arXiv:2611.32210v1 [math.CA] 24 Nov 2026

三次曲线上的离散 L^8 限制的改进估计

XUDONG LAI 和 HONGXU WU

Abstract. 我们证明了三次曲线上的离散 L^8 限制的一个改进估计（$n,\ n^3$）。更确切地说，对每个 $\varepsilon>0$，以下八阶矩估计成立

$$\int_{[0,1]^2}\left|\sum_{n=1}^{N} b_n \exp\big(2\pi i(nx+n^3y)\big)\right|^8 dxdy \ll_\varepsilon N^{1/2-1/47500+\varepsilon}\left(\sum_{n=1}^{N}|b_n|^2\right)^4.$$

1. Introduction and main result引言与主要结果

三次曲线上的离散傅里叶限制（$n,\ n^3$）出现在柯尔特韦格–德弗里斯方程的周期斯特里查茨估计研究中（见 [1]）。设 N 为正整数，设 $b_1,\ .....,\ b_N$为复数，并设 $r>0$。记

$$I_r(b)=\int_{[0,1]^2}\left|\sum_{n=1}^{N} b_n \exp\big(2\pi i(nx+n^3y)\big)\right|^r dx\,dy.$$

布尔甘 [1, 式（8.37）] 证明了带有任意小的 N 次幂损失的 L^6 限制估计。对于 $r\geq 8$，带有 ε 损失的猜想界，在矩形式下为

$$I_r(b)\ll_{r,\varepsilon} N^{r/2-4+\varepsilon}\left(\sum_{n=1}^{N}|b_n|^2\right)^{r/2}.$$

当 $r=8$ 时，N是临界点；除去 ε 损失后，所猜想的 N 次幂为零。

胡和李 [4, 定理 1.1] 证明了 $r\geq 14$的猜想界。第一作者和丁 [9, 利用布尔甘、德梅特和格思 [2] 关于完整矩曲线的估计，在定理 1.1 和推论 1.4] 中为具有单项式坐标的曲线建立了离散限制定理。对于（$n,\ n^3$），他们的定理将范围扩展到 $r\geq 12$，特别得出

$$I_{12}(b)\ll_\varepsilon N^{2+\varepsilon}\left(\sum_{n=1}^{N}|b_n|^2\right)^6.$$

2010 *Mathematics Subject Classification.* 主要分类号 42B25，42B20。*Key words and phrases.* 离散限制、三次指数和、整数弦、差集、有限差分。

Hughes 和 Wooley [7, 定理 1.2] 达到了 $r = 10$，证明了

$$I_{10}(b) \ll_\varepsilon N^{1+\varepsilon}\left(\sum_{n=1}^{N}|b_n|^2\right)^5. \tag{1.1}$$

此外，也有一些研究探讨了三次曲线之外的相关限制问题，参见 [5, 6, 10, 11, 12]。

我们还结合第三节证明的三重表示数界（3.2），与柯西–施瓦茨不等式，重新得到正支撑集上的六阶矩界。这给出3，并得到

$$\begin{aligned} I_6(b) &= \sum_{(s,v)\in\mathbb{Z}^2}\Bigg|\sum_{\substack{1\le a_1,a_2,a_3\le N\\ a_1+a_2+a_3=s\\ a_1^3+a_2^3+a_3^3=v}} b_{a_1}b_{a_2}b_{a_3}\Bigg|^2 \\ &\ll_\varepsilon N^\varepsilon \sum_{a_1,a_2,a_3=1}^{N}|b_{a_1}|^2|b_{a_2}|^2|b_{a_3}|^2 = N^\varepsilon\left(\sum_{n=1}^{N}|b_n|^2\right)^3. \end{aligned} \tag{1.2}$$

通过对（1.2）和（1.1）进行插值，并应用 H¨older 不等式，我们得到

$$I_8(b) \le I_6(b)^{1/2}I_{10}(b)^{1/2} \ll_\varepsilon N^{1/2+\varepsilon}\left(\sum_{n=1}^{N}|b_n|^2\right)^4. \tag{1.3}$$

本文将这一八阶矩界提升了 N 的一个固定幂次。

定理 1.1。 对每个 $\varepsilon > 0$，都存在一个常数 $C_\varepsilon > 0$，使得对每个正整数 N 以及任意复数 $b_1, \dots, b_N$，

$$I_8(b) \le C_\varepsilon N^{1/2-1/47500+\varepsilon}\left(\sum_{n=1}^{N}|b_n|^2\right)^4.$$

对定理1.1 两边取八次方根，得到以下 L^8 范数界：

$$\left\|\sum_{n=1}^{N} b_n \exp\big(2\pi i(nx+n^3y)\big)\right\|_{L^8([0,1]^2)} \ll_\varepsilon N^{1/16-1/380000+\varepsilon}\left(\sum_{n=1}^{N}|b_n|^2\right)^{1/2}.$$

本文的主要策略如下。我们首先研究示性函数。如果八阶矩较大，我们将得到其支撑集大小的上界和下界。然后，我们在一个较短的水平区间内找到一个较大的整数弦点集合，其差集较小。为得到差集的下界，我们将整数斜率的有限差分与整除性估计及加性立方体的计数结合起来。这一论证适用于一般的单项式曲线。对于三次曲线，取五次差分会与由较大的八阶矩得到的界矛盾。最后，我们从示性函数推广到任意复系数。

