 2.15**

对于任何整数  $k \geq 2$ ，都存在一个常数  $C$ ，使得每个至少有  $Cn^{1+1/k}$  条边的  $n$  顶点图  $G$  包含一个长度最多为  $2k$  的偶数圈。



为了证明这个定理，我们将首先对图进行“清理”，使得图的最小度足够大并且图是二分图。下面两个引理允许我们专注于这些满足好性质的  $G$  的子图。

**引理 2.5**

$t \in \mathbb{R}$ ，令  $G$  是一个平均度数为  $2t$  的图，则  $G$  包含一个最小度数大于  $t$  的子图。



**证明** 我们有  $e(G) = v(G)t$ 。删除度数小于等于  $t$  的顶点不能降低平均度数。我们可以继续删除度数小于等于  $t$  的顶点，直到每个顶点的度数都大于  $t$ 。该算法一定在到达空子图之前终止，否则平均度数不可能为  $2t$ 。算法终止时剩余的子图就是最小度数大于  $t$  的子图。

**引理 2.6**

每个  $G$  都有一个二部子图，该二分图至少有  $e(G)/2$  条边。



**证明** 用两种颜色中均匀随机地为每个顶点着色。那么非单色边的期望值为  $e(G)/2$ 。因此存在至少具有  $e(G)/2$

非单色边的着色方案。

**证明** [定理2.15]

假设  $G$  不包含长度最多为  $2k$  的偶数圈。由引理 2.5 和引理 2.6 知，存在一个最小度至少为  $\delta := Cn^{1/k}/2$  二部子图  $G'$ 。令  $A_0 = \{u\}$ ，其中  $u \in V(G')$ 。令  $A_{i+1} = N_{G'}(A_i) \setminus A_{i-1}$ 。  $A_i$  是一组顶点，因为  $G'$  是二分图，它们到起始顶点  $u$  的距离正好为  $i$ 。(图2.9)

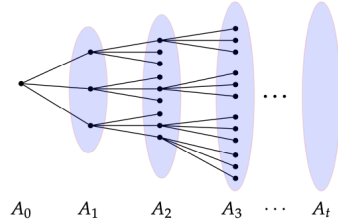


图 2.9: 定理 2.15 的证明示意图

$1 \leq i \leq k$ ，对于  $A_{i-1}$  中两个不同的顶点  $v, v'$ ，如果它们在  $A_i$  中有一个共同的邻点  $w$ ，那么从  $u$  到  $w$  有两条不同的最短路径。两个不同路径的并集（即使它们重叠）包含一个长度最多为  $2i \leq 2k$  的偶数圈，这与我们的假设矛盾。因此  $A_{i-1}$  中任意两个顶点的公共邻点只能在  $A_{i-2}$  中，这意味着  $|A_i| \geq (\delta - 1)|A_{i-1}|$ 。因此  $|A_k| \geq (\delta - 1)^k \geq (Cn^{1/k} - 1)^k$ 。如果选择的  $C$  足够大，就会有  $|A_k| > n$ ，矛盾。

如果  $H$  是一个二分图，顶点集  $A \cup B$  且  $A$  中每个顶点的度数最多为 2，则  $\text{ex}(n, H) = O(n^{3/2})$ 。指数  $3/2$  是最优的，因为  $\text{ex}(n, K_{2,2}) = \Theta(n^{3/2})$ 。事实上，只要  $H$  不包含  $K_{2,2}$  的任何副本，我们就可以改进该指数。

**定理 2.16 (Colon and Lee 2019+)**

令  $H$  是顶点集为  $A \cup B$  的二分图且  $A$  中的每个顶点的度数最多为 2，并且  $H$  不包含  $K_{2,2}$ 。则存在依赖于  $H$  的  $c, C > 0$  满足

$$\text{ex}(n, H) \leq Cn^{\frac{3}{2}-c}$$

为了证明这个定理，我们展示了一个使用细分 (subdivision) 概念表述的等效陈述。对于图  $H$ ， $H$  的 1-细分  $H^{1-\text{sub}}$  是通过在  $H$  的每条边的中间添加一个额外的顶点来获得的 (图2.10)。请注意，定理2.16 中的任一  $H$  都是某个  $K_t^{1-\text{sub}}$  的子图，因此我们可以考虑以下定理2.16 的替代表述

**定理 2.17 (Janzer 2018)**

对于任意  $t \geq 3$ ，存在  $c_t > 0$  使得

$$\text{ex}\left(n, K_t^{1-\text{sub}}\right) = O\left(n^{\frac{3}{2}-c_t}\right)$$

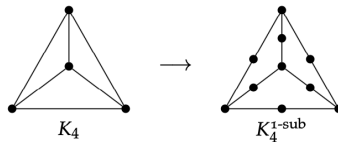


图 2.10: 1-subdivision of  $K_4$

现在我们给出 Janzer 关于定理 2.17 的证明。在定理 2.15 中，将参数传递给子图是很有用的，这帮助我们在子图中能够更好地控制顶点的度数。为此，我们将使用以下引理（省略证明）来找到一个几乎正则的子图。

## 引理 2.7

对于所有  $0 < \alpha < 1$ ，存在常数  $\beta, k > 0$  使得对于所有  $C > 0$ ，当  $n$  足够大时，每个边数大于等于  $Cn^{1+\alpha}$  的  $n$  顶点图  $G$  都有一个子图  $G'$  满足

- (a)  $v(G') \geq n^\beta$
- (b)  $e(G') \geq \frac{1}{10} C v(G')^{1+\alpha}$
- (c)  $\max \deg(G') \leq K \min \deg(G')$
- (d)  $G'$  是二分的，且有两个顶点集的大小最多相差 2。



从现在开始，我们将  $t$  视为一个常数。对于任意两个顶点  $u, v \in A$ ，如果  $u$  和  $v$  的公共邻点数至少为 1 且小于  $\binom{t}{2}$ ，我们称点对  $uv$  是轻的；相反，如果  $u$  和  $v$  的公共邻点数大于等于  $\binom{t}{2}$ ，我们称点对  $uv$  是重的。声明， $u, v$  没有任何共同邻点时点对  $uv$  既不轻也不重。下面的引理给出了轻点对数量的下界。

## 引理 2.8

令  $G$  是一个顶点集为  $U \cup B$  的  $K_t^{1-\text{sub}}$ -free 二分图，且对于所有  $x \in U$  有  $d(x) \geq \delta$ ，并且满足  $|U| \geq 4|B|t/\delta$ 。那么存在  $u \in U$ ，出现在  $U$  中  $\Omega(\delta^2|U|/|B|)$  个轻点对中。



**证明** 令  $S$  是  $\{(\{u, v\}, x) \mid u, v \in U, x \in B\}$  的集合，其中  $\{u, v\}$  是  $U$  中的无序点对， $x$  是  $\{u, v\}$  的公共邻点。首先，我们通过选择  $x \in B$  来计算：

$$|S| = \sum_{x \in B} \binom{d(x)}{2} \geq |B| \binom{e(G)/|B|}{2} \geq \frac{|B|}{4} \left( \frac{\delta|U|}{|B|} \right)^2 = \frac{\delta^2|U|^2}{4|B|}$$

请注意， $B$  中的低度顶点贡献很小，因为

$$\sum_{\substack{x \in B \\ d(x) < 2t}} \binom{d(x)}{2} \leq 2t^2|B| \leq \frac{\delta^2|U|^2}{8|B|}$$

因此

$$\sum_{\substack{x \in B \\ d(x) \geq 2t}} \binom{d(x)}{2} \geq \frac{\delta^2|U|^2}{8|B|}$$

注意，如果  $U$  中有  $t$  个互相之间是重点对的顶点，那么我们可以为每对  $\{v_i, v_j\}$  选择一个共同的邻点  $u_{ij}$ ，在这里  $i < j$ 。由于每一对  $\{v_i, v_j\}$  至少有  $\binom{t}{2}$  个这样的邻点，所以我们选择所有的  $u_{ij}$  可以是不同的。这会产生一个  $K_t^{1-\text{sub}}$  子图，矛盾。因此  $U$  中不存在  $t$  个互相之间是重点对的点，根据图兰定理， $x \in B$ ， $N(x)$  中的重点对的数目至多为  $e(T_{d(x), t-1})$ 。这是因为  $N(x)$  中的任何两个顶点至少有一个共同的邻点  $x$ ，它们要么形成轻点对或重点对。这表明在  $N(x)$  中至少有  $\binom{d(x)}{2} - e(T_{d(x), t-1})$  个轻点对。如果  $d(x) \geq 2t$ ，则有

$$\begin{aligned} \binom{d(x)}{2} - e(T_{d(x), t-1}) &\geq \binom{d(x)}{2} - \binom{t-1}{2} \left( \frac{d(x)}{t-1} \right)^2 \\ &= \frac{1}{2(t-1)} d(x)^2 - \frac{1}{2} d(x) \\ &\gtrsim d(x)^2 \end{aligned}$$

如果我们对所有  $x \in B$  求和，根据定义，那么每个轻点对最多只会被计算  $\binom{t}{2}$  次。因为我们将  $t$  视为常数所以  $\binom{t}{2}$  是常数。因此

$$\# \text{light pairs in } U \gtrsim \sum_{x \in B} d(x)^2 \gtrsim |S| \gtrsim \frac{\delta^2|U|^2}{|B|}$$

并且根据鸽巢原理，存在一个顶点  $u \in U$  在  $\Omega(\delta^2|U|/|B|)$  个轻点对中。

有了这些引理，我们准备来证明定理 2.17。

**证明** [定理 2.17]

令  $G$  是任意  $K_t^{1-\text{sub}}$ -free 图。首先选择  $\alpha = (t-2)/(2t-3)$  时引理 2.7 中的  $G'$ ，两个部分分别记作  $A$  和  $B$ 。

设  $\delta$  为  $G'$  的最小度数。我们将反证法证明  $\delta \leq C\nu(G')^{(t-2)/(2t-3)}$ 。假设  $\delta > C\nu(G')^{(t-2)/(2t-3)}$ 。我们的计划是选择这样的  $v_1, v_2, \dots, v_t$ ：对于所有  $i < j$ ， $v_i v_j$  都是轻的，并且  $v_1, \dots, v_t$  的任意三个没有共同的邻点。这会给我们带来一个  $K_t^{1\text{-sub}}$ ，从而矛盾。

我们将通过重复使用引理 2.8 并介绍一个更强的假设来做到这一点：对于任意  $1 \leq i \leq t$ ，存在  $A = U_1 \supseteq U_2 \supseteq \dots \supseteq U_i$  和  $v_j \in U_j$  使得

- (a) 对于所有  $1 \leq j \leq i-1$ ， $v_j$  至少在  $U_j$  中  $\Theta(\delta^2 |U_j| / \nu(G'))$  个轻点对中。
- (b) 对于所有  $1 \leq j \leq i-1$ ， $v_j$  对  $U_{j+1}$  中的所有顶点都是轻的。
- (c)  $v_1, \dots, v_i$  中任意三个没有共同邻点。
- (d) 对于所有  $1 \leq j \leq i-1$ ， $|U_{j+1}| \gtrsim \delta^2 |U_j| / \nu(G')$  成立。

当  $i = 1$  时，根据引理 2.8，可以找到  $v_1$  作为所需的顶点。现在假设我们已经构造出了  $A = U_1 \supseteq \dots \supseteq U_{i-1}$  与  $v_j \in U_j$ ， $j = 1, \dots, i-1$ 。为了构造  $U_i$ ，令  $U'_i$  是与  $v_{i-1}$  形成轻点对的顶点集。然后由归纳假设 (a) 我们有  $|U'_i| \gtrsim \delta^2 |U_{i-1}| / \nu(G')$ 。现在我们去掉  $U'_i$  中所有违反 (c) 的顶点得到  $U_i$ 。检查每一对  $v_j v_k$ ，查看它们的共同点  $u$ ，从  $U'_i$  中删除  $u$  的所有邻点。 $U'_i$  中一共有  $\binom{i-1}{2}$  个  $v_j v_k$ ，它们最多有  $\binom{t}{2}$  公共邻点（因为它们形成一个轻点对），并且每个这样的邻点的度数最多为  $K\delta$ 。因此移除的顶点数最多为

$$\binom{i-1}{2} \binom{t}{2} K\delta = O(\delta)$$

因为  $t$  和  $K$  是常数。因此，在进行修改之后，只要  $C$  选择得足够大且等式  $|U'_i| = \Omega(\delta)$  继续成立，(d) 就仍然成立。(d) 确实仍然成立，因为

$$|U'_i| \gtrsim \left( \frac{\delta^2}{\nu(G')} \right)^{i-1} |A| \gtrsim \delta^{2t-2} \nu(G')^{t-2} = \Theta(\delta)$$

当  $i \leq t$  时成立。因此 (d) 对  $i$  成立，我们只需要根据引理 2.8 从  $U_i$  选择出顶点  $v_i$ ，(a), (b), (c) 直接自动满足。因此，通过归纳，这也适用于  $i = t$ 。现在通过 (b) 和 (c)，在  $G'$  中存在  $K_t^{1\text{-sub}}$  的副本，矛盾。

上面的论证表明  $\delta \leq C\nu(G')^{(t-2)/(2t-3)}$ ，所以最大度数最多为  $K C \nu(G')^{(t-2)/(2t-3)}$ 。因此  $e(G') \leq K C \nu(G')^{1+\alpha}$ ，假设我们有  $e(G) > 10 K C n^{1+\alpha}$ ，根据引理 2.7 (c) 得到的结果与  $e(G') \leq K C \nu(G')^{1+\alpha}$  矛盾。所以有  $e(G) \leq 10 K C n^{1+\alpha}$ ，这是我们想要的。

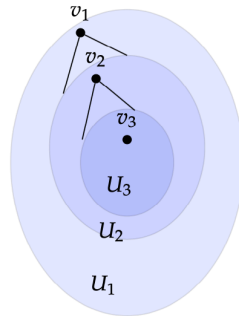


图 2.11: 重复利用引理 2.17 得到  $v_i$  和  $U_i$

## 第 3 章 Szemerédi 正则性引理

### 3.1 定理陈述和证明

Szemerédi 正则性引理是图论中最重要的结果之一，尤其是对比较大的图的研究非常重要。引理指出，对于所有大的稠密图  $G$ ，我们可以将  $G$  的顶点划分为有限数量的部分，以便大多数不同部分之间的边表现出“类似随机”（“random-like”）的特征。

为了给出“类似随机”的概念，我们首先陈述一些定义。

#### 定义 3.1

令  $X$  和  $Y$  是图  $G$  中的顶点集。令  $e_G(X, Y)$  为  $X$  和  $Y$  之间的边数；即，

$$e_G(X, Y) = |\{(x, y) \in X \times Y \mid xy \in E(G)\}|$$

由此，我们可以定义  $X$  和  $Y$  之间的边密度为

$$d_G(X, Y) = \frac{e_G(X, Y)}{|X||Y|}$$

如果上下文表述清楚，我们将省略下标  $G$ 。

#### 定义 3.2 ( $\epsilon$ -regular pair)

令  $G$  是一个图并且  $X, Y \subseteq V(G)$  我们称  $(X, Y)$  为  $G$  中的一个  $\epsilon$ -正则对，如果对于任意满足  $|A| \geq \epsilon|X|, |B| \geq \epsilon|Y|$  的子集  $A \subset X, B \subset Y$ ，都有

$$|d(A, B) - d(X, Y)| \leq \epsilon$$

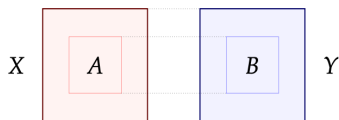


图 3.1:  $\epsilon$ -正则对的子集对在边密度上与原对相似

**笔记** 定义 3.2 中不同的  $\epsilon$  扮演着不同的角色，但区分它们并不重要。为了方便，我们只使用一个  $\epsilon$  来表示。

如果满足  $|A| \geq \epsilon|X|, |B| \geq \epsilon|Y|$  的子集  $A \subset X, B \subset Y$  有  $|d(A, B) - d(X, Y)| > \epsilon$ ，则  $(X, Y)$  不是  $\epsilon$ -正则的。我们把这样的子集  $A \subset X, B \subset Y$  称为见证  $X, Y$  非  $\epsilon$ -正则的子集。

#### 定义 3.3 ( $\epsilon$ -regular partition)

$V(G)$  的一个划分<sup>a</sup>  $\mathcal{P} = \{V_1, \dots, V_k\}$  是  $\epsilon$ -正则划分，如果

$$\sum_{\substack{(i,j) \in [k]^2 \\ (V_i, V_j) \text{ not } \epsilon\text{-regular}}} |V_i||V_j| \leq \epsilon|V(G)|^2$$

<sup>a</sup>集合  $X$  的划分是把  $X$  分割到覆盖了  $X$  的全部元素而又不重叠的“块”中。

请注意，此定义允许一些非正则的对，只要它们的总大小不太大。现在我们来陈述正则性引理。

#### 定理 3.1 (Szemerédi 正则性引理 1978)

对于任意  $\epsilon > 0$ ，存在一个常数  $M$ ，使得每个图都有一个  $\epsilon$ -正则划分，最多可分为  $M$  个区域。



更强版本的引理允许我们找到一个均衡的划分——也就是说，划分的每个部分的大小都是  $\lfloor \frac{n}{k} \rfloor$  或  $\lceil \frac{n}{k} \rceil$ ，其中  $n$  是顶点数， $k$  是划分的块数。

### 定理 3.2 (Szemerédi 正则性引理均衡版本 1978)

对于任意  $\epsilon > 0$  和  $m_0$ ，存在一个常数  $M$ ，使得每个图都有一个  $\epsilon$ -均衡正则划分，顶点集被划分成  $k$  部分，其中  $m_0 \leq k \leq M$ 。

我们先说下证明的主要思路。我们将根据以下算法生成我们想要的划分：

- 从简单的划分开始（1 个部分）。
- 如果划分不是  $\epsilon$ -正则的：
  - 对于每个不是  $\epsilon$ -正则的  $(V_i, V_j)$ ，找到见证  $(V_i, V_j)$  的非正则性的子集  $A^{i,j} \subset V_i$  和  $A^{j,i} \subset V_j$ 。
  - 对划分加细<sup>1</sup>，消除所有见证非正则性的子集  $A^{i,j}$ 。

如果此过程在有限步后停止，则将成功证明正则性引理。为了表明我们将在有限的时间内停止，我们将使用一种称作能量增量参数（energy increment argument）的技术。

### 定义 3.4 (Energy)

设  $U, W \subseteq V(G)$ ， $n = |V(G)|$ 。定义

$$q(U, W) = \frac{|U||W|}{n^2} d(U, W)^2$$

对于  $U$  的划分  $\mathcal{P}_U = \{U_1, \dots, U_k\}$  和  $W$  的划分  $\mathcal{P}_W = \{W_1, \dots, W_l\}$  定义

$$q(\mathcal{P}_U, \mathcal{P}_W) = \sum_{i=1}^k \sum_{j=1}^l q(U_i, W_j)$$

最后，对于  $V(G)$  的划分  $\mathcal{P} = \{V_1, \dots, V_k\}$ ，定义  $\mathcal{P}$  的能量为  $q(\mathcal{P}, \mathcal{P})$ 。具体的，

$$q(\mathcal{P}) = \sum_{i=1}^k \sum_{j=1}^k q(V_i, V_j) = \sum_{i=1}^k \sum_{j=1}^k \frac{|V_i||V_j|}{n^2} d(V_i, V_j)^2$$

因为边密度以 1 为上界，所以能量在 0 和 1 之间：

$$q(\mathcal{P}) = \sum_{i=1}^k \sum_{j=1}^k \frac{|V_i||V_j|}{n^2} d(V_i, V_j)^2 \leq \sum_{i=1}^k \sum_{j=1}^k \frac{|V_i||V_j|}{n^2} = 1$$

为了能够证明 Szemerédi 正则性引理，我们将介绍证明一系列引理，这些引理将表明能量不会在加细时减少。如果我们加细的划分非正则，则能量可以显著增加。

### 引理 3.1

对于顶点集  $U$  和  $W$  的任何划分  $\mathcal{P}_U$  和  $\mathcal{P}_W$ ，

$$q(\mathcal{P}_U, \mathcal{P}_W) \geq q(U, W)$$

**证明** 设  $\mathcal{P}_U = \{U_1, \dots, U_k\}$  和  $\mathcal{P}_W = \{W_1, \dots, W_l\}$ 。

在  $U$  中均匀随机选择  $x$ ，在  $W$  中均匀随机选择  $y$ 。令  $U_i$  是包含  $x$  的  $\mathcal{P}_U$  中的一个块，而  $W_j$  是包含  $y$  的  $\mathcal{P}_W$  中的一个块。然后定义随机变量  $Z = d(U_i, W_j)$ ，它的期望是

$$\mathbb{E}[Z] = \sum_{i=1}^k \sum_{j=1}^l \frac{|U_i||W_j|}{|U||W|} d(U_i, W_j) = \frac{e(U, W)}{|U||W|} = d(U, W)$$

<sup>1</sup>对于覆盖  $D = \{V_\beta\}_{\beta \in B}$ ， $C = \{U_\alpha\}_{\alpha \in A}$ ，如果对任意的  $V_\beta$ ，都存在某个  $U_\alpha$  使得  $V_\beta \subseteq U_\alpha$ ，我们则说  $D$  是覆盖  $C$  的加细（精细）。

二阶矩为

$$\mathbb{E}[Z^2] = \sum_{i=1}^k \sum_{j=1}^l \frac{|U_i|}{|U|} \frac{|W_j|}{|W|} d(U_i, W_j)^2 = \frac{n^2}{|U||W|} q(\mathcal{P}_U, \mathcal{P}_W)$$

显然我们有  $\mathbb{E}[Z^2] \geq \mathbb{E}[Z]^2$ ，这意味着引理成立。

### 引理 3.2

如果  $\mathcal{P}'$  是  $\mathcal{P}$  的加细，则  $q(\mathcal{P}') \geq q(\mathcal{P})$ 。

**证明** 令  $\mathcal{P} = \{V_1, \dots, V_m\}$  并将引理 3.1 应用到每个  $(V_i, V_j)$  对。

### 引理 3.3 (能量提升引理)

如果  $(U, W)$  不是  $\epsilon$ -正则的，且反例是  $U_1 \subset U$  和  $W_1 \subset W$  (也就是说  $|d(U_1, W_1) - d(U, W)| > \epsilon$ )，那么

$$q(\{U_1, U \setminus U_1\}, \{W_1, W \setminus W_1\}) > q(U, W) + \epsilon^4 \frac{|U||W|}{n^2}$$

**证明** 定义  $Z$  和引理 3.1 证明中的相同。然后

$$\begin{aligned} \text{Var}(Z) &= \mathbb{E}[Z^2] - \mathbb{E}[Z]^2 \\ &= \frac{n^2}{|U||W|} (q(\{U_1, U \setminus U_1\}, \{W_1, W \setminus W_1\}) - q(U, W)) \end{aligned}$$

观察到  $|Z - \mathbb{E}[Z]| = |d(U_1, W_1) - d(U, W)|$  的概率是  $\frac{|U_1|}{|U|} \frac{|W_1|}{|W|}$  (对应于  $x \in U_1$  且  $y \in W_1$ )，所以

$$\begin{aligned} \text{Var}(Z) &= \mathbb{E}[(Z - \mathbb{E}[Z])^2] \\ &\geq \frac{|U_1|}{|U|} \frac{|W_1|}{|W|} (d(U_1, W_1) - d(U, W))^2 \\ &> \epsilon \cdot \epsilon \cdot \epsilon^2 \end{aligned}$$

证毕。

### 引理 3.4

如果  $V(G)$  的划分  $\mathcal{P} = \{V_1, \dots, V_k\}$  不是  $\epsilon$ -正则的，则存在  $\mathcal{P}$  的加细  $\mathcal{Q}$ ，其中每个  $V_i$  最多分为  $2^k$  个部分，且  $q(\mathcal{Q}) \geq q(\mathcal{P}) + \epsilon^5$ 。

**证明** 对于使得  $(V_i, V_j)$  非  $\epsilon$ -正则的所有  $(i, j)$ ，找到见证非正则性的子集  $A^{i,j} \subset V_i$  和  $A^{j,i} \subset V_j$  (对所有非正则对同时进行)。令  $\mathcal{Q}$  是  $\mathcal{P}$  根据这些  $A^{i,j}$  形成的公共加细<sup>2</sup>。每个  $V_i$  根据需要最多分为  $2^k$  个部分。然后

$$\begin{aligned} q(\mathcal{Q}) &= \sum_{(i,j) \in [k]^2} q(\mathcal{Q}_{V_i}, \mathcal{Q}_{V_j}) \\ &= \sum_{\substack{(i,j) \in [k]^2 \\ (V_i, V_j) \in \text{-regular}}} q(\mathcal{Q}_{V_i}, \mathcal{Q}_{V_j}) + \sum_{\substack{(i,j) \in [k]^2 \\ (V_i, V_j) \text{ not } \epsilon\text{-regular}}} q(\mathcal{Q}_{V_i}, \mathcal{Q}_{V_j}) \end{aligned}$$

其中  $\mathcal{Q}_{V_i}$  是  $\mathcal{Q}$  给出的  $V_i$  的划分。通过引理 3.1，上面等式的值至少为

$$\sum_{\substack{(i,j) \in [k]^2 \\ (V_i, V_j) \in \text{-regular}}} q(V_i, V_j) + \sum_{\substack{(i,j) \in [k]^2 \\ (V_i, V_j) \text{ not } \epsilon\text{-regular}}} q(\{A^{i,j}, V_i \setminus A^{i,j}\}, \{A^{j,i}, V_j \setminus A^{j,i}\})$$

由于在创建  $\mathcal{Q}$  时  $V_i$  被  $A^{i,j}$  切分，所以  $\mathcal{Q}_{V_i}$  是  $\{A^{i,j}, V_i \setminus A^{i,j}\}$  的一个加细。根据引理 3.3，上述总和至少为

$$\sum_{(i,j) \in [k]^2} q(V_i, V_j) + \sum_{\substack{(i,j) \in [k]^2 \\ (V_i, V_j) \text{ not } \epsilon\text{-regular}}} \epsilon^4 \frac{|V_i||V_j|}{n^2}$$

因为  $\mathcal{P}$  不是  $\epsilon$ -正则的，所以第二个总和至少是  $\epsilon^5$ ，我们推导出所需的不等式。

<sup>2</sup>对于划分  $\mathcal{P}_1$  和  $\mathcal{P}_2$ ， $\mathcal{P}_1 \cup \mathcal{P}_2 = \mathcal{P}$  称为他们的公共加细

现在我们可以来证明 Szemerédi 正则性引理。

**证明** [定理 3.1]

从一个简单的划分开始。每当当前划分不是  $\epsilon$ -正则时，重复应用引理 3.4。根据能量的定义， $0 \leq q(\mathcal{P}) \leq 1$ 。然而，根据引理 3.4， $q(\mathcal{P})$  在每次迭代中至少增加  $\epsilon^5$ 。所以我们将最多在  $\epsilon^{-5}$  步后停止，从而产生  $\epsilon$ -正则划分。

一个有趣的问题是算法给出划分的块的数量是多少？如果  $\mathcal{P}$  有  $k$  个块，引理 3.4 将  $\mathcal{P}$  加细为最多  $k2^k \leq 2^{2^k}$  个块。迭代  $\epsilon^{-5}$  次会产生  $2^{2^{\epsilon^{-5}}}$  的上限。因为在上述证明中我们没有力求加细的块数是最小的，人们可能会认为更好的证明可以产生更好的上界。令人惊讶的是，这本质上就是最好的上界。

**定理 3.3 (Gowers 1997)**

存在一个常数  $c > 0$  使得对于所有足够小的  $\epsilon > 0$ ，存在一个图，其所有  $\epsilon$ -正则的划分至少需要  $2^{2^{\epsilon^{-c}}}$  个块。

该证明的另一个问题是我们如何使分割均衡？下面是对上述算法的修改，它证明了定理 3.2：

- 首先将图形任意平均地划分为  $m_0$  个部分。
- 如果划分不是  $\epsilon$ -正则的：
  - 使用见证非正则性的对来加细划分。
  - 进一步加细并调整来使划分均衡。为此，我们将移动和合并具有少量顶点的集合。


与以前一样，加细步骤至少增加了  $\epsilon^5$  的能量。在调整步骤中，能量可能会下降，但事实证明，这种下降不会最终影响结果。最后，能量增加的仍然是  $\Omega(\epsilon^5)$ ，这使得进程在  $O(\epsilon^{-5})$  步骤后终止。

## 3.2 三角形记数和删除引理

Szemerédi 的正则性引理是解决极值图论和加性组合问题的强大工具。在本节中，我们应用正则性引理来证明定理 1.6，即 Roth 的 3 项等差数列定理。我们首先介绍三角形计数引理，它提供了一种从规则划分中提取信息的方法，然后用这个结果来证明三角形删除引理，从而证明 Roth 定理。正如我们在上一节中提到的，如果图  $G$  顶点的两个子集是  $\epsilon$ -正则的，那么直观地讲，这些子集之间的二部图表现得像误差为  $\epsilon$  的“类似随机”。对“类似随机”的一种解释是，“小图案”的副本数应大致等于我们在具有相同边密度的随机图中看到的计数。通常，这些图案对应于固定的子图，例如三角形。

如果具有顶点子集  $X, Y, Z$  的图  $G$  是随机的，三元组  $(x, y, z) \in X \times Y \times Z$  表示  $x, y, z$  在  $G$  中构成的三角形，我们希望三元组的数量大致为

$$d(X, Y)d(X, Z)d(Y, Z) \cdot |X||Y||Z| \quad (3.1)$$


 **笔记** 请注意，集合  $X, Y, Z$  不一定是相交的。

三角形计数引理确保了这种直觉是对的。

**定理 3.4 (三角形计数引理)**

设  $X, Y, Z$  为图  $G$  的顶点的子集，满足  $(X, Y), (Y, Z), (Z, X)$  都是  $\epsilon$ -正则对， $\epsilon > 0$ 。让  $d_{XY}, d_{XZ}, d_{YZ}$  分别表示边缘密度  $d(X, Y), d(X, Z), d(Y, Z)$ 。若  $d_{XY}, d_{XZ}, d_{YZ} \geq 2\epsilon$ ，则使  $x, y, z$  在  $G$  中形成一个三角形的三元组  $(x, y, z) \in X \times Y \times Z$  的数量至少是

$$(1 - 2\epsilon)(d_{XY} - \epsilon)(d_{XZ} - \epsilon)(d_{YZ} - \epsilon) \cdot |X||Y||Z|$$

 **笔记** 定理中给出的三角形  $X \times Y \times Z$  中的三元组数量的下界类似于 3.1 中的表达式，但由于图不是完全随机的，我们引入了依赖于  $\epsilon$  的附加误差项。

**证明** 根据假设,  $(X, Y)$  是一个  $\epsilon$ -正则对。  $X$  中满足如下条件的顶点数少于  $\epsilon|X|$ : 该顶点在  $Y$  中的邻点数少于  $(d_{XY} - \epsilon)|Y|$ 。如果不成立, 那么  $Y$  与满足条件的  $X$  顶点构成的子集可以见证  $(X, Y)$  非正则性, 这与我们的假设相矛盾。直观地说, 这一上界是合理的, 因为如果  $X$  和  $Y$  之间的边是随机的, 我们会希望  $X$  中的大多数顶点在  $Y$  中有大约  $d_{XY}|Y|$  邻点, 这也意味着  $X$  中没有太多顶点可以在  $Y$  中具有很小的度。

我们对  $\epsilon$ -正则对  $(X, Z)$  应用相同的证明方法得到了类似的结果, 即在  $Z$  有少于  $(d_{XZ} - \epsilon)|Z|$  个邻点的  $X$  的顶点数量少于  $\epsilon|X|$ 。结合这两个结果, 我们可以找到大小至少为  $(1 - 2\epsilon)|X|$  的  $X$  的子集  $X'$ , 满足所有  $x \in X'$  至少与  $Y$  中  $(d_{XY} - \epsilon)|Y|$  个元素和  $Z$  中  $(d_{XZ} - \epsilon)|Z|$  个元素相邻。根据假设  $d_{XY}, d_{XZ} \geq 2\epsilon$  以及  $(Y, Z)$  是  $\epsilon$ -正则的事实, 我们看到对于任何  $x \in X'$ ,  $Y$  和  $Z$  中  $x$  的邻域之间的边密度至少为  $(d_{YZ} - \epsilon)$ 。

现在, 对于  $X'$  中的每个顶点  $x$ ,  $Y$  中  $x$  的邻域和  $Z$  中  $x$  的邻域之间的边的数量至少为  $(d_{XY} - \epsilon)(d_{XZ} - \epsilon)(d_{YZ} - \epsilon)|Y||Z|$ , 我们在  $G$  中得到一个唯一确定的  $(X, Y, Z)$ -三角形。注意到  $X'$  的大小至少为  $(1 - 2\epsilon)|X|$ , 因此, 这种三角形的数量至少是

$$(1 - 2\epsilon)(d_{XY} - \epsilon)(d_{XZ} - \epsilon)(d_{YZ} - \epsilon) \cdot |X||Y||Z|$$


这是我们想要的。

我们的下一步是使用定理3.4来证明三角形删除引理, 它指出我们可以通过去除“少量”边使具有“很少”三角形的图变成 triangle-free 的。

#### 定理 3.5 (三角形删除引理)

对于任意  $\epsilon > 0$ , 存在  $\delta > 0$  使得任何三角形数量小于等于  $\delta n^3$  的  $n$  顶点图都可以通过删除至多  $\epsilon n^2$  边变成 triangle-free 图。



 **笔记** 一种等效但偷懒的三角形删除引理的表述是说,

任何带有  $o(n^3)$  个三角形的  $n$  顶点图都可以通过删除  $o(n^2)$  条边来变成 triangle-free 的。

这一表述是考虑定理 3.5 的一种有用方式, 但由于使用了渐近符号, 因此有些模糊。一种更细致的表述是,

对于任何函数  $f(n) = o(n^3)$ , 存在一个函数  $g(n) = o(n^2)$  使得每当  $n$  顶点图具有小于或等于  $f(n)$  的三角形时, 我们最多可以删除  $g(n)$  边以使图变成 triangle-free 的。

另一种形式的陈述是将其视为关于图序列的结论,

给定一系列图  $\{G_n\}$ , 其性质是对于每个自然数  $n$ , 图  $G_n$  具有  $n$  个顶点和  $o(n^3)$  三角形, 我们可以通过从每个图  $G_n$  中删除  $o(n^2)$  条边来使序列中的所有图都是 triangle-free 的。

定理 3.5 的证明使用了 Szemerédi 正则性引理, 并很好地演示了通常情况下我们如何应用正则引理。我们使用正则引理的方法主要分以下三步进行。

1. 通过应用定理3.1来划分图的顶点以获得  $\epsilon$ -正则划分,  $\epsilon > 0$ 。
2. 去除在正则引理的结构中表现不佳的边。具体来说, 去除非正则对、边密度低的对和某一端点在小块的对。此步骤中移除的边总数很小。
3. 计算清洁后图中特定图案的副本数, 应用计数引理(例如, 当图案为三角形时, 定理 3.4)得到副本数。

**证明** [定理3.5]

假设我们有一个  $n$  顶点图, 其中三角形副本数少于  $\delta n^3$ , 参数  $\delta$  我们稍后会选择。首先对图进行  $\epsilon/4$ -正则划分, 划分结果为  $V_1, V_2, \dots, V_M$ 。接下来, 对于每对有序对  $(V_i, V_j)$ , 删除  $V_i$  和  $V_j$  之间的所有边, 如果下面几种情况之一

- (a)  $(V_i, V_j)$  是非正则对,
- (b) 密度  $d(V_i, V_j)$  小于  $\epsilon/2$ ,
- (c)  $V_i$  或  $V_j$  最多有  $(\epsilon/4M)n$  个顶点。

我们考虑在这个过程中一共去除了多少边？由于我们采用了  $\epsilon/4$ -正则划分，根据定义

$$\sum_{\substack{i,j \\ (V_i, V_j) \text{ not } \epsilon/4\text{-regular}}} |V_i| |V_j| \leq \frac{\epsilon}{4} n^2$$

所以至多  $(\epsilon/4)n^2$  条边在 (a) 中被移除。(b) 中移除的边数为

$$\sum_{\substack{i,j \\ d(V_i, V_j) < \epsilon/2}} d(V_i, V_j) |V_i| |V_j| \leq \frac{\epsilon}{2} \sum_{i,j} |V_i| |V_j| = \frac{\epsilon}{2} n^2$$

(c) 中去掉的边数最多为

$$n \cdot \frac{\epsilon}{4M} n \cdot M = \frac{\epsilon}{4} n^2$$

这是因为  $n$  顶点中每个顶点最多与  $(\epsilon/4M)n$  个“小”块中的顶点相邻，并且最多有  $M$  个“小”的块。

我们看到，通过删除“表现不佳”的对之间的边来清理图并不会删除太多边。我们声称在这个过程中之后，对于某些  $\delta$ ，该图是 **triangle-free** 的。删除引理和该声明相恰，因为前一步从图中删除的边数小于  $\epsilon n^2$ 。

我们假设在遵循上述过程并（可能）移除一些边后，得到的图中仍然有三角形。然后我们可以找到包含这个三角形的每个顶点所在的块  $V_i, V_j, V_k$ （不一定是不同的）。因为 (a) 和 (b) 中描述的对之间的边被删除， $V_i, V_j, V_k$  满足三角形计数引理的假设。将定理 3.4 应用于这三组子集，该图仍然至少有

$$\left(1 - \frac{\epsilon}{2}\right) \left(\frac{\epsilon}{4}\right)^3 \cdot |V_i| |V_j| |V_k|$$

个三角形。通过 (c) 知，这些区域中的每一个的大小都至少为  $(\epsilon/4M)n$ ，所以实际上  $(V_i, V_j, V_k)$  是三角形的数量至少是

$$\left(1 - \frac{\epsilon}{2}\right) \left(\frac{\epsilon}{4}\right)^3 \left(\frac{\epsilon}{4M}\right)^3 \cdot n^3$$

然后通过选择正的

$$\delta < \frac{1}{6} \left(1 - \frac{\epsilon}{2}\right) \left(\frac{\epsilon}{4}\right)^3 \left(\frac{\epsilon}{4M}\right)^3$$

我们得到了一个矛盾，因为根据假设，原始图有少于  $\delta n^3$  个三角形，但是三角形计数引理表明，在删除图中的一些边后，图中严格地多于这么多三角形。此处存在  $1/6$  的系数用来处理可能发生的重复计数（例如，当  $V_i = V_j = V_k$  时）。因此假设不成立。由于  $\delta$  仅取决于  $\epsilon$  和定理 3.1 中的常数  $M$ ，这就完成了证明。

### 笔记

在上述证明中， $\delta$  取决于  $M$ ，即定理 3.1 中的常数。如定理 3.3 所述，常数  $M$  的增长是迅速的。我们的证明仅表明我们可以选择  $\delta$  使得  $1/\delta$  被高度为  $\epsilon^{-O(1)}$  的 2 的迭代幂次控制。事实上，只要我们选择  $\delta$  使得  $1/\delta$  被一个高度为  $O(\log(1/\epsilon))$  的 2 的迭代幂次控制，三角形删除引理成立。相比之下，在本文中最著名的“下界”结果是，如果  $\delta$  满足定理 3.5 的条件，则  $1/\delta$  的上界为  $\epsilon^{-O(\log(1/\epsilon))}$ （这个上界来自我们很快将讨论到的  $3-AP$ -free 集的构造）。这些上界和下界之间的差距很大，缩小这个差距是图论中的一个主要的开放性问题。

从历史上看，证明定理 3.5 的一个主要动机是该引理与 Roth 定理的联系。这种联系来自于前面在问题 1.2 中提到的一种特殊类型的图。三角形删除引理的以下推论有助于研究此类图。

#### 推论 3.1

$G$  是一个  $n$  顶点图，且  $G$  的每条边都位于一个唯一的三角形中，则  $G$  有  $o(n^2)$  条边。

**证明** 假设  $G$  有  $m$  条边。因为每条边都在一个三角形中，所以  $G$  中的三角形数是  $m/3$ 。由于  $m < n^2$ ，所以  $G$  有  $o(n^3)$  个三角形。通过备注 3.2，我们可以删除  $o(n^2)$  条边，使  $G$  变成 **triangle-free** 图。但是根据假设，删除一条边最多从图中删除一个三角形，因此在此过程中删除的边数至少为  $m/3$ 。因此  $m = o(n^2)$ 。

### 3.3 Roth 定理

#### 定理 3.6 (Roth 定理)

每个具有正上密度的整数的子集都包含一个长度为 3 的等差数列。

#### 证明

取没有长度为 3 的等差数列的  $[N]$  的子集  $A$ 。我们将证明  $A$  有  $o(N)$  个元素，从而证明了定理。为了简化证明并且避免处理  $A$  中涉及大元素的边缘情况，我们将  $A$  嵌入到一个循环群中。取  $M = 2N + 1$ ，我们有  $A \subseteq \mathbb{Z}/M\mathbb{Z}$ 。由于我们选取的  $M$  足够大，满足  $A$  中任意两个元素的总和小于  $M$ ，因此不会发生回绕，并且  $A$  没有长度为 3 的等差数列在  $\mathbb{Z}/M\mathbb{Z}$  中。

现在，我们构造一个三部图  $G$ ，其中的部分  $X, Y, Z$  都是  $\mathbb{Z}/M\mathbb{Z}$  的拷贝。如果  $y - x \in A$ ，则将顶点  $x \in X$  连接到顶点  $y \in Y$ 。类似地，如果  $z - y \in A$ ，则将  $z \in Z$  与  $y \in Y$  连接起来。最后，如果  $(z - x)/2 \in A$ ，则连接  $x \in X$  和  $z \in Z$ 。因为我们选择的  $M$  为奇数，所以 2 是模  $M$  可逆的，最后一步是合理的。

如果  $x, y, z$  构成一个三角形，那么元素

$$y - x, \frac{z - x}{2}, z - y$$

都属于  $A$ 。这些数字按所列顺序形成等差数列。然后，对  $A$  的假设告诉我们上面列出的元素都是相等的。这个条件等价于说  $x, y, z$  是  $\mathbb{Z}/M\mathbb{Z}$  中的等差数列。

因此， $G$  的每条边都恰好位于一个三角形中。这是因为给定一条边（即  $\mathbb{Z}/M\mathbb{Z}$  的两个元素），存在一种方法可以将该边扩展为唯一的三角形（以正确的顺序添加该组的另一个元素以形成等差数列）。

那么推论 3.1 意味着  $G$  有  $o(M^2)$  条边。但是通过构造  $G$  正好有  $3M|A|$  条边。由于  $M = 2N + 1$ ，因此  $|A|$  是  $o(N)$  的。

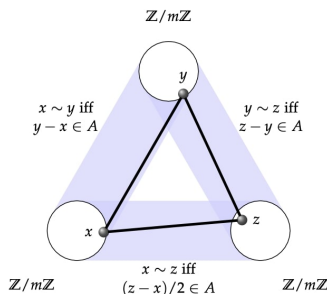


图 3.2: Roth 定理定理证明的图构造

在本书的后面，我们讨论了 Roth 定理的傅里叶分析证明，尽管它使用了不同的方法，但和上述证明具有相似的思路。

如果我们注意三角形删除引理所隐含的上界，我们在这里的证明会得到  $|A|$  的上界  $N/(\log^* N)^c$ ，其中  $\log^* N$  表示必须对  $N$  取对数多次直到值小于 1，而  $c$  是某个常数。这是我们之前看到的 2 的迭代次幂的反函数。目前为止  $A$  的最佳上界为：如果  $A$  没有长度为 3 的等差数列，则

$$|A| \leq \frac{N}{(\log N)^{1-o(1)}}$$

在下一节中，我们将证明任何没有长度为 3 的等差数列的  $[N]$  子集大小的下界。事实证明，存在大小为  $N^{1-o(1)}$  的  $A \subseteq [N]$  不包含长度为 3 的等差数列。实际上，我们将提供一个示例，其中对于某些常量  $C$ ， $|A| \geq Ne^{-C\sqrt{\log N}}$ 。

#### 笔记

除了推论 3.1 中给出的结果之外，对问题 1.2 的答案我们知之甚少。在 Roth 定理的证明中，我们知道，给定




$[N]$  的任何没有 3 项等差数列的子集  $A$ , 我们可以在  $O(N)$  顶点上构造一个图, 该图具有  $N|A|$  数量级的边, 并且它的每条边都包含在一个唯一的三角形中。这或多或少是构造相对稠密图的唯一已知方法, 其特性是每条边都包含在一个唯一的三角形中。

### 3.4 构造没有三项等差数列的集合

构造没有三项等差数列 (长度为 3 的等差数列) 的子集  $A \subseteq [N]$  的一种方法是贪婪构造具有这种性质的自然数的子序列。产生的序列如下, 我们称之为 Stanley 序列:

0 1 3 4 9 10 12 13 27 28 30 31

 **笔记** 给定任何三个不同的数字  $a, b, c$ , 他们的三进制表示中不包含数字 2, 所以我们将任意两个这样的三进制数相加, 不会出现进位的情况。然后,  $2b = b + b$  的三进制表示中每个数字都是 0 或 2, 而  $a + c$  的三进制表示中数字 1 将出现在  $a$  和  $c$  不同的位上<sup>3</sup>。因此  $a + c \neq 2b$ , 即任意三个这样的数都不构成等差数列。

这个序列全由三进制表示只有数字 0 和 1 的自然数组成。  $N = 3^k$ , 如此构造的子集  $A \subseteq [N]$  大小为  $|A| = 2^k = N^{\log_3 2}$ 。很长一段时间, 人们都认为这个例子接近最优。但在 1940 年代, Salem 和 Spencer 发现了更好的构造 (1942)。他们的证明后来被 Behrend 简化和改进 (1946), 我们将在下面介绍他的版本。令人惊讶的是, 自从上世纪 40 年代以来, 这个下界几乎没有被改进。

#### 定理 3.7

存在一个常数  $C > 0$  使得对于每个正整数  $N$ , 存在一个子集  $A \subseteq [N]$ , 该子集的大小  $|A| \geq N e^{-C\sqrt{\log N}}$ , 并且该子集不包含长度为 3 的等差数列。