本文概述。 在第 2 节中，我们通过五个命题证明主要定理。我们首先化归到示性函数，随后控制支撑集的大小，最后比较局部弦集的差集的上界与下界。这五个命题将在第3–5节中证明。

记号。本文始终用 $\mathbf{1}_A$ 表示 A的示性函数。所有解的计数均指有序元组。对于有限集 U、$V \subseteq \mathbb{Z}^2$，U 中的一个加法四元组是一个元组 $(P_1, P_2, P_3, P_4) \in U^4$ 满足 $P_1+P_2 = P_3+P_4$。我们记 $U \pm V = \{u \pm v : u \in U, v \in V\}$，其中符号相匹配，并记 $-U = \{-u : u \in U\}$。集合 jU 由 U中 j 个元素的和组成，允许重复。对于 $z \in \mathbb{Z}^2$，pz 表示按坐标与 p相乘。对于素数 p，$\mathbb{Z}/p\mathbb{Z}$ 是模 p的剩余类域，点的同余关系按坐标解释。对于正整数 m，令 $\tau(m)$ 表示其正因子的数量。我们使用标准的因子界 $\tau(m) \ll_\eta m^\eta$，其对每个 $\eta > 0$ [3, Chapter XVIII]均成立。对数取自然对数。θ 固定，而 N 趋于无穷。在上界中，因子 $N^{o(1)}$ 被C_θ、$_\eta N^\eta$所界定，对每个 $\eta > 0$均成立。在下界中，$N^{-o(1)}$ 表示此类因子的倒数。常数对于这些集合、水平区间和所选素数是一致的。

2. Core Propositions

我们汇总导出定理1.1的各项估计。第一个命题将问题化简为示性函数。其余命题阐述八阶矩较大时的推论，并给出排除这种情况的差集估计。

对于 $A \subseteq \{1, \dots, N\}$，令 $\mathbf{1}_A$ 表示其示性函数。

命题 2.1。固定 $N \geq 1$。若 $D > 0$ 满足 $I_8(\mathbf{1}_A) \leq D|A|^4$ 对每个 $A \subseteq \{1, \dots, N\}$ 均成立，则对所有复系数 b_1，……，b_N，

$$I_8(b) \leq D(1+\log N)^4 \left(\sum_{n=1}^{N} |b_n|^2 \right)^4. \tag{2.1}$$

我们将在第 2.1 节证明命题 5。这将主证明化简为示性函数估计。因此，只需证明，对于每个固定的 $1/2 - 1/47500 < \theta < 1/2$，

$$I_8(\mathbf{1}_A) \leq C_\theta N^\theta |A|^4 \qquad (N \geq 1,\ A \subseteq \{1, \dots, N\}). \tag{2.2}$$

对于示性函数，正交性将八阶矩转化为有序解的计数：

$$I_8(\mathbf{1}_A) = \#\left\{ (a_1, \dots, a_4, c_1, \dots, c_4) \in A^8 : \begin{array}{l} \sum_{j=1}^4 a_j = \sum_{j=1}^4 c_j, \\ \sum_{j=1}^4 a_j^3 = \sum_{j=1}^4 c_j^3 \end{array} \right\}. \tag{2.3}$$

我们首先考察条件 $I_8(\mathbf{1}_A) \geq N^\theta |A|^4$ 对 $|A|$告诉了我们什么。下一个命题给出了上界和下界。

命题 2.2。设 $13/27 < \theta < 1/2$，且 A 是 $\{1, \dots, N\}$的非空子集。如果 $I_8(\mathbf{1}_A) \geq N^\theta |A|^4$，那么

$$N^{\theta - o(1)} \leq |A| \leq N^{1-\theta+o(1)}.$$

注记 2.3。命题 2.2给出

$$N^{1/2-(1/2-\theta)-o(1)} \leq |A| \leq N^{1/2+(1/2-\theta)+o(1)}.$$

上指数与下指数之间的差距为 $1 - 2\theta > 0$。当 θ 从下方趋近于 $1/2$时，两个指数都趋近于 $1/2$。如果我们从

下指数中减去上指数，并省略 $o(1)$ 项，就得到

$$\theta-(1-\theta)=2\theta-1=2\left(\theta-\frac{1}{2}\right).$$

当且仅当 $\theta>1/2$ 时，下指数大于上指数。因此，这些界无法对 $\theta<1/2$ 导出矛盾。当 θ 从下方接近 $1/2$ 时，我们需要更强的界。假设我们能够证明

$$N^{k_1\theta-k_2-o(1)}\le|A|\le N^{k_3-k_4\theta+o(1)},$$

其中 k_1,k_2,k_3,k_4 是固定实常数，且 $k_1+k_4>0$。现在将上指数从下指数中减去，得到

$$\begin{aligned}\Delta_\theta&=(k_1\theta-k_2-o(1))-(k_3-k_4\theta+o(1))\\&=(k_1+k_4)\theta-(k_2+k_3)-o(1).\end{aligned}$$

If

$$\theta>\frac{1}{2}-\left(\frac{1}{2}-\frac{k_2+k_3}{k_1+k_4}\right)=\frac{k_2+k_3}{k_1+k_4},$$

那么，当 N 足够大时，$\Delta_\theta>0$ 对所有情况都成立。此时，下界 $|A|$ 将超过上界。为了使这种情况对某个 $\theta<1/2$ 成立，我们寻找满足以下条件的 $(k_1,\ k_2,\ k_3,\ k_4)$：

$$k_1+k_4>2(k_2+k_3).$$

注记 2.4. 现在转向三次曲线的弦。对于 $a,b\in A$，其中 $a>b$，考虑从 (b,b^3) 到 (a,a^3) 的弦。若正整数 p 整除 $a-b$，则其弦向量除以 p 后是一个整数点：

$$\left(\frac{a-b}{p},\frac{a^3-b^3}{p}\right)\in\mathbb{Z}^2.$$

命题 2.5 和 2.6 表明，较大的八阶矩会在较短的水平区间内产生大量这样的点，并且其差集较小。

命题 2.5。设 $13/27<\theta<1/2$，且 N 充分大。若非空集合 $A\subseteq\{1,\dots,N\}$ 满足 $I_8(\mathbf{1}_A)\ge N^\theta|A|^4$，则存在一个素数 p、一个尺度 $X=2^j$，其中 j 是一个非负整数，以及一个非空集合

$$E\subseteq\left\{\left(\frac{a-b}{p},\frac{a^3-b^3}{p}\right):\ \begin{array}{l}a,b\in A,\ a>b,\ p\mid(a-b),\\ X\le(a-b)/p<2X\end{array}\right\}$$

使得

$$|E|\ge N^{2\theta-1/2-o(1)}.$$

对每个整数 $1\le H\le X$，将 $[X,2X)$ 划分为

$$I_j=[X+jH,\ \min\{X+(j+1)H,\ 2X\}),\qquad j=0,\dots,\lceil X/H\rceil-1.$$

若 h_0 是使 $\#\{(h,k)\in E:\ h\in I_j\}$ 达到最大值的区间的左端点，则非空集合

$$B=\{(h,k)\in E:h_0\le h<h_0+H\}$$

满足

$$\frac{|B-B|}{|B|}\le N^{153(1/2-\theta)+o(1)}.$$

p, X, E的选取与 H无关，并且该界关于 H 以及最大化区间的选取是一致的。

接下来我们选取 H，并得到 $|B|$的下界。对于同一个 B, $|B-B|/|B|$的估计仍然成立。

命题 2.6. 设 $1/2-1/1550<\theta<1/2$且设 N充分大。假设非空集 $A\subseteq\{1,\dots,N\}$满足 $I_8(\mathbf{1}_A)\geq N^{\theta}|A|^4$。设 p,X,E如命题2.5中所述。则

$$X\geq N^{1/2-155(1/2-\theta)-o(1)}.$$

当 N 充分大时，整数

$$H=\lfloor XN^{-2/5}\rfloor$$

满足 $1\leq H\leq XN^{-2/5}$。在此宽度下，命题 B 中选取的集合 2.5 满足

$$|B|\geq N^{2\theta-9/10-o(1)}.$$

其水平坐标位于 $[h_0,h_0+H]$ 中，其中 $h_0\geq X$，并且

$$B\subseteq\left\{\left(\frac{a-b}{p},\frac{a^3-b^3}{p}\right):a,b\in A,\ a>b,\ p\mid(a-b)\right\}.$$

对于同一个集合 B，命题2.5中的差集估计仍然成立。

注记 2.7。 在命题2.5 和 2.6中，当 θ 从下方趋近于 $1/2$时，

$$2\theta-\frac{9}{10}\longrightarrow\frac{1}{10},\qquad 153\left(\frac{1}{2}-\theta\right)\longrightarrow 0.$$

因此， $|B|$ 的下界仍保留 N的固定正幂，而 $|B-B|/|B|$ 上界中的幂趋近于零。下一个命题将用 $|B|$给出$|B-B|/|B|$ 的下界。将此下界与命题 2.5和2.6 比较，即可得到矛盾。

命题 2.8。 设 $N\geq 2$和 $p\geq 1$ 为整数，且 B 是以下整数弦点集合的任意非空子集，

$$B\subseteq\left\{\left(\frac{a-b}{p},\frac{a^3-b^3}{p}\right):a,b\in\mathbb{Z},\ 1\leq b<a\leq N,\ p\mid(a-b)\right\}.$$

设 $1\leq H\leq X\leq h_0$。若 B 的所有水平坐标均属于 $[h_0,h_0+H]$ 和 $H\leq XN^{-2/5}$，则对每个 $\eta>0$，存在一个仅依赖于 η 的常数 $C_\eta>0$，使得

$$\frac{|B-B|}{|B|}\geq C_\eta N^{-\eta}|B|^{1/31}.$$

现在我们可以证明定理1.1。

定理 *1.1* 的证明。 固定

$$\frac{1}{2}-\frac{1}{47500}<\theta<\frac{1}{2}.$$

我们首先证明示性函数的估计。反设，对于任意大的 N，存在一个非空的 $A \subseteq \{1,\dots,N\}$，满足 $I_8(\mathbf{1}_A) \geq N^{\theta}|A|^4$。命题 2.5和 2.6 给出一个非空集合 B 满足

$$|B| \geq N^{2\theta-9/10-o(1)}, \qquad \frac{|B-B|}{|B|} \leq N^{153(1/2-\theta)+o(1)},$$

$$1 \leq H = \lfloor XN^{-2/5} \rfloor \leq XN^{-2/5}.$$

宽度条件使我们能够将命题 2.8 应用于同一个 B。对于每个固定的$\eta > 0$，其差集比的下界和上界给出

$$C_\eta N^{-\eta+(2\theta-9/10-o(1))/31} \leq \frac{|B-B|}{|B|} \leq N^{153(1/2-\theta)+o(1)}.$$