#### 证明

令  $m$  和  $d$  为两个正整数, 他们的取值我们稍后指明。考虑在  $d$  维中的格点盒  $X := [m]^d$ , 以及它与半径为  $\sqrt{L} (L \in \mathbb{N})$  的球体的交点

$$X_L := \{(x_1, \dots, x_d) \in X : x_1^2 + \dots + x_d^2 = L\}$$

设  $M := dm^2$ , 我们有  $X = X_1 \sqcup \dots \sqcup X_M$ 。根据鸽巢原理, 存在  $L_0 \in [M]$  使得  $|X_{L_0}| \geq m^d/M$ 。考虑映射  $\varphi : X \rightarrow \mathbb{N}$ , 其定义为

$$\varphi(x_1, \dots, x_d) := \sum_{i=1}^d x_i (2m)^{i-1}$$

显然,  $\varphi$  是单射的。此外, 又因为  $(x_1, \dots, x_d)$  中的每个元素都在  $[m]$  中, 容易发现任何三个不同的  $\vec{x}, \vec{y}, \vec{z} \in X$  映射到  $\mathbb{N}$  中形成等差数列当且仅当  $\vec{x}, \vec{y}, \vec{z}$  在  $X$  中构成等差数列。作为球的子集, 集合  $X_{L_0}$  没有长度为 3 的等差数列。所以  $X_{L_0}$  的像  $\varphi(X_{L_0})$  也没有长度为 3 的等差数列。因此, 取  $m = \frac{1}{2} \lceil e^{\sqrt{\log N}} \rceil$  和  $d = \lfloor \sqrt{\log N} \rfloor$  我们可以找到  $[N]$  的一个子集, 即  $A = \varphi(X_{L_0})$ , 不包含长度为 3 的等差数列, 其大小

$$|A| = |X_{L_0}| \geq \frac{m^d}{dm^2} \geq N e^{-C\sqrt{\log N}}$$

其中  $C$  是某大于 0 的常数。

接下来, 让我们研究 Roth 定理的一些变体。我们将从 Roth 定理的更高维版本开始, 它是第 1 章中提到的多维 Szemerédi 定理的一个特例。

#### 定义 3.5

$\mathbb{Z}^2$  中的角 (corner) 是形如  $\{(x, y), (x+d, y), (x, y+d)\}$  的三元集, 其中  $d > 0$ 。



<sup>3</sup> $a$  和  $c$  在某一位置上的数字不同, 他们只能一个是 0 一个是 1, 所以  $a + c$  该位上是 1

**定理 3.8**

如果子集  $A \subseteq [N]^2$  中没有角，则  $|A| = o(N^2)$ 。

**证明**

考虑和集<sup>4</sup>  $A+A \subseteq [2N]^2$ 。根据鸽巢原理，存在点  $z \in [2N]^2$  使得至少有  $\frac{|A|^2}{(2N)^2}$  对  $(a, b) \in A \times A$  满足  $a+b=z$ 。令  $A' = A \cap (z-A)$  那么， $A'$  的大小正好是  $z$  写成  $A$  的两个元素之和的方案数。所以， $|A'| \geq \frac{|A|^2}{(2N)^2}$ ，接下来我们只需证明  $|A'| = o(N^2)$  即可。另外，注意到  $A' = z - A'$ ，所以集合  $A'$  没有  $d \neq 0$  的角。

现在，构建一个三部分分别为  $X = \{x_1, \dots, x_N\}, Y = \{y_1, \dots, y_N\}$  和  $Z = \{z_1, \dots, z_{2N}\}$  的三部图。其中，每个顶点  $x_i$  对应一条垂直线  $\{x=i\} \subseteq \mathbb{Z}^2$ ，每个顶点  $y_j$  对应一条水平线  $\{y=j\}$ ，每个顶点  $z_k$  对应一条斜率为  $-1$  的斜线  $\{y=-x+k\}$ 。当且仅当相应的线的交点属于  $A'$ ， $G$  的两个不同顶点用边相连。然后，图  $G$  中的每个三角形对应于一组三条线，且每对线的交点在  $A'$  中。由于  $A'$  没有  $d \neq 0$  的角，当且仅当三条对应的线经过  $A'$  中同一个点并且形成一个  $d=0$  的角，三个顶点  $x_i, y_j, z_k$  在  $G$  中诱导出一个三角形。由于恰好有一条垂直线、一条水平线和一条斜率为  $-1$  的线穿过  $A'$  中的每个点，因此  $G$  的每条边都恰好属于一个三角形。因此，根据推论 3.1，

$$3|A'| = e(G) = o(N^2)$$

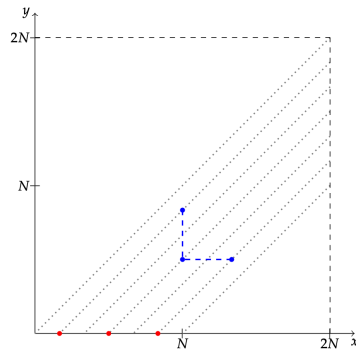


图 3.3: 三条线相交示意图

请注意，我们可以通过以下方式从角定理推导出 Roth 定理。

**推论 3.2**

令  $r_3(N)$  为不包含长度为 3 的等差数列的  $[N]$  的最大子集的大小， $r_L(N)$  为不包含角的  $[N]^2$  的最大子集的大小。则， $r_3(N)N \leq r_L(2N)$ 。

**证明** 给定任一集合  $A \subseteq [N]$ ，定义集合

$$B := \{(x, y) \in [2N]^2 : x - y \in A\}$$

因为对于每个  $a \in [N]$  至少有  $n$  对  $(x, y) \in [2N]^2$  使得  $x - y = a$ ，所以我们有  $|B| \geq N|A|$ 。此外，由于  $B$  中的每个角  $\{(x, y), (x+d, y), (x, y+d)\}$  将通过  $(x, y) \mapsto x - y$  被投影成  $A$  中长度为 3 的等差数列  $\{x - y - d, x - y, x - y + d\}$ 。所以，如果  $A$  没有长度为 3 的等差数列，则  $B$  没有角。因此， $r_3(N)N \leq r_L(2N)$ 。

因此，任何 corner-free 集上界都是  $3-AP$ -free 集的上界，而任何的  $3-AP$ -free 下界都是 corner-free 集的下界。值得一提的是，Behrend 的  $3-AP$ -free 集的构造很容易扩展到大型  $3-AP$ -free 集的构造。我们目前所知的  $[N]^2$  的 corner-free 子集大小的最佳上界是  $N^2(\log \log N)^{-C}$ ，其中  $C > 0$  是某常数，Shkredov 使用傅立叶分析的方法证明了这一点 (2006)。

<sup>4</sup>在加性组合中，阿贝尔群  $G$  中的两个子集  $A$  与  $B$  的和集（也被称为闵可夫斯基和）被定义为  $A$  中任意元素与  $B$  中任意元素之和的集合。

### 3.5 图嵌入、计数和删除引理

如三角形删除引理定理 3.5 的证明所展示的, 删除引理的一个关键前奏是计数引理。因此, 我们想将三角形计数引理推广到一般图形。为了实现我们的目标, 我们有两种策略: 一种是将计数图的顶点一个一个嵌入, 使得嵌入的顶点有很多选择; 另一种是分析一次删除一条边。

#### 定理 3.9 (图嵌入引理)

令  $H$  为顶点度不超过  $\Delta$  的  $r$  部图。在图  $G$  中, 令  $V_1, \dots, V_r \subseteq V(G)$  是大小至少为  $\frac{1}{\epsilon} v(H)$  的顶点集。如果每对  $(V_i, V_j)$  是  $\epsilon$ -正则的并且密度  $d(V_i, V_j) \geq 2\epsilon^{1/\Delta}$ , 则  $G$  包含  $H$  的副本。

**笔记** 定理中的顶点集  $V_1, \dots, V_r$  不需要不相交甚至不需要不同。

我们将介绍证明的一些想法, 省略细节。定理 3.9 的证明是定理 3.4 证明的扩展。

假设我们试图嵌入  $H = K_4$ , 其中  $K_4$  的每个顶点都进入到自己的块, 其中四个块是两两之间是  $\epsilon$ -正则的且边密度不太小。我们按顺序嵌入顶点, 大多数第一个顶点的选择不会将剩余顶点的可能性减少一个比基于边密度的预期的要多得多的因子。第一个顶点已经嵌入后, 我们继续第二个顶点, 再次选择一个嵌入, 以便为第三个和第四个顶点保留较多的可能性, 依此类推。

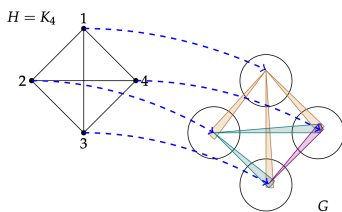


图 3.4: 嵌入  $H = K_4$  的示意图

接下来, 我们使用我们的第二个策略来证明计数引理。

#### 定理 3.10 (图计数引理)

令  $H$  是一个  $V(H) = [k]$  的图, 令  $\epsilon > 0$ 。令  $G$  是一个  $n$  顶点图, 顶点子集  $V_1, \dots, V_k \subseteq V(G)$  对于任意  $\{i, j\} \in E(H)$ ,  $(V_i, V_j)$  是  $\epsilon$ -正则的。则元组  $(v_1, \dots, v_k) \in V_1 \times \dots \times V_k$  的数量大约为

$$\left( \prod_{\{i, j\} \in E(H)} d(V_i, V_j) \right) \left( \prod_{i=1}^k |V_i| \right)$$

且最大相差  $e(H)\epsilon |V_1| \cdots |V_k|$ 。其中, 元组  $(v_1, \dots, v_k)$  满足对于所有的  $\{i, j\} \in E(H)$ ,  $\{v_i, v_j\} \in E(G)$ 。

**笔记** 该定理可以改写为以下概率形式: 均匀随机且独立地选择  $v_1 \in V_1, \dots, v_k \in V_k$ 。则,

$$\left| \mathbb{P}(\{v_i, v_j\} \in E(G) \text{ for all } \{i, j\} \in E(H)) - \prod_{\{i, j\} \in E(H)} d(V_i, V_j) \right| \leq e(H)\epsilon \quad (3.2)$$

**证明** 我们可以假设  $\{1, 2\}$  是  $H$  的边 (如果不是可以通过对顶点重新标号实现)。为了简化符号, 记

$$P = \mathbb{P}(\{v_i, v_j\} \in E(G) \text{ for all } \{i, j\} \in E(H))$$

我们将证明

$$|\mathbb{P} - d(V_1, V_2) \mathbb{P}(\{v_i, v_j\} \in E(G) \text{ for all } \{i, j\} \in E(H) \setminus \{\{1, 2\}\})| \leq \epsilon \quad (3.3)$$

合并两个选择  $v_i$  的随机过程, 我们证明当  $v_3 \dots v_k$  是任意给定的并且只有  $v_1$  和  $v_2$  是随机时 (3.3) 成立即可。

定义

$$A_1 := \{v_1 \in V_1 : \{v_1, v_i\} \in E(G) \text{ whenever } i \in N_H(1) \setminus \{2\}\}$$

$$A_2 := \{v_2 \in V_2 : \{v_2, v_i\} \in E(G) \text{ whenever } i \in N_H(2) \setminus \{1\}\}$$

如果  $|A_1| \leq \epsilon |V_1|$  或者  $|A_2| \leq \epsilon |V_2|$ , 则

$$\frac{e(A_1, A_2)}{|V_1| |V_2|} \leq \frac{|A_1| |A_2|}{|V_1| |V_2|} \leq \epsilon$$

显然有

$$d(V_1, V_2) \frac{|A_1| |A_2|}{|V_1| |V_2|} \leq \epsilon$$

所以

$$\left| \frac{e(A_1, A_2)}{|V_1| |V_2|} - d(V_1, V_2) \frac{|A_1| |A_2|}{|V_1| |V_2|} \right| \leq \epsilon$$

否则, 如果  $|A_1| > \epsilon |V_1|$  且  $|A_2| > \epsilon |V_2|$ , 则由  $(V_1, V_2)$  的  $\epsilon$ -正则性, 我们也有

$$\begin{aligned} & \left| \frac{e(A_1, A_2)}{|V_1| |V_2|} - d(V_1, V_2) \frac{|A_1| |A_2|}{|V_1| |V_2|} \right| \\ &= \left| \frac{e(A_1, A_2)}{|A_1| |A_2|} - d(V_1, V_2) \right| \cdot \frac{|A_1| |A_2|}{|V_1| |V_2|} < \epsilon \end{aligned}$$

因此, 无论哪种情况, 当  $v_3 \dots v_k$  分别被视为  $V_3 \dots V_k$  中的固定顶点时, (3.3) 都成立。

为了完成计数引理的证明, 我们对  $e(H)$  进行归纳。令  $H'$  表示从  $H$  中去除边  $\{1, 2\}$  得到的图, 并假设当  $H$  被  $H'$  代替时 (3.2) 始终成立。然后,

$$\begin{aligned} & \left| P - \prod_{\{i,j\} \in E(H)} d(V_i, V_j) \right| \\ & \leq d(V_1, V_2) \left| \mathbb{P}(\{v_i, v_j\} \in E(G) \text{ for all } \{i, j\} \in E(H')) - \prod_{\{i,j\} \in E(H')} d(V_i, V_j) \right| \\ & \quad + \left| P - d(V_1, V_2) \mathbb{P}(\{v_i, v_j\} \in E(G) \text{ for all } \{i, j\} \in E(H')) \right| \\ & \leq d(V_1, V_2) e(H') \epsilon + \epsilon \\ & \leq (e(H') + 1) \epsilon = e(H) \epsilon \end{aligned}$$

第一个不等号成立是因为  $|a - b| \leq |a - c| + |c - b|$ 。

#### 定理 3.11 (图删除引理)

对于任意图  $H$  和任意常数  $\epsilon > 0$ , 存在一个常数  $\delta > 0$ , 使得每个  $H$  副本数小于  $\delta n^{v(H)}$  的  $n$  顶点图  $G$  可以通过删除不超过  $\epsilon n^2$  条边, 变成  $H$ -free 图。

图删除引理的证明和定理3.5的证明是类似的, 思路如下:

- 使用图正则性引理划分顶点集。
- 删除边密度低的对、非正则对和其中一个块较小的对之间的所有边。
- 计算剩余边的数量, 并证明如果图中仍然包含  $H$  的副本, 那么它将包含非常多的  $H$  的副本, 从而得出矛盾。

我们现在准备证明定理 2.3, 我们先来回顾一下该定理。

#### 定理 3.12 (Erdős-Stone-Simonovits)

对于任何给定的图  $H$ , 我们有

$$\text{ex}(n, H) = \left( 1 - \frac{1}{\chi(H) - 1} + o(1) \right) \frac{n^2}{2}$$

## 证明

固定常数  $\epsilon > 0$ 。令  $r+1$  表示  $H$  的色数， $G$  是任意具有至少  $\left(1 - \frac{1}{r} + \epsilon\right) \frac{n^2}{2}$  条边的  $n$  顶点图。我们断言如果  $n = n(\epsilon, H)$  足够大，则  $G$  中一定包含  $H$  的副本。令  $V(G) = V_1 \sqcup \cdots \sqcup V_m$  是图  $G$  顶点集的  $\eta$ -正则划分，其中  $\eta := \frac{1}{2e(H)} \left(\frac{\epsilon}{8}\right)^{e(H)}$ 。我们移除一条边  $(x, y) \in V_i \times V_j$  如果满足以下任一条件：

(a)  $(V_i, V_j)$  不是  $\eta$ -正则的

(b)  $d(V_i, V_j) < \frac{\epsilon}{8}$

(c)  $|V_i|$  或  $|V_j|$  小于  $\frac{\epsilon}{8m}n$

落入情况 (a) 的边数不超过  $\eta n^2$ ，落入情况 (b) 的边数不超过  $\frac{\epsilon}{8} n^2$ ，且落入情况 (c) 的边数不超过  $mn \frac{\epsilon}{8m} n = \frac{\epsilon}{8} n^2$ 。因此，删除的边总数不超过  $\eta n^2 + \frac{\epsilon}{8} n^2 + \frac{\epsilon}{8} n^2 \leq \frac{3\epsilon}{8} n^2$ 。所以，删完之后的图  $G'$  具有最少  $\left(1 - \frac{1}{r} + \frac{\epsilon}{4}\right) \frac{n^2}{2}$  条边。根据图兰定理，我们知道  $G'$  一定包含一个  $K_{r+1}$  的副本。我们用数字  $1, 2, \dots, r+1$  标记这个  $K_{r+1}$  副本的顶点。假设  $K_{r+1}$  的顶点分别位于  $V_{i_1}, \dots, V_{i_{r+1}}$  中，下标为  $i_1, \dots, i_{r+1}$  可能重复。注意到，每对  $(V_{i_r}, V_{i_s})$  都是  $\eta$ -正则的。由于  $\chi(H) = r+1$ ，因此存在正确的着色  $c: V(H) = [k] \rightarrow [r+1]$ 。对于每个  $j \in [k]$ ，令  $\tilde{V}_j := V_{c(j)}$ 。然后，我们可以应用图计数引理（定理 3.10）到  $\{\tilde{V}_j : j \in [k]\}$ ，并发现从  $H$  到  $G'$  的图同态数至少是

$$\begin{aligned} & \left( \prod_{\{i,j\} \in E(H)} d(\tilde{V}_i, \tilde{V}_j) \right) \left( \prod_{i=1}^k |\tilde{V}_i| \right) - e(H) \eta \left( \prod_{i=1}^k |\tilde{V}_i| \right) \\ & \geq \left( \left( \frac{\epsilon}{8} \right)^{e(H)} - e(H) \eta \right) \left( \frac{\epsilon n}{8m} \right)^{v(H)} \end{aligned}$$

鉴于只有  $O_H(n^{v(H)-1})$  个非单射的映射  $V(H) \rightarrow V(G)$ （多个  $H$  中的点映射到  $G$  中同一个点的情况）。因此对于足够大的  $n$ ， $G$  包含  $H$  的副本。

## 3.6 导出子图的删除引理

我们现在将考虑不同版本的图删除引理。我们现在考虑  $H$  的导出子图的副本，而不是  $H$  的副本。说明一下，如果可以通过删除  $G$  的顶点获得  $H$ ，我们说  $H$  是  $G$  的导出子图。如果  $G$  不包含与  $H$  同构的导出子图，则  $G$  是 induced- $H$ -free 的。

## 定理 3.13 (导出子图的删除引理)

对于任意图  $H$  和常数  $\epsilon > 0$ ，存在一个常数  $\delta > 0$  使得如果  $n$  顶点图的  $H$  副本数少于  $\delta n^{v(H)}$ ，则可以通过添加或删除少于  $\epsilon n^2$  条边变成 induced- $H$ -free。

我们首先尝试使用图删除引理证明中的策略（定理 3.11）。

**划分。** 使用 Szemerédi 正则性引理对顶点集正则划分。

**清除。** 删除边密度低的对（边密度小于  $\epsilon$ ）之间的所有边，并添加边密度高的对（边密度大于  $1 - \epsilon$ ）之间的所有边。但是，我们不清楚如何处理非正则对。之前，我们只是删除了非正则对之间的所有边。问题是这可能会创建许多以前并不存在的  $H$  导出副本（请注意，这对于一般的子图而言并非如此），并且在这种情况下，没有希望表明在计数过程中没有（或只有非常少的） $H$  副本。如果我们要在非正则对之间添加所有边，情况也是如此。

这就提出了一个问题，是否有一种方法可以保证划分没有非正则对。答案是否定的，可以看出半图  $H_n$  就无法做到这一点。半图  $H_n$  是顶点集为  $\{a_1, \dots, a_n, b_1, \dots, b_n\}$  上的二部图，边的集合为  $\{a_i b_j : i \leq j\}$ 。

我们的策略是证明存在另一种很好的划分，即另一个正则性引理。首先我们注意到，导出子图的删除引理是下面定理的一个特例。

## 定理 3.14 (染色图删除引理)

对于所有正整数  $k, r$  和常数  $\epsilon > 0$ ，存在一个常数  $\delta > 0$ ，如果  $\mathcal{H}$  是  $K_k$  的一组色数为  $r$  的边着色方案，则任意一组  $K_n$  的色数为  $r$  的边着色（该着色方案的所有  $k$  顶点子图的着色方案有  $\delta$  占比包含于  $\mathcal{H}$ ），可以通过对  $m$  条边进行的重新  $r$ -着色变成  $\mathcal{H}$ -free。其中， $m$  小于  $\epsilon$  乘以边的总数。

要说明的是, 导出子图的删除引理是  $r = 2$  的特殊情况。  $K_k$  的边红蓝着色, 蓝色边形成的图与  $H$  同构, 红色边形成的图是它的补图。我们不会证明染色图的删除引理, 但我们将证明导出子图的删除引理, 并且染色图的删除引理的证明思路与之类似。

为了证明导出子图的删除引理, 我们将用到一个新的正则性引理。回想一下, 对于  $V(G)$  的划分  $\mathcal{P} = \{V_1, \dots, V_k\}$ , 其中  $n = |V(G)|$ , 我们定义了能量

$$q(\mathcal{P}) = \sum_{i,j=1}^n \frac{|V_i||V_j|}{n^2} d(V_i, V_j)^2$$

在 Szemerédi 的正则性引理 (定理 3.1) 的证明中, 我们从能量递增的角度入手, 即如果  $\mathcal{P}$  不是  $\epsilon$ -正则的, 那么存在一个  $\mathcal{P}$  的加细  $\mathcal{Q}$ , 使得  $|\mathcal{Q}| \leq |\mathcal{P}|2^{|\mathcal{P}|}$  且  $q(\mathcal{Q}) \geq q(\mathcal{P}) + \epsilon^5$ 。新的正则引理如下。

### 定理 3.15 (强正则性定理)

对于任意的常数序列  $\epsilon_0 \geq \epsilon_1 \geq \epsilon_2 \dots > 0$ , 存在一个整数  $M$ , 使得每个图都有两个顶点的划分  $\mathcal{P}, \mathcal{Q}$  满足:

- $\mathcal{Q}$  是  $\mathcal{P}$  的加细,
- $|\mathcal{Q}| \leq M$ ,
- $\mathcal{P}$  是  $\epsilon_0$ -正则的,
- $\mathcal{Q}$  是  $\epsilon_{|\mathcal{P}|}$ -正则的,
- $q(\mathcal{Q}) \leq q(\mathcal{P}) + \epsilon_0$ 。



### 证明

我们反复应用下面版本的 Szemerédi 正则引理 (定理 3.1):

对于任意  $\epsilon > 0$ , 存在一个整数  $M_0 = M_0(\epsilon)$  使得对于  $V(G)$  的任意划分  $\mathcal{P}$ , 存在  $\mathcal{P}$  的加细  $\mathcal{P}'$  将  $\mathcal{P}$  中的每个部分加细为  $\leq M_0$  个块, 使得  $\mathcal{P}'$  是  $\epsilon$ -正则的。

上述版本的证明与我们定理 3.1 给出的证明基本完全相同, 除了不是从平凡划分开始而是从划分  $\mathcal{P}$  开始。

通过迭代应用上述引理, 我们获得了  $V(G)$  的一系列划分  $\mathcal{P}_0, \mathcal{P}_1, \dots$ 。其中,  $\mathcal{P}_0$  是一个平凡的划分。由定理知, 每个  $\mathcal{P}_{i+1}$  是  $\mathcal{P}_i$  的加细,  $\mathcal{P}_{i+1}$  是  $\epsilon_{|\mathcal{P}_i|}$ -正则的, 而  $|\mathcal{P}_{i+1}| \leq |\mathcal{P}_i| M_0(\epsilon_{|\mathcal{P}_i|})$ 。

由于  $0 \leq q(i) \leq 1$ , 存在  $i \leq \epsilon_0^{-1}$  使得  $q(\mathcal{P}_{i+1}) \leq q(\mathcal{P}_i) + \epsilon_0$ 。令  $\mathcal{P} = \mathcal{P}_i, \mathcal{Q} = \mathcal{P}_{i+1}$ 。因为我们最多迭代  $\epsilon_0^{-1}$  次, 每次加细增加有限数量个部分 (仅取决于相应的  $\epsilon_{|\mathcal{P}_i|}$ ), 我们有  $|\mathcal{Q}| = O_{\epsilon}(1)$ 。

这个证明给出的常数  $M$  的界是什么?  $M$  取决于序列  $\epsilon_i$ 。例如, 如果  $\epsilon_i = \frac{\epsilon}{i+1}$ , 则  $M$  本质上是  $M_0$  连续迭代  $\frac{1}{\epsilon}$  次。注意,  $M_0$  是一个塔函数<sup>5</sup>, 所以  $M$  是迭代  $i$  次的塔函数  $\text{Tower}(\text{Tower}(\text{Tower}(\dots)))$ 。我们把这个迭代的塔函数称为 wowzer 函数。

事实上, 我们可以进一步保证  $\mathcal{P}$  和  $\mathcal{Q}$  的划分是均衡的, 其证明思路与定理 3.2 相同。

接下来, 我们给出如下形式的强正则性引理, 它将帮助我们证明导出子图的删除引理。

### 推论 3.3

对于任意常数序列  $\epsilon_0 \geq \epsilon_1 \geq \epsilon_2 \dots > 0$ , 存在一个常数  $\delta > 0$  使得每个  $n$  顶点图有一个均衡的顶点划分  $V_1, \dots, V_k$  和  $W_i \subset V_i$  使得

- (a)  $|W_i| \geq \delta n$
- (b) 对于所有  $1 \leq i \leq j \leq k$ ,  $(W_i, W_j)$  是  $\epsilon_k$ -正则对
- (c) 对于所有的  $(i, j) \in [k]^2$ ,  $|d(V_i, V_j) - d(W_i, W_j)| \leq \epsilon_0$  成立的次数少于  $\epsilon_0 k^2$



<sup>5</sup> $\text{Tower}(i) :=$  高度为  $i$  的 2 的迭代次幂, 即 2 连续取幂于自己  $n$  次,  $\underbrace{2^{2^{\dots^2}}}_{i \text{ times}}$



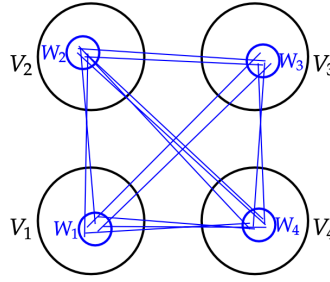


图 3.5: 具有正则子集的顶点划分

**证明 [概要]**

让我们首先解释如何获得几乎满足 (b) 的划分。请注意，在不要求  $(W_i, W_i)$  是正则的情况下，我们可以通过在均衡强正则引理中  $\mathcal{P}$  的每个块中均匀随机选取  $Q$  的块来得到  $W_i \subseteq V_i$ 。因为  $Q$  是强正则的，所以  $i \neq j$  的所有  $(W_i, W_j)$  都是正则的概率很高。更进一步，我们也可以使得每个  $(W_i, W_i)$  都是正则的，细节留给读者。

通过这种构造，(c) 可由  $q(Q) \leq q(\mathcal{P}) + \epsilon_0$  推导出。回想一下引理 3.1 的证明，能量  $q$  是随机变量  $Z$  的平方的期望。对于随机的  $i, j$ ， $Z_{\mathcal{P}} = d(V_i, V_j)$ 。所以  $q(Q) - q(\mathcal{P}) = \mathbb{E}[Z_Q^2] - \mathbb{E}[Z_{\mathcal{P}}^2] = \mathbb{E}[(Z_Q - Z_{\mathcal{P}})^2]$ ，其中最后一个等号是通过等式  $\mathbb{E}[(X - \mu)^2] = \mathbb{E}[X^2] - \mu^2$  得到的，下面我们会详细说明。为了证明最后一个等号，我们将期望扩展为  $\mathcal{P}$  的所有对的总和。在每一对上， $Z_{\mathcal{P}}$  是常数，而  $Z_Q$  是它的平均值，因此每一对和总和都遵循等式。然后将随机变量重新解释为边密度便得到 (c)。

最后，注意到  $|Q| \leq M$ ，又因为划分是均衡的，所以存在  $\delta$  满足 (a)。

我们现在将使用推论 3.3 证明导出子图的删除引理。

**证明 [定理 3.13]** 我们将分 3 步进行。

**1. 划分**

我们应用推论得到一个划分  $V_1 \cup \dots \cup V_k$  和  $W_1 \subseteq V_1, \dots, W_k \subseteq V_k$ ，使得下面的内容成立：

- 对于所有  $i \leq j$ ， $(W_i, W_j)$  是  $\frac{1}{(v(H))} \left(\frac{\epsilon}{4}\right)^{\binom{v(H)}{2}}$ -正则的
- 对于所有的  $(i, j) \in [k]^2$ ， $|d(V_i, V_j) - d(W_i, W_j)| \leq \frac{\epsilon}{2}$  成立的对数小于  $\frac{\epsilon k^2}{2}$
- $|W_i| \geq \delta_0 n$ ，其中  $\delta_0 = \delta_0(\epsilon, H) > 0$

**2. 删除**

对于所有  $i \leq j$ （包括  $i = j$ ）：

- 如果  $d(W_i, W_j) \leq \frac{\epsilon}{2}$ ，我们移除  $(V_i, V_j)$  之间的所有边。
- 如果  $d(W_i, W_j) \geq 1 - \frac{\epsilon}{2}$ ，那么我们添加  $(V_i, V_j)$  之间的所有边。

根据构造，从  $G$  添加/删除的边总数小于  $2\epsilon n^2$ 。

**3. 计数**

我们只需证明完成删除步骤后  $G$  中没有导出子图  $H$  的副本。假设有导出子图  $H$  的副本。令  $\phi: V(H) \rightarrow [k]$  是  $H$  副本的每个顶点所在的块的函数。换句话说，对于  $H$  的副本，顶点  $v \in V(H)$  位于  $V_{\phi(v)}$  中。现在的目标是应用计数引理来证明实际上在  $G$  中有很多  $H$  的副本，其中  $v \in V(H)$  映射到  $W_{\phi(v)}$  中的一个顶点。我们将使用以下技巧：修改  $G$  得到图  $G'$ 。对于该图  $G'$ ，当且仅当在  $G$  上出现导出子图  $H$  的副本时，存在  $V(H)$  顶点上的完全图，该完全图的顶点来自  $\phi$  给出的块。

我们以如下方式构造  $G'$ 。 $H$  中同一顶点的两个拷贝之间的边将永远不会出现在  $G'$ 。对于  $G'$  中的所有其他顶点对，它们之间是否存在边由以下方式确定：如果  $uv$  是边，则  $G'$  中的  $V_{\phi(v)}$  和  $V_{\phi(u)}$  之间的边与  $G$  中的相同。如果  $uv$  不是边，则  $G'$  中的  $V_{\phi(v)}$  和  $V_{\phi(u)}$  之间的边与  $G$  的补图中的相同。

请注意，此  $G'$  确实满足所需的属性——如果  $G'$  在这些块  $V_{\phi(v)}$  的顶点上存在完全子图，则  $G$  在相同的顶点上有一个导出子图  $H$ 。现在通过图计数引理（定理 3.10）， $K_{v(H)}$ （每一个  $u \in V(H)$  来自  $W_{\phi(u)}$ ）的数量大约为

$$\prod_{uv \in E(H)} d(W_{\phi(u)}, W_{\phi(v)}) \prod_{uv \in E(\bar{H})} (1 - d(W_{\phi(u)}, W_{\phi(v)})) \prod_{u \in V(H)} |W_{\phi(u)}|$$

误差最大不超过

$$\left(\frac{\epsilon}{4}\right)^{\binom{v(H)}{2}} \prod_{u \in V(H)} |W_{\phi(u)}|$$

因此, 在  $G$  中导出子图  $H$  的数量至少是

$$\left(\left(\frac{\epsilon}{2}\right)^{\binom{v(H)}{2}} - \left(\frac{\epsilon}{4}\right)^{\binom{v(H)}{2}}\right) \delta_0^{v(H)} n^{v(H)}$$

矛盾。所以删除边之后的图不存在导出子图  $H$  的副本。

值得一提的是, 强正则性引理很有用, 因为它允许我们在有限的意义上摆脱非正则划分的限制。

**定理 3.16 (无限版本删除引理 Alon and Shapira 2008)**

对于任意 (可能是无限的) 图  $\mathcal{H}$  和  $\epsilon > 0$ , 都存在  $h_0$  和  $\delta > 0$ , 使得对于任意  $n$  顶点图, 如果它的  $H$  副本数少于  $\delta n^{v(H)}$  (其中  $H \in \mathcal{H}$  且  $v(H) \leq h_0$ ), 则可以通过添加或删除少于  $\epsilon n^2$  条边变成 induced- $H$ -free。

该定理的证明与导出子图的删除引理证明类似。

### 3.7 属性检测 (property testing)

我们正在寻找一种有效的随机算法来区分 triangle-free 的大图和  $\epsilon$ -远离 triangle-free 的图。我们说一个图是  $\epsilon$ -远离属性  $\mathcal{P}$  的, 如果为了获得属性  $\mathcal{P}$  需要改变 (添加或删除) 的最小边数大于  $\epsilon n^2$ 。我们给出算法如下。

**命题 3.1 (算法)**

对顶点的随机三元组进行采样, 并检查它们是否形成三角形。重复  $C(\epsilon)$  次, 如果没有找到三角形, 则返回该图是 triangle-free 的。否则, 返回该图是  $\epsilon$ -远离 triangle-free 的。

**定理 3.17**

对于任意常数  $\epsilon > 0$ , 存在一个常数  $C(\epsilon)$ , 使得算法 3.1 给出正确答案的概率大于  $\frac{2}{3}$ 。

**证明** 如果图  $G$  是 triangle-free 的, 则算法总是成功的, 因为没有采样的三元组会形成三角形。如果  $G$  是  $\epsilon$ -远离 triangle-free 的, 那么根据三角形删除引理,  $G$  至少有  $\delta n^3$  个三角形, 其中  $\delta = \delta(\epsilon)$  来自三角形删除引理 (定理 3.5)。我们固定样本数为  $C(\epsilon) = \frac{1}{\delta}$ 。算法失败的概率等于我们完全没有对三角形进行采样的概率, 由于每个样本是独立挑选的, 这个概率是

$$\left(1 - \frac{\delta n^3}{\binom{n}{3}}\right)^{1/\delta} \leq (1 - 6\delta)^{1/\delta} \leq e^{-6}$$

到目前为止, 我们已经看到有一个采样算法可以测试一个图是 triangle-free 的还是  $\epsilon$ -远离 triangle-free 的。我们能找到任何其他可测试的属性吗? 更确切地说, 对于哪些属性  $\mathcal{P}$  有一种算法可以确定图  $G$  处于两种情况中的哪一种? (要么具有属性  $\mathcal{P}$  要么是  $\epsilon$ -远离属性  $\mathcal{P}$ )。特别的, 对于哪些图可以轻易检测出结果, 换句话说, 仅通过采样  $k = O(1)$  个顶点就知道答案?

如果某属性在删除顶点后仍然保持, 我们称该属性是可遗传的。具有遗传特性的一些例子是  $H$ -free、平面性<sup>6</sup>、induced- $H$ -free、3-可着色和完美图<sup>7</sup>。无限版本删除引理 (定理 3.16) 意味着每个遗传属性都可以轻易检测出结果, 结果为满足属性或者不满足属性。我们选择  $\mathcal{H}$  作为所有不具有  $\mathcal{P}$  属性的图的族。注意对于遗传属性  $\mathcal{P}$ , 没有  $\mathcal{P}$  属性意味着不包含任何具有  $\mathcal{P}$  属性的图。这也解释了为什么这种单边检测方法不适用于检测非

<sup>6</sup>在图论中, 平面图是可以画在平面上并且使得不同的边可以互不交叠的图。

<sup>7</sup>在图论中, 完美图是其任意导出子图的色数等于该子图的团数 (最大团的顶点数) 的图。

遗传属性。事实上，非遗传属性几乎都无法轻易检测出来。

## 3.8 超图的删除引理

对于图的每一个有趣的结论，一个自然的问题就是如何推广到超图上。我们现在介绍定理 3.11 的扩展版本，超图删除引理。回想一下  $r$ -uniform 超图，简称  $r$ -图 ( $r$ -graph)，是一对  $(V, E)$ ，其中  $E \subset \binom{V}{r}$ ，即边是  $V$  中  $r$  个元素构成的子集。

### 定理 3.18 (超图删除引理 Rödl et al. 2005, Gowers 2007)

对于任意的  $r$ -图  $H$  和任意的  $\epsilon > 0$ ，存在  $\delta > 0$  使得，如果  $n$  顶点图  $G$  中  $H$  的副本数少于  $\delta n^{V(H)}$ ，则可以通过从  $G$  中删除少于  $\epsilon n^r$  条边来使  $G$  变成  $H$ -free。



为什么我们关注这个引理？回想一下，我们从三角形删除引理的推论中推导出了 Roth 定理（定理 3.6），即每一条边恰好位于一个三角形的图都有  $o(n^2)$  条边。我们可以在这里做相同的操作，使用定理 3.18 来证明 Roth 定理的推广版本，即 Szemerédi 定理（定理 1.7）。该定理告诉我们，对于固定的  $k$ ，如果  $A \subset [N]$  是  $k$ -AP-free 的，则  $|A| = o(N)$ 。

你可能会问：我们能否对普通的图做同样的事情吗？事实上，我们不能这样做！原因在于一个叫做“线性模式的复杂性”的想法，我们在此不再详述。事实证明， $4$ -AP 的复杂度为 2，而  $3$ -AP 的复杂度为 1。到目前为止，我们介绍的技术对于复杂度为 1 的模式非常有效，但很难处理更高复杂度的模式。

我们现在介绍定理 3.18 的推论，它与推论 3.1 非常相似：

### 推论 3.4

如果  $G$  是一个 3-图，且满足每条边都包含在一个唯一的四面体中，则  $G$  有  $o(n^3)$  条边。



这个推论可由超图删除引理直接推导得到。我们现在使用这个推论来证明 Szemerédi 定理：

### 证明 [定理 1.7]

我们将证明等差数列长度  $k = 4$  的情形， $k$  取更大的值时证明是类似的。令  $M = 6N + 1$ （这里重要的是保证  $M > 3N$  并且  $M$  与 6 互质）。用  $X, Y, Z, W$  四部分构建一个 4 部的 3-图  $G$ ，每一个部分都是包含  $M$  个元素的集合，顶点的标号由  $\mathbb{Z}/M\mathbb{Z}$  构成。假设  $x, y, z, w$  分别代表  $X, Y, Z, W$  中的元素，我们按照如下规则来定义边：

$$xyz \in E(G) \quad \text{当且仅当} \quad 3x + 2y + z \in A$$

$$xyw \in E(G) \quad \text{当且仅当} \quad 2x + y - w \in A$$

$$xzw \in E(G) \quad \text{当且仅当} \quad x - z - 2w \in A$$

$$yzw \in E(G) \quad \text{当且仅当} \quad -y - 2z - 3w \in A$$

请注意， $xyzw$  是四面体当且仅当  $3x + 2y + z, 2x + y - w, x - z - 2w, -y - 2z - 3w \in A$ 。但是，这些值构成了公差为  $-x - y - z - w$  的  $4$ -AP。由于  $A$  不含  $4$ -AP，所以  $A$  中的四面体是平凡的  $4$ -AP（公差为 0）。因此，每条边都恰好位于一个四面体中。由上面的推论，边的数量为  $o(M^3)$ 。但是根据构造，边的数量是  $4M^2|A|$ ，所以我们可以得出  $|A| = o(M) = o(N)$ 。

与上述证明类似的思路可用于证明定理 1.8，该定理保证了任意正上密度的  $\mathbb{Z}^d$  的子集都包含任意星座。一个简单的例子是  $\mathbb{Z}^2$  中的正方形，由点  $(x, y), (x + d, y), (x, y + d), (x + d, y + d)$  组成，其中  $x, y \in \mathbb{Z}$  且  $d$  为正整数。

## 3.9 超图的正则性

超图正则性是一个比普通图正则性更难的概念。我们不会详细讨论，但会简单地讨论一些核心思想。请参阅 Gowers (2006) 以了解一份精彩的证明。

定义超图正则性的一个简单的尝试是将其定义为类似于普通图正则性，如下所示：

**定义 3.6 (3-graph 正则性的简单版本)**

给定一个 3-graph  $G^{(3)}$  和三个子集  $V_1, V_2, V_3 \subset V(G^{(3)})$ , 我们说  $(V_1, V_2, V_3)$  是  $\epsilon$ -正则的, 如果对于所有满足  $|A_i| \geq \epsilon |V_i|$  的  $A_i \subset V_i$ , 我们有  $|d(V_1, V_2, V_3) - d(A_1, A_2, A_3)| \leq \epsilon$ 。其中,

$$d(X, Y, Z) = \frac{e_{G^{(3)}}(X, Y, Z)}{|X||Y||Z|}$$

$$e_{G^{(3)}}(X, Y, Z) = |\{(x, y, z) \in X \times Y \times Z \mid xyz \in E(G^{(3)})\}|$$

如果你用这个定义来完成 Szemerédi 正则引理的证明, 你可以构造一个非常相似的超图版本的证明。它表明, 对于任意  $\epsilon > 0$ , 存在  $M = M(\epsilon)$  使得每个图最多可划分为  $M$  个部分, 且不是  $\epsilon$ -正则的三元组的占比小于  $\epsilon$  (回顾定义 3.3)。事实上, 如果愿意, 我们甚至可以做到划分是均衡的。

那么我们将遇到什么问题呢? 回想一下, 我们涉及 Szemerédi 正则引理的证明通常包含三个步骤: 分区、清理和计数。事实上, 我们在计数步骤将遇到麻烦。

回想一下, 正则性应该代表着伪随机性。正因为如此, 我们为什么不尝试真正的随机超图, 一起来看看会发生什么? 让我们考虑两种不同的随机 3-图结构:

1. 首先选择常量  $p, q \in [0, 1]$ 。构建一个随机图  $G^{(2)} = G(n, p)$ , 这是一个普通的 Erdős-Renyi 图。然后通过将  $G^{(2)}$  中的每个三角形作为  $G^{(3)}$  的边以概率  $q$  放进  $G^{(3)}$ 。将此称为 3-图  $A$ 。
2. 对于每条可能的边 (即顶点集的所有三元组), 以概率  $p^3 q$  生成边, 不同边的生成是独立的。将此称为 3-图  $B$ 。

$A$  和  $B$  的每个三元组都以概率  $p^3 q$  独立出现, 并且两个图都大概率满足我们上述  $\epsilon$ -正则性的概念。然而, 我们可以在这两个图中计算  $K_4^{(3)}$  (四面体) 的密度, 发现它们的概率并不相同。在图  $B$  中, 每条边出现的概率为  $p^3 q$ , 并且边独立出现, 所以四面体出现的概率为  $(p^3 q)^4$ 。然而, 在图  $A$  中, 四面体要求  $G^{(2)}$  中存在  $K_4$ 。由于  $K_4$  有 6 条边, 它以概率  $p^6$  出现在  $G^{(2)}$  中, 然后构成四面体的每个三角形以  $q$  独立出现。因此, 任何给定的四面体出现在  $A$  中的概率是  $p^6 q^4$ , 这显然与  $(p^3 q)^4$  不同。因此, 上述超图正则性的概念并没有很好地限制子图的出现频率。

然而, 这种超图正则性的概念仍然有用。事实证明, 如果  $H$  是线性的, 则超图  $H$  有一个计数引理, 它告诉我们每对边最多与 1 个顶点相交。该定理的证明类似于图计数引理 (定理 3.10)。但现在, 让我们把目标转向寻找更好的超图正则性概念。

**定义 3.7 (Triple density on top of 2-graphs)**

给定  $A, B, C \subset E(K_n)$  (将  $A, B, C$  视为子图) 和一个 3-图  $G$ ,  $d_G(A, B, C)$  被定义为三元组  $\{xyz \mid yz \in A, xz \in B, xy \in C\}$  的数量除以  $G$  中三元组的数量。

使用上面的定义, 我们可以定义一个正则的边子集三元组和一个正则划分, 我们在这里非正式地描述这两者。考虑一个划分  $E(K_n) = G_1^{(2)} \cup \dots \cup G_l^{(2)}$ , 满足对大多数三元组  $(i, j, k)$ ,  $(G_i^{(2)}, G_j^{(2)}, G_k^{(2)})$  上有许多三角形。我们认为  $(G_i^{(2)}, G_j^{(2)}, G_k^{(2)})$  是正则的, 如果对于任意满足  $(A_i^{(2)}, A_j^{(2)}, A_k^{(2)})$  上没有太少三角形的子图  $A_i^{(2)} \subset G_i^{(2)}, A_j^{(2)} \subset G_j^{(2)}, A_k^{(2)} \subset G_k^{(2)}$ , 有

$$\left| d(G_i^{(2)}, G_j^{(2)}, G_k^{(2)}) - d(A_i^{(2)}, A_j^{(2)}, A_k^{(2)}) \right| \leq \epsilon$$

接着, 我们将正则划分定义为这样的一个划分, 该划分中非正则的三元组最多占划分中所有三元组的  $\epsilon$  倍 (参考定理 3.3)。除此之外, 我们还需要对顶点集进行划分来进一步正则化  $G_1^{(2)}, \dots, G_l^{(2)}$ 。因此, 我们得到超图正则性的信息如下:

1. 给出  $E(K_n)$  的一个划分 (每一部分是一个子图), 使得  $G^{(3)}$  是伪随机的;
2. 给出  $V(G)$  的一个划分, 使得上述步骤中的图是强伪随机的 (类似于定理 3.15)。

需要提醒的是, 文献中存在许多版本的超图正则性, 并非所有版本都是明显等价的。事实上, 在某些情况下, 证明它们之间的等价性需要做很多工作。我们仍然不太确定哪种超图正则性的概念 (如果有的话) 是最“自

然的”。

与一般图正则性类似，我们可以询问超图正则性的上界是什么，该问题的答案同样令我们苦恼。对于 2-uniform 超图，即一般图，上界需要一个 TOWER 函数。对于 3-uniform 超图，上界要求我们在 Ackermann 层级向上一步，到达 WOWZER 函数（重复应用 TOWER），也称作 Pentation。对于 4-uniform 超图，我们必须在 Ackermann 层级向上再多一步，依此类推。因此，超图正则性的应用往往会给我们提供非常差的关于逆 Ackermann 的定量上界。事实上，最著名的  $k-AP$  上界如下：

**定理 3.19 (Gowers 2001)**

对于任意  $k \geq 3$ ，存在  $c_k > 0$  使得  $[N]$  的所有  $k-AP$ -free 子集至多有  $N(\log \log N)^{-c_k}$  个元素。



**笔记**  $k \geq 5$  时，这是已知最好的的上界，但对于  $k = 3, 4$  有已知更好的上界。

对于高维 Szemerédi 定理（定理 1.8），已知最好的上界一般通过超图正则性引理得到。第一个证明来自遍历理论，由于依赖于紧致性论证，它实际上没有给出定量的上界。使用超图正则性的一个主要动机是去获得定理 1.8 的定量上界。