将两个外侧表达式提升至 **31** 次方，并将 N 的幂移到左边。由于 $31 \cdot 153 = 4743$,

$$C_\eta^{31} N^{2\theta-9/10-4743(1/2-\theta)-31\eta-o(1)} \leq 1. \tag{2.4}$$

在减去 $31\eta + o(\mathbf{1})$ 之前，（2.4）中的指数在 $1/2-\theta < 1/(10\cdot 4745) = 1/47450$ 时为正。定理 **1.1** 中的节省量留下了如下余量。

$$\begin{aligned} 2\theta - \frac{9}{10} - 4743\left(\frac{1}{2}-\theta\right) &= \frac{1}{10} - 4745\left(\frac{1}{2}-\theta\right) \\ &> \frac{1}{10} - \frac{4745}{47500} = \frac{1}{9500} > 0. \end{aligned}$$

选择 $\eta > 0$ 足够小，使得

$$0 < 31\eta < \frac{1}{2}\left(\frac{1}{10} - 4745\left(\frac{1}{2}-\theta\right)\right).$$

固定选择 η后，当 $N \to \infty$时，（2.4）中的指数仍为正。因此左端趋于无穷大，这与（2.4）矛盾。因此，对于所有充分大的N，每个非空的 $A \subseteq \{1,\dots,N\}$都满足 $I_8(\mathbf{1}_A) < N^{\theta}|A|^4$。只剩下有限个 N。对于这些情形，使用 $I_8(\mathbf{1}_A) \leq |A|^8$ 并增大常数。我们得到

$$I_8(\mathbf{1}_A) \leq C_\theta N^{\theta}|A|^4 \qquad (N \geq 1,\ A \subseteq \{1,\dots,N\}).$$

给定 $\varepsilon > 0$，取

$$\frac{1}{2} - \frac{1}{47500} < \theta < \min\left\{\frac{1}{2}, \frac{1}{2} - \frac{1}{47500} + \frac{\varepsilon}{2}\right\}.$$

根据刚刚证明的示性函数估计（2.2），我们可以在（ $D = C_\theta N^{\theta}$ 中取2.1）。上界 $(1+\log N)^4 \ll_\varepsilon N^{\varepsilon/2}$将对数因子吸收到 N的剩余幂次中，从而得到

$$I_8(b) \leq C_\theta N^{\theta}(1+\log N)^4 \left(\sum_{n=1}^{N}|b_n|^2\right)^4 \leq C_\varepsilon N^{1/2-1/47500+\varepsilon}\left(\sum_{n=1}^{N}|b_n|^2\right)^4.$$

定理1.1的证明至此完成。 □

我们在第2.2 节证明3中的命题2.5 和2.6 ，并在第4节证明。在第5节中，我们首先证明具有整数斜率的点的差集界，然后将其应用于单项式曲线上的弦点。取曲线次数 $d = 3$ 和差分阶数 $r = 5$ ，即可得到命题2.8。

3. Proof of Proposition 2.2

引理 3.1。 设 $N \geq 2$ 和 $p \geq 1$ 为整数，并设

$$U \subseteq \left\{ \left(\frac{a-b}{p}, \frac{a^3-b^3}{p} \right) : a, b \in \mathbb{Z},\ 1 \leq b < a \leq N,\ p \mid (a-b) \right\}.$$

每个 点 $(h, k) \in U$ 唯一确定其端点 $a > b$。对于每个 $t \in \mathbb{Z} \setminus \{0\}$ ，

$$\#\{(h,k) \in U : (h, k+t) \in U\} \leq 2\tau(|t|)^2.$$

此外，

$$\#\{(h,k) \in U : (h, k+t) \in U\} \leq N^{o(1)},$$

关于 p、t、U一致成立。

证明。取具有 $1 \leq b < a \leq N$ 和 $p \mid (a-b)$ 的整数端点。其弦点满足

$$h = \frac{a-b}{p}, \qquad k = \frac{a^3-b^3}{p} = \frac{(b+ph)^3-b^3}{p} = 3hb^2 + 3ph^2b + p^2h^3.$$

对于固定的 p、$h > 0$ 和 $3hb^2 + 3ph^2b + p^2h^3$，其关于 $b \geq 1$ 严格递增。一旦 p、h、k 固定下来，因此至多存在一个正整数 b。随后， a 的值由 $a = b + ph$ 唯一确定。

Let

$$U \subseteq \left\{ \left(\frac{a-b}{p}, \frac{a^3-b^3}{p} \right) : a, b \in \mathbb{Z},\ 1 \leq b < a \leq N,\ p \mid (a-b) \right\}.$$

固定 $t \in \mathbb{Z} \setminus \{0\}$。对于 $(h$、$k)$、$(h$、$k+t) \in U$，分别将较小的端点记为 b 和 $b + w$。由于两个弦点的水平坐标均为 h,

$$(h,k) = \left(h, \frac{(b+ph)^3-b^3}{p} \right),$$
$$(h,k+t) = \left(h, \frac{(b+w+ph)^3-(b+w)^3}{p} \right).$$

相减它们的垂直坐标可得

$$\begin{aligned} t &= \frac{(b+w+ph)^3-(b+w)^3}{p} - \frac{(b+ph)^3-b^3}{p} \\ &= 3h\big((b+w)^2-b^2\big) + 3ph^2w = 3hw(2b+w+ph). \end{aligned}$$

由于 $t \neq 0$,

$$h \mid |t|, \qquad h > 0, \qquad w \neq 0, \qquad |w| \mid |t|.$$

固定 h, w 后，该方程确定 b，进而确定 k:

$$b = \tfrac{1}{2}\left(\frac{t}{3hw} - w - ph \right), \qquad k = \frac{(b+ph)^3-b^3}{p}.$$

因此，每种 $(h,\ w)$ 的取值至多对应一个点 $(h,\ k)$。正因子 h 有 $\tau(|t|)$ 种可能，带符号因子 w 至多有 $2\tau(|t|)$ 种可能。有些取值可能不会产生可容许的端点，但将它们全部计入，可得上界

$$\begin{aligned}\#\{(h,k)\in U:(h,k+t)\in U\} &\le \#\{h>0:h\mid |t|\}\,\#\{w\neq 0:|w|\mid |t|\}\\ &= 2\tau(|t|)^2.\end{aligned}\tag{3.1}$$

如果一对元素出现，则其垂直差的绝对值至多为 N^3。因此，(3.1) 中的因子界给出一致估计；如果 $|t|>N^3$，则计数为零：

$$\begin{gathered}(h,k),(h,k+t)\in U \implies 0<k,\ k+t\le N^3 \implies 0<|t|\le N^3,\\ 0<|t|\le N^3 \implies 2\tau(|t|)^2\le N^{o(1)},\\ |t|>N^3 \implies \#\{(h,k)\in U:(h,k+t)\in U\}=0.\end{gathered}$$

□

命题 5.5 将引理 3.1中的垂直差界推广到次数至少为三的整数多项式。

命题 *2.2*。令 $13/27<\theta<1/2$，且令 A 为 $\{1,\dots,N\}$的非空子集。如果 $I_8(\mathbf{1}_A)\ge N^\theta|A|^4$，则

$$N^{\theta-o(1)}\le |A|\le N^{1-\theta+o(1)}.$$

命题 *2.2* 的证明。我们首先考虑表示固定的$(s,v)\in\mathbb{Z}^2$的三元组数量。如果 $a+b+c=s,\ a^3+b^3+c^3=v$ 在 A^3中没有解，则计数为零。否则，任取一个解 (a,b,c)。将其代入 s^3-v，并展开 $((a+b)+c)^3$，再使用 $(a+b)^3,$，得到

$$\begin{aligned}s^3-v&=(a+b+c)^3-a^3-b^3-c^3\\ &=3c(a+b)(a+b+c)+3ab(a+b)\\ &=3(a+b)\left(ab+ac+bc+c^2\right)\\ &=3(a+b)(a+c)(b+c).\end{aligned}$$

由于 $1\le a,\ b,\ c\le N$,

$$2\le a+b,\ a+c,\ b+c\le 2N,$$

$$8\le\frac{s^3-v}{3}=(a+b)(a+c)(b+c)\le(2N)^3=8N^3.$$

因此（s^3-v）/3 是由（$s,\ v$）确定的正整数。乘积（$a+b$）（$a+c$）（$b+c$）是固定的，因此在 $a+b,\ a+c,\ b+c$ 中任取两个即可确定第三个。例如，

$$b+c=\frac{s^3-v}{3(a+b)(a+c)}.$$

$a+b$ 和 $a+c$ 都必须是（s^3-v）/3的正因子。因此，有序三元组（$a+b,\ a+c,\ b+c$）至多有 τ（（s^3-v）/3）种选择。这样的选择

至多确定一个（a，b，c），因为

$$\begin{aligned} a &= \tfrac{1}{2}\big((a+b)+(a+c)-(b+c)\big),\\ b &= \tfrac{1}{2}\big((a+b)+(b+c)-(a+c)\big),\\ c &= \tfrac{1}{2}\big((a+c)+(b+c)-(a+b)\big). \end{aligned}$$

固定 $\eta>0$ 并使用指数为 $\eta/6$的因子界。平方运算会使该指数加倍，而（s^3-v）$/3\le 8N^3$，因此 τ（（s^3-v）$/3$）$^2\ll_\eta$（$8N^3$）$^{\eta/3}\ll_\eta N^\eta$。隐含常数与（s，v）无关。由于 $\eta>0$ 是任意的，且不具有表示的二元组（s，v）贡献为零，我们得到

$$\#\{(a,b,c)\in A^3 : a+b+c=s,\ a^3+b^3+c^3=v\}\le N^{o(1)}. \tag{3.2}$$

现在我们利用这个计数来界定 I_6（$\mathbf{1}_A$）。将模数的六次方写成和的立方乘以其复共轭的立方：

$$\left|\sum_{a\in A} e^{2\pi i(ax+a^3y)}\right|^6 = \left(\sum_{a\in A} e^{2\pi i(ax+a^3y)}\right)^3\left(\sum_{c\in A} e^{-2\pi i(cx+c^3y)}\right)^3.$$

取复共轭会改变指数函数中的符号。展开这两个立方会引入三个变量 a_1，a_2，a_3 以及三个变量 c_1，c_2，c_3。逐项积分所得的有限和，得到

$$\begin{aligned} I_6(\mathbf{1}_A) = \sum_{\substack{a_1,a_2,a_3\in A\\ c_1,c_2,c_3\in A}} &\left(\int_0^1 \exp\big(2\pi i x(a_1+a_2+a_3-c_1-c_2-c_3)\big)\,dx\right)\\ &\times\left(\int_0^1 \exp\big(2\pi i y(a_1^3+a_2^3+a_3^3-c_1^3-c_2^3-c_3^3)\big)\,dy\right). \end{aligned}$$