## 3.10 Szemerédi 正则性引理的谱证明

我们之前使用能量递增的思路证明了 Szemerédi 正则性引理。我们现在解释另一种使用谱图论的证明方法。就像上面关于超图正则性的讨论一样，这个讨论将略过一些细节。

给定一个  $n$  顶点图  $G$ ，其邻接矩阵记为  $A_G$ 。由于邻接矩阵始终是实对称矩阵，因此，它一定具有实数特征值，并且可以找到一组特征向量的标准正交基。假设  $A_G$  具有特征值  $\lambda_i$  ( $1 \leq i \leq n$ )，其基于绝对值递减的排序为： $|\lambda_1| \geq |\lambda_2| \geq \dots \geq |\lambda_n|$ 。我们一个谱分解

$$A_G = \sum_{i=1}^n \lambda_i u_i u_i^T$$

其中  $u_i$  是单位特征向量，满足  $A_G u_i = \lambda_i u_i$ 。另外注意到

$$\begin{aligned} \sum_{i=1}^n \lambda_i^2 &= \text{tr}(A^2) \\ &= \sum_{i=1}^n \sum_{j=1}^n A_G(i, j)^2 \\ &= 2e(G) \\ &\leq n^2 \end{aligned}$$

其中第二个等号成立是因为  $A$  是对称的， $\text{tr}(AA) = \sum_{i=1}^n (AA)_{ii} = \sum_{i=1}^n \sum_{j=1}^m A_{ij} A_{ji} = \sum_{i=1}^n \sum_{j=1}^m A_{ij}^2$ 。

**引理 3.5**

$\lambda_i$  的定义如上，我们有

$$|\lambda_i| \leq \frac{n}{\sqrt{i}}$$

**证明** 如果  $|\lambda_k| > \frac{n}{\sqrt{k}}$  对某些  $k$  成立，则  $\sum_{i=1}^k \lambda_i^2 > n^2$ ，矛盾。

**引理 3.6**

取  $\epsilon > 0$ ， $F: \mathbb{N} \rightarrow \mathbb{N}$  是一个任意的“增长函数”，满足对所有的  $j$ ，有  $F(j) \geq j$ 。则存在  $C = C(\epsilon, F)$  使得对于所有如前所述的  $G, A_G$ ，存在  $J < C$  满足

$$\sum_{J \leq i < F(J)} \lambda_i^2 \leq \epsilon n^2$$



**证明** 令  $J_1 = 1$ ,  $J_{i+1} = F(J_i)$  ( $i \geq 1$ )。对所有的  $k \leq \frac{1}{\epsilon}$ ,  $\sum_{J_k \leq i < J_{k+1}} \lambda_i^2 > \epsilon n^2$  不总是成立, 否则总和将大于  $n^2$ 。因此, 上述不等式一定对于对某  $J = J(k)$  成立, 其中  $k \leq \frac{1}{\epsilon}$ 。因此,  $J$  是有界的; 特别的,  $J < F(F(\dots F(1)\dots))$ , 其中  $F$  迭代  $\frac{1}{\epsilon}$  次。

请将上述结论与 Szemerédi 正则性引理原始证明中的能量递增进行类比。我们现在介绍由陶哲轩提出的正则分解的思想。选择上面引理中的  $J$ , 我们可以将  $A_G$  分解为

$$A_G = A_{\text{str}} + A_{\text{sml}} + A_{\text{psr}}$$

其中“str”代表“structured”, “sml”代表“small”, “psr”代表“pseudorandom”。他们各自的定义如下:

$$\begin{aligned} A_{\text{str}} &= \sum_{i < J} \lambda_i u_i u_i^T \\ A_{\text{sml}} &= \sum_{J \leq i < F(J)} \lambda_i u_i u_i^T \\ A_{\text{psr}} &= \sum_{i \geq F(J)} \lambda_i u_i u_i^T \end{aligned}$$

其中,  $A_{\text{str}}$  大致对应有界的划分,  $A_{\text{sml}}$  大致对应非正则对,  $A_{\text{psr}}$  大致对应之间的伪随机性。

现在我们定义两个矩阵范数的概念。矩阵  $A$  的谱半径 (也称作谱范数) 定义为特征值绝对值中的最大值  $\max |\lambda_i(A)|$ 。另外, 算子范数定义为

$$\|A\| = \max_{v \neq 0} \frac{|Av|}{|v|} = \max_{u, v \neq 0} \frac{|u^T Av|}{|u||v|}$$

注意到, 对于实对称矩阵, 谱半径和算子范数是相等的。

注意到  $A_{\text{str}}$  有特征向量  $u_1, \dots, u_{J-1}$ 。这些是  $A_G$  的大特征值的特征向量。我们假设  $u_i \in \{-1, 1\}^n$ ,  $i = 1, \dots, J-1$ 。尽管这一假设是错误的, 但为了说明起见, 让我们假设情况确实如此。通过取这些坐标值, 我们看到  $u_1, \dots, u_{J-1}$  的水平集<sup>8</sup>将  $V(G)$  划分为  $P$  个部分  $V_1, \dots, V_P$  ( $P = O_{\epsilon, J}(1)$ ), 使得每个  $A_{\text{str}}$  在由该划分定义的矩阵的块上大致恒定。(  $P$  依赖  $\epsilon$  是因为坐标值的四舍五入; 实际操作中, 我们让特征向量有微小的抖动。) 然后, 对于两个顶点子集  $U \subset V_k$  和  $W \subset V_l$ , 我们有:

$$\begin{aligned} |1_U^T A_{\text{psr}} 1_W| &\leq |1_U| |1_W| \|A_{\text{psr}}\| \\ &\leq \sqrt{n} \cdot \sqrt{n} \cdot \frac{n}{\sqrt{F(J)}} \end{aligned}$$

通过选择比  $P$  大的多的  $F(J)$ , 我们可以保证上述值较小。实际上, 我们可以证明它远小于  $\epsilon \left(\frac{n}{P}\right)^2$ 。  $1_U^T A_{\text{psr}} 1_W$  的意义在于它等于  $e(U, W) - d_{kl}|U||W|$ , 其中  $d_{kl}$  是  $A_{\text{str}}$  中  $V_k \times V_l$  块中边数的平均值。因此, 这个数量很小意味着正则性的成立。

我们还可以得到  $A_{\text{sml}}$  项的平方和 (称为 Frobenius 范数) 的上界。对于实对称矩阵, 它等于 Hilbert-Schmidt 范数 (特征值的平方和):

$$\begin{aligned} \|A_{\text{sml}}\|_F &= \|A_{\text{sml}}\|_{\text{HS}} \\ &= \sum_{J \leq i \leq F(J)} \lambda_i^2 \\ &\leq \epsilon n^2 \end{aligned}$$

因此,  $A_{\text{sml}}$  最多可能破坏  $\epsilon n^2$  个对的  $\epsilon$ -正则性。所以划分仍然是正则的。

最后要说明的是, 有一些方法可以通过这种方式来得到 Szemerédi 正则性引理的其他修改版本, 例如使划分均衡。我们不会在这里讨论相关内容。

<sup>8</sup>一个具有  $n$  变量的实值函数  $f$  的水平集是具有以下形式的集合,  $\{(x_1, \dots, x_n) \mid f(x_1, \dots, x_n) = c\}$ 。



## 第4章 伪随机图

术语“伪随机”广泛指代了一系列的思想和现象。它指的是一个并不随机的对象（在某种意义下）表现得像真正随机的情况一样。比如说质数并不是随机分布的，但是它的分布有许多和正整数的随机子集相似的性质。著名的黎曼猜想就是一个典型案例，它（在某种意义上）就是在断言质数具有伪随机性。

更精准得说，我们具体的定义出一个（真随机的对象满足的）性质，然后我们就可以问这样的问题：一个给定的对象是否也具有相似的性质？在这一章中，我们就来研究图论中这样的问题，并且我们将研究一个并不随机的图可以有哪些与随机图相似的性质。

### 4.1 拟随机图

接下来，我们将介绍一个这个领域非常根本的定理，它列出了图可以具有的许多伪随机性质。这些性质看上去两两不同（有些看似很好验证，有些看似很难），但这个定理却告诉我们，这些性质全都等价。

#### 定理 4.1 (Chung, Graham, and Wilson (1989))

令序列  $\{G_n\}$  是一个图的序列，其中每个  $G_n$  都是  $n$  个点， $(p+o(1))\binom{n}{2}$  个边的图（固定一个常数  $0 < p < 1$ ）。我们把  $G_n$  简写为  $G$ 。以下的性质全部是等价的：

1. **DISC** (“discrepancy”)：对于任意  $X, Y \subset V(G)$ ,  $|e(X, Y) - p|X||Y|| = o(n^2)$ 。
2. **DISC'**：对于任意  $X \subset V(G)$ ,  $|e(X) - p\binom{|X|}{2}| = o(n^2)$ 。
3. **COUNT**：对于任意的图  $H$ ,  $H$  在  $G$  里 **带标号**（也就是说  $H$  里不同的点看作是有区别的）地出现了  $(p^{e(H)} + o(1))n^{v(H)}$  次。其中低阶项  $o(1)$  只与  $H$  有关。
4. **C<sub>4</sub>**： $C_4$  在  $G$  里 **带标号** 地出现了至多  $(p^4 + o(1))n^4$  次。
5. **CODEG** (codegree)：令  $\text{codeg}(u, v)$  表示  $u$  和  $v$  的公共邻居数，那么  $\sum_{u, v \in V(G)} |\text{codeg}(u, v) - p^2 n| = o(n^3)$ 。
6. **EIG** (eigenvalue)：假设图  $G$  的邻接矩阵的特征值是  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_{v(G)}$ ，那么  $\lambda_1 = pn + o(n)$  并且  $\max_{i \neq 1} |\lambda_i| = o(n)$ 。



**注** 特别的，对于  $d$ -正则图，最大的特征值就是  $d$  (对应的特征向量就是全壹向量)，**EIG** 在  $d$ -正则图上相当于说  $\lambda_2 = o(n)$ 。

我们可以等价地以  $\epsilon$  语言来叙述这些性质，比如说 **DISC** 可以写成这样：

$$\text{DISC}(\epsilon) : \forall X, Y \subset V(G), |e(X, Y) - p|X||Y|| < \epsilon n^2.$$

我们将会从定理4.1的证明中看到，这些性质全部都在关于  $\epsilon$  的多项式意义下等价，也就是说，对于任意两个性质 **Prop1** 与 **Prop2**，都存在一个常数  $c$ ，使得 **Prop1**( $\epsilon$ )  $\implies$  **Prop2**( $\epsilon^c$ )。

在这个定理的证明中，我们会多次用到 Cauchy-Schwarz 不等式，所以我们不如从它的一个小练习开始。

#### 引理 4.1

如果  $G$  是一个  $n$  个点的图，并且  $e(G) \geq pn^2/2$ ，那么在  $G$  中  $C_4$  带标号地出现了  $\geq (p^4 - o(1))n^4$  次。



**证明** 这里我们想要的是  $S = \text{Hom}(C_4, G)$  的大小，也就是从  $C_4$  到  $G$  的图同态的个数。这里  $S$  把不是单射的映射也包括在内，也就是说  $C_4$  里不同的点可以被映射到  $G$  中的同一个点。但这不影响我们的结论，因为反正这种映射最多也只有  $O(n^3)$  个。

固定  $C_4$  的对角线在  $G$  中的两个端点  $u$  和  $v$ ，分别考虑对角线上下对称的两部分（见图 4.1），我们可以发现，

$|S| = \sum_{u,v} \text{codeg}(u,v)^2$ 。我们应用两次 Cauchy-Schwarz 不等式就可以得到

$$\begin{aligned}
 |\text{Hom}(C_4, G)| &= \sum_{u,v \in V(G)} \text{codeg}(u,v)^2 \\
 &\geq \frac{1}{n^2} \left( \sum_{u,v \in V(G)} \text{codeg}(u,v) \right)^2 \\
 &= \frac{1}{n^2} \left( \sum_{x \in V(G)} \deg(x)^2 \right)^2 \\
 &\geq \frac{1}{n^2} \left( \frac{1}{n} \left( \sum_{x \in V(G)} \deg(x) \right)^2 \right)^2 \\
 &= \frac{1}{n^2} \left( \frac{1}{n} (pn^2)^2 \right)^2 \\
 &= p^4 n^4
 \end{aligned}$$

其中第二行,我们对长度为2的路径的条数用“算两次”的办法,得到了  $\sum_{u,v \in V(G)} \text{codeg}(u,v) = \sum_{x \in V(G)} \deg(x)^2$ 。

**注** 我们可以可视化的展示两次应用 Cauchy-Schwarz 的过程, 见图4.1。我们可以发现 Cauchy-Schwarz 其实是利用了图的对称性。<sup>1</sup>

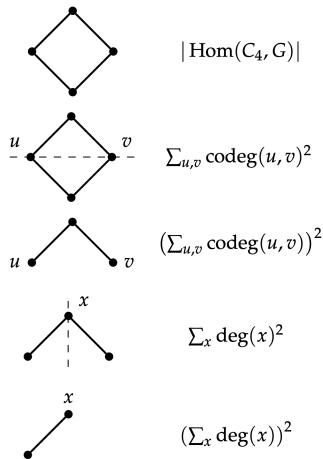


图 4.1: Cauchy-Schwarz 的可视化

接下来我们来证明定理 4.1。

**证明**  $\text{DISC} \implies \text{DISC}'$ : 在  $\text{DISC}$  中, 令  $Y = X$ 。

$\text{DISC}' \implies \text{DISC}$ : 我们把在  $e(X, Y)$  中的边分类, 应用容斥原理把它表示出来:

$$e(X, Y) = e(X \cup Y) + e(X \cap Y) - e(X \setminus Y) - e(Y \setminus X).$$

这样我们就可以用  $\text{DISC}$  得到:

$$\begin{aligned}
 &p \left( \binom{|X \cup Y|}{2} + \binom{|X \cap Y|}{2} + \binom{|X \setminus Y|}{2} + \binom{|Y \setminus X|}{2} + o(n^2) \right) \\
 &= p|X||Y| + o(n^2)
 \end{aligned}$$

<sup>1</sup>译者注: 这个证明也可以看成等价的是利用了两次  $x^2$  的凸性, 动机如下: 因为  $\text{codeg}(u,v)^2$  的和在不同的  $u, v$  的  $\text{codeg}(u,v)$  比较“均匀”的时候最小, 所以用平均数的平方来 bound 住平方的和。

**DISC  $\Rightarrow$  COUNT:** 在图计数引理 (定理3.10) 中, 令  $V_i = G$  ( $i = 1, \dots, v(H)$ ), 就可以直接得到这个结论。

**COUNT  $\Rightarrow$  C<sub>4</sub>:** C<sub>4</sub> 只是 **COUNT** 的一个特殊情况。

**C<sub>4</sub>  $\Rightarrow$  CODEG:** 假设 C<sub>4</sub> 成立, 我们有

$$\sum_{u,v \in G} \text{codeg}(u, v) = \sum_{x \in G} \deg(x)^2 \geq n \left( \frac{2e(G)}{n} \right)^2 = (p^2 + o(1)) n^3.$$

与此同时  $\sum_{u,v} \text{codeg}(u, v)^2$  等于 C<sub>4</sub> 有标号地在  $G$  中出现的次数, 也就是:

$$\begin{aligned} \sum_{u,v} \text{codeg}(u, v)^2 &= \text{Number of labeled copies of } C_4 + o(n^4) \\ &\leq (p^4 + o(1)) n^4 \end{aligned}$$

从而我们可以用 Cauchy-Schwartz 来得到我们想要的:

$$\begin{aligned} \sum_{u,v \in G} |\text{codeg}(u, v) - p^2 n| &\leq n \left( \sum_{u,v \in G} (\text{codeg}(u, v) - p^2 n)^2 \right)^{1/2} \\ &= n \left( \sum_{u,v \in G} \text{codeg}(u, v)^2 - 2p^2 n \sum_{u,v \in G} \text{codeg}(u, v) + p^4 n^4 \right)^{1/2} \\ &\leq n \left( p^4 n^4 - 2p^2 n \cdot p^2 n^3 + p^4 n^4 + o(n^4) \right)^{1/2} \\ &= o(n^3) \end{aligned}$$

**注** 这个技巧类似于概率组合 (probabilistic combinatorics) 里的 **二阶矩方法**: 我们希望证明  $\text{codeg}(u, v)$  的方差不会太大。<sup>2</sup>

**CODEG  $\Rightarrow$  DISC:** 我们首先注意到

$$\begin{aligned} \sum_{u \in G} |\deg(u) - pn| &\leq n^{1/2} \left( \sum_{u \in G} (\deg(u) - pn)^2 \right)^{1/2} \\ &= n^{1/2} \left( \sum_{u \in G} (\deg(u))^2 - 2pn \sum_{u \in G} \deg(u) + p^2 n^3 \right)^{1/2} \\ &= n^{1/2} \left( \sum_{u,v \in G} \text{codeg}(u, v) - 4pn \cdot e(G) + p^2 n^3 \right)^{1/2} \\ &= n^{1/2} \left( p^2 n^3 - 2p^2 n^3 + p^2 n^3 + o(n^3) \right)^{1/2} \\ &= o(n^2). \end{aligned}$$

从而有

$$\begin{aligned} |e(X, Y) - p|X||Y|| &= \left| \sum_{x \in X} (\deg(x, Y) - p|Y|) \right| \\ &\leq n^{1/2} \left( \sum_{x \in X} (\deg(x, Y) - p|Y|)^2 \right)^{1/2}. \end{aligned}$$

<sup>2</sup>译者注: 这里的想法是用已知的二阶矩来 bound 一阶矩。

因为求和的每一项都是非负的，我们可以把求和范围从  $X$  扩大到  $V(G)$ ，从而得到：

$$\begin{aligned} |e(X, Y) - p|X||Y|| &\leq n^{1/2} \left( \sum_{x \in V(G)} \deg(x, Y)^2 - 2p|Y| \sum_{x \in V(G)} \deg(x, Y) + p^2 n |Y|^2 \right)^{1/2} \\ &= n^{1/2} \left( \sum_{y, y' \in Y} \text{codeg}(y, y') - 2p|Y| \sum_{y \in Y} \deg(y) + p^2 n |Y|^2 \right)^{1/2} \\ &= n^{1/2} \left( |Y|^2 p^2 n - 2p|Y| \cdot |Y|pn + p^2 n |Y|^2 + o(n^3) \right)^{1/2} \\ &= o(n^2). \end{aligned}$$

现在我们已经证明了这些定理间的一个“ $C_4$ ”， $\text{DISC} \Rightarrow \text{COUNT} \Rightarrow C_4 \Rightarrow \text{CODEG} \Rightarrow \text{DISC}$ ，我们最后证明 **EIG** 与  $C_4$  的等价性。

**EIG**  $\Rightarrow C_4$ :  $C_4$  在  $G$  中的带标号出现次数与长度为 4 的封闭路径的个数，最多只相差  $O(n^3)$ ，而长度为 4 的封闭路径个数等于  $\text{tr}(A_G^4)$ （这里  $A_G$  是图  $G$  的邻接矩阵）。由线性代数我们知道， $\text{tr}(A_G^4) = \sum_{i=1}^n \lambda_i^4$ 。其中最大的一项是  $\lambda_1^4$ ，而根据我们的假设， $\lambda_1^4 = p^4 n^4 + o(n^4)$ 。那么接下来，我们就是要证明其它  $\lambda_i^4$  的和不会太大，如果你把它们分开一个一个 bound，你会得到一个  $o(n^5)$  的误差项（这太大了！）。所以我们放在一起 bound，我们有

$$\sum_{i \geq 2} \lambda_i^4 \leq \max_{i \neq 1} |\lambda_i|^2 \sum_{i \geq 1} \lambda_i^2$$

注意到  $\sum_{i \geq 1} \lambda_i^2 = \text{tr}(A_G^2) = 2e(G)$ ，从而

$$\sum_{i=1}^n \lambda_i^4 = p^4 n^4 + o(n^4) + o(n^2)n^2 = p^4 n^4 + o(n^4).$$

$C_4 \Rightarrow \text{EIG}$ : 我们要用 **Courant-Fischer 定理**（也叫极大极小定理）：对于一个实对称矩阵  $A$ ，最大的特征值是

$$\lambda_1 = \sup_{x \neq 0} \frac{x^T A x}{x^T x}.$$

令矩阵  $A_G$  的特征值是  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ ，然后令  $\mathbf{1}$  是  $R^{V(G)}$  中的全壹向量。那么我们有

$$\lambda_1 \geq \frac{\mathbf{1}^T A_G \mathbf{1}}{\mathbf{1}^T \mathbf{1}} = \frac{2e(G)}{n} = (p + o(1))n.$$

另一方面，因为  $C_4$  成立，我们有

$$\lambda_1^4 \leq \sum_i \lambda_i^4 = \text{tr} A_G^4 \leq p^4 n^4 + o(n^4),$$

这就意味着  $\lambda_1 \leq pn + o(n)$ 。从而  $\lambda_1 = pn + o(n)$ 。余下就是，

$$\max_{i \neq 1} |\lambda_i|^4 \leq \text{tr}(A_G^4) - \lambda_1^4 \leq p^4 n^4 - p^4 n^4 + o(n^4) = o(n^4)$$

定理4.1最精彩的就是  $C_4$  性质，它看上去是所有性质中最弱的，但是却能够推出其它所有性质。

我们说过这个定理是关于稠密图的（也就是说  $p$  是个常数），当然也可以写出它在稀疏情形下的推广（在这个情形下，随着  $n \rightarrow \infty$ ,  $p = p_n \rightarrow 0$ ）。比如说，对 **DISC** 而言，我们需要把  $o(n^2)$  改成  $o(pn^2)$ ，从而使其可以蕴含这样的事实：一个拟随机图的边数应该接近于真随机图中的期望边数。类似的，在 **COUNT** 里， $H$  带标号地出现的次数应该是  $(1 + o(1))p^{e(H)}n^{v(H)}$ 。但是对稀疏图来说，这些性质并不等价。具体来说，稀疏图上计数引理不再成立了。比如说，下面这个图满足了 **DISC** 在稀疏情形下的推广，但是它甚至不包含任何的  $C_3$ 。

**例题 4.1** 令  $p = o(n^{-1/2})$ ，那么我们期望中， $C_3$  带标号出现的次数应该接近于  $\binom{n}{3}p^3$ ，并且图中的边数应该是  $\binom{n}{2}p$ 。但是因为我们现在  $p = o(n^{-1/2})$ ，图中  $C_3$  的出现次数要比边数低阶。所以我们可以在这个  $G(n, p)$  图里面，每个三角形都删去一条边，这样也只删了  $o(n^2 p)$  条边，从而 **DISC** 的稀疏推广仍然成立，但是现在这个图却没有三角形了。这个图在 **DISC** 性质的意义下是伪随机的，但是在三角形个数的意义上就不是伪随机的了。

## 4.2 Expander mixing 引理

现在我们来讨论一类特殊的图，叫做 expander，它们具有非常强的 discrepancy 性质。

### 定理 4.2 (Expander mixing 引理)

令  $G$  是一个  $n$  个点， $d$ -正则的图，并且令它的邻接矩阵的特征值为  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ 。令  $\lambda = \max\{|\lambda_2|, |\lambda_n|\}$ 。那么对于所有的  $X, Y \subseteq V(G)$ ，我们有

$$\left| e(X, Y) - \frac{d}{n} |X| |Y| \right| \leq \lambda \sqrt{|X| |Y|}.$$

**证明** 令  $J$  是全壹矩阵，我们有

$$\begin{aligned} \left| e(X, Y) - \frac{d}{n} |X| |Y| \right| &= \left| \mathbf{1}_X^T \left( A_G - \frac{d}{n} J \right) \mathbf{1}_Y \right| \\ &\leq \left\| A_G - \frac{d}{n} J \right\| |\mathbf{1}_X| |\mathbf{1}_Y| \\ &= \left\| A_G - \frac{d}{n} J \right\| \sqrt{|X| |Y|}. \end{aligned}$$

接下来只要证明  $A_G - \frac{d}{n} J$  的最大特征值至多是  $\lambda$  即可。

令  $v$  是  $A_G$  的一个特征向量。因为  $G$  是  $d$ -正则的， $v$  可以等于  $\mathbf{1}$ ，此时对应的特征值是  $d$ 。 $\mathbf{1}$  也是  $A_G - \frac{d}{n} J$  的一个特征向量，对应的特征值为  $0$ 。如果  $v \neq \mathbf{1}$ ，那么它与  $\mathbf{1}$  正交，也就是说  $v \cdot \mathbf{1} = \sum_{i=1}^n v_i = 0$ 。从而， $Jv = 0$ ，所以  $v$  也是  $A_G - \frac{d}{n} J$  的一个特征向量，并且对应着与它相对于  $A_G$  一样的特征值。那么  $A_G - \frac{d}{n} J$  的特征值就是  $0, \lambda_2, \lambda_3, \dots, \lambda_n$ ，所以它最大的特征值就是  $\lambda$ 。

Expander 与伪随机图之间具有联系：它们都满足，当你有一个比较小的顶点集合的时候，你会期望它们有许多相连的邻居。<sup>3</sup> 这种图被叫做 expander 的原因是，图中大部分的点都能快速的通过这些邻居到达。

我们接下来把我们的注意力集中到一类特殊的图上。

### 定义 4.1

一个  $(n, d, \lambda)$ -图是一个满足如下条件的图：

1. 它有  $n$  个点并且是  $d$ -正则图。
2. 它的邻接矩阵的特征值是  $d = \lambda_1 \geq \dots \geq \lambda_n$ ，并且满足  $\max\{|\lambda_2|, |\lambda_n|\} \leq \lambda$ 。

Expander mixing 引理 (定理 4.2) 可以等价的表述成：如果  $G$  是一个  $(n, d, \lambda)$ -图，那么对于任意的  $X, Y \subseteq V(G)$ ，

$$\left| e(X, Y) - \frac{d}{n} |X| |Y| \right| \leq \lambda \sqrt{|X| |Y|}.$$

一个随机图以高概率满足伪随机的性质。但是我们希望得到伪随机性的确定性构造，下面是一个这样的构造的例子。

### 定义 4.2

令  $\Gamma$  是一个有限群，而  $S \subset \Gamma$  是一个满足  $S = S^{-1}$  的子集。**Cayley 图**  $\text{Cay}(\Gamma, S) = (V, E)$  的定义为点集  $V = \Gamma$ ，并且边集

$$E = \{(g, gs) : g \in \Gamma, s \in S\}.$$

**例题 4.2 Paley 图** 是一个  $\text{Cay}(\mathbb{Z}/p\mathbb{Z}, S)$  图，这里  $p \equiv 1 \pmod{4}$  是一个质数，而  $S$  是所有  $\mathbb{Z}/p\mathbb{Z}$  中的非零二次剩余。

<sup>3</sup>译者注：对随机图而言，这是因为大部分的边会随机指向这个子集外。

## 命题 4.1

Paley 图  $G = \text{Cay}(\mathbb{Z}/p\mathbb{Z}, S)$  满足  $|\lambda_2|, |\lambda_p| \leq \frac{\sqrt{p-1}}{2}$ , 这里  $\lambda_1, \dots, \lambda_p$  是它的邻接矩阵的特征值。

**证明** 我们直接列出它的特征向量。令顶点 0 对应第一维坐标, 顶点 1 对应第二维坐标, 以此类推。

$$\begin{aligned} v_1 &= (1, \dots, 1) \\ v_2 &= (1, \omega, \omega^2, \dots, \omega^{p-1}) \\ v_3 &= (1, \omega^2, \omega^4, \dots, \omega^{2(p-1)}) \\ &\vdots \\ v_p &= (1, \omega^{p-1}, \dots, \omega^{(p-1)(p-1)}) \end{aligned}$$

这里  $\omega$  是  $p$  次单位根。

我们先验证这些都确实是特征向量。全壹向量  $v_1$  的特征值是  $d = \lambda_1$ 。我们算出来  $A_G v_2$  的第  $j$  维坐标是

$$\sum_{s \in S} \omega^{j+s} = \omega^j \sum_{s \in S} \omega^s.$$

因为  $\omega^j$  是  $v_2$  的第  $j$  维坐标, 所以  $v_2$  对应的特征值就是  $\sum_{s \in S} \omega^s$ 。一般的, 对于任意的  $0 \leq k \leq p-1$ ,

$$\lambda_{k+1} = \sum_{s \in S} \omega^{ks}.$$

值得注意的是, 这是  $\mathbb{Z}/p\mathbb{Z}$  上的 Cayley 图都具有的性质, 并且这些特征向量与  $S$  的选取无关。接下来, 我们来计算每个  $\lambda_i$  的大小。对于任意  $k > 0$ , 我们有

$$2\lambda_{k+1} + 1 = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ka^2}.$$

这里我们用到了  $S$  是所有二次剩余的集合的性质。等式右边的和被称作高斯和, 我们可以这样求:

把等式右边平方, 得到

$$\left| \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ka^2} \right|^2 = \sum_{a, b \in \mathbb{Z}/p\mathbb{Z}} \omega^{k((a+b)^2 - a^2)} = \sum_{a, b \in \mathbb{Z}/p\mathbb{Z}} \omega^{k(2ab + b^2)}.$$

如果  $b \neq 0$ , 那么  $k(2ab + b^2)$  在固定  $b$ , 让  $a$  遍历  $\mathbb{Z}/p\mathbb{Z}$  时, 是  $\mathbb{Z}/p\mathbb{Z}$  的一个重排, 所以

$$\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{k(2ab + b^2)} = 0$$

如果  $b = 0$ , 那么

$$\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{k(2ab + b^2)} = p.$$

因为高斯和的平方等于  $p$ , 所以说  $\lambda_{k+1} = \frac{\pm\sqrt{p-1}}{2}$  (对于任意的  $k > 0$ )。

你也许认出了  $\sum_{s \in S} \omega^{ks}$  是  $S$  的指示函数 ( $f(s) = 1$  当且仅当  $s \in S$ , 否则  $f(s) = 0$ , 其中  $s \in \mathbb{Z}/p\mathbb{Z}$ ) 的傅里叶系数。事实上, 在定义在阿贝尔群上的 Cayley 图的特征值与这个群的傅里叶变换之间, 有着很紧密的联系。事实上这两个谱只相差一个常数倍 (这也是我们对特征值和傅里叶变换都用“谱”这个说法的原因)。对非阿贝尔群来说, 情况也差不多, 虽然非阿贝尔群的傅里叶变换就需要表示论了。



### 4.3 拟随机凯莱图

我们已经看到 Chung–Graham–Wilson 定理 (定理 4.1) 在稀疏情形下的版本并不成立。但是有些惊讶的是, 如果我们只考虑群的 Cayley 图 (包括非阿贝尔群), 无论边密度是多少, 稀疏版本的 **DISC** 和 **EIG** 都是等价的。

对一般的稀疏图而言, 稀疏版本的 **DISC** 并不能推出稀疏版本的 **EIG**。考虑一个很大的随机  $d$ -正则图和一个  $K_{d+1}$  的不交并, 这个图满足稀疏版本的 **DISC** (因为那个很大的随机  $d$ -正则图满足稀疏版本的 **DISC**), 但是最大的两个特征值是  $\lambda_1 = \lambda_2 = d$  (因为两个连通分量上的两个全壹向量都分别是特征向量), 这违背了稀疏版本的 **EIG** 对  $\lambda_2 = o(d)$  的要求。

#### 定理 4.3 (Conlon-Zhao)

令  $\Gamma$  是一个有限群, 并且  $S \subset \Gamma$  是一个满足  $S = S^{-1}$  的子集。令  $G = \text{Cay}(\Gamma, S)$ ,  $n = |\Gamma|$  并且  $d = |S|$ 。对于任意  $\epsilon > 0$ , 我们定义以下两个性质:

- **DISC**( $\epsilon$ ): 对所有  $X, Y \subseteq G$ , 我们有  $|e(X, Y) - \frac{d}{n}|X||Y|| \leq \epsilon dn$
- **EIG**( $\epsilon$ ):  $G$  是一个  $(n, d, \lambda)$ -图, 并且  $\lambda \leq \epsilon d$ 。

那么如果  $G$  满足 **EIG**( $\epsilon$ ), 它就会满足 **DISC**( $\epsilon$ )。如果  $G$  满足 **DISC**( $\epsilon$ ), 那么它就会满足 **EIG**( $8\epsilon$ )。

定理 4.3 的证明需要用到 **Grothendieck 不等式**。

#### 定理 4.4 (Grothendieck 不等式)

存在一个绝对常数  $K > 0$ , 满足对于任意矩阵  $A = (a_{i,j}) \in \mathbb{R}^{n \times n}$ ,

$$\sup_{\substack{x_i \in B \\ y_i \in B}} \sum_{i,j} a_{i,j} \langle x_i, y_j \rangle \leq K \sup_{\substack{x_i \in \{\pm 1\} \\ y_i \in \{\pm 1\}}} \sum_{i,j} a_{i,j} x_i y_j$$

在式子左边, 上极限的范围是某个空间  $\mathbb{R}^m$  里的单位球  $B$ 。

**Grothendieck 不等式**的右边是一个离散定义域的二次型  $\langle x, Ay \rangle$ 。它 (往往) 有很重要的组合意义, 但是很难优化。左边是右边的一个“半正定松弛”, 有许多高效的算法。左边的求和始终比右边大求和, 并且 **Grothendieck 不等式**告诉我们, 左边的求和比右边的求和至多大了常数倍。所以左边的求和是右边的求和的一个近似。

**注** 人们知道  $K = 1.78$  可以让这个不等式成立, 但是最优的值 (被称作“实数 **Grothendieck 常数**”) 还是未知的。

**证明** [定理 4.3] 由 expander mixing 引理可知, **EIG**( $\epsilon$ ) 可以推出 **DISC**( $\epsilon$ )。具体来说, 用这个引理可以推出对于所有的  $X, Y \subseteq V(G)$  有,

$$\left| e(X, Y) - \frac{d}{n}|X||Y| \right| \leq \lambda \sqrt{|X||Y|} \leq \epsilon dn.$$

这正是我们想要的。

为了证明另外一个方向, 假设 **DISC**( $\epsilon$ ) 成立, 对于每个  $x, y \in \{\pm 1\}^\Gamma$ , 我们定义  $x^+, x^-, y^+, y^- \in \{0, 1\}^\Gamma$ , 使得

$$x_g^+ = \begin{cases} 1 & \text{if } x_g = 1 \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad x_g^- = \begin{cases} 1 & \text{if } x_g = -1 \\ 0 & \text{otherwise} \end{cases}$$

那么  $x = x^+ - x^-$ 。我们类似的定义  $y^+$  和  $y^-$ 。

考虑矩阵  $A \in \mathbb{R}^{\Gamma \times \Gamma}$ ,  $A_{g,h} = 1_S(g^{-1}h) - \frac{d}{n}$  (这里  $1_S$  是  $S$  的指示函数)。那么,

$$x_g^+ = \begin{cases} 1 & \text{if } x_g = 1 \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad x_g^- = \begin{cases} 1 & \text{if } x_g = -1 \\ 0 & \text{otherwise} \end{cases}$$

这里面每一项都可以被 **DISC** 控制住。比如说,

$$\langle x^+, Ay^+ \rangle = e(X^+, Y^+) - \frac{d}{n}|X^+||Y^+|$$

这里  $X^+ = \{g \in \Gamma : x_g = 1\}$ ,  $Y^+ = \{g \in \Gamma : y_g = 1\}$ 。所以我们知道  $|\langle x^+, Ay^+ \rangle| \leq \epsilon dn$ 。这对于其它项也成立,

所以我们有

$$|\langle x, Ay \rangle| \leq 1 \quad \forall x, y \in \{\pm 1\}^\Gamma \quad (4.1)$$

我们接下来用极大极小的方式来表示特征值

$$\max\{|\lambda_2|, |\lambda_n|\} = \sup_{\substack{|x|, |y|=1 \\ x, y \in \mathbb{R}^\Gamma}} \langle x, Ay \rangle.$$

对于每个  $x \in \mathbb{R}^\Gamma$ , 我们用  $x_s^g = x_{sg}$  (其中  $s$  遍历  $\Gamma$ ) 来定义向量  $x^g \in \mathbb{R}^\Gamma$ . 那么由于  $x^g$  只是把  $x$  的下标重新排列了一下, 我们有  $|x| = |x^g|$ . 所以对于任意  $|x|, |y| = 1$  的  $x, y \in \mathbb{R}^\Gamma$ , 我们有

$$\begin{aligned} \langle x, Ay \rangle &= \sum_{g,h} A_{g,h} x_g y_h \\ &= \frac{1}{n} \sum_{g,h,s} A_{sg,sh} x_{sg} y_{sh} \\ &= \frac{1}{n} \sum_{g,h,s} A_{g,h} x_{sg} y_{sh} \\ &= \frac{1}{n} \sum_{g,h} A_{g,h} \langle x^g, y^h \rangle \leq 8\epsilon d \end{aligned}$$

最后的不等式是应用了 Grothendieck 不等式 ( $K < 2$ ) 与 (4.1). 所以  $\text{EIG}(8\epsilon)$  成立。

## 4.4 Alon-Boppana 界

在一个  $(n, d, \lambda)$  图中,  $\lambda$  越小, 那么这个图就越伪随机 (译者注: 见 Expander Mixing 引理)。随之而来的一个问题是, 对于一个确定的  $d$ ,  $\lambda$  最小可以有多小? 对此我们有 Alon-Boppana 界。

### 定理 4.5 (Alon-Boppana 界)

对于一个确定的  $d$ , 如果  $G$  是一个  $n$  个点的图, 并且邻接矩阵  $A_G$  的特征值是  $\lambda_1 \geq \dots \geq \lambda_n$ , 那么

$$\lambda_2 \geq 2\sqrt{d-1} - o(1).$$

随着  $n$  趋于无穷, 这里低阶项  $o(1)$  会趋于 0。

**证明** 令  $V = V(G)$ 。根据 Courant-Fischer 定理, 我们只要证明存在一个向量  $z \in \mathbb{R}^V - \{0\}$ , 使得  $\langle z, 1 \rangle = 0$  并且

$$\frac{z^T A z}{z^T z} \geq 2\sqrt{d-1}.$$

令  $r \in \mathbb{N}$ 。任选一个  $v \in V$ , 令  $V_i$  是离  $v$  距离为  $i$  的点的集合 ( $V_0 = \{v\}$ ,  $V_1 = N(v)$ )。令  $x \in \mathbb{R}^V$  是这样的向量:

$$x_u = w_i := (d-1)^{-i/2} \quad \text{for } u \in V_i, 0 \leq i \leq r-1,$$

并且对于  $\text{dis}(u, v) \geq r$  的  $u$ ,  $x_u = 0$ 。我们接下来会证明

$$\frac{x^T A x}{x^T x} \geq 2\sqrt{d-1} \left(1 - \frac{1}{2r}\right). \quad (4.2)$$

为了证明它, 我们要计算

$$x^T x = \sum_{i=0}^{r-1} |V_i| w_i^2$$

以及

$$\begin{aligned}
 x^T A x &= \sum_{u \in V} x_u \sum_{u' \in N(u)} x_{u'} \\
 &\geq \sum_{i=0}^{r-1} |V_i| w_i (w_{i-1} + (d-1)w_{i+1}) - (d-1)|V_{r-1}|w_{r-1}w_r \\
 &= 2\sqrt{d-1} \left( \sum_{i=0}^{r-1} |V_i| w_i^2 - \frac{1}{2} |V_{r-1}| w_r^2 \right)
 \end{aligned}$$

其中的不等式成立的原因是  $u \in V_i$  的每个邻居离  $v$  的距离都至多是  $i+1$ , 并且至少一个邻居的距离是  $i-1$  (注意  $w_i$  是单调递减的)。但是因为一旦距离  $\text{dist}(u', v) \geq r$ , 就会有  $x_{u'} = 0$ , 所以我们必须再减去  $(d-1)|V_{r-1}|w_{r-1}w_r$ 。再带入  $w_i$  的定义就得到了上面的式子。注意因为  $V_{i+1} \leq (d-1)|V_i|$ , 所以  $|V_{r-1}| \leq |V_i|(d-1)^{r-i-1}$ , 从而  $|V_{r-1}| \geq \frac{1}{r} \sum_{i=0}^{r-1} |V_i| w_i^2$ , 上面的式子

$$\geq 2\sqrt{d-1} \left( \sum_{i=1}^{r-1} |V_i| w_i^2 \right) \left( 1 - \frac{1}{2r} \right)$$

这就证明了 (4.2)。但是我们需要有  $\langle z, 1 \rangle = 0$ 。如果  $n > 1 + (d-1) + (d-1)^2 + \dots + (d-1)^{2r-1}$ , 那么就一定存在距离至少  $2r$  的两个顶点  $u, v \in V(G)$ 。令  $x \in \mathbb{R}^V$  是以顶点  $v$  为中心时的这个构造。让  $y \in \mathbb{R}^V$  是以  $u$  为中心时的这个构造。那么  $x$  和  $y$  的非零位置是不相交的, 并且对应的两个点集之间也没有边。也就是说  $x^T A y = 0$ 。

选择一个常数  $c \in \mathbb{R}$ , 使得  $z = x - cy$  满足  $\langle z, q \rangle = 0$ 。那么

$$z^T z = x^T x + c^2 y^T y$$

并且

$$z^T A z = x^T A x + c^2 y^T A y \geq 2\sqrt{d-1} \left( 1 - \frac{1}{2r} \right) z^T z。$$

随着  $n \rightarrow \infty$ , 相应地令  $r \rightarrow \infty$ , 我们就证明了这个定理。

我们再给出第二种证明方法, 它只能证明一个弱一点的结论, 但是与定理 4.5 表达的意思是一致的。

**证明** [弱一点的结论] 我们将会证明  $\max\{|\lambda_2|, |\lambda_n|\} \geq 2\sqrt{d-1} - o(1)$ 。这是一个运用迹方法的例子, 这个方法也叫矩方法。我们有

$$\sum_{i=1}^n \lambda_i^{2k} = \text{tr}(A^{2k})$$

等式右边是长度为  $2k$  的回路个数。接下来注意到,  $d$ -正则图里, 从点  $v$  开始的长度为  $2k$  的回路个数至少等于一个无限大的  $d$ -正则的树里的回路个数。这是因为, 在一个无限大  $d$ -正则的树里的每个回路, 放在图  $G$  里一样是一个回路, 但是因为  $G$  里面包含一些环, 所以它还包含了一些额外的回路。

在无限大的  $d$ -正则树里, 至少有  $C_k(d-1)^k$  ( $C_k = \frac{1}{k+1} \binom{2k}{k}$  是第  $k$  个卡特兰数) 条长为  $2k$  的回路。所以在  $G$  里, 至少有  $\frac{n}{k+1} \binom{2k}{k} (d-1)^k$  条长度为  $2k$  的回路。另一方面,

$$d^{2k} + (n-1)\lambda^{2k} \geq \sum_{i=1}^n \lambda_i^{2k}$$

所以,

$$\lambda^{2k} \geq \frac{1}{k+1} \binom{2k}{k} (d-1)^k - \frac{d^{2k}}{n}。$$

其中  $\frac{1}{k+1} \binom{2k}{k}$  这一项在  $k \rightarrow \infty$  的时候是  $(2 - o(1))^{2k}$ 。随着  $n \rightarrow \infty$ , 令  $k \rightarrow \infty$ , 并且  $k = o(\log n)$ , 我们既可以得到  $\lambda \geq 2\sqrt{d-1} - o(1)$ 。

**注** 注意  $2\sqrt{d-1}$  是无限大  $d$ -正则的树的谱半径 (spectral radius)。

## 4.5 Ramanujan 图

### 定义 4.3

一个 Ramanujan 图 是如下的一个  $d$ -正则图：假设它的邻接矩阵的特征值是  $d = \lambda_1 \geq \dots \geq \lambda_n$ ，那么它需要满足  $|\lambda_2|, |\lambda_n| \leq 2\sqrt{d-1}$ 。也就是说，它是一个  $\lambda \leq 2\sqrt{d-1}$  的  $(n, d, \lambda)$ -图。

一个 Ramanujan 图的例子是  $K_{d+1}$ ，因为  $\lambda_2 = \dots = \lambda_n = -1$ 。但是我们更感兴趣的情况是，固定  $d$  而让  $n$  趋于无穷的情况。对于一个固定的  $d$ ，是否存在无限多个  $d$ -正则的 Ramanujan 图呢？

对于所有的  $d \geq 3$ ，都存在无限多个  $d$ -正则的 Ramanujan 图。

我们会讨论关于这个猜想的一些部分结果。

### 定理 4.6 (Lubotzky-Phillips-Sarnak, Margulis)

以上猜想对所有  $d-1$  是质数的  $d$  成立。

定理4.6的证明方法是显示地构造群  $PSL(2, q)$  的 Cayley 图，它用到了数论中关于 Ramanujan 的一些猜想的深刻结论 (Ramanujan 图的名字就是这么来的)。1944 年，Morgenstern 加强了定理4.6的结论，证明到了所有的  $d-1$  是质数的幂的  $d$ 。这基本上就是现在我们所知道的全部，特别的，猜想 4.5 对  $d=7$  是否成立都还是未知的。

一个有趣的问题是：考虑随机图中，除了  $\lambda_1$  以外，最大的特征值如何分布呢？

### 定理 4.7 (Friedman)

固定  $d \geq 3$ 。一个随机的  $n$  个点的  $d$ -正则图，以  $1 - o(1)$  的概率，几乎是一个 Ramanujan 图，具体来说

$$\max\{|\lambda_2|, |\lambda_n|\} \leq 2\sqrt{d-1} + o(1)$$

这里  $o(1)$  项随着  $n \rightarrow \infty$  而趋近于 0。

一些实验的结果显示，似乎  $n$  个点的图中固定比例 (0 到 1 之间) 的一部分 ( $n \rightarrow \infty$ ) 应该是 Ramanujan 图。但是，在这条线上还没有严格的结论。

最近对于这个问题在二分图的情况，有一些重要进展：

注意对于所有的二分图， $\lambda_i = -\lambda_{n+1-i}$ 。这是因为，如果令二分图的两个部分分别是  $A$  和  $B$ ，然后有一个特征值为  $\lambda$  的特征向量，它在  $A$  的位置上等于  $v_A$ ，在  $B$  的位置上等于  $v_B$ ，那么我们把  $v_B$  取反，就得到了一个特征值是  $-\lambda$  的特征向量。所以说一个二分图是二分 Ramanujan 图，当且仅当  $\lambda_2 \leq 2\sqrt{d-1}$ 。

每一个 Ramanujan 图  $G$  都有一个对应的二分 Ramanujan 图：我们可以构造  $G \times K_2$ ；如果  $G$  有特征值  $\{\lambda_i\}$ ，那么  $G \times K_2$  就有特征值  $\{\lambda_i\} \cup \{-\lambda_i\}$ ，所以  $d$ -正则二分 Ramanujan 图问题是原问题的一个弱化。

### 定理 4.8 (Marcus-Spielman-Srivastava)

对于任意的  $d$ ，都存在无穷多个  $d$ -正则二分 Ramanujan 图。

定理 4.8 的证明用了一个特备聪明的随机图构造。

## 4.6 稀疏图正则性和 Green-Tao 定理

接下来，我们要把伪随机图与稀疏图的正则性结合起来。稀疏意味着边的密度是  $o(1)$ ，这里我们始终考虑的是一个包含无穷个图的序列，其中它们的顶点数  $n$  趋于无穷。三角形删除引理最直接的推广在稀疏的情况下并不成立，所以我们需要再加一个限制：

**定理 4.9 (稀疏图的三角形删除引理)**

对于所有的  $\epsilon > 0$ , 都存在一个  $\delta > 0$ , 使得对于足够伪随机的  $n$  个点、边密度为  $p$  的图  $\Gamma$  和它的所有不超过  $\delta np$  条边子图  $G$ , 都存在一种删去  $\delta n^3 p^3$  条边的方法, 可以删去  $G$  里的所有三角形。



因为我们并没有显式地定义“足够伪随机”, 我们把它称作一个**元定理**: 我们接下来会代入一些不同的伪随机条件, 从而从它出发得到一些不同的定理。我们可以把经典的三角形删除引理看成是它在  $\Gamma$  是完全图时的一个特殊情况。

**注** 元定理 4.9 去掉对  $\Gamma$  的伪随机假设之后就不成立了: 令  $G$  像推论 3.1 一样, 有  $n$  个点和  $n^{2-o(1)}$  条边, 并且每条边都恰好在一个三角形里。(这里我们取  $\Gamma = G$ )

**注** 如果  $\Gamma = G(n, p)$  是一个 Erdős-Rényi 图。并且  $p \geq \frac{C}{\sqrt{n}}$ , 那么元定理 4.9 成立。

之所以要有上面这个元定理, 是为了证明 Green-Tao 定理。

**定理 4.10 (Green-Tao)**

质数中包含任意长的等差数列。



这个定理在某种意义上, 是 Szemerédi 定理的一个稀疏推广: 根据质数定理, 质数的密度相对于  $n$  来说大致按照  $\frac{1}{\log n}$  (的阶) 递减。

定理 4.10 的证明策略是, 先把质数集 (以很高的相对密度) 嵌入“伪质数”集之中 (作为一个子集), 这里“伪质数”就是没有小质数作非平凡因子。这个集合更容易用解析数论分析, 特别的用筛法分析。特别的我们可以比较简单的证明, “伪质数”足够伪随机, 让我们可以对它应用稀疏版本的超图删除引理。

施工中.....