对于每个整数 m，

$$\int_0^1 e^{2\pi i m x}\,dx = \begin{cases} 1, & m=0,\\ (e^{2\pi i m}-1)/(2\pi i m)=0, & m\neq 0. \end{cases} \tag{3.3}$$

由（3.3），当两个三元组的和相同且立方和相同时，一个六元组恰好贡献 1。将这两个公共值记为 s，v，则有

$$\begin{aligned} s &= a_1+a_2+a_3 = c_1+c_2+c_3,\\ v &= a_1^3+a_2^3+a_3^3 = c_1^3+c_2^3+c_3^3. \end{aligned}$$

其他所有六元组均贡献 0。将保留下来的六元组按（s，v）分组，得到

$$I_6(\mathbf{1}_A) = \sum_{(s,v)\in\mathbb{Z}^2}\big(\#\{(a,b,c)\in A^3 : a+b+c=s,\ a^3+b^3+c^3=v\}\big)^2. \tag{3.4}$$

根据（3.2），

$$I_6(\mathbf{1}_A)\le N^{o(1)}\sum_{(s,v)\in\mathbb{Z}^2}\#\{(a,b,c)\in A^3 : a+b+c=s,\ a^3+b^3+c^3=v\}.$$

每个 $(a,\ b,\ c)\ \in\ A^3$ 恰好确定一对 $(s,\ v)$。先按三元组而不是按 $(s,\ v)$ 计数，我们得到

$$\begin{aligned}&\sum_{(s,v)\in\mathbb{Z}^2}\#\{(a,b,c)\in A^3 : a+b+c=s,\ a^3+b^3+c^3=v\}\\&=\sum_{(a,b,c)\in A^3}\#\{(s,v)\in\mathbb{Z}^2 : (s,v)=(a+b+c,a^3+b^3+c^3)\}\\&=\sum_{a\in A}\sum_{b\in A}\sum_{c\in A}1=|A|^3.\end{aligned}$$

对于每个 $(x,\ y)\ \in [0,1]^2$，由三角不等式可得

$$\left|\sum_{a\in A}e^{2\pi i(ax+a^3y)}\right|\le\sum_{a\in A}\left|e^{2\pi i(ax+a^3y)}\right|=\sum_{a\in A}1=|A|.$$

因此，

$$\begin{aligned}&I_6(\mathbf{1}_A)\le N^{o(1)}|A|^3,\\&I_8(\mathbf{1}_A)=\int_{[0,1]^2}\left|\sum_{a\in A}e^{2\pi i(ax+a^3y)}\right|^2\left|\sum_{a\in A}e^{2\pi i(ax+a^3y)}\right|^6dx\,dy\\&\qquad\le|A|^2I_6(\mathbf{1}_A)\le N^{o(1)}|A|^5.\end{aligned}\tag{3.5}$$

由（3.5）以及命题 2.2 的假设，

$$N^\theta|A|^4\le I_8(\mathbf{1}_A)\le N^{o(1)}|A|^5,\qquad |A|>0\quad\Longrightarrow\quad|A|\ge N^{\theta-o(1)}.$$

接下来我们证明 $|A|$ 的上界。我们在三元组和上构造一个图，并利用引理 3.1 来界定同一垂直列中两个顶点的公共邻居数量。

使用集合

$$\mathcal{T}=\{(a+b+c,a^3+b^3+c^3) : a,b,c\in A\}$$

以其为顶点集。当两个顶点之差为非零弦向量 $(a-b,\ a^3-b^3)$ 且满足 $a,\ b\ \in\ A$ 时，将它们连接起来。交换 $a,\ b$ 会使向量反向，因此邻接关系是对称的。计数边时，我们分别计算两个方向。

固定 $P\ =(s,\ v)$ 和 $P'\ =(s,\ v')$，其中 $v\ \neq\ v'$。它们的水平坐标相等，因此共同邻点问题将转化为垂直差计数。假设$Q=(Q_1,\ Q_2)$ 同时与二者相邻。必有 $Q_1\neq s$，因为水平坐标为零的弦向量必为零。选择两个弦向量的方向，使其水平坐标均为正。根据 Q 位于该列哪一侧，我们得到

$$\begin{aligned}Q_1<s:&\quad(P'-Q)-(P-Q)=(0,v'-v),\\Q_1>s:&\quad(Q-P')-(Q-P)=(0,v-v').\end{aligned}$$

当 $Q_1<s$ 时，将 (3.1) 应用于 $P-Q,\ P'-Q$，其垂直差为 $v'-v$。当$Q_1>s$ 时，将其应用于 $Q-P,\ Q-P'$，其垂直差为 $v-v'$。在每种情况下 $p=1$,

而涉及 P 的弦向量唯一确定了 Q。因此

$$\begin{aligned}&\#\{Q\in\mathcal{T}: Q \text{ is adjacent to both } P,P'\}\\&=\#\{Q\in\mathcal{T}: Q_1<s,\ Q \text{ is adjacent to both } P,P'\}\\&\quad+\#\{Q\in\mathcal{T}: Q_1>s,\ Q \text{ is adjacent to both } P,P'\}\\&\le 2\tau(|v'-v|)^2+2\tau(|v-v'|)^2\le N^{o(1)}.\end{aligned}\tag{3.6}$$

为论证最终的界，注意到 P，$P'\in\mathcal{T}$和 $A\subseteq\{1,\dots,N\}$可推出

$$3\le v,v'\le 3N^3,\qquad v\ne v'\quad\Longrightarrow\quad 1\le|v'-v|=|v-v'|\le 3N^3.$$

对于每个 $\eta>0$，在 $\tau(m)$ 中取 $\varepsilon=\eta/6$ 可得

$$\tau(m)\le C_{\eta/6}m^{\eta/6}\qquad(m\in\mathbb{Z}_{\ge1}).$$

因此

$$\begin{aligned}2\tau(|v'-v|)^2+2\tau(|v-v'|)^2&=4\tau(|v'-v|)^2\\&\le 4C_{\eta/6}^2|v'-v|^{\eta/3}\\&\le 4C_{\eta/6}^2(3N^3)^{\eta/3}\\&=4\cdot3^{\eta/3}C_{\eta/6}^2N^{\eta}\ll_\eta N^{\eta}.\end{aligned}$$

这对每个 $\eta>0$都成立，且常数与 P，P'无关。因此，我们可以将公共邻点界写为 $N^{o(1)}$。

现在利用（3.6）来界定边的数量。记

$$\mathcal{T}_s=\{(s',v)\in\mathcal{T}: s'=s\},\qquad \deg_s(Q)=\#\{P\in\mathcal{T}_s: P \text{ is adjacent to } Q\}.$$

计数具有不同 P、$P'\in\mathcal{T}_s$且 Q与二者都相邻的有序三元组（P、P'、Q）。先按 Q 计数，再按（P、P'）计数，得到

$$\begin{aligned}\sum_{Q\in\mathcal{T}}\deg_s(Q)(\deg_s(Q)-1)&=\sum_{\substack{P,P'\in\mathcal{T}_s\\P\ne P'}}\#\{Q\in\mathcal{T}: Q \text{ is adjacent to both } P,P'\}\\&\le N^{o(1)}|\mathcal{T}_s|(|\mathcal{T}_s|-1).\end{aligned}$$

利用

$$j\le 1+\sqrt{j(j-1)}\qquad(j\in\mathbb{Z}_{\ge0})$$

并应用柯西–施瓦茨不等式，再结合（3.6），可得

$$\begin{aligned}\sum_{Q\in\mathcal{T}}\deg_s(Q)&\le|\mathcal{T}|+|\mathcal{T}|^{1/2}\left(\sum_{Q\in\mathcal{T}}\deg_s(Q)(\deg_s(Q)-1)\right)^{1/2}\\&\le|\mathcal{T}|+N^{o(1)}|\mathcal{T}|^{1/2}|\mathcal{T}_s|.\end{aligned}$$

由于

$$\#\{s:\mathcal{T}_s\ne\varnothing\}\le 3N,\qquad\sum_s|\mathcal{T}_s|=|\mathcal{T}|\le|A|^3,$$

对所有非空列求和可得有向边数量的以下界：

$$\begin{aligned}\sum_{s:\,\mathcal{T}_s\neq\varnothing}\sum_{Q\in\mathcal{T}}\deg_s(Q) &\le 3N|\mathcal{T}| + N^{o(1)}|\mathcal{T}|^{3/2}\\ &\le 3N|A|^3 + N^{o(1)}|A|^{9/2}.\end{aligned}\tag{3.7}$$

现在我们将这些边与 $I_8(\mathbf{1}_A)$ 联系起来。展开指数和的四个副本及其复共轭的四个副本，并利用 (3.3)，得到恒等式 (2.3) 的如下形式：

$$I_8(\mathbf{1}_A) = \#\left\{(a_1,\dots,a_4,c_1,\dots,c_4)\in A^8:\ \begin{array}{l}\sum_{j=1}^4(a_j-c_j)=0,\\ \sum_{j=1}^4(a_j^3-c_j^3)=0\end{array}\right\}.$$

首先考虑 $a_4=c_4$。项 a_4、c_4 在线性方程中相消，而 a_4^3、c_4^3 在三次方程中相消。它们的公共值有 $|A|$ 种选择。其余六个变量根据 (3.4) 由 $I_6(\mathbf{1}_A)$ 计数，因此此情形贡献 $|A|I_6(\mathbf{1}_A)$ 个解。

现在假设 $a_4\neq c_4$，并取

$$P=(a_1+a_2+a_3,\ a_1^3+a_2^3+a_3^3),$$
$$Q=(c_1+c_2+c_3,\ c_1^3+c_2^3+c_3^3).$$

由于 $\sum_{j=1}^4(a_j-c_j)=\sum_{j=1}^4(a_j^3-c_j^3)=0$，

$$P-Q=(c_4-a_4,\ c_4^3-a_4^3).$$

由于 $P,\ Q\in\mathcal{T}$、$a_4,\ c_4\in A$ 和 $a_4\neq c_4$，

$$P-Q=(c_4-a_4,c_4^3-a_4^3)\in\{(a-b,a^3-b^3):a,b\in A,\ a\neq b\}.$$

因此，P 和 Q 相邻，而（P，Q）是我们已计数的有向边之一。相应弦的端点为

$$\begin{aligned}c_4>a_4:&\quad P-Q=(c_4,c_4^3)-(a_4,a_4^3),\\ a_4>c_4:&\quad Q-P=(a_4,a_4^3)-(c_4,c_4^3).\end{aligned}$$