## 第5章 图极限

### 5.1 主要结论的介绍和说明

图极限关注的是图的极限分析。考虑以下两个示例，它们展现了有理数集和图之间的潜在平行关系：

**例题 5.1** 对于  $x \in [0, 1]$ ， $x^3 - x$  的最小值点为  $x = 1/\sqrt{3}$ 。但是如果我们把范围限制在  $\mathbb{Q}$ （假装我们不知道实数），一种表达这个最小值点的方法是找到一个收敛到  $1/\sqrt{3}$  的有理数序列  $x_1, x_2, \dots$ 。

**例题 5.2** 给定  $p \in (0, 1)$ ，在所有边密度为  $p$  的图中我们希望最小化  $C_4$  的密度。根据定理 4.1 我们知道， $C_4$  密度最小值是  $p^4$ 。（可以通过一系列拟随机图得到，单个有限图无法得到这个最小值。）

我们可以将所有图的集合视为一组离散对象（类似于  $\mathbb{Q}$ ），并寻求他的“完备空间”（类似于  $\mathbb{R}$ ）。

#### 定义 5.1

一个 graphon（“graph function”）是一个对称<sup>a</sup>的可测函数  $W : [0, 1]^2 \rightarrow [0, 1]$ 。

<sup>a</sup>一个包含  $n$  个变量的函数是对称的，如果它的值与自变量的顺序无关。

**笔记** 定义 5.1 可以推广到  $\Omega \times \Omega \rightarrow [0, 1]$ ，其中  $\Omega$  是任何可测概率空间。但简单起见，我们通常令  $\Omega = [0, 1]$ （实际上，大多数“好”的可测概率空间都可以用  $[0, 1]$  表示）。函数的值域也可以推广到  $\mathbb{R}$ ，在这种情况下，我们将把函数称为核（kernel）。请注意这种命名在文献中并不总是一致的。

graphon 可以看作是一种广义类型的图。事实上，我们可以将任何图转换为 graphon，转换后我们可以试着想象一些图序列的极限应该是什么样子。

**例题 5.3** 考虑一个半图  $G_n$ ，这是一个二部图，其中一个部分标记为  $1, 2, \dots, n$ ，另一个部分标记为  $n+1, \dots, 2n$ ，顶点  $i$  和  $n+j$  连通当且仅当  $i \leq j$ 。如果我们将邻接矩阵  $\text{Adj}(G_n)$  视为 0/1 位图，我们可以定义 graphon  $W_{G_n} : [0, 1]^2 \rightarrow [0, 1]$ （由  $(2n)^2$  个大小为  $1/(2n) \times 1/(2n)$  的“像素”组成）。当  $n$  趋于无穷大时，graphon（逐点）收敛到一个函数，如图 5.1 所示。

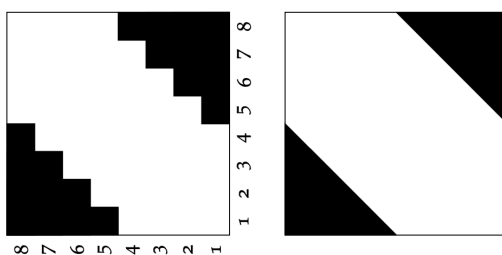


图 5.1:  $W_{G_n}$  的图 ( $n=4$ ) 和  $n$  趋于无穷大

我们可以很容易的概括这种将图转换为 graphon 的过程。

#### 定义 5.2

给定一个有  $n$  个顶点（标记为  $1, \dots, n$ ）的图  $G$ ，我们将其对应的 graphon 定义为  $W_G : [0, 1]^2 \rightarrow [0, 1]$ 。该 graphon 将  $[0, 1] = I_1 \cup I_2 \cup \dots \cup I_n$  等分并且  $\lambda(I_i) = 1/n$ ，满足对于  $(x, y) \in I_i \times I_j$ ，如果  $i$  和  $j$  在  $G$  中连接则  $W(x, y) = 1$ ，否则为 0。（ $\lambda(I)$  是  $I$  的勒贝格测度。）

但是，随着我们分析更多的示例，我们发现使用示例 5.3 中逐点的极限通常不足以满足我们的目的。

**例题 5.4** 考虑任何边密度为  $1/2$ （顶点数接近无穷大）的随机（或伪随机）图序列，那么极限（应该）接近常值函数  $W = 1/2$ 。



**例题 5.5** 考虑一个完全二部图  $K_{n,n}$ ，其中两部分分别是奇数标号顶点和偶数标号顶点。由于邻接矩阵看起来像棋盘格，我们可能希望其极限看起来也是常值函数  $1/2$ ，但事实并非如此：如果我们将两部分标号改为  $1, \dots, n$  和  $n+1, \dots, 2n$ ，则我们看到 graphon 实际上应该收敛到  $2 \times 2$  的棋盘。

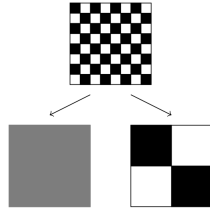


图 5.2:  $W_{K_{n,n}}$  和  $W_{K_{n,n}}$  的两个可能的图极限， $n$  趋于无穷大

上面的例子表明我们需要在我们的 graphon 定义中注意重新标记顶点。

### 定义 5.3

从  $H$  到  $G$  的图同态是一个映射  $\phi: V(H) \rightarrow V(G)$ ，满足  $uv \in E(H)$  当且仅当  $\phi(u)\phi(v) \in E(G)$ 。令  $\text{Hom}(H, G)$  是所有此类同态的集合，并令  $\text{hom}(H, G) = |\text{Hom}(H, G)|$ 。定义同态密度为

$$t(H, G) = \frac{\text{hom}(H, G)}{|V(G)|^{|V(H)|}}$$

同态密度等于一个均匀随机映射是图同态的概率。

### 例题 5.6

- $\text{hom}(K_1, G) = |V(G)|$
- $\text{hom}(K_2, G) = 2|E(G)|$
- $\text{hom}(K_3, G)$  是  $G$  中三角形个数的 6 倍。
- $\text{hom}(G, K_3)$  是对  $G$  顶点 3 着色的方案数（要保证相邻顶点的颜色不同）。

**笔记** 请注意，因为同态可以是非单射的，所以从  $H$  到  $G$  的同态并不完全对应于  $G$  内的子图  $H$  的副本。由于非单射同态的数量最多贡献  $O_H(|V(G)|^{|V(H)-1|})$ ，当  $H$  固定且  $n \rightarrow \infty$  时，非单射同态数量是相对少的。

### 定义 5.4

给定对称可测函数  $W: [0, 1]^2 \rightarrow \mathbb{R}$ ，定义

$$t(H, W) = \int_{[0, 1]^{|V(H)|}} \prod_{ij \in E(H)} W(x_i, x_j) \prod_{i \in V(H)} dx_i$$

注意，对于每个  $G$  和  $H$ ， $t(H, G) = t(H, W_G)$ 。

**例题 5.7** 当  $H = K_3$  时，我们有

$$t(K_3, W) = \int_{[0, 1]^3} W(x, y)W(y, z)W(z, x)dx dy dz$$

这可以看作是  $W$  的“三角形密度”。

我们现在可以定义图收敛以及图极限。

### 定义 5.5

我们说一图序列  $G_n$ （或一个 graphon 序列  $W_n$ ）收敛如果对每个图  $H$ ， $t(H, G_n)$ （或  $t(H, W_n)$ ）随  $n$  趋于无穷大收敛。如果对于每个图  $H$ ， $t(H, G_n)$ （或  $t(H, W_n)$ ）收敛，则序列收敛到  $W(H, W)$ 。

一个自然的问题是图的收敛序列是否有“极限”。（剧透一下，确实存在。）我们还应该考虑我们以这种方式定义的“极限”是否与我们期望的一致。为此，我们需要定义图之间“距离”的概念。

我们尝试将  $G$  和  $G'$  之间的距离定义为  $\sum_k 2^{-k} |t(H_k, G) - t(H_k, G')|$ ，其中  $H_1, H_2, \dots$  是所有可能的图。（之所以添加了  $2^{-k}$  是为了确保总和收敛到 0 和 1 之间的数字。）这在与定义 5.5 中的收敛概念是同胚的，所以这种

定义没什么用。

另一种可能的想法是考虑两个图之间的编辑距离（需要边的编辑次数），通过因子  $1/|V(G)|^2$  进行归一化。但这种方法也不是很有用，因为任意两个  $G(n, 1/2)$  之间的距离约为  $1/4$ ，但我们希望它们之间有  $o(1)$  的距离。

尽管上面两种定义都行不通，但这激励我们回顾之前对随机图的讨论，我们考虑图接近常数  $p$ （即与  $G(n, p)$  相似）的情况。回忆定理 4.1 中的 DISC，我们希望图足够随机时  $|e(X, Y) - p|X||Y||$  很小。借助这个想法，我们可以这样比较两个图之间的距离：直观地说， $|e_G(X, Y) - e_{G'}(X, Y)|/n^2$  是否对于所有子集  $X$  和  $Y$  来说都很小。为了说清楚这一点，我们需要更多的定义。

#### 定义 5.6

$W : [0, 1]^2 \rightarrow \mathbb{R}$  的切割范数定义为

$$\|W\|_{\square} = \sup_{S, T \subseteq [0, 1]} \left| \int_{S \times T} W \right|$$

其中  $S$  和  $T$  是可测集。

我们还定义了一些相关的范数。

#### 定义 5.7

对于  $W : [0, 1]^2 \rightarrow \mathbb{R}$ ，将  $L^p$  范数定义为  $\|W\|_p = (\int |W|^p)^{1/p}$ 。定义  $L^\infty$  范数作为  $m$  的下界，其中  $m$  满足：集合  $\{(x, y) : W(x, y) > m\}$  的测度为零。（这也称为  $W$  的本质确界）。

#### 定义 5.8

如果  $\lambda(A) = \lambda(\phi^{-1}(A))$  对于所有可测集  $A \subseteq [0, 1]$  成立，我们说  $\phi : [0, 1] \rightarrow [0, 1]$  是保测（measure-preserving）的。

**例题 5.8** 函数  $f(x) = x + 1/2 \bmod 1$  显然是保测的。 $f(x) = 2x \bmod 1$  也是保测的（可能不太明显）。虽然每个区间通过  $f$  被扩大了 2 倍，但每个点都有两个原像，所以这两种效果相互抵消。

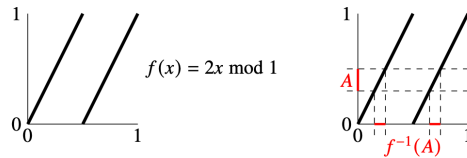


图 5.3:  $f(x) = 2x \bmod 1$

#### 定义 5.9

记  $W^\phi(x, y) = W(\phi(x), \phi(y))$ （直观地说，相当于重新标记顶点）。我们定义切割距离

$$\delta_{\square}(U, W) = \inf_{\phi} \|U - W^\phi\|_{\square}$$

其中  $\phi$  是一个保测的双射。

对于图  $G, G'$ ，定义切割距离  $\delta_{\square}(G, G') = \delta_{\square}(W_G, W_{G'})$  我们将图和 graphon 之间的切割距离定义为  $\delta_{\square}(G, U) = \delta_{\square}(W_G, U)$

请注意， $\phi$  与顶点置换并不完全相同：它也允许拆分顶点或覆盖不同的顶点。相比于直接考虑图同构，这种做法使我们能更好地优化最小差异/切割范数。

**笔记** 定义中的  $\inf$  不一定总能取到。假设  $U(x, y) = xy$  且  $W = U^\phi$ ，其中  $\phi(x) = 2x \bmod 1$ 。因为  $\phi$  不是双射的，对于任何  $\phi'$ ，我们不能保证  $\|U - W^{\phi'}\|_{\square} = 0$ （尽管切割距离为 0）。

现在我们介绍图极限理论中的主要定理，我们将在后面给出证明。首先，人们可能会怀疑使用切割（距离）

度量存在收敛的替代定义，但事实证明该定义等价于定义 5.5。

**定理 5.1 (收敛等价定理 Borgs, Chayes, Lovász, Sós, and Vesztergombi 2008)**

graphon 序列或图序列收敛当且仅当它是关于切割（距离）度量的柯西序列。

关于度量  $d$  的柯西序列是满足如下要求的序列：当  $n \rightarrow \infty$  时， $\sup_{m \geq 0} d(x_n, x_{n+m}) \rightarrow 0$ 。


**定理 5.2 (极限存在定理 Lovász and Szegedy 2006)**

每个 graphon 或图的收敛序列都有一个极限 graphon。

将  $\widetilde{\mathcal{W}}_0$  表示为 graphon 的空间，其中切割距离为 0 的 graphon 视为同一个 graphon。

**定理 5.3 (graphons 空间的紧致性)**

集合  $\widetilde{\mathcal{W}}_0$  是切割度量下的紧致度量空间。

 **笔记** 直观地说，这意味着“本质上不同”的图组成的空间不是很大。紧致性类似于正则性引理，其中每个图都有一个大小固定的描述，可以很好地近似该图。事实上，我们可以将这个紧致性定理视为正则性引理的定性分析版本。

## 5.2 W-随机图

回想一下我们之前见过的 Erdős-Rényi 随机图  $G(n, p)$ 。我们现在介绍它的 graphon。我们从一个特殊情形开始，即随机块模型。2-随机块模型是一个顶点颜色随机（蓝色或红色）的图，两个红色顶点以概率  $p_{rr}$  相连，一个红色顶点和一个蓝色顶点以概率  $p_{rb} = p_{br}$  相连，并且两个蓝色顶点以概率  $p_{bb}$  相连。

	$q_r$	$q_b$
$q_r$	$p_{rr}$	$p_{rb}$
$q_b$	$p_{rb}$	$p_{bb}$

图 5.4: 2-随机块模型


**定义 5.10**

从区间  $[0, 1]$  中均匀随机选取  $x_1, \dots, x_n$ 。我们记一个  $W$ -随机图为  $G(n, W)$ ，其顶点集  $[n]$ ，顶点  $i$  和  $j$  以概率  $W(x_i, x_j)$  连接。

一个重要的统计问题是给定一个图，是否有一种好的构造方法来构造该图？这是我们研究  $W$ -随机图的重要动力。我们还了解到 Erdős-Rényi 随机图的序列收敛到一个常数 graphon，下面是一个类似的陈述。

**定理 5.4**

记  $W$  是一个 graphon。假设对于所有的  $n$ ， $G_n$  是从  $W$ -随机图中独立选出的，那么  $G_n \xrightarrow{a.s.} W$ 。

 **笔记** 具体的，每个 graphon  $W$  都是某个图序列的极限。这为我们提供了某种形式的图近似。

## 5.3 正则性和计数引理

我们现在介绍一系列用来证明定理 5.3 的工具。

**定理 5.5 (记数引理)**

对于 graphon  $W, U$  和图  $F$ , 我们有

$$|t(F, W) - t(F, U)| \leq |E(F)| \delta_{\square}(W, U)$$

**证明** 我们只需证明  $|t(F, W) - t(F, U)| \leq |E(F)| \|W - U\|_{\square}$  即可 (该不等式两边对  $\phi$  取  $\inf$  即可得到引理中的不等式)。

回顾切割范数的定义  $\|W\|_{\square} = \sup_{S, T \subseteq [0,1]} \left| \int_{S \times T} W \right|$ 。现在我们证明一个切割范数很有用的表述: 对于可测的函数  $u$  和  $v$ ,

$$\sup_{S, T \subseteq [0,1]} \left| \int_{S \times T} W \right| = \sup_{u, v: [0,1] \rightarrow [0,1]} \left| \int_{[0,1]^2} W(x, y) u(x) v(y) dx dy \right|$$

该等式成立的原因如下: 我们取  $u = 1_S$  和  $v = 1_T$ , 右边等于左边, 所以左边小于等于右边; 被积函数对于  $u, v$  是双线性的, 所以极值在  $u, v$  取 0 或 1 时取到, 所以右边小于等于左边。现在我们考虑  $F = K_3$  时的情形。

$$\begin{aligned} t(K_3, W) - t(K_3, U) &= \int ((W(x, y)W(x, z)W(y, z) - U(x, y)U(x, z)U(y, z)) dx dy dz \\ &= \int (W - U)(x, y)W(x, z)W(y, z) dx dy dz \\ &\quad + \int U(x, y)(W - U)(x, z)W(y, z) dx dy dz \\ &\quad + \int U(x, y)U(x, z)(W - U)(y, z) dx dy dz \end{aligned}$$

以第一项为例, 对于固定的  $z$ ,

$$\left| \int (W - U)(x, y)W(x, z)W(y, z) dx dy dz \right| \leq \|W - U\|_{\square}$$

对于第二项第三项我们有同样的结果。因此, 总上界为  $3\|W - U\|_{\square}$ , 这是我们想要的。

推广  $F = K_3$  的证明, 对于一般图  $F$ , 我们有

$$\begin{aligned} |t(F, W) - t(F, U)| &= \left| \int \left( \prod_{u_i v_i \in E} W(u_i, v_i) - \prod_{u_i v_i \in E} U(u_i, v_i) \right) \prod_{v \in V} dv \right| \\ &\leq \sum_{i=1}^{|E|} \left| \int \left( \prod_{j=1}^{i-1} U(u_j, v_j) (W(u_i, v_i) - U(u_i, v_i)) \prod_{k=i+1}^{|E|} W(u_k, v_k) \right) \prod_{v \in V} dv \right| \end{aligned}$$

如果我们固定所有其他无关变量 (除  $u_i$  和  $v_i$  之外的所有变量), 我们发现求和中的每个绝对值项都以  $\|W - U\|_{\square}$  为上界。所以我们有切割函数  $|t(F, W) - t(F, U)| \leq |E(F)| \delta_{\square}(W, U)$ 。

我们现在为 graphon  $W$  引入一个“平均函数”。

**定义 5.11**

对于  $[0, 1]$  的一个划分  $\mathcal{P} = \{S_1, \dots, S_k\}$  (要求划分的子集是可测集), 以及对称可测函数  $W: [0, 1]^2 \rightarrow \mathbb{R}$ , 定义 stepping 算子  $W_{\mathcal{P}}: [0, 1]^2 \rightarrow \mathbb{R}$ , 该算子在  $S_i \times S_j$  上的取值为常数, 满足: 如果  $(x, y) \in S_i \times S_j$ ,  $W_{\mathcal{P}}(x, y) = \frac{1}{\lambda(S_i)\lambda(S_j)} \int_{S_i \times S_j} W$ 。(我们忽略分母为 0 时的定义, 因为此时集合的测度为零)。

实际上, 这是希尔伯特空间  $L^2([0, 1]^2)$  上对每一  $S_i \times S_j$  到常值函数的投影。也可以看作是关于由  $S_i \times S_j$  生成的  $\sigma$ -代数的条件期望。

**定理 5.6 (弱正则性引理)**

对于任何  $\epsilon > 0$  和任何 graphon  $W: [0, 1]^2 \rightarrow \mathbb{R}$ , 存在  $[0, 1]$  的划分  $\mathcal{P}$  (要求划分得到的可测子集测度不超过  $4^{1/\epsilon^2}$ ), 满足  $\|W - W_{\mathcal{P}}\|_{\square} \leq \epsilon$ 。

**定义 5.12**

给定图  $G$ ,  $V(G)$  的划分  $\mathcal{P} = \{V_1, \dots, V_k\}$  被称为是弱  $\epsilon$ -正则的, 如果对于所有的  $A, B \subset V(G)$  有

$$\left| e(A, B) - \sum_{i,j=1}^k d(V_i, V_j) |A \cap V_i| |B \cap V_j| \right| \leq \epsilon |V(G)|^2$$

这与我们在介绍定理 3.1 时看到的概念相似但不同。

**定理 5.7 (图的弱正则性引理)**

对于任意  $\epsilon > 0$  和图  $G$ , 存在  $V(G)$  的弱  $\epsilon$ -正则划分, 最多可分为  $4^{1/\epsilon^2}$  个块。

**引理 5.1 ( $L^2$  能量递增引理)**

令  $W$  是一个 graphon,  $\mathcal{P}$  是  $[0, 1]$  的划分, 满足  $\|W - W_{\mathcal{P}}\|_{\square} > \epsilon$ 。存在  $\mathcal{P}$  的加细  $\mathcal{P}'$ ,  $\mathcal{P}'$  将  $\mathcal{P}$  中的每个块划分成不超过 4 个块, 并保证

$$\|W_{\mathcal{P}'}\|_2^2 > \|W_{\mathcal{P}}\|_2^2 + \epsilon^2$$

**证明** 因为  $\|W - W_{\mathcal{P}}\|_{\square} > \epsilon$ , 所以存在子集  $S, T \subset [0, 1]$  使得  $|\int_{S \times T} (W - W_{\mathcal{P}})| > \epsilon$ 。令  $\mathcal{P}'$  是  $\mathcal{P}$  通过引入  $S$  和  $T$  的加细 (根据每个部分是否在  $S \setminus T, T \setminus S, S \cap T, \bar{S} \cap \bar{T}$  来再次划分), 每个部分最多被分为 4 个子块。

定义  $\langle W, U \rangle := \int WU$ 。查看“平均函数” $W_{\mathcal{P}}$  的定义, 可以轻松得到  $\langle W_{\mathcal{P}}, W_{\mathcal{P}} \rangle = \langle W_{\mathcal{P}'}, W_{\mathcal{P}} \rangle$ 。从而  $\langle W_{\mathcal{P}'} - W_{\mathcal{P}}, W_{\mathcal{P}} \rangle = 0$ 。根据勾股定理,

$$\|W_{\mathcal{P}'}\|_2^2 = \|W_{\mathcal{P}'} - W_{\mathcal{P}}\|_2^2 + \|W_{\mathcal{P}}\|_2^2 > \|W_{\mathcal{P}}\|_2^2 + \epsilon^2$$

其中后一个不等式来自柯西-施瓦茨不等式,

$$\|1_{S \times T}\|_2 \|W_{\mathcal{P}'} - W_{\mathcal{P}}\|_2 \geq |\langle W_{\mathcal{P}'} - W_{\mathcal{P}}, 1_{S \times T} \rangle| = |\langle W - W_{\mathcal{P}}, 1_{S \times T} \rangle| > \epsilon$$

**命题 5.1**

对于任何  $\epsilon > 0$ 、graphon  $W$  和  $[0, 1]$  上的划分  $\mathcal{P}_0$ , 存在划分  $\mathcal{P}_0$  的加细  $\mathcal{P}$  将  $[0, 1]$  分成不超过  $4^{1/\epsilon^2}$  个块, 并保证  $\|W - W_{\mathcal{P}}\|_{\square} \leq \epsilon$ 。

这个命题告诉我们, 从任何给定的划分开始, 关于正则性的论证仍然有效。

**证明** 我们反复应用引理 5.1 来得到  $[0, 1]$  上的划分  $\mathcal{P}_0, \mathcal{P}_1, \dots$ 。每一次加细操作, 我们要么有  $\|W - W_{\mathcal{P}}\|_{\square} \leq \epsilon$  从而停止迭代, 要么有  $\|W_{\mathcal{P}'}\|_2^2 > \|W_{\mathcal{P}}\|_2^2 + \epsilon^2$ 。

因为  $\|W_{\mathcal{P}_i}\|_2^2 \leq 1$ , 我们保证在少于  $\epsilon^{-2}$  次加细操作后停止。我们还知道每个块在每一次加细操作后最多分为 4 个部分, 因此最终最多分为  $4^{\epsilon^{-2}}$  个块。

下面我们介绍一个计算机科学中的相关结论, MAXCUT 问题: 给定一个图  $G$ , 我们想在所有顶点子集  $S \subset V(G)$  中寻求  $\max e(S, \bar{S})$ 。Goemans 和 Williamson 给出了多项式时间近似算法, 该算法理论上能够做到最优值 0.878 的近似。唯一游戏猜想 (Unique games conjecture: Khot, Kindler, Mossel, and O'Donnell 2007) 如果成立, 我们将不可能获得比 G-W 算法更好的近似值。事实上我们还知道, 近似超过  $\frac{16}{17} \approx 0.941$  是 NP-hard 的 (Håstad 2001)。

另一方面, 对于稠密图, MAXCUT 问题变得很容易解决。对于  $n$  顶点图, 我们有绝对误差小于  $\epsilon n^2$  的多项式时间算法, 其中  $\epsilon > 0$  是一个固定的常数。算法的思路是应用弱正则性引理, 通过对每一部分的所有可能的划分的大小进行暴力搜索。这一应用正是研究弱正则性引理的原始动机之一。

## 5.4 Graphon 空间的紧致性

### 定义 5.13

鞅是一个随机变量的序列  $X_0, X_1, X_2, \dots$ , 且对于任意的  $n$ ,

$$\mathbb{E}[X_n | X_{n-1}, X_{n-2}, \dots, X_0] = X_{n-1}$$



**例题 5.9** 令  $X_n$  表示在公平赌场  $n$  轮游戏后的余额, 其中每轮收益的预期值为 0, 那么  $\{X_n\}_{n \geq 0}$  是鞅。

### 定理 5.8 (鞅收敛定理)

任意有界的鞅以概率 1 收敛 (即 a.s. 收敛)。



**笔记** 实际上, 不必要求有界,  $L^1$  有界或一致可积就已经足够, 这两者都可以保证  $\sup \mathbb{E}(X_n^+) < \infty$ 。

我们将给出一个受投注策略启发的证明思路。下面的证明省略了一些技术细节, 但对于有概率基础的人来说可以很容易地完善省去的细节。

**证明**  $[a, b]$  的“上交叉”由区间  $[n, n+t]$  组成, 其中  $X_n < a$  且  $X_{n+t}$  是  $X_n$  之后第一个满足  $X_{n+t} > a$  的变量。参考图 5.5, 假设有一个不收敛的有界鞅  $\{X_n\}$ , 则存在有理数  $0 < a < b < 1$  使得  $\{X_n\}$  无限次向上穿过区间  $[a, b]$ 。我们将证明该事件发生的概率为 0。

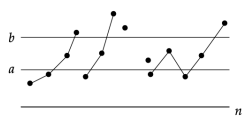


图 5.5: “上交叉”的例子

将  $u_N$  记作从开始到时间  $N$  之间的上交叉次数 (从区间下方穿到上方的次数)。考虑以下投注策略: 在任何时候, 我们持有 0 或 1 的份额。如果  $X_n < a$ , 则买入 1 股并持有, 直到价格  $(X_n)$  第一次取值超过  $b$  卖出。考虑我们从这种投注策略中的获利? 每个“上交叉”我们赚到差价  $b - a$ 。考虑我们的初始余额和最终余额之间的差异, 我们的至少获利  $(b - a)u_N - 1$ 。另一方面, 可选抽样定理<sup>1</sup>告诉我们所有“公平”的投注策略收益预期为零。所以

$$0 = \mathbb{E} \text{ profit} \geq (b - a)\mathbb{E}u_N - 1$$

所以  $\mathbb{E}u_N \leq \frac{1}{b-a}$ 。令  $u_\infty = \lim_{N \rightarrow \infty} u_N$  表示“上交叉”的总次数。根据单调收敛定理, 我们有  $\mathbb{E}u_\infty \leq \frac{1}{b-a}$ , 因此  $\mathbb{P}(u_\infty = \infty) = 0$ , 证明完毕。

我们现在使用之前介绍的工具来证明 graphon 的主要定理。所需的工具为弱正则性引理 (定理 5.6) 和鞅收敛定理 (定理 5.8)。我们将首先证明 graphon 的空间是紧致的 (定理 5.3)。在下一节中, 我们将应用这个结果来依次证明定理 5.2 和定理 5.1。我们还将看到如何使用紧致性来证明 graphon 的强正则性引理。

回想一下, 如果  $\delta_\square(W, U) = 0$ ,  $\tilde{W}_0$  是模掉等价关系  $W \sim U$  的 graphon 空间。我们可以看到  $(\tilde{W}_0, \delta_\square)$  是一个度量空间。

### 定理 5.9 (graphon 空间的紧致性)

度量空间  $(\tilde{W}_0, \delta_\square)$  是紧致的。



**证明** 由于  $\tilde{W}_0$  是一个度量空间, 我们证明序列紧致就足够。固定一个序列  $W_1, W_2, \dots$  的 graphon。我们想证明存在一个子序列在  $\delta_\square$  意义下收敛到某个极限 graphon。

<sup>1</sup>在特定条件下, 停时的鞅的期望值等于其初始值。



对于任意的  $n$ , 重复应用弱正则性引理 (定理 5.6), 我们得到一系列划分

$$\mathcal{P}_{n,1}, \mathcal{P}_{n,2}, \mathcal{P}_{n,3}, \dots$$

满足

- (a) 对于所有的  $n, k$ ,  $\mathcal{P}_{n,k+1}$  是  $\mathcal{P}_{n,k}$  的加细。
- (b)  $|\mathcal{P}_{n,k}| = m_k$ , 其中  $m_k$  是只关于  $k$  的函数。
- (c)  $\|W_n - W_{n,k}\|_{\square} \leq 1/k$ , 其中  $W_{n,k} = (W_n)_{\mathcal{P}_{n,k}}$

弱正则性引理仅能够保证  $|\mathcal{P}_{n,k}| \leq m_k$ , 但如果我们允许划分中空集的存在, 那么我们可以保证等号成立。

最初, 每个块是一个任意的可测集。然而, 对于任意的  $n$ , 我们可以对  $W_{n,1}$  和  $\mathcal{P}_{n,1}$  作用一个保测的双射  $\phi$ , 使得  $\mathcal{P}_{n,1}$  将  $[0, 1]$  划分为多个区间。对于任意的  $k \geq 2$ , 假设  $\mathcal{P}_{n,k-1}$  是  $[0, 1]$  到区间的划分, 我们可以对  $W_{n,k}$  和  $\mathcal{P}_{n,k}$  作用一个保测的双射, 使得  $\mathcal{P}_{n,k}$  是  $[0, 1]$  到区间的划分, 并且是  $\mathcal{P}_{n,k-1}$  的加细。通过归纳, 我们得到: 对于任意的  $n, k$ ,  $\mathcal{P}_{n,k}$  是满足 (a) 和 (b) 的划分。虽然性质 (c) 可能不成立,  $W_{n,k} = (W_n)_{\mathcal{P}_{n,k}}$  不再成立, 我们仍然有  $\delta_{\square}(W_n, W_{n,k}) \leq 1/k$  对于所有  $n, k$  成立。对我们来说这已经足够。

现在, 证明的关键是在可数多步骤中的对角化论证。从序列  $W_1, W_2, \dots$  开始, 我们将反复挑选子序列。在第  $k$  步中, 我们选择一个子序列  $W_{n_1}, W_{n_2}, \dots$  满足:

1.  $i \rightarrow \infty$  时,  $\mathcal{P}_{n_i,k}$  中各部分的端点都分别收敛。
2.  $i \rightarrow \infty$  时,  $W_{n_i,k}$  几乎处处收敛于某个 graphon  $U_k$ 。

因为每个划分  $\mathcal{P}_{n,k}$  正好有  $m_k$  个部分, 并且每个部分的长度都在  $[0, 1]$  中, 所以满足 (1) 的子序列一定存在。我们考虑满足 (1) 的子序列  $(W_{n_i})_{i=1}^{\infty}$ , 每个  $W_{n_i,k}$  可以很自然地通过函数  $f_{a_i,k} : [m_k]^2 \rightarrow [0, 1]$  来确定。此类函数的空间是有界的, 因此  $(f_{a_i,k})_{i=1}^{\infty}$  收敛到  $f : [m_k]^2 \rightarrow [0, 1]$ 。因为  $f$  对应一个 graphon  $U_k$  ( $U_k$  为子序列  $(W_{n_i})_{i=1}^{\infty}$  的极限), 所以 (2) 也是满足的。

我们将子序列重新标记为  $W_1, W_2, \dots$  并且忽略序列的丢弃项。相应的分区也重新标记。不失一般性的, 在步骤  $k$  中, 我们得到含有  $W_1, \dots, W_k$  的子序列。因此, 步骤  $k = 1, 2, \dots$  的最终结果是一个无限长的序列, 它满足: 对于所有  $k$ ,  $(W_{n,k})_{n=1}^{\infty}$  几乎处处 (a.e.) 逐点收敛到  $U_k$ :

$$\begin{array}{ccccccc} & W_1 & W_2 & W_3 & \dots & & \\ k=1 & W_{1,1} & W_{2,1} & W_{3,1} & \dots & \rightarrow U_1 & \text{pointwise a.e.} \\ k=2 & W_{1,2} & W_{2,2} & W_{3,2} & \dots & \rightarrow U_2 & \text{pointwise a.e.} \\ k=3 & W_{1,3} & W_{2,3} & W_{3,3} & \dots & \rightarrow U_3 & \text{pointwise a.e.} \end{array}$$

类似地, 对于任意  $k$ ,  $(\mathcal{P}_{n,k})_{n=1}^{\infty}$  收敛到区间划分  $\mathcal{P}_k$ 。

根据性质 (a), 每个划分  $\mathcal{P}_{n,k+1}$  是  $\mathcal{P}_{n,k}$  的加细, 这意味着  $W_{n,k} = (W_{n,k+1})_{\mathcal{P}_{n,k}}$ 。令  $n \rightarrow \infty$ , 我们得到  $U_k = (U_{k+1})_{\mathcal{P}_k}$ 。现在每个  $U_k$  都可以被认为是概率空间  $[0, 1]^2$  上的一个随机变量。从这个角度看, 等式  $U_k = (U_{k+1})_{\mathcal{P}_k}$  暗示序列  $U_1, U_2, \dots$  是鞅。

每个  $U_k$  的范围都在  $[0, 1]$  中, 因此鞅是有界的。由鞅收敛定理 (定理 5.8), 存在一个 graphon  $U$ , 使得当  $k \rightarrow \infty$  时  $U_k \xrightarrow{\text{pointwise a.e.}} U$ 。

回想一下, 我们的目标是找到在  $\delta_{\square}$  意义下的收敛子序列  $W_1, W_2, \dots$ 。我们已经通过上述对角化论证找到一个子序列, 并且该子序列在  $\delta_{\square}$  意义下收敛到  $U$ 。也就是说, 我们想证明当  $n \rightarrow \infty$  时  $\delta(W_n, U)_{\square} \rightarrow 0$ 。下面我们将通过将 “3-epsilons” 操作来证明这一点。

对任意  $\epsilon > 0$ , 根据勒贝格控制收敛定理, 存在  $k > 3/\epsilon$  使得  $\|U - U_k\|_1 < \epsilon/3$ 。由于  $W_{n,k} \xrightarrow{\text{pointwise a.e.}} U_k$  (应用控制收敛定理), 存在  $n_0 \in \mathbb{N}$  使得  $\|U_k - W_{n,k}\|_1 < \epsilon/3$  对所有的  $n > n_0$  成立。最后, 因为我们选择  $k > 3/\epsilon$ , 所以我们有  $\delta(W_n, W_{n,k})_{\square} < \epsilon/3$  对于所有  $n$  成立。综上,

$$\begin{aligned} \delta(U, W_n)_{\square} &\leq \delta(U, U_k)_{\square} + \delta(U_k, W_{n,k})_{\square} + \delta(W_{n,k}, W_n)_{\square} \\ &\leq \|U - U_k\|_1 + \|U_k - W_{n,k}\|_1 + \delta(W_{n,k}, W_n)_{\square} \\ &\leq \epsilon \end{aligned}$$

第二个不等号是因为对于任意的 graphon  $W_1, W_2$  我们有

$$\delta(W_1, W_2)_{\square} \leq \|W_1 - W_2\|_{\square} \leq \|W_1 - W_2\|_1$$

## 5.5 紧致性的应用

我们现在将使用  $(\tilde{W}_0, \delta_{\square})$  的紧致性来证明几个结论，分别是 graphon 的强正则性引理，图同态密度和切割范数定义的收敛之间的等价性，以及任意图同态密度收敛的 graphon 序列都存在极限。

作为热身，我们将对于证明任意的 graphon，存在图在切割距离意义下一致收敛到该 graphon。下面的引理证明无需用到紧致性：

### 引理 5.2

对于任意  $\epsilon > 0$  和任意 graphon  $W$ ，存在满足  $\delta_{\square}(G, W) < \epsilon$  的图  $G$ 。

**证明** 根据测度论的知识，存在一个阶跃函数  $U$  满足  $\|W - U\|_1 < \epsilon/2$ 。对于任何常值 graphon  $p$ ，存在一个图  $G$  使得  $\|G - p\|_{\square} < \epsilon/2$ 。实际上，对于足够大的  $n$ ，随机图  $G(n, p)$  满足这个上界的概率很大。因为阶跃函数由许多常值函数构成，所以我们可以通过拼凑各种密度的随机图来找到一个满足  $\|G - U\|_{\square} < \epsilon/2$  的图  $G$ 。所以

$$\delta_{\square}(G, W) \leq \|W - U\|_1 + \|U - G\|_{\square} < \epsilon$$

这是我们想要的。

然而，在上述引理中，图的大小可能取决于  $W$ 。这一点可以通过紧致性来完善。

### 命题 5.2

对于任意  $\epsilon > 0$ ，存在  $N \in \mathbb{N}$  使得对于任意 graphon  $W$ ，存在一个满足  $\delta_{\square}(G, W) < \epsilon$  的  $N$  顶点图  $G$ 。

**证明** 对于一个图  $G$ ，定义开球  $B_{\epsilon}(G) = \{W \in \tilde{W}_0 : \delta_{\square}(G, W) < \epsilon\}$ ，用来表示  $G$  的  $\epsilon$  邻域。

令  $G$  取遍所有的图，根据引理 5.2， $G$  对应的  $B_{\epsilon}(G)$  构成了  $\tilde{W}_0$  的一个开覆盖。根据紧致性，这个开覆盖有一个有限子覆盖。所以存在一组数量有限的图  $G_1, \dots, G_k$ ，满足  $B_{\epsilon}(G_1), \dots, B_{\epsilon}(G_k)$  覆盖  $\tilde{W}_0$ 。令  $N$  是  $G_1, \dots, G_k$  顶点数量的最小公倍数。所以对于每个  $G_i$ ，存在  $N$  顶点图  $G'_i$  满足  $\delta_{\square}(G_i, G'_i) = 0$ 。（通过将  $G_i$  的每个顶点替换成用  $N/|V(G_i)|$  个顶点得到  $G'$ ，见图 5.6）。所以  $W$  包含在某个  $N$  顶点图  $G$  的  $\epsilon$  开球内，这就是我们想要的。

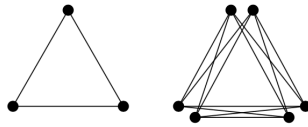


图 5.6:  $K_3$  及其 2-blowup



**笔记** 不幸的是，上述证明没有提供关于  $N$  如何依赖于  $\epsilon$  的信息。这是应用紧致性的副作用。我们可以使用正则性找到给出界限的替代证明。

直观上，紧致性与正则性引理具有相似性：两者都表明图空间在某种意义上非常小。事实上，他们之间有着更明确的联系：我们在紧致性证明中使用了弱正则性引理，而强正则性引理则可以直接从紧致性推导出来。

### 定理 5.10 (graphon 的强正则性引理 Lovász and Szegedy 2007)

令  $\epsilon = (\epsilon_1, \epsilon_2, \dots)$  是一个正实数序列。存在  $M = M(\epsilon)$  使得每个 graphon  $W$  都可以写成

$$W = W_{str} + W_{psr} + W_{sml}$$

其中

- $W_{str}$  是一个由  $k$  个部分组成的阶跃函数，其中  $k < M$ 。

- $\|W_{psr}\|_{\square} \leq \epsilon_k$ 。
- $\|W_{sml}\|_1 \leq \epsilon_1$ 。



**笔记** 如果  $\epsilon_k = \epsilon/k^2$ ，该定理近似等价于 Szemerédi 正则性引理。如果  $\epsilon_k = \epsilon$ ，那么它近似等价于弱正则性引理。

**证明** 熟悉测度论的读者应该知道，任何可测函数都可以通过阶跃函数很好的近似。因此，对于每个 graphon  $W$  都存在阶跃函数  $U$  使得  $\|W - U\|_1 \leq \epsilon_1$ 。不幸的是，阶跃函数的阶数可能取决于  $W$ ；我们将在这个地方使用紧致性。

对于 graphon  $W$ ，令  $k(W)$  是满足  $\|W - U\|_1 \leq \epsilon_1$  ( $U$  是步数为  $k$  的阶跃函数) 条件下最小的  $k$ 。则  $\{B_{\epsilon_k(W)}\}_{W \in \widetilde{W}_0}$  显然是  $\widetilde{W}_0$  的开覆盖，根据紧致性，存在一组有限的 graphon  $S \subset \widetilde{W}_0$  使得  $\{B_{\epsilon_k(W)}(W)\}_{W \in S}$  覆盖  $\widetilde{W}_0$ 。

令  $M = \max_{W \in S} k(W)$ 。根据紧致性，对于任意 graphon  $W$ ，存在  $W' \in S$  满足  $\delta_{\square}(W, W') \leq \epsilon_{k(W')}$ 。此外，存在一个 graphon  $U$  ( $U$  是阶数为  $k$  的阶跃函数，且  $k = k(W') \leq M$ ) 使得  $\|W' - U\|_1 \leq \epsilon_1$ 。因此，

$$W = U + (W - W') + (W' - U)$$

所以我们得到了想要的分解，其中  $W_{str} = U$ ， $W_{psr} = W - W'$  和  $W_{sml} = W' - U$ 。

之前我们通过  $F$  密度的序列定义了 graphon 序列的收敛性。然而，直到现在我们还不知道收敛的 graphon 序列的极限的  $F$  密度是否可以通过单个 graphon 来实现。如果包含 graphon 的图空间不是完备的，这是不正确的，正如我们在拟随机图的中看到的那样。但在 graphon 空间中，该结果是正确的，通过紧致性我们可以快速验证这一点。

#### 定理 5.11 (极限存在定理)

设 graphon 序列  $W_1, W_2, \dots$  满足：对应  $F$  密度的序列  $\{t(F, W_n)\}_n$  对所有图  $F$  收敛。则 graphon 的序列收敛到某一 graphon  $W$ 。也就是说，存在一个 graphon  $W$  满足：对于每个  $F$ ， $t(F, W_n) \rightarrow t(F, W)$  都成立。



**证明**

根据序列紧致性，存在一个子序列  $(n_i)_{i=1}^{\infty}$  和一个 graphon  $W$  使得当  $i \rightarrow \infty$  时， $\delta_{\square}(W_{n_i}, W) \rightarrow 0$ 。固定一个图  $F$ ，由定理 5.5 我们知道  $t(F, W_{n_i}) \rightarrow t(F, W)$ 。回顾条件，序列  $\{t(F, W_n)\}_n$  收敛，所以所有子序列都有相同的极限。因此  $t(F, W_n) \rightarrow t(F, W)$ 。

图极限的最后一个重要结论是我们之前定义的两个收敛概念的等价性。

#### 定理 5.12 (收敛的等价性 Borgs, Chayes, Lovász, Sós, and Veszteg 2008)

$F$  密度的收敛等价于切割范数意义下的收敛。也就是说，对于一个 graphon 序列  $W_1, W_2, \dots$ ，以下是等价的：

- 对于所有图  $F$ ， $F$  密度的序列  $\{t(F, W_n)\}_n$  收敛。
- 序列  $\{W_n\}_n$  是  $\delta_{\square}$  意义下的柯西列。



**证明** 一个方向通过定理 5.5 可以立即得到。回顾计数引理，如果序列  $\{W_n\}_n$  是  $\delta_{\square}$  意义下的柯西列，那么计数引理意味着对于每个图  $F$ ， $F$  密度的序列是柯西列，因此是收敛的。

对于反方向，假设对所有图  $F$ ， $F$  密度的序列收敛。设  $W$  和  $U$  为  $\{W_n\}_n$  的极限点（即收敛子序列的极限）。我们想要证明  $W = U$ 。

令  $(n_i)_{i=1}^{\infty}$  是满足  $W_{n_i} \rightarrow W$  的子序列。根据计数引理，对于所有的图  $F$ ， $t(F, W_{n_i}) \rightarrow t(F, W)$  成立。由于  $F$  密度的序列收敛，对于所有的图  $F$  我们有  $t(F, W_n) \rightarrow t(F, W)$ 。类似地，对于所有的  $F$  我们有  $t(F, W_n) \rightarrow t(F, U)$ 。因此，对于所有的  $F$  我们有  $t(F, U) = t(F, W)$ 。

根据随后将介绍的引理 5.3，我们最终得到  $U = W$ 。

**引理 5.3 (矩引理)**

如果 graphon  $U$  和  $W$  满足：对于所有的图  $F$ ,  $t(F, W) = t(F, U)$ , 则

$$\delta_{\square}(U, W) = 0$$

**证明 [概要]**

令  $\mathbb{G}(k, W)$  表示  $k$  顶点上的  $W$  随机图 (见定义 5.10)。可以证明, 对于任意  $k$  顶点图  $F$ ,

$$\Pr[\mathbb{G}(k, W) \cong F \text{ as labeled graph}] = \sum_{F' \supseteq F} (-1)^{E(F') - E(F)} t(F', W)$$

这意味着  $W$  随机图的分布完全由  $F$  密度决定。所以  $\mathbb{G}(k, W)$  和  $\mathbb{G}(k, U)$  具有相同的分布。

令  $\mathbb{H}(k, W)$  是一个顶点集为  $[k]$  的边加权的  $W$  随机图。边权重设置如下。设  $x_1, \dots, x_k \sim$  是  $[0, 1]$  上的独立均匀随机变量。设置  $(i, j)$  的边权重为  $W(x_i, x_j)$ 。

我们不加证明的给出如下两个结论：

- 当  $k \rightarrow \infty$ ,  $\delta_{\square}(\mathbb{H}(k, W), \mathbb{G}(k, W)) \rightarrow 0$  (以概率 1 收敛)。
- 当  $k \rightarrow \infty$  时  $\delta_1(\mathbb{H}(k, W), W) \rightarrow 0$  (以概率 1 收敛)。

由于  $\mathbb{G}(k, W)$  和  $\mathbb{G}(k, U)$  具有相同的分布, 所以从上述结论和三角不等式可以得出  $\delta_{\square}(W, U) = 0$ 。

紧致性和矩引理的一个结论是 graphon 计数引理的“逆”也成立:  $F$  密度的界限暗含着切割距离的上界。证明留作练习。

**推论 5.1 (逆计数引理)**

对于任意  $\epsilon > 0$ , 存在  $\eta > 0$  和整数  $k > 0$  满足: 如果  $U$  和  $W$  对于任意最多  $k$  顶点图  $F$  有

$$|t(F, U) - t(F, W)| \leq \eta$$

则  $\delta_{\square}(U, W) \leq \epsilon$ 。

**笔记**

矩引理意味着可以通过其  $F$  密度复原 graphon。我们可能会问是否所有的  $F$  密度都是必要的, 或者是否可以从有限多个密度中恢复一个 graphon? 例如, 我们已经看到, 如果  $W$  是密度为  $p$  的伪随机 graphon, 则  $t(K_2, W) = p$ ,  $t(C_4, W) = p^4$ ; 并且该 graphon 是由这些  $F$  密度唯一确定的。所以如果这两个等式成立, 则  $\delta_{\square}(W, p) = 0$ 。

以这种方式从有限多个  $F$  密度中恢复的 graphon 称为“finitely forcible graphon”。已知任意的阶跃函数和 half graphon  $W(x, y) = \mathbf{1}_{x+y \geq 1}$  是 finitely forcible graphon (Lovász and Sós 2008)。更一般地说, 对于任何在  $[0, 1]$  上单调递减的对称多项式  $p \in \mathbb{R}[x, y]$ ,  $W(x, y) = \mathbf{1}_{p(x, y) \geq 0}$  是 finitely forcible graphon (Lovász and Szegedy 2011)。

## 5.6 子图密度间的不等式

研究图极限的动机之一是图极限提供了一种有效的语言来考虑图不等式。例如, 我们可以回答以下问题:

**问题 5.1** 如果  $t(K_2, G) = 1/2$ ,  $t(C_4, G)$  的最小可能值是多少?

我们知道这个问题的答案。如前所述, 根据定理 4.1, 我们可以考虑一个拟随机图序列, 他们的极限是一个满足  $t(K_2, W) = 2^{-4}$  的 graphon  $W$ 。

在本节中, 我们将研究此类关于同态密度不等式的问题。本书前面已经讨论了两个图不等式, 分别为 Mantel 定理 (定理 2.1) 和 Turán 定理 (定理 2.2):

**定理 5.13 (Mantel 定理)**

令  $W : [0, 1]^2 \rightarrow [0, 1]$  是一个 graphon。如果  $t(K_3, W) = 0$ , 则  $t(K_2, W) \leq 1/2$ 。



**定理 5.14 (Turán 定理)**

让  $W : [0, 1]^2 \rightarrow [0, 1]$  是一个 graphon。如果  $t(K_{r+1}, W) = 0$ ，则  $t(K_2, W) \leq 1 - 1/r$ 。

我们在本节的目标是确定 graphon  $W$  的所有可行的边密度、三角形密度构成的对的集合，我们将其正式地写成：

$$D_{2,3} = \{(t(K_2, W), t(K_3, W)) : \text{graphon } W\} \subseteq [0, 1]^2$$

我们知道图序列的极限点是一个 graphon (定理 5.2)，因此  $D_{2,3}$  是闭集。此外，Mantel 定理 (定理 5.13) 告诉我们，当三角形密度为零时，该区域的水平可行线最多延伸到点  $(\frac{1}{2}, 0) \in [0, 1]^2$  (见图 5.7)。

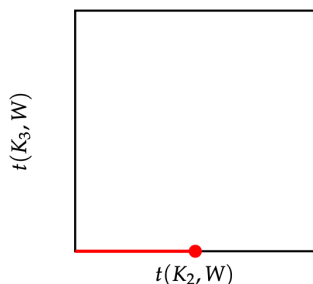


图 5.7: Mantel 定理在  $D_{2,3}$  中的示意图

我们可以通过区域的横截面来描述  $D_{2,3}$ 。下面的一个简单的结论表明  $D_{2,3}$  的每个垂直截面都是一条“竖直”的线段：

**命题 5.3**

对于所有的  $0 \leq r \leq 1$ ，集合  $D_{2,3} \cap \{r\} \times [0, 1]$  都是一条没有间隙的线段。

**证明** 考虑两个具有相同边密度的 graphon  $W_0, W_1$ 。则我们有一个 graphon：

$$W_t = (1 - t)W_0 + tW_1$$

随着  $t$  从 0 变化到 1，它的三角形密度是  $t$  的连续映射。 $t(K_3, W_t)$  的初值和终值分别是  $t(K_3, W_0)$  和  $t(K_3, W_1)$ ，所以三角形密度可以取到对应区间里的所有值。

为了更好地认识  $D_{2,3}$ ，我们想确定在给定边密度的情况下可以达到的最小子图和最大子图密度。我们从解决下面这个问题开始：

**问题 5.2**  $n$  顶点  $m$  条边图中的最大三角形数是多少？

一个直观的想法是边应该排列成团的形式。事实证明这是正确的。Kruskal-Katona 定理<sup>2</sup>告诉我们一个带有  $\binom{k}{2}$  条边的图最多有  $\binom{k}{3}$  个三角形。在这里，我们证明比这个上界稍弱的版本。

**定理 5.15**

对于任意的 graphon  $W : [0, 1]^2 \rightarrow [0, 1]$ ，有

$$t(K_3, W) \leq t(K_2, W)^{\frac{3}{2}}$$

**笔记** 这个通过图 5.8 中所示的图来达到该上界，它是  $G$  中团的图极限，其边密度和三角形的密度分别为，

$$t(K_2, W) = a^2, \quad t(K_3, W) = a^3$$

因此， $D_{2,3}$  区域的上边界由曲线  $y = x^{3/2}$  给出，如图 5.9 所示。

**证明** [定理 5.15]

<sup>2</sup>Kruskal-Katona 定理可以使用“压缩”的方法来证明：我们反复将边“推”向团，并说明在此过程中三角形的数量永远不会减少。

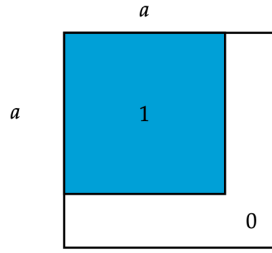


图 5.8: 达到  $D_{2,3}$  上界的 Graphon:  $t(K_2, W) = a^2$ ,  $t(K_3, W) = a^3$  (左上角为原点)

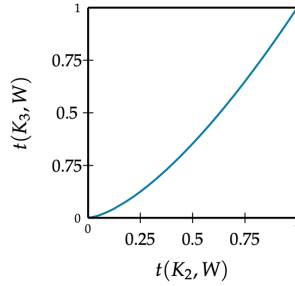


图 5.9:  $D_{2,3}$  上边界, 曲线为  $y = x^{3/2}$

我们证明任意图  $G$  中下面的不等式成立即可。

$$t(K_3, G) \leq t(K_2, G)^{3/2}$$

回顾  $\text{hom}(K_3, G)$  和  $\text{hom}(K_2, G)$ , 他们分别表示图中长度为 3 和 2 的闭环的数量。这些值对应于图  $G$  频谱的二阶矩和三阶矩:

$$\text{hom}(K_3, G) = \sum_{i=1}^k \lambda_i^3 \quad \text{hom}(K_2, G) = \sum_{i=1}^k \lambda_i^2$$

其中  $\{\lambda_i\}_{i=1}^n$  是邻接矩阵  $A_G$  的特征值。

$$\text{hom}(K_3, G) = \sum_{i=1}^n \lambda_i^3 \leq \left( \sum_{i=1}^n \lambda_i^2 \right)^{3/2} = \text{hom}(K_2, G)^{3/2}$$

其中不等号成立是因为对于  $t > 1$ ,  $a_1, \dots, a_n \geq 0$  下述不等式成立 (这里我们取  $a_i = \lambda_i^2$ ,  $t = 3/2$ ):

$$a_1^t + \dots + a_n^t \leq (a_1 + \dots + a_n)^t$$

两边除以  $|V(G)|^3$  后, 我们得到  $t(K_3, W) \leq t(K_2, W)^{3/2}$ 。

您可能想知道, 是否有一种方法可以在不使用图  $G$  的特征值的情况下证明这个结论。事实上我们有以下结论, 其证明不需要用到谱图理论:

#### 定理 5.16

对于任意对称的  $W: [0, 1]^2 \rightarrow \mathbb{R}$ ,

$$t(K_3, W) \leq t(K_2, W^2)^{3/2}$$

其中  $W^2$  是  $W$  逐点平方后得到的 graphon。

注意, 当  $W$  是一个 graphon 时, 所有点都在 0 和 1 之间, 因此  $W^2$  是一个更“小”的 graphon (01 之间的小数平方后更小)。因此, 上述定理比定理 5.15 更紧。这个定理的证明是对 Cauchy-Schwarz 不等式的三次应用, 每一次对应于三角形  $K_3$  的一条边。

**证明** 我们知道


$$t(K_3, W) = \int_{[0,1]^3} W(x, y)W(x, z)W(y, z) dx dy dz$$



现在, 我们放弃积分区间的记号。我们可以将 Cauchy-Schwarz 不等式应用于下面的积分。首先是关于变量  $dx$ , 然后是关于变量  $dy, dz$ , 每次保持其他两个变量不变:

$$\begin{aligned}
 t(K_3, W) &= \int W(x, y)W(x, z)W(y, z)dx dy dz \\
 &\leq \int \left( \int W(x, y)^2 dx \right)^{1/2} \left( \int W(x, z)^2 dx \right)^{1/2} W(y, z) dy dz \\
 &\leq \int \left( \int W(x, y)^2 dx dy \right)^{1/2} \left( \int W(x, z)^2 dx \right)^{1/2} \left( \int W(y, z)^2 dy \right)^{1/2} dz \\
 &\leq \left( \int W(x, y)^2 dx dy \right)^{1/2} \left( \int W(x, z)^2 dx dz \right)^{1/2} \left( \int W(y, z)^2 dy dz \right)^{1/2} \\
 &= \|W\|_2^3 \\
 &= t(K_2, W^2)^{3/2}
 \end{aligned}$$

证毕。

 **笔记** 如果我们没有  $W$  对称的条件, 我们仍然可以使用 Hölder 不等式得到一个较弱的陈述。在这种情况下, Hölder 不等式告诉我们

$$\int_{[0,1]^3} f(x, y)g(x, z)h(y, z)dx dy dz \leq \|f\|_3 \|g\|_3 \|h\|_3$$

设置  $f = g = h = W$ , 我们可以推导出一个比定理 5.16 更弱的上界, 因为一般来说,  $\|W\|_2 \leq \|W\|_3$ 。

下一个定理我们将证明团密度之间的线性不等式。

#### 定理 5.17 (Bollobás 1986)

取  $c_1, \dots, c_n \in \mathbb{R}$ 。下面不等式对任意的图  $G$

$$\sum_{r=1}^n c_r t(K_r, G) \geq 0$$

成立当且仅当它对所有的  $G = K_m$  ( $m \geq 1$ ) 成立。

更明确地说, 不等式  $\sum_{r=1}^n c_r \cdot \frac{m(m-1)\cdots(m-r+1)}{m^r} \geq 0$  对任意的图  $G$  成立当且仅当

$$\sum_{r=1}^n c_r \cdot \frac{m(m-1)\cdots(m-r+1)}{m^r} \geq 0$$

对所有的  $m \geq 1$  都成立。



**证明** 命题的一个方向可以立刻得到, 因为团是图全集的子集。

我们现在证明另一个方向。因为图全集在  $\tilde{W}_0$  (切割距离度量下) 中是稠密的。所以该不等式对于所有图成立当且仅当它对所有的 graphon 成立。现在我们考虑顶点加权简单图的集合  $\mathcal{S}$ , 其中  $\sum a_i = 1$ 。

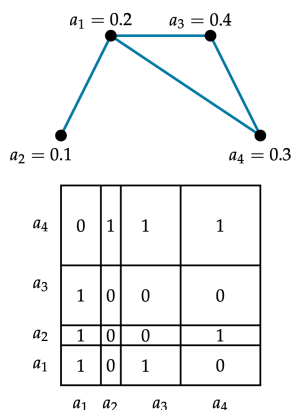


图 5.10: 四顶点上的节点加权图示例, 其权重和为 1, 及其对应的 graphon。

每个节点加权图可以用一个 **graphon** 来表示。注意到集合  $\mathcal{S}$  在  $\tilde{W}_0$  中是稠密的，所以我们只需证明  $\mathcal{S}$  中的图满足这个不等式即可。

使用反证法，假设存在节点加权简单图  $H$  使得

$$f(H) := \sum_{r=1}^n c_r t(K_r, H) < 0$$

在所有这些  $H$  中，我们选择一个节点数最小的图，最小节点数记为  $m$ 。我们选择节点权重  $a_1, \dots, a_m$ ，他们的总和等于 1 并且使  $f(H)$  最小化。因为我们的参数数量是有限的，并且  $f$  是紧集上的连续函数，所以我们一定可以找到这样的  $H$ 。

显然，我们有  $a_i > 0$ 。否则我们删除该节点后  $f(H) < 0$  仍然成立，矛盾。

此外， $H$  是一个完全图；否则存在  $i, j$  满足  $ij \notin E(H)$ 。注意，团密度是关于节点权重的多项式；这个多项式没有  $a_i^2$  项，因为 **graphon** 的集合  $\mathcal{S}$  对应于简单图，并且顶点  $i$  不会与其自身相邻。这个多项式也没有  $a_i a_j$  项，因为  $i$  和  $j$  并不相邻。因此， $f(H)$  在变量  $a_i$  和  $a_j$  中是多重线性的。

固定所有其他节点的权重并考虑将  $a_i, a_j$  作为我们的多元线性函数  $f(H)$  的变量，我们假设该函数取  $a_i = 0$  或  $a_j = 0$  时得到最小值。我们可以移动  $a_i$  和  $a_j$  同时保证两者之和  $a_i + a_j$  不变。这两权重之一将变为零，此时  $f(H)$  值变小了，同时这也意味着节点数量减少。这与  $H$  中节点数量的最小相矛盾。因此这种假设情况不会发生。

换句话说， $H$  必须是一个完全图；变量  $a_i$  上的多项式  $f(H)$  必须是对称的：

$$f(H) = \sum_{r=1}^n c_r r! s_r$$

其中每个  $s_r$  是一个阶数为  $r$  的基本对称多项式

$$s_r = \sum_{i_1 < \dots < i_r} a_{i_1} \cdots a_{i_r}$$

特别地，通过使除  $a_1, a_2$  之外的所有变量保持不变，多项式  $f(H)$  可以写为


$$f(H) = A + B_1 a_1 + B_2 a_2 + C a_1 a_2$$

其中  $A, B_1, B_2, C$  是常量。根据对称性，我们有  $B_1 = B_2$ 。另外，由于  $\sum a_i = 1$ ，我们知道  $a_1 + a_2$  是常数，所以

$$f(H) = A' + C a_1 a_2$$

如果  $C > 0$ ，则  $f$  将在  $a_1 = 0$  或  $a_2 = 0$  时取最小，因为  $H$  中的节点数量最少所以这并不会发生。如果  $C = 0$  那么  $a_1, a_2$  的任何取值都将产生与  $f(H)$  相同的最小值。因此，常数  $C$  必须为负，这意味着当  $a_1 = a_2$  时  $f(H)$  最小。所以所有的  $a_i$  必须相等， $H$  可以被看作是一个未加权的图。

换句话说，如果不等式对于某个图  $H$  不成立，那么对于某个未加权的团  $H$ ，它一定也不成立。证毕。

 **笔记** 在上面的证明中我们只考虑了团的密度，不等式对于其他类型的图不一定成立。

有了上面的定理，测试密度之间的线性不等式变得简单，因为我们只需要验证它们对团是否成立。我们有以下推论：

### 推论 5.2

对于任意的  $n$ ，凸包的极值点

$$\{(t(K_2, W), t(K_3, W), \dots, t(K_n, W)) : W \text{ graphon}\} \subset [0, 1]^{n-1}$$

由  $W = K_m$  ( $m \geq 1$ ) 给出。



注意，上述结论可以推出 Turán 定理，因为定理 5.17 告诉我们，凸包的极值点在  $W$  为一个团时取到。如果  $(K_{r+1}, W) = 0$ ，则在较高维立方体  $[0, 1]^r$  中的横截面有上界  $t(K_2, W) = t(K_2, K_r) = 1 - \frac{1}{r}$ 。特别的，我们考虑凸包  $D_{2,3} \subset [0, 1]^2$  中的极值点，它们为

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

所有这样形式的点都落在曲线  $y = x(2x - 1)$  上。

因为  $D_{2,3}$  包含在红点  $\{p_m\}_{m \geq 0}$  构成的凸包中，红点落在  $y = x(2x - 1)$  上。我们可以在凸包点之间连线，从而得到一个多边形区域。

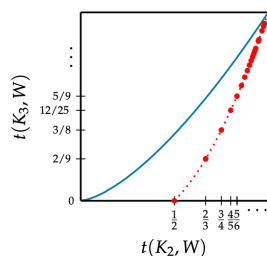


图 5.11:  $D_{2,3}$  的下界点，均在曲线  $y = x(2x - 1)$  上

Razborov 最终确定了  $D_{2,3}$  的模样，他用数理逻辑中的模型论 (Model Theory) 开发了旗代数 (flag algebras) 理论，这一理论给计算平方和不等式提供了一个有效的框架。简单来说，我们可大量、系统性地使用柯西-施瓦茨不等式来证明图密度不等式。

**定理 5.18 (Razborov 2008)**

对于属于以下区间的固定的边密度  $t(K_2, W)$

$$t(K_2, W) \in \left[1 - \frac{1}{k-1}, 1 - \frac{1}{k}\right], \quad k \in \mathbb{N}$$

可行的最小  $t(K_3, W)$  是通过一个唯一确定的阶跃函数 graphon 得到的，它对应于一个具有节点权重  $a_1, a_2, \dots, a_k$  的图，其中权重总和等于 1 并且  $a_1 = \dots = a_{k-1} \geq a_k$ 。



完整模样的  $D_{2,3}$  见图 5.12。为了更好的视觉效果，我们放大了区域下界的凹形（使凹型曲线变得更明显）。

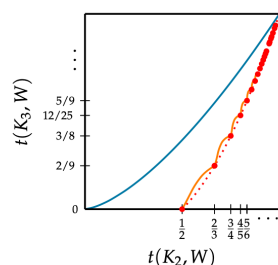


图 5.12:  $D_{2,3} \subset [0, 1]^2$  的完整模样

值得一提的是，在 Turán 定理中，极值对应的图的构造是唯一的；然而，在所有中间值  $t(K_2, W) \neq 1 - 1/k$  中，该定理为我们提供了非唯一的构造。graphon 的非唯一性意味最小化  $t(K_3, W)$  在实际操作中会很困难。在给定边密度的图中最小化  $K_r$  密度的问题由 Nikiforov (2011) 和 Reiher (2016) 解决，他们分别解决了  $r = 4$  和  $r$  任意取值的情形。

更一般地，考虑各种子图密度之间的不等式，我们能否确定这种不等式是否适用于所有 graphon? 对于同态密度之间的多项式不等式，只考虑线性密度就已经足够了，因为  $t(H, W)t(H', W) = t(H \sqcup H', W)$ 。

**问题 5.3** 给定一个多元多项式  $p \in \mathbb{R}[x_1, x_2, \dots, x_n]$ ，对于所有的  $x = (x_1, \dots, x_n)$ ，是否有  $p(x) \geq 0$ ?

这个问题是可判定的，Tarski 已经告诉我们实数的所有一阶逻辑都是可判定的。事实上，非负实多项式有以下特征。

**定理 5.19 (Artin)**

多项式  $p \in \mathbb{R}[x_1, x_2, \dots, x_n]$  是非负的当且仅当它可以写成有理函数的平方和。



然而，当我们将目标转化为一组格点时，情况发生了变化：

**问题 5.4** 给定一个多元多项式  $p \in \mathbb{R}[x_1, x_2, \dots, x_n]$ ，能否确定  $p(x_1, \dots, x_n) \geq 0$  对所有  $x \in \mathbb{Z}^n$  成立？

上述问题的答案是否定的。它与下面的事实有关。人们无法求解丢番图方程，甚至无法判断是否有解：

**定理 5.20 (Matiyasevich 2011; Hilbert's 10th problem)**

一个一般的丢番图方程的求解是一个不可判定的问题，甚至仅确定其是否存在整数解也是不可判定的。

回到我们最初感兴趣的问题，我们想知道以下问题是否可判定：

**问题 5.5** 对于一组给定的图  $\{H_i\}_{i \in [k]}$  和  $a_1, \dots, a_k \in \mathbb{R}$ ，对于所有的图  $G$  来说， $\sum_{i=1}^k a_i t(H_i, G) \geq 0$  是否成立？

下面的定理给出了这个问题的答案：

**定理 5.21 (Hatami - Norine 2011)**

给定一组图  $\{H_i\}_{i \in [k]}$  和  $a_1, \dots, a_k \in \mathbb{R}$ ，不等式

$$\sum_{i=1}^k a_i t(H_i, G) \geq 0$$

是否对于所有图  $G$  都成立是不可判定的。

上述定理成立的一个粗略的直觉是，我们实际上在  $D_{2,3}$  的下界上有一组离散点，然后我们可以将上述问题简化为证明红色曲线与区域的交点。这个交点构成一个离散集合，我们的思路是利用  $D_{2,3}$  下界上的特殊点将整数不等式（不可判定的）编码为图不等式。

另一种有趣的问题是询问特定的不等式是否正确；这种类型有几个尚未解决的问题。下面是极值图论中的一个重要猜想：

**命题 5.4 (Sidorenko's Conjecture 1993)**

如果  $H$  是一个二部图，则

$$t(H, W) \geq t(K_2, W)^{e(H)}$$

我们在讨论伪随机性时遇到了上述不等式的一个  $H = C_4$  的实例。但是，上述问题是开放的。现在让我们考虑 Möbius 带状图——它从完整的二部图  $K_{5,5}$  中删除一个长度为 10 的圈。对于该图不等式是否成立是未知的。

即使一般线性图不等式的非负性是不可判定的，如果人们想在  $\varepsilon$ -误差之内确定它们是否为真，问题就变得更容易解决：

**定理 5.22**

存在一个算法，对于任意  $\varepsilon > 0$ ，该算法能够正确地作出选择：是认为对于所有的图  $G$

$$\sum_{i=1}^n c_i t(H_i, G) \geq -\varepsilon$$

成立；还是输出一个图  $G$ ，满足

$$\sum_{i=1}^n c_i t(H_i, G) < 0$$

**证明 [概要]**

由于弱正则性引理，我们可以采用弱  $\varepsilon$ -正则划分。所有关于边密度的信息都可以用这个划分来表示。换句话说，我们只需要在带有  $\leq M(\varepsilon)$  部分的加权节点图上测试，这些部分的边权重是  $\varepsilon$  的倍数。如果对于从弱正则引理得到的辅助图对应的图密度加权总和的估计是正确的，那么对于原始图也是正确的，最多有  $\varepsilon$  的误差；否则，我们可以输出一个反例。


## 第二部分

# 加性组合

## 第 6 章 Roth 定理

在 3.3 章中，我们使用三角形删除引理和 Szemerédi 正则性引理证明了 Roth 定理。在本章节，我们将使用傅立叶分析的方法研究 Roth 定理的原始证明。首先，让我们回顾一下 Roth 定理的陈述：记  $r_3([N])$  表示  $[N]$  的 3-AP-free 子集大小的最大值，Roth 定理指出  $r_3([N]) = o(N)$ 。

事实上，使用 Szemerédi 正则性引理的缺点之一是证明所给出的上界类似于  $\frac{N}{\log^* N}$ 。而 Roth 的傅立叶分析版本的证明会给我们一个类似  $\frac{N}{\log \log N}$  的上界，这是一个更好的上界。

 **笔记** 目前已知的最佳上界是 Sanders 于 2011 年给出的  $r_3([N]) \leq N(\log^{1-o(1)} N)$ ，而已知的最佳下界是由 Behrend 于 2016 年给出的  $r_3(N) \geq Ne^{-O(\sqrt{\log N})}$ 。一些证据似乎表明下界更接近真实值，但缩小上下界之间的距离仍是一个悬而未决的问题。

### 6.1 有限域 Roth 定理

我们首先来查看有限域版本的 Roth 定理。在应用于一般整数情况之前，有限域版本是一个很好的尝试思路，因为在有限域中许多令人头疼的技术问题都消失了。

令  $r_3(\mathbb{F}_3^n)$  表示  $\mathbb{F}_3^n$  的 3-AP-free 子集大小的最大值。注意，给定  $\mathbb{F}_3^n$  中的  $x, y, z$ ，以下是等价的：

- $x, y, z$  构成长度为 3 的等差数列
- $x - 2y + z = 0$
- $x + y + z = 0$
- $x, y, z$  构成一条直线
- 对于所有的  $i$ ， $x, y, z$  的第  $i$  个坐标都不同或都相等。

我们将陈述并证明 Roth 定理的有限域版本。有限域版本的证明与 Roth 定理的原理相同，但稍微容易一些。

#### 定理 6.1

$$r_3(\mathbb{F}_3^n) = O\left(\frac{3^n}{n}\right)$$



回顾三角形删除引理的证明，我们可以直接得到  $r_3(\mathbb{F}_3^n) = o(3^n)$ ，但上述定理给出更好的上界。不久之后我们会证明定理 6.1。

我们先简要回顾一下这个问题的历史。2004 年，Edel 发现  $r_3(\mathbb{F}_3^n) \geq 2.21^n$ 。很久以来，命题  $r_3(\mathbb{F}_3^n) = (3 - o(1))^n$  是否正确一直是开放的。最近，一个令人惊讶的突破表明  $r_3(\mathbb{F}_3^n) \leq 2.76^n$  (2016, Ellenberg and Gijswijt)。

回顾 Szemerédi 正则性引理的证明过程，我们有一个能量增量的论证。有趣的是，Roth 定理的策略也是能量增量的一种变体。我们将关注于密度增量，给定  $A \subset \mathbb{F}_3^n$ ，我们采取如下步骤：

1. 如果  $A$  是伪随机的（我们将看到它等价于 Fourier uniform，粗略地说，它的所有傅立叶系数都很小），那么有一个计数引理将表明  $A$  有很多的 3-AP。
2. 如果  $A$  不是伪随机的，那么我们将证明  $A$  具有很大的傅立叶系数。然后我们可以找到一个维数为 1 的仿射子空间（即超平面），该子空间  $A$  的密度会增大。现在我们将  $A$  限制在这个超平面上，并重复前面的步骤。
3. 每次我们重复时，我们都会获得一个密度增量。由于密度的上界为 1，所以步数是有限的。

接下来，我们回顾一些对我们的证明很重要的傅立叶分析思想。在  $\mathbb{F}_3^n$  中，我们定义  $\mathbb{F}_3^n \rightarrow \mathbb{C}$  的映射  $\gamma_r(x) = \omega^{r \cdot x}$ ，下标  $r \in \mathbb{F}_3^n$ ， $\omega = e^{2\pi i/3}$ ， $r \cdot x = r_1 x_1 + \cdots + r_n x_n$ 。接下来我们定义傅立叶变换。对于  $f: \mathbb{F}_3^n \rightarrow \mathbb{C}$ ，傅立叶变换由  $\hat{f}: \mathbb{F}_3^n \rightarrow \mathbb{C}$  给出，其中

$$\hat{f}(r) = \mathbb{E}_{x \in \mathbb{F}_3^n} f(x) \omega^{-r \cdot x} = \langle f, \gamma_r \rangle$$

傅立叶变换是  $f$  和  $\gamma_r$  的内积。



更一般的, 我们有

**定义 6.1** ( $\mathbb{F}_p^n$  上的傅立叶变换)

$f: \mathbb{F}_p^n \rightarrow \mathbb{C}$  的傅立叶变换由  $\widehat{f}: \mathbb{F}_p^n \rightarrow \mathbb{C}$  给出, 对于每个  $r \in \mathbb{F}_p^n$ ,

$$\widehat{f}(r) := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x) \omega^{-r \cdot x} = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} f(x) \omega^{-r \cdot x}$$

其中  $r \cdot x = r_1 x_1 + \cdots + r_n x_n$ 。



**笔记** 为了方便我们作以下约定: 平均或求和的变量在  $\mathbb{F}_p^n$  上均匀变化。

我们注意到傅里叶变换的一些关键性质如下。

**命题 6.1**

- $\widehat{f}(0) = \mathbb{E} f$
- (Parseval)  $\mathbb{E}_{x \in \mathbb{F}_p^n} f(x) \overline{g(x)} = \sum_{r \in \mathbb{F}_p^n} \widehat{f}(r) \overline{\widehat{g}(r)}$
- (反演)  $f(x) = \sum_{r \in \mathbb{F}_p^n} \widehat{f}(r) \omega^{r \cdot x}$
- (卷积) 定义  $(f * g)(x) = \mathbb{E}_y f(y) g(x - y)$ , 我们有  $\widehat{f * g}(x) = \widehat{f}(x) \widehat{g}(x)$



下面我们证明这些性质。第一条是显然的, 我们来证明第二到四条。首先我们注意到

$$\{\gamma_r : r \in \mathbb{F}_p^n\}$$

构成一组正交基, 我们称其为傅立叶基, 可以验证

$$\langle \gamma_r, \gamma_s \rangle = \mathbb{E}_x [\gamma_r(x) \overline{\gamma_s(x)}] = \mathbb{E}_x [\omega^{-(r-s) \cdot x}] = \begin{cases} 1 & \text{if } r = s \\ 0 & \text{otherwise} \end{cases}$$

我们可以将傅立叶变换看作从  $\mathbb{F}_p^n$  到傅立叶基构成的空间的酉变换, 立即得到傅立叶反演和 Parseval 等式。最后, 我们检查卷积公式的正确性,

$$\mathbb{E}_x [(f * g) \omega^{r \cdot x}] = \mathbb{E}_{x, y} [f(y) g(x - y) \omega^{-r \cdot (y + (x - y))}] = \mathbb{E}_r [f(x) \omega^{-r \cdot x}] \mathbb{E}_s [g(x) \omega^{-s \cdot x}]$$

下面的引理将傅立叶变换与 3-AP 联系在一起。

**命题 6.2**

如果  $f, g, h: \mathbb{F}_3^n \rightarrow \mathbb{C}$ , 则

$$\mathbb{E}_{x, y} [f(x) g(x + y) h(x + 2y)] = \sum_r \widehat{f}(r) \widehat{g}(-2r) \widehat{h}(r)$$



我们将给出这个命题的两个证明, 其中第二个证明更具概念性。

**证明** [版本 1]

我们用傅立叶反演公式对等式左边处理。

$$\begin{aligned} LHS &= \mathbb{E}_{x, y} \left( \sum_{r_1} \widehat{f}(r_1) \omega^{r_1 \cdot x} \right) \left( \sum_{r_2} \widehat{g}(r_2) \omega^{r_2 \cdot (x + y)} \right) \left( \sum_{r_3} \widehat{h}(r_3) \omega^{r_3 \cdot (x + 2y)} \right) \\ &= \sum_{r_1, r_2, r_3} \widehat{f}(r_1) \widehat{g}(r_2) \widehat{h}(r_3) \mathbb{E}_x \omega^{x \cdot (r_1 + r_2 + r_3)} \mathbb{E}_y \omega^{y \cdot (r_2 + 2r_3)} \\ &= \sum_r \widehat{f}(r) \widehat{g}(-2r) \widehat{h}(r) \end{aligned}$$

最后的等号成立是因为

$$\mathbb{E}_x \omega^{x \cdot (r_1 + r_2 + r_3)} = \begin{cases} 1 & \text{if } r_1 + r_2 + r_3 = 0 \\ 0 & \text{otherwise} \end{cases}$$

和

$$\mathbb{E}_y \omega^{y \cdot (r_2 + 2r_3)} = \begin{cases} 1 & \text{if } r_2 + 2r_3 = 0 \\ 0 & \text{otherwise} \end{cases}$$

**证明** [版本 2]

在这个证明中，我们将等式左边视为卷积。令  $g_1(y) = g(-y/2)$ ，所以  $\widehat{g_1}(r) = \widehat{g}(-2r)$ 。

$$\begin{aligned} \mathbb{E}_{x,y} f(x)g(x+y)h(x+2y) &= \mathbb{E}_{x,y,z: x-2y+z=0} f(x)g(y)h(z) \\ &= \mathbb{E}_{x,y,z: x+y+z=0} f(x)g_1(y)h(z) \\ &= (f * g_1 * h)(0) \\ &= \sum_r \widehat{f * g_1 * h}(r) \\ &= \sum_r \widehat{f}(r) \widehat{g_1}(r) \widehat{h}(r) \\ &= \sum_r \widehat{f}(r) \widehat{g}(-2r) \widehat{h}(r) \end{aligned}$$

需要注意的是，在  $\mathbb{F}_3$  中  $-2 = 1$ 。因此，如果我们取  $f, g, h = 1_A$ ，其中  $A \subset \mathbb{F}_3^n$ ，则

$$3^{-2n} \# \{(x, y, z) \in A^3 : x + y + z = 0\} = \sum_r \widehat{1}_A(r)^3$$



**笔记** 如果  $A = -A$ ，那么得到的式子与计算 Cayley 图中长度为 3 的闭圈的公式相同。

#### 引理 6.1 (计数引理)

如果  $A \subset \mathbb{F}_3^n$  且  $|A| = \alpha 3^n$ ，令  $\Lambda_3(A) = \mathbb{E}_{x,y} [1_A(x)1_A(x+y)1_A(x+2y)]$ 。则

$$|\Lambda_3(A) - \alpha^3| \leq \alpha \max_{r \neq 0} |\widehat{1}_A(r)|$$



**证明** 根据命题 6.2

$$\Lambda_3(A) = \sum_r \widehat{1}_A(r)^3 = \alpha^3 + \sum_{r \neq 0} \widehat{1}_A(r)^3$$

因此，

$$\begin{aligned} |\Lambda_3(A) - \alpha^3| &= \left| \sum_{r \neq 0} \widehat{1}_A(r)^3 \right| \\ &\leq \sum_{r \neq 0} |\widehat{1}_A(r)|^3 \\ &\leq \max_{r \neq 0} |\widehat{1}_A(r)| \cdot \sum_r |\widehat{1}_A(r)|^2 \\ &= \max_{r \neq 0} |\widehat{1}_A(r)| \cdot \mathbb{E} 1_A^2 \\ &= \alpha \max_{r \neq 0} |\widehat{1}_A(r)| \end{aligned}$$

d 下面我们开始证明定理 6.1。

设  $N = 3^n$  为  $\mathbb{F}_3^n$  中的元素个数。

**第 1 步**，如果集合是 3-AP-free 的，则有一个大的傅立叶系数。

#### 引理 6.2

$A \subset \mathbb{F}_3^n$  且  $|A| = \alpha 3^n$ 。如果  $A$  是 3-AP-free 的且  $N \geq 2\alpha^{-2}$ ，则存在  $r \neq 0$  使得  $|\widehat{1}_A(r)| \geq \alpha^2/2$ 。



**证明** 注意到

$$\Lambda_3(A) = N^{-2} \# \{(x, y, z) \in A^3 : x + y + z = 0\} = \frac{|A|}{N^2} = \frac{\alpha}{N}$$

其中第二个等号成立是因为 3-AP-free 中只有  $x = y = z$  时满足  $x + y + z = 0$ 。根据计数引理，我们有

$$\alpha \max_{r \neq 0} |\widehat{1}_A(r)| \geq \alpha^3 - \frac{\alpha}{N} \geq \frac{\alpha^3}{2}$$

**第 2 步.** 大的傅立叶系数意味着超平面上的密度增量。

### 引理 6.3

$A \subset \mathbb{F}_3^n$  且  $|A| = \alpha 3^n$ 。如果  $|\widehat{1}_A(r)| \geq \delta$  对于某  $r \neq 0$  成立，则当  $A$  限制在某个超平面上时， $A$  的密度至少为  $\alpha + \frac{\delta}{2}$ 。

**证明** 我们有

$$\begin{aligned} \widehat{1}_A(r) &= \mathbb{E}_{x \in \mathbb{F}_3^n} 1_A(x) w^{-r \cdot x} \\ &= \frac{1}{3} (\alpha_0 + \alpha_1 w + \alpha_2 w^2) \end{aligned}$$

其中  $\alpha_0, \alpha_1, \alpha_2$  是  $A$  在  $r^\perp$  的陪集上的密度。我们想要证明  $\alpha_0, \alpha_1, \alpha_2$  中有一个是显著大于  $\alpha$  的。注意到  $\alpha = \frac{\alpha_0 + \alpha_1 + \alpha_2}{3}$ 。由三角不等式，

$$\begin{aligned} 3\delta &\leq |\alpha_0 + \alpha_1 w + \alpha_2 w^2| \\ &= |(\alpha_0 - \alpha) + (\alpha_1 - \alpha)w + (\alpha_2 - \alpha)w^2| \\ &\leq \sum_{j=0}^2 |\alpha_j - \alpha| \\ &= \sum_{j=0}^2 (|\alpha_j - \alpha| + (\alpha_j - \alpha)) \end{aligned}$$

(最后一步的技巧也将在下一节中用到) 请注意，最后一个求和中的每一项  $|\alpha_j - \alpha| + (\alpha_j - \alpha)$  都是非负的。因此，存在  $j$  使得  $\delta \leq |\alpha_j - \alpha| + (\alpha_j - \alpha)$ ，所以有  $\alpha_j \geq \alpha + \frac{\delta}{2}$ 。

**第 3 步，迭代密度增量。**

到目前为止，如果  $A$  是 3-AP-free 的且  $N \geq 2\alpha^{-2}$ ，那么在某个超平面上  $A$  的密度至少为  $\alpha + \alpha^2/4$ 。我们令初始密度为  $\alpha_0 = \alpha$ 。在第  $i$  步，我们将  $A$  限制在某个超平面上，使得子空间内  $A$  的密度为

$$\alpha_i \geq \alpha_{i-1} + \alpha_{i-1}^2/4$$

令  $N_i = 3^{n-i}$ ，只要  $N_i \geq 2\alpha_i^{-2}$  我们就可以继续做第  $i$  步。因为  $\alpha_i$  最大为 1，因此迭代过程一定在有限次数后终止。我们关心的是，多少次迭代后会终止？显然  $\frac{4}{\alpha^2}$  次后一定会终止，但这个上界还不够好，它仅能告诉我们  $|A| = O\left(\frac{3^n}{\sqrt{n}}\right)$ 。下面我们将去找一个更好的上界。


考虑从  $\alpha_0$  开始到第一次翻倍的迭代次数  $i_1$ ， $\alpha_{i_1} > 2\alpha_0$ 。显然  $i_1 \leq \frac{4}{\alpha}$ 。接着我们考虑从  $\alpha_{i_1}$  到下一次翻倍的迭代次数  $i_2$ ， $\alpha_{i_2} > 2^2\alpha_0$ ，整理得到  $i_2 \leq \frac{2}{\alpha}$ 。依次类推，第  $k$  次翻倍需要的迭代次数  $i_k \leq \frac{4}{\alpha^{2^{k-1}}}$ 。对于任意的  $k$ ，有

$$\frac{4}{\alpha} + \frac{2}{\alpha} + \cdots + \frac{4}{2^{k-1}\alpha} \leq \frac{8}{\alpha}$$

所以在  $\frac{8}{\alpha}$  次迭代后一定终止。假设该过程在  $m$  步后终止，密度为  $\alpha_m$ 。那么最后一步中子空间的大小为  $3^{n-m} < 2\alpha_m^{-2} \leq 2\alpha^{-2}$ 。对不等式两边取对数有

$$n \leq \frac{8}{\alpha} + \log_3 \left( \frac{2}{\alpha^2} \right) = O\left(\frac{1}{\alpha}\right)$$

因此， $\frac{|A|}{N} = \alpha = O(1/n)$ 。等价的， $|A| = \alpha N = O\left(\frac{3^n}{n}\right)$ ，这正是我们想要的。

 **笔记** 该证明在整数中会变得困难得多，因为整数时子空间不能向下传递。

一个自然的问题是这种技术是否可以推广到 4-AP 的计数。在基于正则性引理的 Roth 定理证明中，我们看到图删除引理是不够的，实际上我们还需要超图正则性和超图删除引理来实现 4-AP 计数。类似地，虽然这里介绍的计数引理表明傅立叶系数控制着 3-AP 的计数，但它们并不控制着 4-AP 的计数。例如，考虑集合  $A = \{x \in \mathbb{F}_5^n : x \cdot x = 0\}$ ，可以证明  $A$  对应的非零傅立叶系数都是小的。然而，我们也可以证明  $A$  的 4-AP 数量是错误的，这意味着傅立叶系数无法控制 4-AP 的数量。Gowers 为了扩展 Roth 定理的证明，专门开发了高阶傅里叶分析（二次傅里叶分析），他证明了 Szemerédi 定理适用于更大的 AP。下面的定理给出了一个二次傅立叶分析的例子。

### 定理 6.2 (Inverse theorem for quadratic Fourier analysis)

对于任意的  $\delta > 0$ ，存在一个常数  $c(\delta) > 0$  使得如果  $A \subset \mathbb{F}_5^n$  具有密度  $\alpha$  并且  $|\Lambda_4(A) - \alpha^4| > \delta$ ，则存在  $\mathbb{F}_5$  上的二次非零多项式  $f(x_1, \dots, x_n)$  满足

$$\left| \mathbb{E}_{x \in \mathbb{F}_5^n} 1_A(x) \omega^{f(x)} \right| \geq c(\delta)$$



## 6.2 Roth 对整数 Roth 定理的证明

在第 6.1 节中，我们看到了 Roth 定理在有限域中（特别是对于集合  $\mathbb{F}_3^n$ ）的证明。现在我们对它进行扩展来证明下面给出的上界，即整数的 Roth 定理：

### 定理 6.3

$$r_3([N]) = O\left(\frac{N}{\log \log N}\right)$$



这个上界的原始证明由 Roth 本人给出。回想一下，有限域中 Roth 定理的证明有以下 3 个步骤：

1. 证明一个 3-AP-free 的集合允许一个大的傅立叶系数。
2. 推导出一定存在一个密度增大的子空间。
3. 迭代密度增量，得到 3-AP-free 集大小的上界。

关于整数 Roth 定理的证明将同样遵循以上 3 个步骤。但是，具体的执行将大不相同。其中，主要的区别在于第 2 步， $[N]$  子空间的概念在这里并不好找到。

之前我们在群  $\mathbb{F}_3^n$  上定义了傅立叶分析。事实上，存在一个关于阿贝尔群的傅立叶分析理论，它将群  $G$  与其对偶群  $\widehat{G}$  联系起来。现在我们来考虑群  $\mathbb{Z}$ 。

$\mathbb{Z}$  的对偶群为  $\widehat{\mathbb{Z}} = \mathbb{R}/\mathbb{Z}$ 。 $f: \mathbb{Z} \rightarrow \mathbb{C}$  的傅里叶变换由如下函数给出  $\widehat{f}: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$  满足

$$\widehat{f}(\theta) = \sum_{x \in \mathbb{Z}} f(x) e(-x\theta)$$

其中  $e(t) = e^{2\pi i t}$ 。这通常被称为  $f$  的傅立叶级数。

和在  $\mathbb{F}_3^n$  中一样，以下恒等式在  $\mathbb{Z}$  中也成立。他们的证明是相同的。

- $\widehat{f}(0) = \sum_{x \in \mathbb{Z}} f(x)$
- (Parseval)  $\sum_{x \in \mathbb{Z}} f(x) \overline{g(x)} = \int_0^1 \widehat{f}(\theta) \overline{\widehat{g}(\theta)} d\theta$
- (反演)  $f(x) = \int_0^1 \widehat{f}(\theta) e(x\theta) d\theta$
- 定义  $\Lambda(f, g, h) = \sum_{x, y \in \mathbb{Z}} f(x) g(x+y) h(x+2y)$ 。然后有

$$\Lambda(f, g, h) = \int_0^1 \widehat{f}(\theta) \widehat{g}(-2\theta) \widehat{h}(\theta) d\theta$$

在有限域的版本中，我们有计数引理用来表明如果两个函数具有相似的傅立叶变换，则它们具有相似数量的 3-AP。同样的，在  $\mathbb{Z}$  中我们有类似的计数引理。

**定理 6.4 (计数引理)**

令  $f, g: \mathbb{Z} \rightarrow \mathbb{C}$  满足  $\sum_{n \in \mathbb{Z}} |f(n)|^2 \leq M, \sum_{n \in \mathbb{Z}} |g(n)|^2 \leq M$ 。定义  $\Lambda_3(f) = \Lambda(f, f, f)$ ，则有

$$|\Lambda_3(f) - \Lambda_3(g)| \leq 3M \|\widehat{f - g}\|_\infty$$



**证明** 注意到

$$\Lambda_3(f) - \Lambda_3(g) = \Lambda(f - g, f, f) + \Lambda(g, f - g, f) + \Lambda(g, g, f - g)$$

我们考虑上式第一项的上界

$$\begin{aligned} |\Lambda(f - g, f, f)| &= \left| \int_0^1 (\widehat{f - g})(\theta) \widehat{f}(-2\theta) \widehat{f}(\theta) d\theta \right| \\ &\leq \|\widehat{f - g}\|_\infty \left| \int_0^1 \widehat{f}(-2\theta) \widehat{f}(\theta) d\theta \right| \\ &\leq \|\widehat{f - g}\|_\infty \left( \int_0^1 |\widehat{f}(-2\theta)|^2 d\theta \right)^{1/2} \left( \int_0^1 |\widehat{f}(\theta)|^2 d\theta \right)^{1/2} \quad (\text{Cauchy-Schwarz}) \\ &\leq \|\widehat{f - g}\|_\infty \left( \sum_{x \in \mathbb{Z}} |f(x)|^2 \right) \quad (\text{Parseval}) \\ &\leq M \|\widehat{f - g}\|_\infty \end{aligned}$$

第二项、第三项的处理是完全相同的。

我们现在来证明 Roth 定理 (定理6.3)。我们的证明步骤与有限域版本的相同。

**第 1 步:** 如果集合是 **3-AP-free** 的, 则有一个大的傅立叶系数。

**引理 6.4**

令  $A \subset [N]$  是一个 3-AP-free 集,  $|A| = \alpha N, N \geq 5/\alpha^2$ 。那么存在  $\theta \in \mathbb{R}$  使得

$$\left| \sum_{n=1}^N (1_A - \alpha)(n) e(\theta n) \right| \geq \frac{\alpha^2}{10} N$$



**证明** 由于  $A$  没有 3-AP, 因此  $1_A(x)1_A(x+y)1_A(x+2y)$  当且仅当  $y=0$  时是非零的。因此  $\Lambda_3(1_A) = |A| = \alpha N$ 。现在考虑  $\Lambda_3(1_{[N]})$ , 该式计算了  $[N]$  中 3-AP 的数量。我们可以通过从  $[N]$  中选出两个元素来构成 3-AP 中的第一个和第三个, 两个元素的奇偶性相同。因此  $\Lambda_3(1_{[N]}) = [N/2]^2 + [N/2]^2 \geq N^2/2$ 。现在, 应用计数引理, 取  $f = 1_A, g = \alpha 1_{[N]}$  (我们使用记号  $f^\wedge = \widehat{f}$ )

$$\frac{\alpha^3 N^2}{2} - \alpha N \leq 3\alpha N \left\| (1_A - \alpha 1_{[N]})^\wedge \right\|_\infty$$

因此

$$\begin{aligned} \left\| (1_A - \alpha 1_{[N]})^\wedge \right\|_\infty &\geq \frac{\frac{1}{2}\alpha^3 N^2 - \alpha N}{3\alpha N} \\ &= \frac{1}{6}\alpha^2 N - \frac{1}{3} \\ &\geq \frac{1}{10}\alpha^2 N \end{aligned}$$

最后一个不等号成立时是因为  $N \geq 5/\alpha^2$ 。因此存在  $\theta$  使得

$$\left| \sum_{n=1}^N (1_A - \alpha)(n) e(\theta n) \right| = (1_A - \alpha 1_{[N]})^\wedge(\theta) \geq \frac{1}{10}\alpha^2 N$$

证毕。



**笔记** 整个证明的核心是关于结构与伪随机性, 我们在讨论图的正则性中也看到了这种想法。如果  $A$  是“伪随机的”, 那么我们希望证明  $A$  具有小的傅立叶系数。但这将表明  $f$  和  $g$  具有相似的傅立叶系数, 这意味着  $A$  具有许多 3-AP 从而矛盾。因此  $A$  不能是伪随机的, 它必须具有某种结构。

**第2步**，大的傅立叶系数会产生密度增量。

在有限域版本中，我们的傅立叶系数对应于超平面，然后我们能够证明在某个超平面陪集上密度很大。然而，现在  $\theta$  是一个实数。 $[N]$  中没有超平面的概念，那么我们如何将  $[N]$  细分从而使用密度增量？

我们将  $[N]$  划分为子级数 (sub-progression)，同时保证  $x \mapsto e(x\theta)$  在每个子级数上大致恒定。

举一个简单的例子，假设  $\theta$  是一个有理数  $a/b$ ，其中  $b$  相当小。那么  $x \mapsto e(x\theta)$  在具有公差  $b$  的算术级数上可近似为常数。

在正式写出这个想法之前，我们需要介绍 Dirichlet 的经典引理。

#### 引理 6.5

令  $\theta \in \mathbb{R}$ ， $0 < \delta < 1$ 。存在正整数  $d \leq 1/\delta$  满足  $\|d\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \delta$  ( $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$  被定义为到最近整数的距离)

**证明**

令  $m = \lfloor \frac{1}{\delta} \rfloor$ 。考虑  $m+1$  个数  $0, \theta, \dots, m\theta$ ，根据鸽巢原理，存在  $i, j$  使得  $i\theta$  和  $j\theta$  的小数部分最多相差  $\delta$ 。令  $d = |i - j|$ ，然后有  $\|d\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \delta$ ，证毕。

下一个引理描述了我们之前将  $[N]$  划分为子级数的想法，映射  $x \mapsto e(x\theta)$  在每个子级数上大致恒定。

#### 引理 6.6

令  $0 < \eta < 1$ ， $\theta \in \mathbb{R}$ 。假设  $N > C\eta^{-6}$  ( $C$  为某常数)。可以将  $[N]$  划分为多个 sub-AP  $P_i$ ，每个 sub-AP 的长度满足  $N^{1/3} \leq |P_i| \leq 2N^{1/3}$ ，且  $P_i$  满足对于任意的  $i$  有  $\sup_{x, y \in P_i} |e(x\theta) - e(y\theta)| < \eta$ 。

**证明**

根据引理 6.5，存在一个整数  $d \leq \frac{4\pi N^{1/3}}{\eta}$  使得  $\|d\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{\eta}{4\pi N^{1/3}}$ 。由于  $N > C\eta^{-6}$ ，取  $C = (4\pi)^6$  我们得到  $d < \sqrt{N}$ 。因此，我们可以将  $[N]$  划分为多个具有公差  $d$  的 sub-AP，并且保证每个 sub-AP 的长度在  $N^{1/3}$  和  $2N^{1/3}$  之间。然后，在每个 sub-AP  $P$  中，我们有

$$\sup_{x, y \in P} |e(x\theta) - e(y\theta)| \leq |P| |e(d\theta) - 1| \leq 2N^{1/3} \cdot 2\pi \|d\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \eta$$

不等式  $|e(d\theta) - 1| \leq 2\pi \|d\theta\|_{\mathbb{R}/\mathbb{Z}}$  成立是因为弦长小于等于对应的弧长。

我们现在可以应用这个引理来得到密度增量。

#### 引理 6.7

令  $A \subset [N]$  是 3-AP-free 的，且  $|A| = \alpha N$ ， $N > C\alpha^{-12}$ 。一定存在一个 sub-AP  $P \subset [N]$ ，其中  $|P| \geq N^{1/3}$  且  $|A \cap P| \geq (\alpha + \alpha^2/40) |P|$ 。

**证明** 根据引理 6.4，一定存在  $\theta$  满足  $\left| \sum_{x=1}^N (1_A - \alpha)(x) e(x\theta) \right| \geq \alpha^2 N/10$ 。然后，使用引理 6.6，取  $\eta = \alpha^2/20$  我们得到  $[N]$  的一个划分  $P_1, \dots, P_k$ ，该划分满足  $N^{1/3} \leq |P_i| \leq 2N^{1/3}$ 。所以我们有

$$\frac{\alpha^2}{10} N \leq \left| \sum_{x=1}^N (1_A - \alpha)(x) e(x\theta) \right| \leq \sum_{i=1}^k \left| \sum_{x \in P_i} (1_A - \alpha)(x) e(x\theta) \right|$$

对于  $x, y \in P_i$ ， $|e(x\theta) - e(y\theta)| \leq \alpha^2/20$ 。因此

$$\left| \sum_{x \in P_i} (1_A - \alpha)(x) e(x\theta) \right| \leq \left| \sum_{x \in P_i} (1_A - \alpha)(x) e(x_0\theta) \right| + \frac{\alpha^2}{20} |P_i| \leq \left| \sum_{x \in P_i} (1_A - \alpha)(x) \right| + \frac{\alpha^2}{20} |P_i|$$

其中， $x_0$  是  $P_i$  中任意一元素。注意到

$$\begin{aligned} \frac{\alpha^2}{10} N &\leq \sum_{i=1}^k \left( \left| \sum_{x \in P_i} (1_A - \alpha)(x) \right| + \frac{\alpha^2}{20} |P_i| \right) \\ &= \sum_{i=1}^k \left| \sum_{x \in P_i} (1_A - \alpha)(x) \right| + \frac{\alpha^2}{20} N \end{aligned}$$



所以

$$\frac{\alpha^2}{20}N \leq \sum_{i=1}^k \left| \sum_{x \in P_i} (1_A - \alpha)(x) \right|$$

因此

$$\frac{\alpha^2}{20} \sum_{i=1}^k |P_i| \leq \sum_{i=1}^k \|A \cap P_i - \alpha|P_i|\|$$

我们想证明存在  $P_i$  使得  $A$  在限制在  $P_i$  时具有密度增量。我们使用以下技巧

$$\begin{aligned} \frac{\alpha^2}{20} \sum_{i=1}^k |P_i| &\leq \sum_{i=1}^k \|A \cap P_i - \alpha|P_i|\| \\ &= \sum_{i=1}^k (\|A \cap P_i - \alpha|P_i|\| + |A \cap P_i - \alpha|P_i||) \end{aligned}$$

所以存在  $i$  满足

$$\frac{\alpha^2}{20} |P_i| \leq \|A \cap P_i - \alpha|P_i|\| + |A \cap P_i - \alpha|P_i||$$

当  $|x| + x$  总是严格大于 0 时  $x$  一定大于等于零，所以一定有  $|A \cap P_i - \alpha|P_i|| \geq 0$ ，因此我们有

$$\frac{\alpha^2}{20} |P_i| \leq 2(|A \cap P_i - \alpha|P_i||)$$

整理后得到

$$|A \cap P_i| \geq \left( \alpha + \frac{\alpha^2}{40} \right) |P_i|$$

因此，我们找到了具有密度增量的 sub-AP，这是我们想要的。

**第 3 步，迭代密度增量。**

第 3 步与有限域版本的非常相似。设初始密度为  $\alpha_0 = \alpha$ ，每次迭代后的密度为  $\alpha_i$ 。我们有  $\alpha_{i+1} \geq \alpha_i + \alpha_i^2/40$ ，并且  $\alpha_i \leq 1$ 。

考虑从  $\alpha_0$  开始到第一次翻倍的迭代次数  $i_1$ ， $\alpha_{i_1} > 2\alpha_0$ 。显然  $i_1 \leq \frac{40}{\alpha}$ 。接着我们考虑从  $\alpha_{i_1}$  到下一次翻倍的迭代次数  $i_2$ ， $\alpha_{i_2} > 2^2\alpha_0$ ，整理得到  $i_2 \leq \frac{20}{\alpha}$ 。依次类推，第  $k$  次翻倍需要的迭代次数  $i_k \leq \frac{40}{\alpha 2^{k-1}}$ 。对于任意的  $k$ ，有

$$\frac{40}{\alpha} + \frac{20}{\alpha} + \cdots + \frac{40}{2^{k-1}\alpha} \leq \frac{80}{\alpha}$$

所以在  $\frac{80}{\alpha}$  次迭代后一定终止。所以总迭代次数必须是  $O(1/\alpha)$ 。

引理 6.7 表明我们可以向下传递给 sub-AP，并且  $N_i > C\alpha^{-12}$  时密度增加。假设迭代过程在第  $i$  步终止，我们必须有  $N_i \leq C\alpha_i^{-12} \leq C\alpha^{-12}$ 。每次迭代我们的集合的大小都会减少为立方根，所以

$$N \leq N_i^{3^i} \leq \left( C\alpha^{-12} \right)^{3^{O(1/\alpha)}} = e^{e^{O(1/\alpha)}}$$

两边取对数得到  $\alpha = O(1/\log \log N)$ ， $|A| = \alpha N = O(N/\log \log N)$ ，这是我们想要的。

我们来比较  $\mathbb{F}_3^n$  和  $[N]$  的证明策略。我们看到  $r_3(\mathbb{F}_3^n) = O(N/\log N)$ 。然而， $[N]$  上的上界为  $O(N/\log \log N)$ ，它相比于有限域的结果弱了一个对数因子。这从何而来？在  $\mathbb{F}_3^n$  的密度增量步骤中，我们能够向下传递到一个子集，该子集的大小是原始子集的常数因子。然而，在  $[N]$  中，每次迭代都会给我们一个子级数，它的大小等于前一个子空间的立方根。一个自然的问题是——是否有可能向下传递到一个看起来更像子空间的子级数？事实证明，这是可以做到的。

对于子集  $S \subset \mathbb{F}_3^n$ ，我们可以将其正交补写作

$$U_S = \{x \in \mathbb{F}_3^n : x \cdot s = 0 \text{ for all } s \in S\}$$

在  $[N]$  中，类似的概念被称为 Bohr 集，这是 Bourgain 在 1999 年提出的一个想法，用于将有限域版本的证明转移到  $\mathbb{Z}$  上。这需要在  $\mathbb{Z}/N\mathbb{Z}$  上工作。对于子集  $S \subset \mathbb{Z}/N\mathbb{Z}$ ，我们可以将其 Bohr 集定义为

$$\text{Bohr}(S, \epsilon) = \left\{ x \in \mathbb{Z}/N\mathbb{Z} : \left\| \frac{sx}{N} \right\| \leq \epsilon \text{ for all } s \in S \right\}$$

这为子空间提供了更自然的类比，并且是现代改进 Roth 定理上界的基础。在第 7 章研究 Freiman 定理时我们还会遇到 Bohr 集。

## 6.3 有限域 Roth 定理的多项式证明

目前， $\mathbb{F}_3^n$  中 Roth 定理最好的上界如下：

**定理 6.5 (Ellenberg and Gijswijt (2017))**

$$r_3(\mathbb{F}_3^n) = O(2.76^n)$$

这个上界改进了之前由 Bateman 和 Katz 于 2012 年给出的上界  $O(3^n/n^{1+\epsilon})$  ( $\epsilon > 0$ )。Bateman 和 Katz 使用傅立叶分析的方法来证明他们的上界，并且直到 17 年 Ellenberg 和 Gijswijt 给出新的上界以来，上界是否可以改进至  $O(c^n)$  ( $c < 3$ ) 一直是开放的。新给出的上界更接近 Edel 于 2004 年给出的下界  $2.21^n$ 。

Croot-Lev-Pach (2017) 给出了在  $(\mathbb{Z}/4\mathbb{Z})^n$  上与 3-AP 上界类似的上界，他们证明了  $(\mathbb{Z}/4\mathbb{Z})^n$  4-AP-free 的集合的大小最大为  $O(3.61^n)$ 。他们使用了多项式方法的一种变体，并且由于元素阶为 2，这使他们的证明变得更容易。正如文献中经常提到的那样，Ellenberg 和 Gijswijt 使用 Croot-Lev-Pach 方法证明了  $\mathbb{F}_3^n$  上新的上界。

令  $A \subseteq \mathbb{F}_3^n$  是 3-AP-free 集（在文献中有时也被称为上限集 cap set）。我们有等式

$$\delta_0(x+y+z) = \sum_{a \in A} \delta_a(x)\delta_a(y)\delta_a(z) \quad (6.1)$$

$x, y, z \in A$ ，其中  $\delta_a$  是 Dirac delta 函数，定义为：

$$\delta_a(x) := \begin{cases} 1 & \text{if } x = a \\ 0 & \text{if } x \neq a \end{cases}$$

因为  $\mathbb{F}_3^n$  中  $x+y+z=0$  当且仅当  $z-y=y-x$ ，这意味着只有  $x=y=z=a$  时  $x, y, z$  才构成等差数列， $a \in \mathbb{F}_3^n$ 。所以 (6.1) 成立。

我们将证明 (6.1) 的左侧是“低秩”的，右侧是我们在下面意义下的“高秩”的。

回想一下线性代数中矩阵秩的概念：给定一个函数  $F: A \times A \rightarrow \mathbb{F}$ ，对于域  $\mathbb{F}$ ，如果我们有  $F(x, y) = f(x)g(y)$ ，函数  $f, g: A \rightarrow \mathbb{F}$ ，我们称  $F$  的秩为 1，简称秩 1。我们定义  $\text{rank } F$  是将  $F$  写为秩 1 函数的线性组合所需的秩 1 函数数量的最小值。

我们应该如何定义函数  $F: A \times A \times A \rightarrow \mathbb{F}$  的秩？函数  $A \times A \rightarrow \mathbb{F}$  对应于矩阵，函数  $A \times A \times A \rightarrow \mathbb{F}$  对应于 3 阶张量。类似的，我们有张量秩的概念，其中秩 1 函数形如  $F(x, y, z) = f(x)g(y)h(z)$ 。张量秩是一个很重要的概念，有很多的性质，但我们不会用到它。我们需要的是切片秩 (slice-rank) 的概念。具体的，

**定义 6.2 (Slice rank)**

函数  $F: A \times A \times A \rightarrow \mathbb{F}$  的切片秩为 1 如果它可以写做如下形式之一

$$f(x)g(y, z), \quad f(y)g(x, z), \quad \text{or} \quad f(z)g(x, y),$$

其中， $f: A \rightarrow \mathbb{F}$  和  $g: A \times A \rightarrow \mathbb{F}$  是非零函数。函数  $F: A \times A \times A \rightarrow \mathbb{F}$  的切片秩是将  $F$  可以写成秩 1 函数的线性组合所需的秩 1 函数数量的最小值。

对角函数的切片秩是多少？回忆线性代数的知识，对角矩阵的秩是非零项的数量。该结论同样适用于切片秩。

**引理 6.8**

如果  $F: A \times A \times A \rightarrow \mathbb{F}$  定义为

$$F(x, y, z) = \sum_{a \in A} c_a \delta_a(x) \delta_a(y) \delta_a(z)$$

则

$$\text{slice-rank } F = |\{a \in A : c_a \neq 0\}|$$

这里的系数  $c_a$  对应于对角线元素。

**证明** 很明显,  $\text{slice-rank } F \leq |\{a \in A : c_a \neq 0\}|$ 。这是因为我们可以将  $F$  秩 1 函数的线性组合

$$F(x, y, z) = \sum_{\substack{a \in A \\ c_a \neq 0}} c_a \delta_a(x) (\delta_a(y) \delta_a(z))$$

对于另一个方向, 我们假设所有对角线元素都不为零; 如果对于某些  $a$ ,  $c_a = 0$ , 那么我们可以在不增加切片秩的情况下从  $A$  中删除  $a$ 。采用反证法, 假设  $\text{slice-rank } F < |A|$ 。我们有

$$\begin{aligned} F(x, y, z) &= f_1(x)g_1(y, z) + \cdots + f_\ell(x)g_\ell(y, z) \\ &\quad + f_{\ell+1}(y)g_{\ell+1}(x, z) + \cdots + f_m(y)g_m(x, z) \\ &\quad + f_{m+1}(z)g_{m+1}(x, y) + \cdots + f_{|A|-1}(z)g_{|A|-1}(x, y) \end{aligned}$$

### 命题 6.3

存在  $h : A \rightarrow \mathbb{F}_3$ ,  $|\text{supp } h| > m$  使得

$$\sum_{z \in A} h(z) f_i(z) = 0 \quad (6.2)$$

对于所有的  $i = m+1, \dots, |A|-1$  成立。这里  $\text{supp } h$  是集合  $\{z \in A : h(z) \neq 0\}$ 。

**证明**

显然, 满足条件的  $h$  一定是一个维数大于  $m$  的子空间。我们声称: 任何  $m+1$  维子空间的支撑集的大小至少为  $m+1$  (这里的支撑集定义与命题中保持一致)。理由如下:

对于任意  $m+1$  维子空间  $X$ , 我们将其  $m+1$  个线性无关的向量按列摆放构成一个  $|A| \times (m+1)$  的矩阵, 不妨记为  $Y$ 。  $Y$  的秩为  $m+1$ 。我们可以在  $Y$  中删去一些行得到一个  $(m+1) \times (m+1)$  且行列式非零的矩阵。新得到的矩阵的列向量我们记作  $v_1, v_2, \dots, v_{m+1} \in \mathbb{F}_3^{m+1}$ 。因为行列式非零, 所以  $v_1, v_2, \dots, v_{m+1}$  是  $\mathbb{F}_3^{m+1}$  的一组基。因此一定存在  $v_1, v_2, \dots, v_{m+1}$  的线性组合是全 1 向量, 全 1 向量的支撑集大小为  $m+1$ 。所以未删除行之前的列向量 (即  $Y$  的列向量) 也能给出一个支撑集大小至少为  $m+1$  的线性组合。

选择上述命题中的  $h$ , 考虑

$$\sum_{z \in A} F(x, y, z) h(z) = \sum_{a \in A} \sum_{z \in A} c_a \delta_a(x) \delta_a(y) \delta_a(z) h(z) = \sum_{a \in A} c_a h(a) \delta_a(x) \delta_a(y)$$

还注意到

$$\begin{aligned} \sum_{z \in A} F(x, y, z) h(z) &= f_1(x) \widetilde{g}_1(y) + \cdots + f_\ell(x) \widetilde{g}_\ell(y) \\ &\quad + f_{\ell+1}(y) \widetilde{g}_{\ell+1}(x) + \cdots + f_m(y) \widetilde{g}_m(x) \end{aligned}$$

其中  $\widetilde{g}_i(y) = \sum_{z \in A} g_i(y, z) h(z)$ ,  $1 \leq i \leq \ell$ 。  $\widetilde{g}_i(x) = \sum_{z \in A} g_i(x, z) h(z)$ ,  $\ell+1 \leq i \leq m$ 。因此

$$\begin{aligned} \sum_{a \in A} c_a h(a) \delta_a(x) \delta_a(y) &= f_1(x) \widetilde{g}_1(y) + \cdots + f_\ell(x) \widetilde{g}_\ell(y) \\ &\quad + f_{\ell+1}(y) \widetilde{g}_{\ell+1}(x) + \cdots + f_m(y) \widetilde{g}_m(x) \end{aligned}$$

注意等号左边有超过  $m$  个对角线元素 (记作  $a$ ,  $h(a) \neq 0$ ), 但等号右边切片秩最多为  $m$ , 矛盾。

使用归纳法, 我们可以轻松地将 3 个变量的情形推广到任何有限数量的变量, 我们省略其证明。

我们已经证明了 (6.1) 右边的切片秩为  $|A|$ , 因此是“高秩”。现在我们来证明左侧是“低秩”。

## 引理 6.9

定义  $F: A \times A \times A \rightarrow \mathbb{F}_3$  如下:

$$F(x+y+z) := \delta_0(x+y+z)$$

则 slice-rank  $F \leq 3M$ , 其中

$$M := \sum_{\substack{a,b,c \geq 0 \\ a+b+c=n \\ b+2c \leq 2n/3}} \frac{n!}{a!b!c!}$$



**证明** 在  $\mathbb{F}_3$  中, 有  $\delta_0(x) = 1 - x^2$ . 因此

$$\delta_0(x+y+z) = \prod_{i=1}^n (1 - (x_i + y_i + z_i)^2) \quad (6.3)$$

其中  $x_i$  是  $x \in \mathbb{F}_3^n$  的坐标, 依此类推. 如果我们展开右侧, 我们会得到一个变量数目为  $3n$  的多项式, 阶数为  $2n$ . 每个单项式形如

$$x_1^{i_1} \cdots x_n^{i_n} y_1^{j_1} \cdots y_n^{j_n} z_1^{k_1} \cdots z_n^{k_n}$$

其中  $i_1, i_2, \dots, i_n, j_1, \dots, j_n, k_1, \dots, k_n \in \{0, 1, 2\}$ . 下面我们对这些单项式分组. 对于每一项, 根据鸽巢原理,  $i_1 + \dots + i_n, j_1 + \dots + j_n, k_1 + \dots + k_n$  三项中至少有一项最多为  $2n/3$ . 我们可以将 (6.3) 写为单项式的和. 具体的, 我们将其写为

$$\prod_{i=1}^n (1 - (x_i + y_i + z_i)^2) = \sum_{\substack{i_1, i_2, \dots, i_n \\ j_1, j_2, \dots, j_n \\ k_1, k_2, \dots, k_n}} c_{i_1, \dots, i_n, j_1, \dots, j_n, k_1, \dots, k_n} x_1^{i_1} \cdots x_n^{i_n} y_1^{j_1} \cdots y_n^{j_n} z_1^{k_1} \cdots z_n^{k_n} \quad (6.4)$$

其中系数  $c_{i_1, \dots, i_n, j_1, \dots, j_n, k_1, \dots, k_n} \in \mathbb{F}_3$ . 然后, 我们可以按以下方式进行分组以将 (6.4) 写为切片秩为 1 的函数的和:

$$\begin{aligned} \prod_{i=1}^n (1 - (x_i + y_i + z_i)^2) &= \sum_{i_1 + \dots + i_n \leq \frac{2n}{3}} x_1^{i_1} \cdots x_n^{i_n} f_{i_1, \dots, i_n}(y, z) + \sum_{j_1 + \dots + j_n \leq \frac{2n}{3}} y_1^{j_1} \cdots y_n^{j_n} g_{j_1, \dots, j_n}(x, z) \\ &\quad + \sum_{k_1 + \dots + k_n \leq \frac{2n}{3}} z_1^{k_1} \cdots z_n^{k_n} h_{k_1, \dots, k_n}(x, y) \end{aligned}$$

其中

$$f_{i_1, \dots, i_n}(y, z) = \sum_{\substack{j_1, j_2, \dots, j_n \\ k_1, k_2, \dots, k_n}} c_{i_1, \dots, i_n, j_1, \dots, j_n, k_1, \dots, k_n} y_1^{j_1} \cdots y_n^{j_n} z_1^{k_1} \cdots z_n^{k_n}$$

$g_{j_1, \dots, j_n}(x, z)$  和  $h_{k_1, \dots, k_n}(x, y)$  是完全类似的.

因此, 每个阶数最多为  $2n/3$  的单项式对 slice-rank 有 3 次贡献, 并且此类单项式的数量最多为  $M$ . 因此 slice-rank 最多为  $3M$ .

现在我们来估计  $M$ . 将  $(1+x+x^2)^n$  展开我们得到

$$(1+x+x^2)^n = \sum_{\substack{a,b,c \geq 0 \\ a+b+c=n}} x^{b+2c} \frac{n!}{a!b!c!}$$

上述等式对任意  $x$  均成立. 令  $x$  的取值为  $0 \leq x \leq 1$ , 两边除以  $x^{2n/3}$ , 我们有

$$f(x) = (x^{-2/3} + x^{1/3} + x^{4/3})^n > \sum_{\substack{a,b,c \geq 0 \\ a+b+c=n \\ b+2c \leq 2n/3}} \frac{n!}{a!b!c!} x^{b+2c-\frac{2}{3}n} > \sum_{\substack{a,b,c \geq 0 \\ a+b+c=n \\ b+2c \leq 2n/3}} \frac{n!}{a!b!c!}$$

第一个不等号是因为  $x > 0$  且增加了约束条件  $b+2c \leq 2n/3$ ; 第二个不等号是因为  $0 < x < 1$ . 为了得到最优上界, 我们最小化  $f(x) = x^{-2/3} + x^{1/3} + x^{4/3}$ ,  $x \in (0, 1)$ . 求导得到  $f'(x) = (4x^2 + x - 2)/3x^{5/3}$ . 令  $f'(x) = 0$  我们得到  $4x^2 + x - 2 = 0$ , 即  $x = -1/8 \pm \sqrt{33}/8$ . 又因为  $0 < x < 1$ , 所以极值点为  $x = (\sqrt{33} - 1)/8$ , 极值为  $f((\sqrt{33} - 1)/8) \approx 2.755 < 2.76$ .

当这个证明出来时，人们震惊了；这基本上只有四页纸，但展示了代数方法的巨大力量。然而，与我们上次使用的傅立叶分析方法相比，这些方法似乎更“脆弱”。扩展此技术得到  $\mathbb{F}_3^n$  的 4-AP-free 子集大小的上界仍是一个悬而未决的问题（在上述参数中，我们可以用任何其他有限域替换  $\mathbb{F}_3$ ，所以域的选择并不重要）。我们也可以将多项式方法扩展到  $\mathbb{F}_2^n \times \mathbb{F}_2^n$  中的无角（corner-free）集。

## 6.4 Roth 定理与流行公差

多项式方法给出了  $\mathbb{F}_3^n$  上 Roth 定理更好的上界，现在我们将给出另一个不同的证明。该证明给出的上界稍差，但是方法有很强的启发性和影响力。这个证明涉及到“流行公差”（popular common difference）。

### 定理 6.6 (Green (2005))

对于任意  $\epsilon > 0$ ，存在  $n_0 = n_0(\epsilon)$  使得以下成立：对于  $n \geq n_0$  和任意满足  $|A| = \alpha 3^n$  的  $A \subseteq \mathbb{F}_3^n$ ，存在  $y \neq 0$  满足

$$|\{x : x, x+y, x+2y \in A\}| \geq (\alpha^3 - \epsilon) 3^n$$

这里的  $y$  是流行公差。该定理给出了在  $A$  中具有公差为  $y$  的 3-AP 的数量的下界。请注意，如果  $A$  是  $\mathbb{F}_3^n$  中大小为  $\alpha 3^n$  的随机子集，则公差为  $y$  的 3-AP 的期望数量大致是  $\alpha^3 3^n$ 。该定理表明我们可以找到一些  $y$ ，使得公差为  $y$  的 3-AP 的数量接近我们在随机集中的所期望的那样。

Green 证明了  $n_0 = \text{tow}((1/\epsilon)^{O(1)})$  这个定理是正确的。Fox-Pham 在 2019 年使用正则性方法将这个下界改进为  $n_0 = \text{tow}\left(O\left(\log \frac{1}{\epsilon}\right)\right)$ 。同时，他们证明了他们的下界是紧的。

### 引理 6.10 (有界增量)

令  $\alpha, \epsilon > 0$ 。如果  $\alpha_0, \alpha_1, \dots \in [0, 1]$  满足  $\alpha_0 \geq \alpha$ ，则存在  $k \leq \lceil \log_2 \frac{1}{\epsilon} \rceil$  使得  $2\alpha_k - \alpha_{k+1} \geq \alpha^3 - \epsilon$ 。

**证明** 反证法。假设不存在，则  $\alpha_1 \geq 2\alpha_0 - \alpha^3 + \epsilon \geq \alpha^3 + \epsilon$ 。同理有  $\alpha_2 \geq 2\alpha_1 - \alpha^3 + \epsilon \geq \alpha^3 + 2\epsilon$ 。继续这个过程，我们会发现对于所有  $1 \leq k \leq \lceil \log_2 \frac{1}{\epsilon} \rceil + 1$  有  $\alpha_k \geq \alpha^3 + 2^{k-1}\epsilon$ 。取  $k = \lceil \log_2 \frac{1}{\epsilon} \rceil + 1$  我们得到  $\alpha_k > 1$ ，矛盾。

令  $f : \mathbb{F}_3^n \rightarrow \mathbb{C}$ 。令  $U \leq \mathbb{F}_3^n$ ，这个符号的意思是  $U$  是  $\mathbb{F}_3^n$  的一个子空间。令  $f_U(x)$  是  $U$  的陪集上  $f(x)$  的平均值。

下面的引理类似正则性引理。

### 引理 6.11

对于任意  $\epsilon > 0$ ，存在  $m = \text{tow}\left(O\left(\log \frac{1}{\epsilon}\right)\right)$  使得对于所有  $f : \mathbb{F}_3^n \rightarrow [0, 1]$ ，存在子空间  $W \leq U \leq \mathbb{F}_3^n$ （并且满足  $\text{codim } W \leq m$ ）使得

$$\|\widehat{f} - \widehat{f_W}\|_\infty \leq \frac{\epsilon}{|U^\perp|}$$

和

$$2\|f_U\|_3^3 - \|f_W\|_3^3 \geq (\mathbb{E}f)^3 - \epsilon$$

同时成立。

**证明** 令  $\epsilon_0 := 1$ ， $\epsilon_{k+1} := \epsilon 3^{-1/\epsilon_k^2}$ ，整数  $k \geq 0$ 。我们发现递归表示  $\epsilon_{k+1}^{-2} = \epsilon^{-2} 3^{2/\epsilon_k^2}$ ，所以对于足够大的  $k$ ，我们有

$$\epsilon_{k+1}^{-2} \leq 2^{2^{\epsilon_k^{-2}}}$$

令

$$R_k := \{r \in \mathbb{F}_3^n : |\hat{f}(r)| \geq \epsilon_k\}$$

根据 Parseval 的恒等式， $\sum_r |\hat{f}(r)|^2 = \mathbb{E}[f^2] \leq 1$ ，所以  $|R_k| \leq \epsilon_k^{-2}$ 。我们定义  $U_k := R_k^\perp$  和  $\alpha_k := \|f_{U_k}\|_3^3$ 。根据凸

性, 容易验证  $\alpha_k \geq (\mathbb{E}f)^3$ 。根据前面引理, 存在  $k = O\left(\log \frac{1}{\epsilon}\right)$  使得  $2\alpha_k - \alpha_{k+1} \geq (\mathbb{E}f)^3 - \epsilon$ 。对于所选的  $k$ , 令  $m := \epsilon_{k+1}^{-2}$ 。整理后我们发现  $m = \text{tow}\left(O\left(\log \frac{1}{\epsilon}\right)\right)$ 。

我们直接给出下述结论 (容易验证)。

$$\widehat{f_W}(r) = \begin{cases} \widehat{f}(r) & \text{if } r \in W^\perp \\ 0 & \text{if } r \notin W^\perp \end{cases}$$

所以

$$\left\|f - \widehat{f_{U_{k+1}}}\right\|_\infty \leq \max_{r \notin R_{k+1}} |\widehat{f}(r)| \leq \epsilon_{k+1} \leq 3^{-|R_{k+1}|} \epsilon \leq \epsilon / |U_k^\perp|$$

因此, 如果我们取  $W = U_{k+1}$  和  $U = U_k$ ,  $\text{codim } U_{k+1} \leq 3^{|R_{k+1}|} \leq m$ , 证明完成。

这个正则性引理带来了一个计数引理, 证明留作练习。定义

$$\Lambda_3(f; U) = \mathbb{E}_{x \in \mathbb{F}_3^n, y \in U} f(x)f(x+y)f(x+2y)$$

#### 引理 6.12 (计数引理)

令  $f, g: \mathbb{F}_3^n \rightarrow [0, 1]$ ,  $U \leq \mathbb{F}_3^n$ 。则

$$|\Lambda_3(f; U) - \Lambda_3(g; U)| \leq 3|U^\perp| \cdot \|\widehat{f-g}\|_\infty$$

#### 引理 6.13

令  $f: \mathbb{F}_3^n \rightarrow [0, 1]$ , 子空间  $W \leq U \leq \mathbb{F}_3^n$ 。则

$$\Lambda_3(f_W; U) \geq 2\|f_U\|_3^3 - \|f_W\|_3^3$$

**证明** 回顾 Schur 不等式:

$$a^3 + b^3 + c^3 + 3abc \geq a^2(b+c) + b^2(a+c) + c^2(a+b)$$

其中  $a, b, c \geq 0$ 。我们发现

$$\begin{aligned} \Lambda(f_W; U) &= \mathbb{E}_{\substack{x, y, z \\ \text{form a 3-AP in} \\ \text{the same } U\text{-coset}}} f_W(x)f_W(y)f_W(z) \\ &\geq 2\mathbb{E}_{\substack{x, y \\ \text{in same } U\text{-coset}}} f_W(x)^2 f_W(y) - \mathbb{E} f_W^3 \\ &\geq 2\mathbb{E} f_W^2 f_U - \mathbb{E} f_W^3 \\ &\geq 2\mathbb{E} f_U^3 - \mathbb{E} f_W^3 \end{aligned}$$

其中第一个不等号来自 Schur 不等式, 最后一个不等号来自凸性。

#### 定理 6.7

对于任意  $\epsilon > 0$ , 存在  $m = \text{tow}\left(O\left(\log \frac{1}{\epsilon}\right)\right)$  满足: 如果  $f$  是从  $\mathbb{F}_3^n$  到  $[0, 1]$  的映射, 则存在维数至多为  $m$  的  $U \leq \mathbb{F}_3^n$  满足

$$\Lambda_3(f; U) \geq (\mathbb{E}f)^3 - \epsilon$$

**证明** 选择正则性引理中的  $U, W$ , 然后有

$$\Lambda_3(f; U) \geq \Lambda_3(f_W; U) - 3\epsilon \geq 2\|f_U\|_3^3 - \|f_W\|_3^3 - 3\epsilon \geq (\mathbb{E}f)^3 - 4\epsilon$$

流行公差在  $\mathbb{Z}$  中的类似概念在也成立。

#### 定理 6.8

对于任意的  $\epsilon > 0$ , 一定存在  $N_0 = N_0(\epsilon)$  满足: 如果  $N > N_0$  且  $A \subseteq [N]$  ( $|A| = \alpha N$ ), 则一定存在  $y > 0$  满足

$$|\{x: x, x+y, x+2y \in A\}| \geq (\alpha^3 - \epsilon)N$$




$\mathbb{Z}$  中相应的陈述对于 4-AP 也是成立的:

**定理 6.9**

对于任意的  $\epsilon > 0$ , 一定存在  $N_0 = N_0(\epsilon)$  满足: 如果  $N > N_0$  且  $A \subseteq [N]$  ( $|A| = \alpha N$ ), 则一定存在  $y > 0$  满足

$$|\{x : x, x+y, x+2y, x+3y \in A\}| \geq (\alpha^4 - \epsilon) N$$



 **笔记** 令人惊讶的是,  $\mathbb{Z}$  中关于 5-AP (或更大) 的相应的陈述是错的。

## 第 7 章 集合的加性结构

### 7.1 Small doubling set 结构

加性组合的一个主要任务可以粗略地描述为理解加法下集合的特征。为了更准确地讨论这一点，我们将从一些定义开始。

#### 定义 7.1

令  $A$  和  $B$  是阿贝尔群的有限子集。它们的加法集 (sumset) 定义为  $A + B = \{a + b \mid a \in A, b \in B\}$ 。我们可以进一步定义  $A - B = \{a - b \mid a \in A, b \in B\}$  和  $kA = \underbrace{A + A + \cdots + A}_{k \text{ times}}$ ，其中  $k$  是一个正整数。注意，这与将  $A$  中的每个元素乘以  $k$  不同，我们每个元素乘以  $k$  记作  $k \cdot A = \{kA \mid a \in A\}$ 。

给定一个有限的整数集  $A$ ，我们想了解在这些操作下它的大小会如何变化。自然的，我们有如下问题：

**问题 7.1** 对于大小  $|A|$  固定的  $A$ （其中  $A \subset \mathbb{Z}$ ）， $|A + A|$  可以有多大或多小？

事实上，这不是一个很难的问题。在  $\mathbb{Z}$  中，给定集合的大小，我们对加法集的大小有精确的界限。

#### 命题 7.1

如果  $A$  是  $\mathbb{Z}$  的有限子集，则

$$2|A| - 1 \leq |A + A| \leq \binom{|A| + 1}{2}$$

**证明** 右边的不等号成立是因为  $A$  中最多构成  $\binom{|A|+1}{2}$  个无序元素对。

如果  $A$  中的元素为  $a_1 < a_2 < \cdots < a_{|A|}$ ，那么

$$a_1 + a_1 < a_1 + a_2 < \cdots < a_1 + a_{|A|} < a_2 + a_{|A|} < \cdots < a_{|A|} + a_{|A|}$$

是一个项数为  $2|A| - 1$  的递增序列，且每一项都包含在集合  $A + A$  中，所以左边的不等号成立。

当  $A + A$  中没有非平凡的碰撞 (collision) 时，上界是紧的。这里的非平凡碰撞是说， $a_1 + a_2 = a'_1 + a'_2$ ， $a_1, a_2, a'_1, a'_2 \in A$  没有非平凡的解。

**例题 7.1** 如果  $A = \{1, a, a^2, \dots, a^{n-1}\} \subset \mathbb{Z}$ ，其中  $a > 1$ 。则我们有  $|A + A| = \binom{n+1}{2}$ 。

当  $A$  是等差数列时，下界很紧。当我们改为考虑任意阿贝尔群时，问题也同样简单。在一般阿贝尔群  $G$  中，我们只有不等式  $|A + A| \geq |A|$ 。如果  $A$  是某个  $G$  的有限子群的陪集，则等号成立。因为没有  $\mathbb{Z}$  的非平凡有限子群，所以在  $\mathbb{Z}$  中我们有更好的界。

我们可以问的一个更有趣的问题，对于大小  $|A + A|$  很小的集合，会发生什么？更确切地说：

#### 定义 7.2

我们定义阿贝尔群的有限子集  $A$  的倍增常数 (doubling constant) 为  $|A + A|/|A|$

**问题 7.2** 如果集合的倍增常数是有界的，那么该集合的结构是怎样的（例如  $|A + A| \leq 100|A|$ ）？

我们已经在  $\mathbb{Z}$  中看到了这样一个集合的例子，即算术级数（等差数列）。

**例题 7.2** 如果  $A \subset \mathbb{Z}$  是有限等差数列，则  $|A + A| = 2|A| - 1 \leq 2|A|$ ，所以它的倍增常数最多为 2。

此外，如果我们删除等差数列中的某些元素，集合的倍增常数应该仍比较小。事实上，如果我们删除等差数列的大部分元素，但保留常数比例的元素，集合的倍增常数仍比较小。

**例题 7.3** 如果  $B$  是有限算术级数且  $A \subseteq B$  满足  $|A| \geq C|B|$ ，则  $|A + A| \leq |B + B| \leq 2|B| \leq 2C^{-1}|A|$ ，所以  $A$  的倍增常数最大为  $2/C$ 。

一个更实质性的概括是  $d$  维算术级数。

**定义 7.3**

维度为  $d$  的广义算术级数 (generalized arithmetic progression, 下文简称 GAP) 是如下形式的集合

$$\{x_0 + \ell_1 x_1 + \cdots + \ell_d x_d \mid 0 \leq \ell_1 < L_1, \dots, 0 \leq \ell_d < L_d, \ell_1, \dots, \ell_d \in \mathbb{Z}\}$$

其中  $x_0, x_1, \dots, x_d \in \mathbb{Z}$  和  $L_1, \dots, L_d \in \mathbb{N}$ 。

GAP 的大小定义为  $L_1 L_2 \cdots L_d$ , 如果 GAP 的某些元素具有多种表示形式, 则集合的基数可能与大小不同。如果 GAP 的基数和大小相同, 则称为适当的。

不难看出, 维数为  $d$  的适当 GAP 倍增常数最大为  $2^d$  (这里用到了等差数列的倍增常数最大为 2)。此外, 删除常数部分的 GAP 元素后, 集合的倍增常数仍比较小。我们已经列举了几个倍增常数较小的集合的例子, 一个很自然的问题是, 我们是否可以对这些集合进行准确的分类? 关于问题 7.2 有一个“逆问题”, 是否所有倍增常数有界的集合都必须是一些示例之一?

这不是一个简单的问题。幸运的是, 加性组合的一个核心结论给出了这个问题的肯定回答。

**定理 7.1 (Freiman 定理 1973)**

如果  $A \subset \mathbb{Z}$  是一个有限集并且  $|A + A| \leq K|A|$ , 则  $A$  包含于维度最多为  $d(K)$  且大小最大为  $f(K)|A|$  的 GAP 中, 其中  $d(K)$  和  $f(K)$  是仅取决于  $K$  的常数。

定理的结论可以进一步加强, 我们可以保证 GAP 是适当的, 但代价是增大  $d(K)$  和  $f(K)$ , 加强版本的定理如下 (您可以在 Tao 和 Vu 06 年的著作中的定理 3.40 查阅该结论的证明)。

**定理 7.2**

如果  $P$  是维度为  $d$  的 GAP, 则  $P$  包含在维度至多为  $d$  且大小最大为  $d^{C_0 d^3} |P|$  的适当 GAP 中,  $C_0 > 0$  是某个正实数。

Freiman 定理让我们对小倍增集合 (倍增常数较小的集合, 后面我们都遵循这一简称) 结构有了一定的认识。我们将在本章的后面看到 Freiman 定理的证明。它的证明结合了傅立叶分析、几何数论和经典加性组合的思想。

Freiman 的原始证明很难读, 最初也没有得到应有的认可。后来 Ruzsa 找到了一个更简单的证明 (1994), 我们将主要按照他的思路介绍。因此, 该定理有时被称为 Freiman-Ruzsa 定理。Freiman 定理在 Gowers 对 Szemerédi 定理的新证明中起到了核心作用, 从而受到大家重视。

如果我们再次考虑示例 7.1, 我们有  $K = \frac{|A|+1}{2} = \Theta(|A|)$ , 并且, 我们没有好的办法将其嵌入到一个 GAP 中。我们记  $A$  中的元素为  $a_1 < a_2 < \cdots < a_{|A|}$ ; 对于  $1 \leq i \leq |A| - 1$ , 令  $x_0 = a_1, x_i = a_{i+1} - a_1, L_i = 2$ 。我们可以看到它包含在维度  $|A| - 1$  且大小  $2^{|A|-1}$  的 GAP 中。这表明我们可以期望的最好结果是  $d(K) = O(K)$  和  $f(K) = 2^{O(K)}$ , 该问题仍是开放的。

**问题 7.3** 对于  $d(K) = O(K)$  和  $f(K) = 2^{O(K)}$ , 定理 7.1 是否成立?

最著名的结果要归功于 Sanders。

**定理 7.3 (Sanders, 2012)**

在  $d(K) = K(\log K)^{O(1)}$ ,  $f(K) = e^{K(\log K)^{O(1)}}$  情况下, 定理 7.1 为真。

与之前讨论 Roth 定理的方式类似, 我们将从分析问题的有限域模型开始。在  $\mathbb{F}_2^n$ , 如果  $|A + A| \leq K|A|$ , 那么  $A$  会是什么样的? 如果  $A$  是一个子空间, 则它的倍增常数为 1。考虑其逆问题的一个自然的类比, 是否所有这样的  $A$  都包含在一个不比  $A$  大太多的子空间中?

**定理 7.4 ( $\mathbb{F}_2^n$ -analogue of Freiman)**

$A \subset \mathbb{F}_2^n$ , 如果  $|A + A| \leq K|A|$ , 则  $A$  包含在一个基数最大为  $f(K)|A|$  的子空间中, 其中  $f(K)$  是一个仅取决于  $K$  的常数。

如果我们令  $A$  是一个线性独立集（即一个基），那么  $K = \Theta(|A|)$ ，包含  $A$  的最小子空间的基数为  $2^{|A|}$ 。因此  $f(K)$  至少是  $K$  的指数。我们将在第三节中证明定理 7.4。

## 7.2 Plünnecke–Ruzsa 不等式

在我们证明 Freiman 定理（定理 7.1）或其有限域版本（定理 7.4）之前，我们需要一些工具。我们从以 Ruzsa 命名的众多结果之一开始。

### 定理 7.5 (Ruzsa 三角不等式)

如果  $A, B, C$  是一个阿贝尔群的有限子集，那么

$$|A||B - C| \leq |A - B||A - C|$$

**证明** 我们将构造一个单射

$$\phi : A \times (B - C) \hookrightarrow (A - B) \times (A - C)$$

对于每个  $d \in B - C$ ，我们可以选择  $b(d) \in B, c(d) \in C$  使得  $d = b(d) - c(d)$ 。定义  $\phi(a, d) = (a - b(d), a - c(d))$ ， $\phi$  是单射。因为如果  $\phi(a, d) = (x, y)$ ，那么我们可以用  $(x, y)$  通过  $d = y - x$  和  $a = x + b(y - x)$  来恢复  $(a, d)$ 。

**笔记** 通过将  $B$  替换为  $-B$  并将  $C$  替换为  $-C$ ，我们可以将不等式中的一些加号更改为减号。但不幸的是，这个技巧不能用来证明类似的不等式  $|A||B + C| \leq |A + B||A + C|$ 。尽管如此，我们很快就会看到该不等式仍然成立。

你可能会疑惑，三角形在哪里？如果我们定义  $\rho(A, B) = \log \frac{|AB|}{\sqrt{|A||B|}}$ ，那么定理 7.5 表明  $\rho(B, C) \leq \rho(A, B) + \rho(A, C)$ 。这看起来像三角不等式，但不幸的是  $\rho$  并不是一个度量，因为通常情况下  $\rho(A, A) \neq 0$ 。但如果限制在子群上， $\rho$  是一个真正的度量。

我们使用定理 7.5 的方式是控制小倍增集合的进一步倍增。下面的例子展示了它的用途。

**例题 7.4** 假设  $A$  是满足  $|2A - 2A| \leq K|A|$  的阿贝尔群的有限子集，在定理 7.5 中令  $B = C = 2A - A$ ，那么我们得到

$$|3A - 3A| \leq \frac{|2A - 2A|^2}{|A|} \leq K^2|A|$$

令  $B = C = 3A - 2A$  我们得到

$$|5A - 5A| \leq \frac{|3A - 3A|^2}{|A|} \leq K^4|A|$$

依此类推，所以对于所有  $m$ ，我们发现， $|mA - mA|$  被  $|A|$  的常数倍控制。

条件  $|2A - 2A| \leq K|A|$  强于条件  $|A + A| \leq K|A|$ 。如果我们想在给定条件  $|A + A| \leq K|A|$  的情况下实现上面的常数倍控制，我们有以下定理。

### 定理 7.6 (Plünnecke–Ruzsa 不等式)

如果  $A$  是一个阿贝尔群的有限子集并且  $|A + A| \leq K|A|$ ，则

$$|mA - nA| \leq K^{m+n}|A|$$

Plünnecke (1970) 最初的定理证明没有受到太多关注。Ruzsa (1989) 后来给出了 Plünnecke 定理更简单的证明。他的证明涉及到对一个被称作可交换分层图的对象的研究，并涉及到 Menger 定理和张量积的技巧。最近，Petridis (2012) 给出了一个非常简单的证明，我们将在下面展示。

在证明这个定理时，我们将原定理推广到以下定理。

### 定理 7.7

如果  $A$  和  $B$  是阿贝尔群的有限子集并且  $|A + B| \leq K|A|$ ，则

$$|mB - nB| \leq K^{m+n}|A|$$

令  $B = A$  我们得到原不等式。

Petridis 的证明依赖于以下关键引理。

### 引理 7.1

假设  $A$  和  $B$  是阿贝尔群的有限子集。如果  $X \subseteq A$  是将  $\frac{|X+B|}{|X|}$  最小化的非空子集，并且  $K' = \frac{|X+B|}{|X|}$ ，则对于任意有限集  $C$ ， $|X+B+C| \leq K'|X+C|$ 。



我们可以借助二分图来考虑这个引理。考虑顶点集  $G_1 \sqcup G_2$  上的二分图，其中  $G_1, G_2$  是环绕的阿贝尔群  $G$  的拷贝，对于所有的  $g \in G_1, g+b \in G_2, b \in B$ ，有从  $g$  到  $g+b$  的边。用集合  $N(S)$  表示顶点  $S$  的邻域，扩展率  $\frac{|N(A)|}{|A|} = \frac{|A+B|}{|A|}$ 。引理指出，如果  $X$  是一个集合，并且其扩展率  $K'$  小于等于它的任何子集的扩展率，则对于任何集合  $C$ ， $X+C$  也最多有  $K'$  的扩展率。

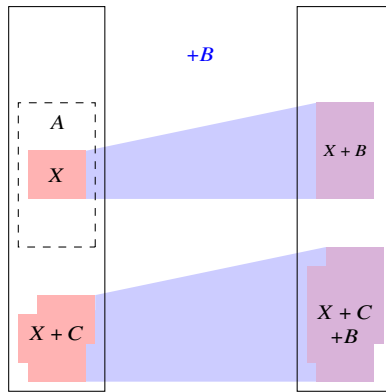


图 7.1: 引理7.1示意图

**证明** [定理 7.7] 我们假设上述引理成立，我们证明定理7.7。

令  $X$  是  $A$  的非空子集，并且  $X$  最小化  $\frac{|X+B|}{|X|}$ 。令  $K' = \frac{|X+B|}{|X|}$ 。注意到  $K' \leq K$ ，应用引理7.1，令  $C = rB$ ，其中  $r \geq 1$ ，我们有  $|X + (r+1)B| \leq K'|X+rB| \leq K|X+rB|$ 。迭代该过程我们得到，对于  $r \geq 0$ ， $|X+rB| \leq K^r|X|$ 。然后应用定理 7.5，我们有  $|mB - nB| \leq \frac{|X+mB||X+nB|}{|X|} \leq K^{m+n}|X| \leq K^{m+n}|A|$ 。

**证明** [引理 7.1]

我们归纳于  $|C|$ 。当  $|C| = 1$  时命题显然成立，因为对于任意有限集  $S$ ， $S+C$  相当于对  $S$  进行平移，所以  $|S+C| = |S|$ ，因此  $|X+B+C| = |X+B| = K'|X| = K'|X+C|$ 。

现在假设  $|C| > 1$ ，令  $\gamma \in C$ ，令  $C' = C \setminus \{\gamma\}$ 。然后有

$$X+B+C = (X+B+C') \cup ((X+B+\gamma) \setminus (Z+B+\gamma))$$

其中，

$$Z = \{x \in X \mid x+B+\gamma \subseteq X+B+C'\}$$

$Z \subseteq X$ ，回顾最小化的条件我们发现  $|Z+B| \geq K'|Z|$ 。所以

$$\begin{aligned} |X+B+C| &\leq |X+B+C'| + |(X+B+\gamma) \setminus (Z+B+\gamma)| \\ &= |X+B+C'| + |X+B| - |Z+B| \\ &\leq K'|X+C'| + K'|X| - K'|Z| \\ &= K'(|X+C'| + |X| - |Z|) \end{aligned}$$

现在我们来关注引理中不等式的右边  $X+C$ 。注意到

$$X+C = (X+C') \sqcup ((X+\gamma) \setminus (W+\gamma))$$

其中

$$W = \{x \in X \mid x+\gamma \in X+C'\}$$

注意到这里的并不相交的，所以

$$|X + C| = |X + C'| + |X| - |W|$$

因为  $x + \gamma \in X + C'$ ，所以  $W \subseteq Z$ ，所以有  $x + B + \gamma \subseteq X + B + C'$ 。因此  $|W| \leq |Z|$ ，所以

$$|X + C| \geq |X + C'| + |X| - |Z|$$

结合上一不等式我们便能完成归纳。

引理7.1还允许我们将定理 7.5 中的所有减号替换为加号。

#### 推论 7.1

如果  $A, B, C$  是阿贝尔群的有限子集，则  $|A||B + C| \leq |A + B||A + C|$

**证明** 令  $X \subseteq A$  是非空的，并且最小化  $\frac{|X+B|}{|X|}$ 。令  $K = \frac{|A+B|}{|A|}, K' = \frac{|X+B|}{|X|} \leq K$ 。则有

$$\begin{aligned} |B + C| &\leq |X + B + C| \\ &\leq K'|X + C| \\ &\leq K'|A + C| \\ &\leq K|A + C| \\ &= \frac{|A + B||A + C|}{|A|} \end{aligned}$$

其中，第二个不等号是由引理7.1得到的。

## 7.3 有限域上的 Freiman 定理

在我们可以证明 Freiman 定理的有限域版本（定理7.4）之前，我们介绍最后一个引理。

#### 定理 7.8 (Ruzsa 覆盖引理, 1999)

令  $X$  和  $B$  是一个阿贝尔群的子集。如果  $|X + B| \leq K|B|$ ，则存在一个子集  $T \subset X$  且  $|T| \leq K$ ，满足  $X \subset T + B - B$ 。

覆盖的类比为我们的证明提供了灵感。我们将覆盖集视为度量空间中的球，如果我们有一个半尺寸球（半径为 0.5 的球）的最大堆积，将每个球扩展成一个单位球应该会产生该区域的覆盖。这里的最大意味着不能放置更多的球，同时要保证圆心在区域内。下面我们将其形式化从而证明 Ruzsa 覆盖引理。

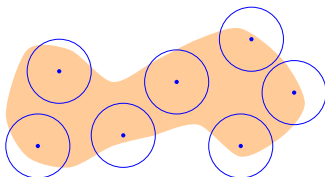


图 7.2: 半尺寸球的最大堆积

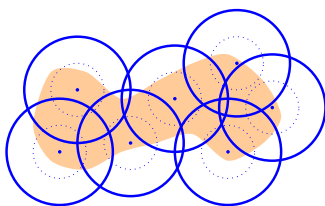


图 7.3: 将半尺寸球扩展为单位球，构成一个覆盖



**证明** 令  $T \subset X$  是一个满足如下条件的最大子集：对于任意的  $t \in T$ ,  $t+B$  都是不相交的。因此,  $|T||B| = |T+B| \leq |X+B| \leq K|B|$ 。所以,  $|T| \leq K$ 。

由于  $T$  是最大子集, 对于任意的  $x \in X$ , 存在  $t \in T$  使得  $(t+B) \cap (x+B) \neq \emptyset$ 。换句话说, 存在  $b, b' \in B$  使得  $t+b = x+b'$ 。因此, 对于某一  $t \in T$ ,  $x \in t+B-B$ 。由于这适用于所有  $x \in X$ , 我们有  $X \subset T+B-B$ 。

Ruzsa 覆盖引理是在有限域上证明 Freiman 定理 (定理 7.4) 所需的最后一个工具。有限域模型比处理  $\mathbb{Z}$  更简单, 因此与原始 Freiman 定理 (定理 7.1) 相比, 它可以使用更少的工具来完成。

现在, 我们将在有限指数群中证明 Freiman 定理。这个限制比有限域稍大些。

#### 定义 7.4

阿贝尔群的指数  $r$  是满足如下条件的最小正整数 (如果存在的话): 对于该群的所有元素  $x$ ,  $rx = 0$ 。

我们使用  $\langle A \rangle$  来指代由  $G$  的某个子集  $A$  生成的群  $G$  的子群。借助这种表示法, 群  $G$  的指数是  $\max_{x \in G} |\langle x \rangle|$ 。下面我们在有限指数阿贝尔群上证明 Ruzsa 对于 Freiman 定理的类比。

#### 定理 7.9 (Ruzsa 1999)

令  $A$  为指数  $r < \infty$  的阿贝尔群中的有限集。如果  $|A+A| \leq K|A|$ , 则

$$|\langle A \rangle| \leq K^2 r^{K^4} |A|$$

**证明** 根据 Plünnecke-Ruzsa 不等式 (定理 7.6), 我们有

$$|A + (2A - A)| = |3A - A| \leq K^4 |A|$$

根据 Ruzsa 覆盖引理 (令  $X = 2A - A, B = A$ ), 存在  $T \subset 2A - A$  且  $|T| \leq K^4$  满足

$$2A - A \subset T + A - A$$

两边同时加上  $A$ , 我们得到

$$3A - A \subset T + 2A - A \subset 2T + A - A$$

重复上一操作, 对任意正整数  $n$ , 我们有

$$(n+1)A - A \subset nT + A - A \subset \langle T \rangle + A - A$$

对于足够大的  $n$ , 我们有  $nA = \langle A \rangle$ 。因此,

$$\langle A \rangle \subset \langle T \rangle + A - A$$

由于指数是有限的,

$$|\langle T \rangle| \leq r^{|T|} \leq r^{K^4}$$

根据 Plünnecke-Ruzsa 不等式 (定理 7.6),

$$|A - A| \leq K^2 |A|$$

因此

$$|\langle A \rangle| \leq |\langle T \rangle| |A - A| \leq r^{K^4} K^2 |A|$$

**例题 7.5** 在  $\mathbb{F}_2^n$  中, 如果  $A$  是一个独立集 (例如,  $A$  是某个子群的基), 则  $A$  具有倍增常数  $K \approx |A|/2$  且  $|\langle A \rangle| = 2^{|A|} \approx 2^{2K} |A|$ 。因此,  $|\langle A \rangle|$  的上界至少是  $K$  的指数。

最近, 我们已经非常精确地确定了  $|\langle A \rangle|/|A|$  的最大可能值。对任意  $A \subset \mathbb{F}_2^\infty$  和  $|A+A|/|A| \leq K$ , 答案是  $\Theta(2^{2K}/K)$  (Even-Zohar, 2012)。对于一般的  $r$ , 我们猜测会有类似的现象。Ruzsa 推测  $|\langle A \rangle| \leq r^{CK} |A|$  (1999)。对于部分  $r$ , 比如素数, 这一猜测得到了验证 (Even-Zohar 和 Lovett, 2014)。

我们对有限指数阿贝尔群的 Freiman 定理 (定理 7.9) 的证明没有推广到整数。

## 7.4 Freiman 同态

了解任何对象，要去了解它们之间的映射以及这些映射保留的性质，这是数学的基本原理之一。例如，在研究群时，我们关心的不是元素本身是什么，而是它们之间根据群操作的关系。对于流形，我们不关注空间中的嵌入，而是关注保留各种基本属性的映射（例如微分同胚）。在加性组合中，我们的研究对象是集合的加法。因此，我们必须了解集合之间保留或者至少部分保留加性结构的映射。这样的映射称为 **Freiman 同态**。

### 定义 7.5

$A, B$  是阿贝尔群中的子集。我们称  $\phi: A \rightarrow B$  是一个 **Freiman  $s$ -同态**（或  $s$  阶的 **Freiman 同态**），如果

$$\phi(a_1) + \cdots + \phi(a_s) = \phi(a'_1) + \cdots + \phi(a'_s)$$

其中  $a_1, \dots, a_s, a'_1, \dots, a'_s \in A$  满足

$$a_1 + \cdots + a_s = a'_1 + \cdots + a'_s$$

### 定义 7.6

如果  $\phi: A \rightarrow B$  是双射，并且  $\phi$  和  $\phi^{-1}$  都是 **Freiman  $s$ -同态**，则称  $\phi$  是 **Freiman  $s$ -同构**。

下面我们看一些例子。

**例题 7.6** 每个群同态都是任意阶的 **Freiman 同态**。

**例题 7.7** 如果  $\phi_1$  和  $\phi_2$  都是 **Freiman  $s$ -同态**，那么它们的组合  $\phi_1 \circ \phi_2$  也是 **Freiman  $s$ -同态**。如果  $\phi_1$  和  $\phi_2$  都是 **Freiman  $s$ -同构**，那么它们的组合  $\phi_1 \circ \phi_2$  是 **Freiman  $s$ -同构**。

**例题 7.8** 假设  $S$  没有加性结构（例如  $\{1, 10, 10^2, 10^3\}$ ）。那么任意映射  $\phi: S \rightarrow \mathbb{Z}$  是一个 **Freiman 2-同态**。

请注意，**Freiman 同构**和**群同态**有细微的差别！

**例题 7.9** 自然嵌入  $\phi: \{0, 1\}^n \rightarrow (\mathbb{Z}/2\mathbb{Z})^n$  是群同态，所以是任意阶的 **Freiman 同态**。它也是一个双射。但是它的逆映射没有保留加性关系，因此它不是 **Freiman 2-同构**！

一般来说， $\text{mod } N$  映射  $\mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$  是群同态，而不是 **Freiman 同态**。即使我们将映射限制在  $[N]$ ，这仍然成立。但是，我们可以通过限制在直径小的子集来找到 **Freiman 同构**。

### 命题 7.2

$A \subset \mathbb{Z}$  的直径小于  $N/s$ ，则  $\text{mod } N$  是 **Freiman  $s$ -同构**。

**证明** 如果  $a_1, \dots, a_s, a'_1, \dots, a'_s \in A$  满足

$$\sum_{i=1}^s a_i - \sum_{i=1}^s a'_i \equiv 0 \pmod{N}$$

则左侧可以被视为一个整数，其绝对值小于  $N$ （因为对任意  $i$ ， $|a_i - a'_i| < N/s$ ）。因此左边必须为 0。所以  $\text{mod } N$  映射的逆是  $A$  上的 **Freiman  $s$ -同态**，因此  $\text{mod } N$  是 **Freiman  $s$ -同构**。

## 7.5 建模引理

当我们试图在整数上证明 **Freiman 定理**时，主要困难是倍增常数较小的子集  $A$  可能分散在  $\mathbb{Z}$  上。我们可以使用 **Freiman 同构**在更小的空间内对  $A$  进行建模，同时保留相应的加性结构。在这个更小的空间里，我们有更好的工具，例如傅立叶分析。为了建立这个模型，我们首先证明一个建模引理。

### 定理 7.10 (有限域上的建模引理)

令  $A \subset \mathbb{F}_2^n$  且对于某个正整数  $m$ ，有  $2^m \geq |sA - sA|$ 。则存在从  $A$  到  $\mathbb{F}_2^m$  某子集的 **Freiman  $s$ -同构**。

如果  $|A + A| \leq K|A|$ , 由 Plünnecke-Ruzsa 不等式 (定理 7.6) 我们有  $|sA - sA| \leq K^{2s}|A|$ , 因此存在  $m = O(s \log K + \log |A|)$  满足该定理。

**证明** 对于线性映射  $\phi: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ , 以下是等价的:

1.  $\phi$  限制在  $A$  上时,  $\phi$  是 Freiman  $s$ -同构的。
2.  $\phi$  在  $sA$  上是单射的。
3. 对于所有非零的  $x \in sA - sA$ ,  $\phi(x) \neq 0$ 。

令  $\phi: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$  为均匀随机线性映射。每个  $x \in sA - sA$  违反 (3) 的概率为  $2^{-m}$ 。因此如果  $2^m \geq |sA - sA|$ , 则满足 (3) 的概率是非零的。这意味着存在 Freiman  $s$ -同构。

这个证明不能直接在  $\mathbb{Z}$  中工作。事实上,  $\mathbb{Z}$  上的建模引理表明, 如果  $A \subset \mathbb{Z}$  有小的倍增常数, 则很大一部分  $A$  可以在一个小的循环群上建模, 该循环群的大小与  $|A|$  相当。所以我们可以对  $A$  的一个大的子集进行建模, 之后我们再使用 Ruzsa 覆盖引理来恢复整个集合  $A$  的结构。

#### 定理 7.11 (Ruzsa 建模引理 1992)

令  $A \subset \mathbb{Z}$ ,  $s \geq 2$ ,  $N$  为正整数, 满足  $N \geq |sA - sA|$ 。则存在  $A' \subset A$  并且  $|A'| \geq |A|/s$  使得  $A'$  是 Freiman  $s$ -同构于  $\mathbb{Z}/N\mathbb{Z}$  的子集。

**证明** 令  $q > \max(sA - sA)$  为素数。对于每一个  $\lambda \in [q-1]$ , 我们将  $\phi$  定义为如下函数的组合,

$$\phi: \mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z} \xrightarrow{\times \lambda} \mathbb{Z}/q\mathbb{Z} \rightarrow [q]$$

未指明的两个映射指的是自然嵌入。前两个映射是群同态, 因此它们也是 Freiman  $s$ -同态。最后一个映射不是整个域上的群同态, 而是在小区间上的。根据鸽巢原理, 对于所有的  $\lambda$ , 都存在一个长度小于  $q/s$  的区间  $I_\lambda \subset [q]$ , 使得  $A_\lambda = \{a \in A: \phi(a) \in I_\lambda\}$  有超过  $|A|/s$  个元素。因此, 当限制在  $A_\lambda$  上时,  $\phi$  是一个 Freiman  $s$ -同态。

我们定义

$$\psi: \mathbb{Z} \xrightarrow{\phi} [q] \rightarrow \mathbb{Z}/N\mathbb{Z}$$

#### 引理 7.2

如果  $\psi$  没有将  $A_\lambda$  Freiman  $s$ -同构映射到它的像, 那么存在非零  $d = d_\lambda \in sA - sA$  使得  $\phi(d) \equiv 0 \pmod{N}$ 。

**证明** 假设  $\psi$  没有将  $A_\lambda$  Freiman 同构映射到它的像。则存在  $a_1, \dots, a_s, a'_1, \dots, a'_s \in A_\lambda$  使得

$$a_1 + \dots + a_s \neq a'_1 + \dots + a'_s$$

但

$$\phi(a_1) + \dots + \phi(a_s) \equiv \phi(a'_1) + \dots + \phi(a'_s) \pmod{N}$$

由于  $\phi(A_\lambda) \subset I_\lambda$ , 这是一个长度小于  $q/s$  的区间, 我们有

$$|\phi(a_1) + \dots + \phi(a_s) - \phi(a'_1) - \dots - \phi(a'_s)| \in (-q, q)$$

我们假设上式左边是非负的, 即位于区间  $[0, q)$ 。否则我们可以交换  $(a_1, \dots, a_s)$  与  $(a'_1, \dots, a'_s)$ 。

设  $d = a_1 + \dots + a_s - a'_1 - \dots - a'_s$ 。因此  $d \in (sA - sA) \setminus \{0\}$ 。由于构成  $\phi$  的所有函数都是群同态  $(\text{mod } q)$ , 所以有

$$\phi(d) \equiv \phi(a_1) + \dots + \phi(a_s) - \phi(a'_1) - \dots - \phi(a'_s) \pmod{q}$$

根据  $\phi$  的定义,  $\phi(d)$  位于  $[0, q)$ 。因此  $\phi(a_1) + \dots + \phi(a_s) = \phi(a'_1) + \dots + \phi(a'_s)$ 。因此,

$$\phi(d) \equiv 0 \pmod{N}$$

现在我们回到原来的证明路线上, 对于每个  $d \in (sA - sA) \setminus \{0\}$ , 满足  $\phi(d) \equiv 0 \pmod{N}$  的  $\lambda$  数量等于  $[q-1]$  中可被  $N$  整除的数量。这个数字最多为  $(q-1)/N$ 。

因此, 满足如下条件的  $\lambda$  的总数最多为  $(|sA - sA| - 1)(q-1)/N < q-1$ : 存在  $d \in (sA - sA) \setminus \{0\}$  且

$\phi(d) \equiv 0 \pmod{N}$ 。所以存在  $\lambda$  使得映射  $\psi$ ，从  $A_\lambda$  Freiman  $s$ -同构映射到它的像上。取  $A' = A_\lambda$ ，我们的证明就完成了。

通过总结到目前为止我们所知道的一切，我们建立了一个有助于我们证明 Freiman 定理的结果。

### 推论 7.2

$A \subset \mathbb{Z}$  且  $|A + A| \leq K|A|$ ，则存在素数  $N \leq 2K^{16}|A|$  和  $A' \subset A$ ， $|A'| \geq |A|/8$ ，使得  $A'$  是 Freiman 8-同构于  $\mathbb{Z}/N\mathbb{Z}$  的子集。



**证明** 根据 Plünnecke-Ruzsa 不等式 (定理 7.6)， $|8A - 8A| \leq K^{16}|A|$ 。我们根据 Bertrand 假设<sup>1</sup>，可以选到素数  $K^{16} \leq N < 2K^{16}$ 。然后我们应用建模引理，取  $s = 8$  和  $N \geq |8A - 8A|$ 。建模引理告诉我们，存在一个子集  $A' \subset A$  同时  $|A'| \geq |A|/8$ ，并且  $A'$  是 Freiman 8-同构于  $\mathbb{Z}/N\mathbb{Z}$  的子集。

## 7.6 Bogolyubov 引理

在 Ruzsa 建模引理 (定理 7.11) 中，我们证明了对于任何小倍增集合  $A$ ， $A$  的大部分元素构成的子集 Freiman 同构于  $\mathbb{Z}/N\mathbb{Z}$ ，且  $N$  的大小不会比  $A$  大太多。为了证明 Freiman 定理，我们需要证明我们可以用 GAP 覆盖  $A$ 。这就引出了一个自然的问题，如何用 GAP 覆盖  $\mathbb{Z}/N\mathbb{Z}$  的大子集？在本节中，我们首先展示如何在  $\mathbb{Z}/N\mathbb{Z}$  的子集中找到加性结构。稍后，我们将展示如何使用这种加性结构来得到覆盖。首先考虑有限域  $\mathbb{F}_2^n$  中的类似问题会更容易些。要说明的是，大小为  $\alpha 2^n$  的  $\mathbb{F}_2^n$  的子集不一定包含任何例如子空间的大型结构。本节的关键想法如下：给定一个集合  $A$ ，加法集  $A + A$  使  $A$  的结构变得平滑。这种想法与卷积平滑函数类似，见图 7.4。借助这种想法，我们得出以下自然问题：

**问题 7.4** 假设  $A \subset \mathbb{F}_2^n$  且  $|A| = \alpha 2^n$ ，其中  $\alpha$  是一个独立于  $n$  的常数。 $A + A$  是否一定包含一个余维数<sup>2</sup>为  $O_\alpha(1)$  的子空间？

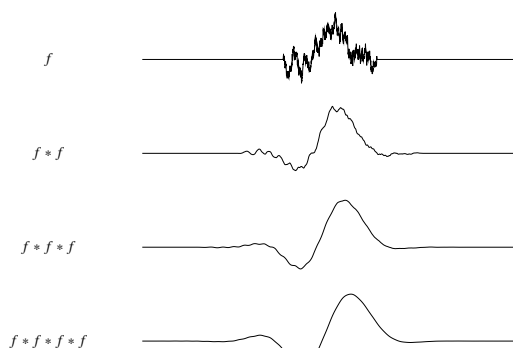


图 7.4: 卷积使函数平滑

问题 7.4 的答案是否定的，如下例所示。

**例 7.10** 令  $A_n$  为  $\mathbb{F}_2^n$  中所有点的集合，汉明权重<sup>3</sup>至多  $(n - c\sqrt{n})/2$ 。根据中心极限定理

$$|A_n| \sim k 2^n$$

其中  $k > 0$  是一个仅取决于  $c$  的常数。然而， $A_n + A_n$  由布尔立方体中的点组成，其汉明权重最多为  $n - c\sqrt{n}$ ，因此不包含任何维度  $> n - c\sqrt{n}$  的子空间。证明留给读者。

回到加集  $A + A$  平滑  $A$  的结构这一思路上来，我们很自然地想到，更多  $A$  副本的和能否有更好的效果。事实上，如果我们在问题 7.4 中将  $A + A$  替换为  $2A - 2A$ ，那么问题答案是肯定的。

<sup>1</sup>贝特朗假设是关于素数分布的一个著名结论，对任一实数  $x \geq 1$ ，在  $x$  及  $2x$  之间必有一素数

<sup>2</sup>若  $W$  是一向量空间  $V$  的一个线性子空间，则  $W$  在  $V$  的余维数是商空间  $V/W$  的维数。若  $V$  是有限维的，则  $\text{codim}(W) = \dim(V) - \dim(W)$

<sup>3</sup>汉明重量是一串符号中非零符号的个数。

**定理 7.12 (Bogolyubov 引理, 1939)**

如果  $A \subset \mathbb{F}_2^n$  且  $|A| = \alpha 2^n$ , 其中  $\alpha$  是一个独立于  $n$  的常数, 则  $2A - 2A$  包含一个余维数至多为  $1/\alpha^2$  的子空间。

**证明** 令  $f = 1_A * 1_A * 1_{-A} * 1_{-A}$ ,  $2A - 2A$  是  $f$  的支撑集。根据卷积性质,

$$\widehat{f} = \widehat{1}_A^2 \widehat{1}_{-A}^2 = |\widehat{1}_A|^4$$

根据傅里叶反演, 我们有

$$f(x) = \sum_{r \in \mathbb{F}_2^n} \widehat{f}(r) (-1)^{r \cdot x} = \sum_{r \in \mathbb{F}_2^n} |\widehat{1}_A(r)|^4 (-1)^{r \cdot x}$$

因为  $f(x) > 0$  将意味着  $x \in 2A - 2A$ , 所以我们只需找到  $f$  为正的子空间即可。我们将通过查看傅立叶系数的大小来选择这个子空间。令

$$R = \{r \in \mathbb{F}_2^n \setminus \{0\} : |\widehat{1}_A(r)| > \alpha^{3/2}\}$$

根据 Parseval 恒等式,  $|R| < 1/\alpha^2$ 。注意到

$$\sum_{r \notin R \cup \{0\}} |\widehat{1}_A(r)|^4 \leq \alpha^3 \sum_{r \notin R \cup \{0\}} |\widehat{1}_A(r)|^2 < \alpha^4$$

如果  $x$  在  $R^\perp$  中, 那么

$$\begin{aligned} f(x) &= \sum_{r \in \mathbb{F}_2^n} |\widehat{1}_A(r)|^4 (-1)^{r \cdot x} \\ &\geq |\widehat{1}_A(0)|^4 + \sum_{r \in R} |\widehat{1}_A(r)|^4 (-1)^{r \cdot x} - \sum_{r \notin R \cup \{0\}} |\widehat{1}_A(r)|^4 \\ &> \alpha^4 + \sum_{r \in R} |\widehat{1}_A(r)|^4 - \alpha^4 \\ &\geq 0 \end{aligned}$$

因此  $R^\perp \subset \text{supp}(f) = 2A - 2A$ , 并且由于  $|R| < 1/\alpha^2$ , 我们找到了一个余维数最多为  $1/\alpha^2$  的  $2A - 2A$  的子空间。

我们现在的目标是在循环群  $\mathbb{Z}/N\mathbb{Z}$  上给出一个类似的结果。第一步是给循环群  $\mathbb{Z}/N\mathbb{Z}$  找一个类似子空间的东西。请注意, 我们在将 Roth 定理的证明从有限域转移到整数时遇到了类似的问题。正确的类比是由 Bohr 集给出的。回想一下 Bohr 集的定义:

**定义 7.7**

假设  $R \subset \mathbb{Z}/N\mathbb{Z}$ , 定义

$$\text{Bohr}(R, \epsilon) = \left\{x \in \mathbb{Z}/N\mathbb{Z} : \left\| \frac{rx}{N} \right\| \leq \epsilon, \text{ for all } r \in R \right\}$$

其中  $\|\cdot\|$  表示到最近整数的距离。我们称  $|R|$  为 Bohr 集的维数,  $\epsilon$  为宽度。

事实证明, 用适当维数的 Bohr 集替换子空间后, Bogolyubov 引理在  $\mathbb{Z}/N\mathbb{Z}$  上成立。 $\mathbb{Z}/N\mathbb{Z}$  的 Bohr 集的维数对应于  $\mathbb{F}_2^n$  的子空间的余维数。

**定理 7.13 ( $\mathbb{Z}/N\mathbb{Z}$  上的 Bogolyubov 引理, 1939)**

如果  $A \subset \mathbb{Z}/N\mathbb{Z}$  且  $|A| = \alpha N$ , 则  $2A - 2A$  包含玻尔集  $\text{Bohr}(R, 1/4)$ , 其中  $|R| < 1/\alpha^2$ 。

回想一下  $\mathbb{Z}/N\mathbb{Z}$  上的傅里叶变换的定义。

**定义 7.8**

$f: \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$  的傅里叶变换是函数  $\widehat{f}: \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$ ,

$$\widehat{f}(r) = \mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f(x) \omega^{-rx}$$

其中  $\omega = e^{(2\pi i)/N}$



我们将其作为练习留给读者验证傅立叶反演公式、Parseval 恒等式、Plancherel 恒等式和傅里叶变换的其他基本性质。现在我们来证明定理 7.13。除了一些小细节外，它与定理 7.12 的证明思路相同。

**证明** [定理 7.13] 令  $f = 1_A * 1_A * 1_{-A} * 1_{-A}$ ,  $\text{supp}(f) = 2A - 2A$ 。根据卷积性质，

$$\widehat{f} = \widehat{1}_A^2 \widehat{1}_{-A}^2 = |\widehat{1}_A|^4$$

根据傅立叶反演，

$$f(x) = \sum_{r \in \mathbb{Z}/N\mathbb{Z}} \widehat{f}(r) \omega^{rx} = \sum_{r \in \mathbb{Z}/N\mathbb{Z}} |\widehat{1}_A(r)|^4 \cos\left(\frac{2\pi rx}{N}\right)$$

因为  $f(x) > 0$  将意味着  $x \in 2A - 2A$ ，所以我们只需找到  $f$  为正的子空间即可。令

$$R = \left\{ r \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\} : |\widehat{1}_A(r)| > \alpha^{3/2} \right\}$$

根据 Parseval 恒等式， $|R| < 1/\alpha^2$ 。注意到

$$\sum_{r \notin R \cup \{0\}} |\widehat{1}_A(r)|^4 \leq \alpha^3 \sum_{r \notin R \cup \{0\}} |\widehat{1}_A(r)|^2 < \alpha^4$$

因为条件  $x \in \text{Bohr}(R, 1/4)$  正好等价于

$$\cos\left(\frac{2\pi rx}{N}\right) > 0 \text{ for all } r \in R$$

对于任意  $x \in \text{Bohr}(R, 1/4)$ ，我们有

$$\begin{aligned} f(x) &= \sum_{r \in \mathbb{Z}/N\mathbb{Z}} |\widehat{1}_A(r)|^4 \cos\left(\frac{2\pi rx}{N}\right) \\ &\geq |\widehat{1}_A(0)|^4 + \sum_{r \notin R \cup \{0\}} |\widehat{1}_A(r)|^4 \cos\left(\frac{2\pi rx}{N}\right) \\ &> 0 \end{aligned}$$

因此  $\text{Bohr}(R, 1/4) \subset \text{supp}(f) = 2A - 2A$  且满足  $|R| < 1/\alpha^2$ 。

我们现在已经证明，对于包含大部分  $\mathbb{Z}/N\mathbb{Z}$  的集合  $A$ ，集合  $2A - 2A$  必须包含一个维数小于  $1/\alpha^2$  的 Bohr 集。在下一节中，我们将分析 Bohr 集中的加性结构。特别是我们将证明低维的 Bohr 集包含大的 GAP。

## 7.7 几何数论

在我们证明本节的主要结果之前，我们首先介绍一些几何数论的内容。几何数论涉及格子 (lattice) 和凸体的研究，在数论中有重要的应用。

**定义 7.9**

集合  $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_d$  被称作  $\mathbb{R}^d$  上的格子 (lattice)，其中  $v_1, \dots, v_d \in \mathbb{R}^d$  是线性无关向量。





**定义 7.10**

格子  $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_d$  的行列式  $\det(\Lambda)$  是  $v_1, \dots, v_d$  作为列的矩阵行列式的绝对值。

$$\det \Lambda := \left| \det \begin{pmatrix} | & \cdots & | \\ v_1 & \cdots & v_d \\ | & \cdots & | \end{pmatrix} \right|$$



**例题 7.11**  $\omega = e^{(2\pi i)/3}$ , 则  $\mathbb{Z} + \mathbb{Z}\omega$  是一个格子, 它的行列式是  $\sqrt{3}/2$ 。

**例题 7.12**  $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subset \mathbb{R}$  不是格子, 因为 1 和  $\sqrt{2}$  不是线性无关的。

我们现在介绍凸体  $K$  的连续最小值这一重要概念。

**定义 7.11**

给定一个中心对称凸体  $K \subset \mathbb{R}^d$  (中心对称意味着  $x \in K$  当且仅当  $-x \in K$ ), 定义第  $i$  个  $K$  关于  $\Lambda$  的连续最小值为

$$\lambda_i = \inf\{\lambda \geq 0 : \dim(\text{span}(\lambda K \cap \Lambda)) \geq i\}$$

$1 \leq i \leq d$ 。等价地,  $\lambda_i$  是使得  $\lambda K$  包含来自  $\Lambda$  的  $i$  个线性无关格向量的最小  $\lambda$ 。



定义  $K$  相对于  $\Lambda$  方向基为  $\mathbf{b}_1, \dots, \mathbf{b}_d \in \mathbb{R}^d$ , 满足对每个  $i = 1, \dots, d$  都有  $\mathbf{b}_i \in \lambda_i K$ 。方向基可能有多个。

**例题 7.13** 令  $e_1, \dots, e_8$  为  $\mathbb{R}^8$  中的标准基向量。令  $v = (e_1 + \cdots + e_8)/2$ 。考虑格子

$$\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_7 \oplus \mathbb{Z}v$$

令  $K$  为  $\mathbb{R}^8$  中的单位球。注意到  $K$  相对于  $\Lambda$  的方向基是  $e_1, \dots, e_8$ 。这说明凸体  $K$  的方向基不一定是  $\Lambda$  的  $\mathbb{Z}$ -基。

如下图所示, 想象这样一个过程, 我们在时间  $\lambda$  时看到凸体  $\lambda K$ 。这个不断增长的凸体最初只是原点, 在某个时间点上它包含了第一个非零晶格点  $\mathbf{b}_1$ 。凸体随着时间变大, 在某个时刻, 它包含了一个新维度中的第一个晶格点  $\mathbf{b}_2$ 。凸体继续扩大下去, 直到包含所有的方向基  $\mathbf{b}_1, \dots, \mathbf{b}_d$ 。

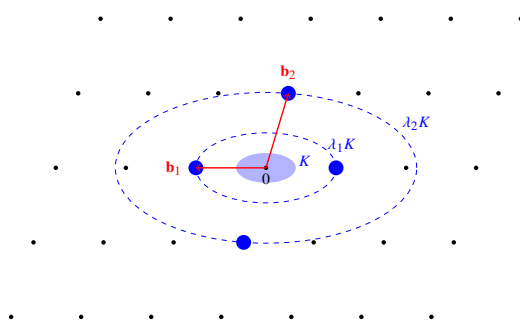


图 7.5: 连续最小值示意图

下面我们介绍 Minkowski 第二定理, 该定理可以用来控制连续最小值的乘积。

**定理 7.14 (Minkowski 第二定理, 1896)**

令  $\Lambda \in \mathbb{R}^d$  为格子,  $K$  为中心对称体。令  $\lambda_1 \leq \cdots \leq \lambda_d$  是  $K$  关于  $\Lambda$  的连续最小值。有

$$\lambda_1 \cdots \lambda_d \text{vol}(K) \leq 2^d \det(\Lambda)$$



**例题 7.14** 值得一提的是, Minkowski 的第二定理是紧的

$$K = \left[-\frac{1}{\lambda_1}, \frac{1}{\lambda_1}\right] \times \cdots \times \left[-\frac{1}{\lambda_d}, \frac{1}{\lambda_d}\right]$$

$\Lambda$  是格子  $\mathbb{Z}^d$ 。

我们省略 Minkowski 第二定理的证明。我们现在用 Minkowski 第二定理来证明: 一个低维的 Bohr 集包含一个大的 GAP。

**定理 7.15**

设  $N$  为素数。 $\mathbb{Z}/N\mathbb{Z}$  中每个维度为  $d$  且宽度  $\epsilon \in (0, 1)$  的 Bohr 集包含一个适当 GAP, 其维度最多为  $d$ , 大小至少为  $(\epsilon/d)^d N$ 。

**证明** 令  $R = \{r_1, \dots, r_d\}$ , 令

$$v = \left(\frac{r_1}{N}, \dots, \frac{r_d}{N}\right)$$

令  $\Lambda \subset \mathbb{R}^d$  是由  $\mathbb{R}^d$  中所有满足下面条件的点组成的格子: 这些点  $\bmod 1$  等于  $v$  的整数倍。我们有  $\det(\Lambda) = 1/N$ 。令凸体  $K = [-\epsilon, \epsilon]^d$ 。令  $\lambda_1, \dots, \lambda_d$  是  $K$  相对于  $\Lambda$  的连续最小值。设  $\mathbf{b}_1, \dots, \mathbf{b}_d$  为方向基。我们知道

$$\|\mathbf{b}_j\|_\infty \leq \lambda_j \epsilon \text{ for all } j$$

对于每个  $1 \leq j \leq d$ , 令  $L_j = \lceil 1/(\lambda_j d) \rceil$ 。如果  $0 \leq l_j < L_j$ , 有

$$\|l_j \mathbf{b}_j\|_\infty < \frac{\epsilon}{d}$$

对于任意  $i$ , 如果有整数  $l_1, \dots, l_d$  且  $0 \leq l_i < L_i$ , 那么

$$\|l_1 \mathbf{b}_1 + \dots + l_d \mathbf{b}_d\|_\infty \leq \epsilon \quad (7.1)$$

每个  $\mathbf{b}_j$  等于  $x_j v$  加上一个具有整数坐标的向量,  $0 \leq x_j < N$ 。(7.1) 中  $i^{\text{th}}$  坐标的上界意味着

$$\left\| \frac{(l_1 x_1 + \dots + l_d x_d) r_i}{N} \right\|_{\mathbb{R} \setminus \mathbb{Z}} \leq \epsilon \text{ for all } i$$

因此, GAP

$$\{l_1 x_1 + \dots + l_d x_d : 0 \leq l_i < L_i \text{ for all } i\}$$

包含在  $\text{Bohr}(R, \epsilon)$  中。我们要证明这个 GAP 很大并且它是适当的。首先我们证明它很大。使用 Minkowski 第二定理, 它的大小

$$\begin{aligned} L_1 \cdots L_d &\geq \frac{1}{\lambda_1 \cdots \lambda_d \cdot d^d} \\ &\geq \frac{\text{vol}(K)}{2^d \det(\Lambda) d^d} \\ &= \frac{(2\epsilon)^d}{2^d \frac{1}{N} d^d} \\ &= \left(\frac{\epsilon}{d}\right)^d N \end{aligned}$$

现在我们检查 GAP 是否适当。我们只需证明

$$l_1 x_1 + \dots + l_d x_d \equiv l'_1 x_1 + \dots + l'_d x_d \pmod{N}$$

所以对于任意的  $i$ , 我们必须有  $l_i = l'_i$ 。令

$$\mathbf{b} = (l_1 - l'_1) \mathbf{b}_1 + \dots + (l_d - l'_d) \mathbf{b}_d$$

我们知道  $\mathbf{b} \in \mathbb{Z}^d$ 。此外

$$\|\mathbf{b}\|_\infty \leq \sum_{i=1}^d \frac{1}{\lambda_i d} \|\mathbf{b}_i\|_\infty \leq \epsilon < 1$$

所以  $\mathbf{b}$  必须是 0。因为  $\mathbf{b}_1, \dots, \mathbf{b}_d$  是一组基, 所以对于所有  $i$  有  $l_i = l'_i$ 。

## 7.8 Freiman 定理的证明

到目前为止, 在本章中, 我们已经在加性组合中展示了许多用来证明 Freiman 定理 (定理 7.1) 的方法和定理。现在, 我们把这些工具放在一起, 形成一个完整的证明。

证明方法如下。从小倍增集合  $A$  开始, 我们首先使用 Ruzsa 建模引理 (定理 7.11)。然后, 我们使用 Bogolyubov

的引理 (定理 7.12) 和几何数论的结论, 在  $2B - 2B$  内找到一个大 GAP。这给了我们一个  $2A - 2A$  中的大 GAP。最后, 我们应用 Ruzsa 覆盖引理 (定理 7.8), 从包含在  $2A - 2A$  中的这个 GAP 上创建一个包含  $A$  的 GAP。回忆 Freiman 定理 (定理 7.1) 的陈述:

如果  $A \subset \mathbb{Z}$  是有限集并且  $|A + A| \leq K|A|$ , 则  $A$  包含在维数最多为  $d(K)$  且大小最多为  $f(K)|A|$  的 GAP 中。

**证明** 因为  $|A + A| \leq K|A|$ , 由 Ruzsa 建模引理的推论 (推论 7.2), 存在一个素数  $N \leq 2K^{16}|A|$  和  $A' \subset A$  且  $|A'| \geq |A|/8$ , 使得  $A'$  是 Freiman 8-同构于  $\mathbb{Z}/N\mathbb{Z}$  的子集  $B$ 。在  $B$  上应用 Bogolyubov 引理 (定理 7.12)

$$\alpha = \frac{|B|}{N} = \frac{|A'|}{N} \geq \frac{|A|}{8N} \geq \frac{1}{16K^{16}}$$

所以  $2B - 2B$  包含玻尔集  $\text{Bohr}(R, 1/4)$ , 其中  $|R| < 256K^{32}$ 。因此, 根据定理 7.15,  $2B - 2B$  包含一个适当 GAP, 其维数  $d < 256K^{32}$ , 大小至少为  $(4d)^{-d}N$ 。

由于  $B$  是到  $A'$  的 Freiman 8-同构, 所以  $2B - 2B$  是到  $2A' - 2A'$  的 Freiman 2-同构。这是从 Freiman  $s$ -同构的定义得到的。注意到  $2B - 2B$  中的每个元素都是  $B$  中四个元素的和和差 ( $2A' - 2A'$  也是如此)。因为  $2B - 2B$  中的任何两个元素之间的差被保留, 所以算术级数被 Freiman 2-同构保留。因此,  $2B - 2B$  中的适当 GAP 被映射到具有相同维度和大小的  $2A' - 2A'$  中的适当 GAP  $Q$ 。

接下来我们将使用 Ruzsa 覆盖引理来覆盖整个集合  $A$  并将其转换为  $Q$ 。因为  $Q \subset 2A - 2A$ , 我们有  $Q + A \subset 3A - 2A$ 。根据 Plünnecke-Ruzsa 不等式 (定理 7.6), 我们有

$$|Q + A| \leq |3A - 2A| \leq K^5|A|$$

因为  $A' \subset \mathbb{Z}/N\mathbb{Z}$ , 我们有  $N \geq |A'| \geq |A|/8$ 。因为  $|Q| \geq (4d)^{-d}N$ , 所以我们有  $K^5|A| \leq K'|Q|$ , 其中  $K' = 8(4d)^d K^5 = e^{K^{O(1)}}$ 。所以上述不等式变为  $|Q + A| \leq K'|Q|$ 。因此, 根据 Ruzsa 覆盖引理 (定理 7.11), 存在  $A$  的子集  $X$  与  $|X| \leq K'$  满足  $A \subset X + Q - Q$ 。

剩下的事情就是证明  $X + Q - Q$  包含在具有所需的 GAP 中。注意,  $X$  包含在维度为  $|X|$  的 GAP 中, 并且  $Q - Q$  的维数是  $d$ 。所以  $X + Q - Q$  包含在具有如下维度的 GAP  $P$  中

$$\dim(P) \leq |X| + d \leq K' + d = 8(4d)^d K^5 + d = e^{K^{O(1)}}$$

因为  $Q$  是维度  $d$  的适当 GAP 并且等差数列的倍增常数是 2, 所以  $Q - Q$  的大小至多为  $2^d|Q|$ 。包含  $X$  的 GAP 大小为  $2^{|X|}$ 。因此, 应用 Plünnecke-Ruzsa 不等式,  $P$  的大小

$$\text{size}(P) \leq 2^{|X|} 2^d |Q| \leq 2^{K'+d} |2A - 2A| \leq 2^{K'+d} K^4 |A| = e^{K^{O(1)}} |A|$$

取  $d(K) = e^{K^{O(1)}}$ ,  $f(K) = e^{K^{O(1)}}$ , 我们完成了 Freiman 定理的证明。

考虑  $A = \{1, 10, 10^2, 10^3, \dots, 10^{|A|-1}\}$  我们看到 Freiman 定理对于  $d(K) < \Theta(K)$ ,  $f(K) < 2^{\Theta(K)}$  是错误的。我们还可以推测 Freiman 的成立的条件为  $d(K) = \Theta(K)$  和  $f(K) = 2^{\Theta(K)}$ 。

虽然上述 Freiman 定理证明中给出的上界与此相差甚远, 但 Chang 已经证明 Ruzsa 的方法可以给出多项式上界 ( $d(K) = K^{O(1)}$  和  $f(K) = \exp(K^{O(1)})$ , 2002)。当我们应用 Ruzsa 的覆盖引理时是点浪费的。我们只对  $A$  使用了一次覆盖, 一个更好的方法是一点一点地覆盖  $A$ 。对其简单叙述如下:

从  $Q$  开始, 我们用  $Q - Q$  覆盖部分  $A$ 。然后重复下面操作: 对剩余的  $A$  找到较小维度的  $Q_1$ , 用  $Q_1 - Q_1$  覆盖  $A$  的其余部分。这种方法显著减少了我们在这一步中损失, 并给出了更好的多项式上界。

如前所述, 最知名的上界 (定理 7.3) 为  $d(K) = K(\log K)^{O(1)}$  和  $f(K) = e^{K(\log K)^{O(1)}}$ , 其证明涉及更多内容。

## 7.9 一般阿贝尔群的 Freiman 定理

我们已经证明了有限域和整数上的 Freiman 定理, 所以我们想知道 Freiman 定理是否适用于一般的阿贝尔群。事实上这也是成立的, 但首先我们必须了解这样的 Freiman 定理有什么含义。

对于固定素数  $p$  的  $\mathbb{F}_p^n$ , Freiman 定理告诉我们任何具有小倍增集合都存在于一个不太大的子群中, 而对于整数, Freiman 定理给出相同的结论, 但 GAP 不会太大。因为有限生成阿贝尔群总是可以表示为素数次幂的循环群和多个  $\mathbb{Z}$  的直和, 为了找到 GAP 和子群的推广, 我们可以尝试这两者的直和。

**定义 7.12**

定义陪集级数为直和  $P+H$ ，其中  $P$  是适当 GAP， $H$  是子群。陪集级数的维度定义为  $P$  的维度，陪集级数的大小定义为整个集合的基数。

**定理 7.16 (一般阿贝尔群的 Freiman 定理, Green Ruzsa 2007)**

如果  $A$  是任意阿贝尔群的子集且  $|A+A| \leq K|A|$ ，则  $A$  包含在维度至多  $d(K)$ 、大小至多  $f(K)|A|$  的陪集级数中，其中  $d(K)$  和  $f(K)$  是仅取决于  $K$  的常数。

该定理的证明遵与 Freiman 定理证明方法类似，但对 Ruzsa 建模引理进行了一些修改。Sanders 再次给出了著名的上界， $d(K) = K(\log K)^{O(1)}$  和  $f(K) = e^{K(\log K)^{O(1)}}$  (2013)。应该注意的是，这些函数仅依赖于  $K$ ，因此无论  $A$  是哪个阿贝尔群的子集，它们都保持不变。

## 7.10 非阿贝尔群中的 Freiman 问题

我们可以对非阿贝尔群提出类似的问题：倍增常数较小的非阿贝尔群的子集的结构是什么？就像阿贝尔群的情况下一样，其子群仍然有小的倍增常数。此外，我们可以采用任何一组交换元素构成的 GAP。然而，事实证明还有其他小倍增集的例子，它们不是直接从这些例子中的任何一个从阿贝尔群中推导出来的。

**例题 7.15** 离散海森堡 (Heisenberg) 群  $H_3(\mathbb{Z})$  是主对角线上为 1 的整数上三角矩阵的集合。该群的乘法定义如下：

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & c+z+ay \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{pmatrix}$$

令

$$S = \left\{ \begin{pmatrix} 1 & \pm 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \pm 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

考虑集合  $S^r$ ，根据乘法规则， $S^r$  的元素都形如

$$\begin{pmatrix} 1 & O(r) & O(r^2) \\ 0 & 1 & O(r) \\ 0 & 0 & 1 \end{pmatrix}$$

因此， $|S^r| \leq O(r^4)$ ，因为这样的矩阵最多有  $O(r^4)$  种。我们可以进一步证明  $|S^r| = \Omega(r^4)$ ，因此  $|S^r| = \Theta(r^4)$ 。所以  $S^r$  的倍增为  $|S^{2r}|/|S^r| \approx 16$ ， $S^r$  的倍增是有界的。

**定义 7.13**

如果存在中心列  $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$ ，则称之为幂零群。换句话说，对于有限次操作，

$$[\dots [[G, G], G] \dots, G] = \{e\}$$

其中， $[H, K]$  定义为  $\{hkh^{-1}k^{-1} : h \in H, k \in K\}$ 。

所有幂零群都具有类似于示例 7.15 的多项式倍增常数，一般定义如下。

**定义 7.14**

令  $G$  是由集合  $S$  生成的有限生成群。如果存在常数  $C, d > 0$ ，对于所有  $r$  都有  $|S^r| \leq Cr^d$ ，则称群  $G$  是多项式倍增的。

Gromov 定理是几何群论的一个深刻结果，它给出了多项式倍增群的完整表征。

**定理 7.17 (Gromov 定理, 1981)**

一个有限生成群具有多项式倍增当且仅当它是几乎幂零的。其中，几乎幂零 (virtually nilpotent) 的意思是其有一个有限指数的幂零子群。

Gromov 使用的技术与希尔伯特的第五个问题有关，该问题涉及李群表示论。后来，Kleiner 在 2010 给出了 Gromov 定理的更简单的证明。

现在，我们在任意的几乎幂零群  $G$  中构造了一个小倍增集合：“幂零球” $S^r$ ，其中  $S$  生成  $G$ 。我们很自然地提出以下问题。

**问题 7.5** 所有小倍增集合（称为近似群的集合）一定表现得像子群和幂零球的某种组合吗？

在这个问题上已经做了很多工作。2012 年，Hrushovski 使用模理论技术展示了非阿贝尔群的 Freiman 定理的弱版本。后来，Breuillard、Green 和 Tao 在 Hrushovski 的方法的基础上，证明了近似群的结构定理，将 Freiman 的定理推广到了非阿贝尔群。然而，由于使用了超滤子，这些方法没有提供明确的界限。

## 7.11 多项式 Freiman-Ruzsa 猜想

在  $\mathbb{F}_2^n$  中，如果  $A$  是一个大小为  $n$  的独立集，它的倍增常数为  $K = |A + A|/|A| \approx n/2$ ，并且任何包含  $A$  的子群的大小必须至少为  $2^{\Theta(K)}|A|$ 。

扩展上一个例子，令  $A$  是  $\mathbb{F}_2^{m+n}$  的子集， $A = \mathbb{F}_2^m \times \{e_1, \dots, e_n\}$ （其中  $\{e_1, \dots, e_n\}$  是  $\mathbb{F}_2^n$  的坐标基）。此结构与前一个结构具有相同的倍增常数，但  $|A|$  可以任意大。这表明 Freiman 定理的阿贝尔群版本中的上界不能比指数更好。

注意，在此示例中， $A$  必须包含非常大的（仿射）子空间  $\mathbb{F}_2^m \times \{e_1\}$ ，其大小与  $A$  相当。因此我们可能会问，如果我们只需要覆盖  $A$  的一个大子集，我们是否可以在 Freiman 定理中获得更好的界？这就引出如下猜想：

**命题 7.3 ( $\mathbb{F}_2^n$  上的多项式 Freiman-Ruzsa 猜想, Green, 2004)**

如果  $A \subset \mathbb{F}_2^n$ ，并且  $|A + A| \leq K|A|$ ，则存在一个仿射子空间  $V \subseteq \mathbb{F}_2^n$  且  $|V| \leq |A|$ ，满足  $|V \cap A| \geq K^{-O(1)}|A|$ 。

这个猜想有几种等价形式。例如，以下三个猜想等价于猜想 7.3：

**命题 7.4**

如果  $A \subset \mathbb{F}_2^n$ ，并且  $|A + A| \leq K|A|$ ，则存在一个子空间  $V \subseteq \mathbb{F}_2^n$  且  $|V| \leq |A|$ ，使得  $A$  可以被  $V$  的  $K^{O(1)}$  陪集所覆盖。

**证明** [等价性证明] 显然猜想 7.4 可以推导出猜想 7.3。

现在假设猜想 7.3 为真，并且假设  $A \subset \mathbb{F}_2^n$  满足  $|A + A| \leq K|A|$ 。那么通过猜想 7.3，存在一个最大为  $|A|$  的仿射子空间  $V$ ，使得  $|V \cap A| \geq K^{-O(1)}|A|$ 。应用 Ruzsa 覆盖引理（定理 7.8）， $X = A, B = V \cap A$ ，我们得到大小为  $K^{O(1)}$  的集合  $X$ ，满足  $A \subseteq V - V + X$ 。对  $X$  的每个元素，我们平移向量空间  $V - V$  得到陪集，所以猜想 7.4 为真。

**命题 7.5**

如果  $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  满足

$$|\{f(x, y) - f(x) - f(y) : x, y \in \mathbb{F}_2^n\}| \leq K$$

那么存在一个线性函数  $g: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  使得

$$|\{f(x) - g(x) : x \in \mathbb{F}_2^n\}| \leq K^{O(1)}$$

**命题 7.6**

如果  $f: \mathbb{F}_2^n \rightarrow \mathbb{C}$  且  $\|f\|_\infty \leq 1$ ,  $\|f\|_{U_3} \geq \delta$  (其中  $\|f\|_{U_3}$  是 Gowers  $U_3$  范数, 与 4-AP 计数有关), 则存在  $\mathbb{F}_2$  上的二次多项式  $q(x_1, \dots, x_n)$  满足

$$\left| \mathbb{E}_{x \in \mathbb{F}_2^n} [f(x)(-1)^{q(x)}] \right| \geq \delta^{O(1)}$$

事实证明, 这些版本都是等价的 (各个  $O(1)$  项之间是线性关系)。迄今为止最好的界限归功于 Sanders, 他实现了  $e^{(\log K)^{O(1)}}$  的拟多项式界限 (2012)。多项式 Freiman-Ruzsa 猜想将通过下面的加强 Bogolyubov 猜想得到:

**命题 7.7 (多项式 Bogolyubov-Ruzsa 猜想, Sanders, 2012)**

如果  $A \subset \mathbb{F}_2^n$  且  $|A| = \alpha 2^n$ , 则  $2A - 2A$  包含一个余维数为  $O(\log(1/\alpha))$  的子空间。

Bogolyubov 引理的标准形式 (定理 7.12) 显示了  $O(\alpha^{-2})$  的界限。这个猜想的最佳结果也归功于 Sanders, 他获得了  $(\log(1/\alpha))^{O(1)}$  的拟多项式界限。

类似地, 可以用  $\mathbb{Z}$  代替  $\mathbb{F}_2^n$  来制作多项式版本的 Freiman-Ruzsa 猜想。首先, 我们必须定义一个类似于子空间的居中凸级数 (centered convex progression, 下面我们简称为 CCP)。

**定义 7.15**

CCP 是如下形式的集合

$$P = \{x_0 + \ell_1 x_1 + \dots + \ell_d x_d : (\ell_1, \dots, \ell_d) \in \mathbb{Z}^d \cap B\}$$

其中  $B$  是  $\mathbb{R}^d$  中的某个凸中心对称体。CCP 的维度是  $d$ , 大小是  $|\mathbb{Z}^d \cap B|$ 。

$\mathbb{Z}$  上的多项式 Freiman-Ruzsa 猜想陈述如下。

**命题 7.8 ( $\mathbb{Z}$  的多项式 Freiman-Ruzsa 猜想)**

如果  $A \subset \mathbb{Z}$  且  $|A + A| \leq K|A|$ , 则存在维度为  $O(\log K)$  且大小最多为  $|A|$  的 CCP, 其与  $A$  的交集大小至少为  $K^{-O(1)}|A|$ 。

更一般地, 阿贝尔群中的多项式 Freiman-Ruzsa 猜想使用 CCCP (centered convex coset progressions), 其定义为直和  $P + H$ , 其中  $P$  是  $\mathbb{Z}^d \cap B$  到群的同态下的像,  $H$  是子群的某个陪集。

这个猜想的最佳界限 (在  $\mathbb{Z}$  和阿贝尔群的情况下) 还是由 Sanders 提出来的。他根据多项式 Bogolyubov-Ruzsa 猜想的拟多项式界限推导得出:

**命题 7.9 ( $\mathbb{Z}$  的多项式 Bogolyubov-Ruzsa 猜想, Sanders, 2012)**

$A \subset \mathbb{Z}/N\mathbb{Z}$  且  $N$  是素数, 则  $2A - 2A$  包含维度为  $O(\log(1/\alpha))$  且大小至少为  $\alpha^{O(1)}N$  的 CCCP。

同样的, 我们可以通过使用 CCCP 来得到一般阿贝尔群的版本。

## 7.12 加性能量和 Balog-Szemerédi-Gowers 定理

到目前为止, 我们已经使用倍增常数测量了对集合添加加性结构后的数量。这里, 我们介绍了加性能量, 这是一种对集合中加性结构的新测量方式。

**定义 7.16**

令  $A$  和  $B$  是一个阿贝尔群的有限子集。它们的加性能量定义为

$$E(A, B) = |\{(a_1, a_2, b_1, b_2) \in A \times A \times B \times B : a_1 + a_2 = b_1 + b_2\}|$$



单个子集  $A$  的加性能量为  $E(A) := E(A, A)$

我们可以将加性能量视为在适当的凯莱图中计算长度为 4 的圈。下面我们将看到加性能量是加性组合学的起到重要的作用。

### 定义 7.17

对于阿贝尔群的两个有限子集  $A$  和  $B$ ，定义

$$r_{A,B}(x) := |\{(a, b) \in A \times B : x = a + b\}|$$

$x$  可以表示为  $A + B$  总和形式的数量即为  $r_{A,B}(x)$ 。

我们可以计算加性能量

$$E(A, B) = \sum_x r_{A,B}(x)^2$$

对于加性能量，我们有命题 7.1 的类似命题如下。

### 命题 7.10

如果  $A$  是  $\mathbb{Z}$  的有限子集，则  $|A|^2 \leq E(A) \leq |A|^3$ 。

**证明** 回顾  $E(A)$  定义我们可以直接得到下界。上界是因为对于任何三元组  $(a_1, a_2, a_3) \in A^3$ ，第四个坐标是固定的，为  $a_1 + a_2 - a_3$ 。

**笔记** 命题 7.10 是紧的。当  $A$  没有加性结构时，下界成立，而当  $A = [n]$  时，上界渐近成立。

到目前为止，我们已经比较了小倍增集合和大加性能量集合。事实上，前者蕴含了后者。

### 命题 7.11

如果  $|A + A| \leq K|A|$ ，则  $E(A) \geq |A|^3/K$ 。

**证明** 根据 Cauchy-Schwarz 不等式我们有

$$\begin{aligned} E(A) &= \sum_{x \in A+A} r_{A,A}(x)^2 \geq \frac{1}{|A+A|} \left( \sum_{x \in A+A} r_{A,A}(x) \right)^2 \\ &= \frac{|A|^4}{|A+A|} \geq \frac{|A|^3}{|K|} \end{aligned}$$

很自然地，我们想要知道命题 7.11 的逆命题是否成立。事实上，具有大加性能量的集合也可能有大倍增，如下面的示例所述。

**例题 7.16** 考虑集合  $A = [N/2] \cup \{-2, -4, -8, \dots, -2^{N/2}\}$ 。注意  $A$  是一小倍增集和一没有加性结构的集合的并集。第一个分量导致了大加性能量  $E(A) = \Theta(N^3)$ ，而第二个分量导致了大倍增  $|A + A| = \Theta(N^2)$

然而，Balog 和 Szemerédi 表明，每个具有大加性能量的集合都必须有一个高度结构化的小倍增子集，即使该集合总体上具有相对较少的加性结构（1994）。他们的证明后来被 Gowers 改进，Gowers 给出了常数的多项式界限（1998），这就是我们将在这里展示的版本。

### 定理 7.18 (Balog-Szemerédi-Gowers 定理)

令  $A$  是一个阿贝尔群的有限子集。如果  $E(A) \geq |A|^3/K$ ，则存在子集  $A' \subset A$ ，并且  $|A'| \geq K^{-O(1)}|A|$ ， $|A' + A'| \leq K^{O(1)}|A'|$

我们提出了一个定理的更强大版本，它考虑了两个不同集合之间的加法结构。

**定理 7.19**

令  $A$  和  $B$  是同一个阿贝尔群的有限子集。如果  $|A|, |B| \leq n$  且  $E(A, B) \geq n^3/K$ ，则存在子集  $A' \subset A$  和  $B' \subset B$ ，并且  $|A'|, |B'| \geq K^{-O(1)}n$ ， $|A' + B'| \leq K^{O(1)}n$

**证明** [证明定理 7.19 蕴含定理 7.18] 假设  $E(A) \geq |A|^3/K$ ，应用定理 7.19，取  $B = A$  得到  $A', B' \subset A$ ，并且  $|A'|, |B'| \geq K^{-O(1)}n$ ， $|A' + B'| \leq K^{O(1)}n$ 。然后根据推论 7.1，我们有

$$|A' + A'| \leq \frac{|A' + B'|^2}{|B'|} \leq K^{O(1)}n$$

为了证明定理 7.19，我们再次考虑从加法组合到图论的转换。定理 7.19 的证明依赖下面的图论中结构。

**定义 7.18**

令  $A$  和  $B$  是一个阿贝尔群的子集，令  $G$  是一个顶点二分图  $A \cup B$ 。定义限制加法集 (restricted sumset)  $A +_G B$  为  $G$  中边的加法集

$$A +_G B := \{a + b : (a, b) \text{ an edge in } G\}$$

**定理 7.20**

令  $A$  和  $B$  是阿贝尔群的有限子集，令  $G$  是顶点二分图  $A \cup B$ 。如果： $|A|, |B| \leq n$ ， $G$  中至少有  $n^2/K$  边，且  $|A +_G B| \leq Kn$ ；则存在子集  $A' \subset A$  和  $B' \subset B$ ，满足  $|A'|, |B'| \geq K^{-O(1)}n$ ， $|A' + B'| \leq K^{O(1)}n$ 。

**证明** [证明定理 7.20 蕴含定理 7.19]

令  $S = \{x \in A + B : r_{A,B}(x) \geq n/2K\}$  为“流行和”的集合。建立顶点集为  $A \cup B$  的二分图  $G$ ， $(a, b) \in A \times B$  是一条边当且仅当  $a + b \in S$ 。

我们声称  $G$  有很多边，下面我们通过证明“非流行和”最多占  $E(A, B)$  的一半来说明这一点。注意到

$$\frac{n^3}{K} \leq E(A, B) = \sum_{x \in S} r_{A,B}(x)^2 + \sum_{x \notin S} r_{A,B}(x)^2$$

因为  $r_{A,B}(x) < n/2K$ ，当  $x \notin S$  时，我们可以将第二项约束为

$$\sum_{x \notin S} r_{A,B}(x)^2 \leq \frac{n}{2K} \sum_{x \notin S} r_{A,B}(x) \leq \frac{n}{2K} |A||B| \leq \frac{n^3}{2K}$$

带回上一不等式得到

$$\sum_{x \in S} r_{A,B}(x)^2 \geq \frac{n^3}{2K}$$

此外，因为对于所有  $x$  满足  $r_{A,B}(x) \leq |A| \leq n$ ，因此

$$e(G) = \sum_{x \in S} r_{A,B}(x) \geq \sum_{x \in S} \frac{r_{A,B}(x)^2}{n} \geq \frac{n^2}{2K}$$

因此，我们可以应用定理 7.20 来找到具有所需性质的集合  $A' \subset A$  和  $B' \subset B$ 。

本节的其余部分将重点证明定理 7.20，我们从几个引理开始。

**引理 7.3 (路径长为 2)**

固定  $\delta, \epsilon > 0$ 。令  $G$  是一个二分图，顶点集为  $A \cup B$ ，至少  $\delta|A||B|$  边。则存在  $U \subset A$  且  $|U| \geq \delta|A|/2$ ，使得至少  $(1 - \epsilon)$  占比的点对  $(x, y) \in U^2$ ，该点对至少有  $\epsilon\delta^2|B|/2$  个共同邻点。

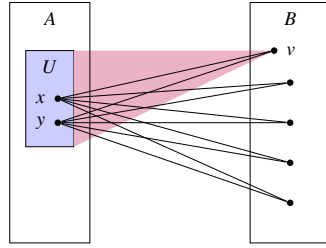


图 7.6: 路径长度为 2 引理示意图

**证明** 我们随机均匀地选择  $v \in B$ , 令  $U = N(v) \cap A$ , 我们有  $\mathbb{E}[|U|] \geq \delta|A|$ 。注意到, 有较少共同邻点的点对不太可能包含在  $U$  中。确实如此, 如果  $x, y \in A$  的公共邻点小于  $\epsilon\delta^2|B|/2$ , 则  $\Pr[\{x, y\} \subset U] < \epsilon\delta^2/2$ 。

如果两点的共同邻点数至少为  $\epsilon\delta^2|B|/2$ , 我们称两点是友好的。令  $X$  为非友好点对  $(x, y) \in U^2$  的数量, 那么

$$\mathbb{E}[X] = \sum_{\substack{(x,y) \in A^2 \\ \text{unfriendly}}} \Pr[\{x, y\} \subset U] < \frac{\epsilon\delta^2}{2}|A|^2$$

因此, 我们有

$$\mathbb{E}\left[|U|^2 - \frac{X}{\epsilon}\right] \geq (\mathbb{E}[|U|])^2 - \frac{\mathbb{E}[X]}{\epsilon} > \frac{\delta^2}{2}|A|^2$$

所以存在  $U$  满足  $|U|^2 - X/\epsilon \geq \delta^2|A|^2/2$ 。对于这个  $U$ , 我们有  $|U|^2 \geq \delta^2|A|^2/2$ , 即  $|U| \geq \delta|A|/2$ 。此外, 我们有  $X \leq \epsilon|U|^2$ , 所以最多有  $\epsilon$  占比的点对  $(x, y) \in U^2$ , 该点对的共同邻点数少于  $\epsilon\delta^2|B|/2$ 。

#### 引理 7.4 (路径长为 3)

存在  $c, C > 0$  使以下结论成立。固定任意取值的  $\epsilon, \delta > 0$ , 令  $G$  是任意顶点集为  $A \cup B$  且至少有  $\delta|A||B|$  条边的二分图。则存在子集  $A' \subset A$  和  $B' \subset B$ , 使得任何  $(a, b) \in A' \times B'$  的两点之间至少有  $\eta|A||B|$  条长度为 3 的路径, 其中  $\eta = c\delta^C$ 。

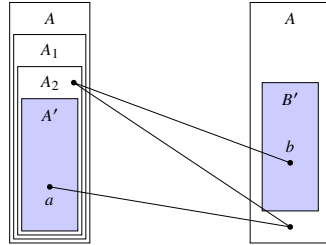


图 7.7: 路径长度为 3 引理示意图

**证明** 如果  $A$  中的点对具有至少  $\frac{\delta^3|B|}{20}$  个共同邻点, 则将它们称为友好点对。定义

$$A_1 := \left\{a \in A : \deg a \geq \frac{\delta}{2}|B|\right\}$$

将  $A$  限制为  $A_1$  使其可以在  $A_1$  和  $B$  之间保证至少  $\delta$  的边密度,  $G$  中删除的边少于  $\delta|A||B|/2$  条。因为我们至少剩下  $\delta|A||B|/2$  条边,  $a \in A_1$  的最大度数是  $|B|$ , 我们有  $|A_1| \geq \delta|A|/2$ 。

通过  $(A_1, B)$  上的路径为 2 引理 (引理 7.3), 构造  $A_2 \subset A_1$ , 其中  $\epsilon = \delta/10$ 。然后,  $|A_2| \geq \delta|A_1|/2 \geq \delta^2|A|/4$ ,  $A_2$  中最多  $\epsilon$  占比的顶点对是不友好的。

令

$$B' = \left\{b \in B : \deg(b, A_2) \geq \frac{\delta}{4}|A_2|\right\}$$

将  $(A_2, B)$  限制为  $(A_2, B')$ , 最多删除  $\delta|A_2||B|/4$  条边。因为  $A_2$  中的最小度数至少是  $\delta/2$ , 所以至少有  $\delta|A_2||B|/2$  条  $A_2$  和  $B$  之间的边。因此, 至少有  $\delta|A_2||B|/4$  条  $A_2$  和  $B'$  之间的边, 并且因为  $b \in B'$  的最大度数是  $|A_2|$ , 我

们有  $|B'| \geq \delta|B|/4$ 。定义

$$A' = \left\{ a \in A_2 : a \text{ is friendly to at least } \left(1 - \frac{\delta}{5}\right)\text{-fraction of } A_2 \right\}$$

我们有  $|A'| \geq |A_2|/2 \geq \delta^2|A|/8$ 。

我们现在固定  $(a, b) \in A' \times B'$  并控制它们之间的路径长度为 3 的数量。因为  $b$  至少与  $A_2$  中  $\delta|A_2|/4$  个顶点相邻,  $a$  至少  $(1 - \delta/5)|A_2|$  个  $A_2$  中的顶点是友好的, 所以  $A_2$  中至少有  $\delta|A_2|/20$  个顶点, 该顶点与  $a$  友好且与  $b$  相邻。对于每一个这样的  $a_1 \in A_2$ , 至少有  $\delta^3|B|/20$  个点  $b_1 \in B$ , 使得  $ab_1a_1b$  是长度为 3 的路径。因此从  $a$  到  $b$  的长度为 3 的路径数量至少是

$$\frac{\delta}{20}|A_2| \cdot \frac{\delta^3}{20}|B| \geq \frac{\delta}{20} \cdot \frac{\delta^2}{4}|A| \cdot \frac{\delta^3}{20}|B| = \frac{\delta^6}{20 \cdot 4 \cdot 80}|A||B|$$

取  $\eta$  等于上述系数, 我们注意到  $|A'| \geq \delta^2|A|/8 \geq \eta|A|$  和  $|B'| \geq \delta|B|/4 \geq \eta|B|$ 。证毕。

我们可以使用引理 7.4 来证明 Balog-Szemerédi-Gowers 定理的图论版本 (定理 7.20)。

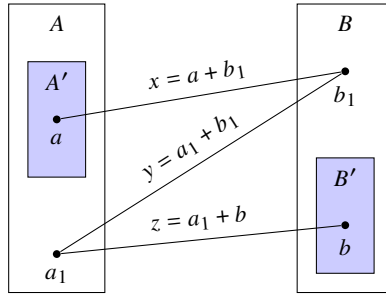


图 7.8: Balog-Szemerédi-Gowers 定理证明示意图

**证明** 注意到  $|A|, |B| \geq \frac{n}{K}$ 。通过引理 7.4, 我们可以找到  $A' \subset A$  和  $B' \subset B$  且大小满足  $|A'|, |B'| \geq K^{-O(1)}n$ , 使得对于每个  $(a, b) \in A' \times B'$ , 至少有  $K^{-O(1)}n^2$  条路径  $ab_1a_1b$ ,  $(a_1, b_1) \in A \times B$ 。因此, 对于每个  $(a, b) \in A' \times B'$ , 方程  $x - y + z = a + b$  至少有  $K^{-O(1)}n^2$  个解, 令解为  $x, y, z \in A +_G B$ ,  $(x, y, z) = (a + b_1, a_1 + b_1, a_1 + b)$  是沿每条路径  $ab_1a_1b$  得到的。

$$K^{-O(1)}n^2 |A' + B'| \leq |A +_G B|^3 = e(G)^3 \leq K^3 n^3$$

所以  $|A' + B'| \leq K^{O(1)}n$ 。

## 第 8 章 Sum-Product 问题

本章节，我们将考虑集合在加法和乘积下的特征。具体的，我们主要研究的是被称为 **sum-product** 的问题（下文中简称为和积问题）：是否存在集合  $A$ ，使得  $A + A$  和  $A \cdot A = \{ab : a, b \in A\}$  都很小。

我们以  $A = [N]$  为例，我们有加法集  $|A + A| = 2N - 1$ ，但乘法集很大， $|A \cdot A| = N^{2-o(1)}$ 。探索乘法集大小的问题被称为 **Erdős 乘法表问题**。我们还可以看出，如果  $A$  是等比数列，则  $A \cdot A$  很小，而  $A + A$  很大。关于和积问题的主要猜想是说，加法集或乘法集的大小非常接近一个极大值。

### 命题 8.1 (Erdős-Szemerédi's conjecture 1983)

对于任意  $\mathbb{R}$  上的有限子集  $A$ ，我们有

$$\max\{|A + A|, |A \cdot A|\} \geq |A|^{2-o(1)}$$

在本章，你会见到和积问题下界的证明的两个版本。作为铺垫，我们先介绍一些工具。

## 8.1 交叉数不等式

图  $G$  的交叉数  $\text{cr}(G)$  被定义为图  $G$  在平面上时边的交叉点的最小数目。我们想知道的是，给定一个有很多边的图，它的交叉数至少有多大？

### 定理 8.1 (交叉数不等式 Ajtai, Chvátal, Newborn and Szemerédi(1982)、Leighton (1984))

如果  $G = (V, E)$  是满足  $|E| \geq 4|V|$  的图，则对于常量  $c > 0$  有  $\text{cr}(G) \geq c|E|^3/|V|^2$ 。

根据该定理我们直接推导出结论：任意一个带有  $\Omega(n^2)$  边的  $n$ -顶点图都有  $\Omega(n^4)$  交叉点。

#### 证明

对于任何至少有一个圈的连通平面图，我们有  $3|F| \leq 2|E|$ ，其中  $|F|$  表示图的面（也称作域）。每个面与至少三个边相邻且每个边与最多两个面相邻，两次计数我们可以得到该不等式。应用欧拉公式<sup>1</sup>，我们得到  $|E| \leq 3|V| - 6$ 。因此，对任意平面图（包括那些非联通或没有圈的平面图） $G$  一定有  $|E| \leq 3|V|$ 。所以，如果  $|E| > 3|V|$  则有  $\text{cr}(G) > 0$ 。

假设图  $G$  满足  $|E| > 3|V|$ 。我们可以通过删除每条造成交叉的边来得到平面图，因此我们有  $|E| - \text{cr}(G) \leq 3|V|$ 。所以对于任意平面图  $G$ ，我们有

$$\text{cr}(G) \geq |E| - 3|V| \quad (8.1)$$

为了证明所需的不等式，我们借助概率方法。令  $p \in [0, 1]$  是一待定的实数，令  $G' = (V', E')$  是一个以概率  $p$  随机保留  $G$  的每个顶点 (iid) 得到的图。根据 (8.1) 我们知道对于任意的  $G'$  一定有  $\text{cr}(G') \geq |E'| - 3|V'|$ 。因此，如果我们两边取期望，不等式仍成立：

$$\mathbb{E} \text{cr}(G') \geq \mathbb{E}|E'| - 3\mathbb{E}|V'|$$

因为当且仅当保留边的两个端点时边仍存在，所以有  $\mathbb{E}|E'| = p^2|E|$ 。类似地我们有  $\mathbb{E}|V'| = p|V|$ 。同样的想法，我们得到不等式  $p^4 \text{cr}(G) \geq \mathbb{E} \text{cr}(G')$ （两条边的四个顶点都保留时交叉点才保留，大于号是因为会出现顶点重复的情况）。因此我们有

$$\text{cr}(G) \geq p^{-2}|E| - 3p^{-3}|V|$$

最后我们通过设置  $p \in [0, 1]$  得到我们想要的的不等式，具体的， $p$  满足  $4p^{-3}|V| = p^{-2}|E|$ 。根据条件  $|E| \geq 4|V|$  这是可以做到的。

<sup>1</sup>Euler 公式：设  $G$  是连通的平面图， $v, e, f$  分别是其顶点数、边数和面数，则  $v - e + f = 2$

## 8.2 重合几何

另一个与和积问题相关的数学领域是重合几何。点集  $\mathcal{P}$  和线集  $\mathcal{L}$  之间的“重合关系”定义为

$$I(\mathcal{P}, \mathcal{L}) = |\{(p, \ell) \in \mathcal{P} \times \mathcal{L} : p \in \ell\}|$$

$n$  个点和  $n$  条线之间发生重合的次数最大是多少？一个简单的上界是  $|\mathcal{P}||\mathcal{L}|$ 。事实上，注意到每一对点最多由一条线确定，基于此我们可以获得更好的上界：

$$\begin{aligned} |\mathcal{P}|^2 &\geq \#\{(p, p', \ell) \in \mathcal{P} \times \mathcal{P} \times \mathcal{L} : pp' \in \ell, p \neq p'\} \\ &\geq \sum_{\ell \in \mathcal{L}} |\mathcal{P} \cap \ell|(|\mathcal{P} \cap \ell| - 1) \\ &\geq \frac{I(\mathcal{P}, \mathcal{L})^2}{|\mathcal{L}|} - I(\mathcal{P}, \mathcal{L}) \end{aligned}$$

最后一个不等号来自柯西-施瓦茨不等式。因此，我们得到  $I(\mathcal{P}, \mathcal{L}) \leq |\mathcal{P}||\mathcal{L}|^{1/2} + |\mathcal{L}|$ 。由点和线的对偶性，我们也有  $I(\mathcal{P}, \mathcal{L}) \leq |\mathcal{L}||\mathcal{P}|^{1/2} + |\mathcal{P}|$ 。这些不等式告诉我们  $n$  点和  $n$  线的发生重合次数为  $O(n^{3/2})$ 。在第一章中我们已经知道  $\text{ex}(n, C_4) = \Theta(n^{3/2})$ ，这与我们的预期是相符的（我们可以将点和线看作是二部图）。回想一下，第一章中的构造来自有限域，并且上界是紧的。但是，在实际平面中， $n^{3/2}$  并不紧，我们将在下一个定理中看到。

### 定理 8.2 (Szemerédi-Trotter 1983)

对于任意  $\mathbb{R}^2$  上的点集  $\mathcal{P}$  和线集  $\mathcal{L}$ ，

$$I(\mathcal{P}, \mathcal{L}) = O(|\mathcal{P}|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{P}| + |\mathcal{L}|)$$

### 推论 8.1

对于  $\mathbb{R}^2$  上  $n$  个点和  $n$  条线，重合的次数为  $O(n^{4/3})$ 。

**例题 8.1** 下面我们给出一个示例，用于说明推论8.1的上界是紧的。令  $\mathcal{P} = [k] \times [2k^2]$  和  $\mathcal{L} = \{y = mx + b : m \in [k], b \in [k^2]\}$ 。则  $\mathcal{L}$  中的每一条线都包含  $\mathcal{P}$  中  $k$  个顶点，所以  $I = k^4 = \Theta(n^{4/3})$ 。

**证明** [定理8.2]

我们首先去掉  $\mathcal{L}$  中所有最多包含  $\mathcal{P}$  中一个点的线。可以看到，这些线最多能够造成  $|\mathcal{L}|$  次重合。

现在我们可以假设  $\mathcal{L}$  中的每一条线至少包含  $\mathcal{P}$  中的两个点。我们构造一个图  $G$  如下：首先，顶点为  $\mathcal{P}$  中的所有点。对于  $\mathcal{L}$  中的每条线，我们在位于该线上的  $\mathcal{P}$  的相邻点之间分配一条边。见图8.1。

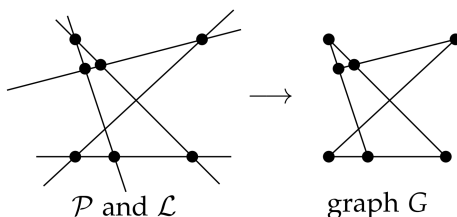


图 8.1: 图  $G$  的构造

因为一条经过  $k$  个顶点的线最多有  $k - 1 \geq k/2$  条边，所以我们有不等式  $|E| \geq I(\mathcal{P}, \mathcal{L})/2$ 。我们假设  $I(\mathcal{L}, \mathcal{P}) \geq 8|\mathcal{P}|$  成立（否则有  $I(\mathcal{P}, \mathcal{L}) \lesssim |\mathcal{P}|$ ），根据定理8.1有

$$\text{cr}(G) \gtrsim \frac{|E|^3}{|V|^2} \geq \frac{I(\mathcal{P}, \mathcal{L})^3}{|\mathcal{P}|^2}$$

此外，因为每两条线最多相交于一个点，所以  $\text{cr}(G) \leq |\mathcal{L}|^2$ 。我们整理得到  $I(\mathcal{P}, \mathcal{L}) \lesssim |\mathcal{P}|^{2/3}|\mathcal{L}|^{2/3}$ 。因此我们得到  $I(\mathcal{P}, \mathcal{L}) \lesssim |\mathcal{P}|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{P}| + |\mathcal{L}|$ 。两个线性的部分分别是考虑到开始时去掉的线和假设  $I(\mathcal{L}, \mathcal{P}) \geq 8|\mathcal{P}|$ 。

当我们在定理8.1的证明中应用欧拉公式时，我们使用了实平面的拓扑性质。现在我们将展示一个关于和积



问题如何与重合几何相关联的例子。

**定理 8.3 (Elekes 1997)**

如果  $A \subset \mathbb{R}$ , 则  $|A + A||A \cdot A| \gtrsim |A|^{5/2}$



**推论 8.2**

如果  $A \subset \mathbb{R}$ , 则  $\max\{|A + A|, |A \cdot A|\} \gtrsim |A|^{5/4}$



**证明** [定理8.3]

令  $\mathcal{P} = \{(x, y) : x \in A + A, y \in A \cdot A\}$  和  $\mathcal{L} = \{y = a(x - a') : a, a' \in A\}$ 。考虑  $\mathcal{L}$  中的任一条线  $y = a(x - a')$ , 对于所有  $b \in A$ ,  $(a' + b, ab) \in \mathcal{P}$  都在这条线上, 所以  $\mathcal{L}$  中的每一条线都包含  $|A|$  次重合。根据  $\mathcal{P}$  和  $\mathcal{L}$  的定义, 我们有

$$|\mathcal{P}| = |A + A||A \cdot A|, \quad |\mathcal{L}| = |A|^2$$

回顾定理8.2, 我们得到

$$\begin{aligned} |A|^3 \leq I(\mathcal{P}, \mathcal{L}) &\leq |\mathcal{P}|^{3/2} |\mathcal{L}|^{3/2} + |\mathcal{P}| + |\mathcal{L}| \\ &\lesssim |A + A|^{3/2} |A \cdot A|^{3/2} |A|^{4/3} \end{aligned}$$

整理后即得到我们想要的 inequality。

## 8.3 从积性能量看 Sum-product 问题

在本节中, 我们将给出命题8.1另一版本的证明, 该证明给出了一个更好的下界。

**定理 8.4 (Solymosi 2009)**

如果  $A \subset \mathbb{R}_{>0}$ , 则

$$|A \cdot A||A + A|^2 \geq \frac{|A|^4}{4 \lceil \log_2 |A| \rceil}$$



**推论 8.3**

如果  $A \subset \mathbb{R}$ , 则

$$\max\{|A + A|, |A \cdot A|\} \geq \frac{|A|^{4/3}}{2 \lceil \log_2 |A| \rceil^{1/3}}$$



我们定义积性能量 (multiplicative energy) 为

$$E_{\times}(A) = |\{(a, b, c, d) \in A^4 : \text{存在 } \lambda \in \mathbb{R} \text{ 满足 } (a, b) = (\lambda c, \lambda d)\}|$$

请注意, 积性能量是加性能量 (additive energy) 的乘积版本。可以看到, 如果  $A$  的乘法集很小, 那么积性能量就很大。

$$\begin{aligned} E_{\times}(A) &= \sum_{x \in A \cdot A} |\{(a, b) \in A^2 : ab = x\}|^2 \\ &\geq \frac{|A|^4}{|A \cdot A|} \end{aligned}$$

等号来自积性能量的等价定义  $E_{\times}(A) = |\{(a, b, c, d) \in A^4 : ad = bc\}|$ , 不等号来自柯西-施瓦茨不等式。因此要证明定理8.4, 我们只需证明

$$\frac{E_{\times}(A)}{\lceil \log_2 |A| \rceil} \leq 4|A + A|^2$$

**证明** [定理 8.4]

我们在这个证明中使用二元分解的方法。令  $A/A$  为集合  $\{a/b : a, b \in A\}$

$$\begin{aligned} E_{\times}(A) &= \sum_{s \in A/A} |(s \cdot A) \cap A|^2 \\ &= \sum_{i=0}^{\lceil \log_2 |A| \rceil} \sum_{\substack{s \in A/A \\ 2^i \leq |(s \cdot A) \cap A| < 2^{i+1}}} |(s \cdot A) \cap A|^2 \end{aligned}$$

根据鸽巢原理，存在  $k$  使得

$$\frac{E_{\times}(A)}{\lceil \log_2 |A| \rceil} \leq \sum_{\substack{s \in A/A \\ 2^k \leq |(s \cdot A) \cap A| < 2^{k+1}}} |(s \cdot A) \cap A|^2$$

我们记  $D = \{s : 2^k \leq |(s \cdot A) \cap A| < 2^{k+1}\}$  并对  $D$  中的元素进行排序： $s_1 < s_2 < \dots < s_m$ 。然后有

$$\frac{E_{\times}(A)}{\lceil \log_2 |A| \rceil} \leq \sum_{s \in D} |(s \cdot A) \cap A|^2 \leq |D| 2^{2k+2}$$

对于每个  $i \in [m]$ ，令  $\ell_i$  为一条线  $y = s_i x$ ，并令  $\ell_{m+1}$  为高于  $\ell_m$  的垂直射线  $x = \min(A)$ 。

令  $L_j = (A \times A) \cap \ell_j$ ，那么我们有  $|L_j + L_{j+1}| = |L_j| |L_{j+1}|$ 。此外，集合  $L_j + L_{j+1}$  对于不同的  $j$  是不相交的，因为它们张成不相交的区域（见图8.2）。我们可以通过对所有  $j$  求和  $|L_j + L_{j+1}|$  来得到  $|A + A|^2$  的下界。

$$\begin{aligned} |A + A|^2 &= |A \times A + A \times A| \\ &\geq \sum_{j=1}^m |L_j + L_{j+1}| \\ &= \sum_{j=1}^m |L_j| |L_{j+1}| \\ &\geq m 2^{2k} \geq \frac{E_{\times}(A)}{4 \lceil \log_2 |A| \rceil} \end{aligned}$$

其中，第一个等号右边的叉号代表笛卡尔积。将上述不等式与  $E_{\times}(A) \geq |A|^4 / |A \cdot A|$  结合我们即可完成证明。

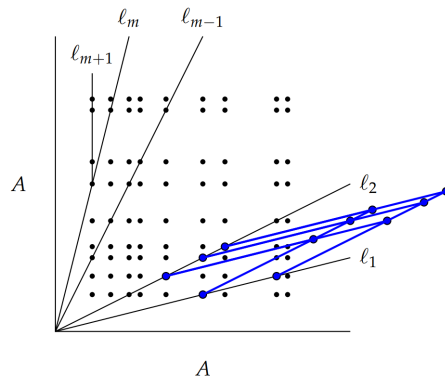


图 8.2:  $L_j + L_{j+1}$  示意图