在任一种情况下，正向弦向量都通过引理3.1 和 $p=1$确定这两个端点。 P_1-Q_1 的符号确定了 $a_4,\ c_4$的顺序。

因此，固定有向边（P，Q）后，（a_4，c_4）至多有一种选择：

$$\#\left\{(a_4,c_4)\in A^2:\ \begin{array}{l}c_4-a_4=P_1-Q_1,\\ c_4^3-a_4^3=P_2-Q_2\end{array}\right\}\le 1.$$

固定 P，Q后，表示它们的两个有序三元组根据（3.2）各自至多有 $N^{o(1)}$种选择。二者合计至多有 $N^{o\ (1)}\cdot N^{o\ (1)}=N^{o(1)}$种选择。加上 $a_4=c_4$的贡献，并利用（3.5）和（3.7），得到

$$\begin{aligned}I_8(\mathbf{1}_A) &\le |A|I_6(\mathbf{1}_A)+N^{o(1)}\big(3N|A|^3+N^{o(1)}|A|^{9/2}\big)\\ &\le N^{o(1)}\big(|A|^4+N|A|^3+|A|^{9/2}\big).\end{aligned}$$

除以 $|A|^4$ 可得

$$\frac{I_8(\mathbf{1}_A)}{|A|^4}\le N^{o(1)}\left(1+\frac{N}{|A|}+|A|^{1/2}\right).\tag{3.8}$$

式项 $|A|^{1/2}$ 在（3.8）中，当 $|A|$较大时可能过大。在该范围内，我们对完整区间 [15,定理 11]:

$$I_8(\mathbf{1}_{\{1,\dots,N\}}) \le N^{13/3+o(1)}. \tag{3.9}$$

八个条目均位于其中的每个解 A 也会在其中计数 $\{1,\dots,N\}$。界$|A|^{1/2}$和 $N^{13/3}/|A|^4$在 $|A| = N^{26/27}$时一致。因此我们在此值处分情况讨论。如果$|A| \le N^{26/27}$，则 $|A|^{1/2} \le N^{13/27}$。如果 $|A| \ge N^{26/27}$，则（3.9）给出

$$\frac{I_8(\mathbf{1}_A)}{|A|^4} \le \frac{I_8(\mathbf{1}_{\{1,\dots,N\}})}{|A|^4} \le N^{13/3-104/27+o(1)} = N^{13/27+o(1)}.$$

将（3.8）对 $|A| \le N^{26/27}$与（3.9）对 $|A| \ge N^{26/27}$给出的界结合起来，并利用 I_8（$\mathbf{1}_A$） $\ge N^\theta|A|^4$，我们得到

$$N^\theta \le \frac{I_8(\mathbf{1}_A)}{|A|^4} \le N^{o(1)}\left(N^{13/27} + \frac{N}{|A|}\right).$$

由于 $\theta > 13/27$ 是固定的，

$$\frac{N^{13/27+o(1)}}{N^\theta} = N^{-(\theta-13/27)+o(1)} \longrightarrow 0.$$

因此，我们可以将 $N^{13/27+o(1)}$项吸收到 N^θ的一半中。当 N充分大时，

$$\frac{N^\theta}{2} \le \frac{N^{1+o(1)}}{|A|} \quad \Longrightarrow \quad |A| \le N^{1-\theta+o(1)}.$$

结合下界 $|A| \ge N^{\theta-o(1)}$，即可证明该断言。 □

注记 3.2。 命题 2.2 表明，大小至少为 $N^\theta|A|^4$ 的八阶矩会同时迫使

$$|A| \ge N^{\theta-o(1)}, \qquad |A| \le N^{1-\theta+o(1)}.$$

下界来自对六阶矩中三元组的计数。对于上界，我们在图中计数公共邻居，然后使用整个区间上的八阶矩估计。因此，当 θ 接近 $1/2$时，剩余论证只需处理介于 N 的幂之间、其指数接近 $1/2$的 $|A|$ 。

4. Proofs of Propositions 2.5 and 2.6

引理 4.1。设 $13/27 < \theta < 1/2$，并假设一个非空集合 $A \subseteq \{1, \dots, N\}$满足 $I_8(\mathbf{1}_A) \geq N^\theta |A|^4$。存在非空集合

$$\Omega \subseteq \{(a+b+c, a^3+b^3+c^3) : a, b, c \in A\}, \qquad S \subseteq A,$$

以及 $(u_0, v_0) \in A^2$，使得

$$|\Omega| \geq N^{3\theta/2 - o(1)} |A|^{3/2}, \quad \frac{|3\Omega - 3\Omega|}{|\Omega|} \leq N^{144(1/2-\theta)+o(1)},$$
$$|S| \geq N^{2\theta - 1/2 - o(1)}, \qquad \frac{|A|}{|S|} \leq N^{3(1/2-\theta)+o(1)}.$$

对于 $a \in A$，若 $(u, v) \in A^2$ 是 a 的伙伴对，则称之为配对，当 $(a+u+v, a^3+u^3+v^3) \in \Omega$。每个$a \in S$ 都有 (u_0, v_0) 作为伙伴对，并且至少有 $|\Omega|/(2|A|)$ 个配对。

证明。假设 $13/27 < \theta < 1/2$ 使我们可以应用命题2.2。取集合 $\mathcal{T} = \{(a+b+c,\ a^3+b^3+c^3) :\ a,\ b,\ c \in A\}$。我们首先证明其中包含许多加性四元组。H¨older 不等式给出

$$\begin{aligned} I_8(\mathbf{1}_A) &= \int_{[0,1]^2} \left| \sum_{a \in A} e^{2\pi i (ax + a^3 y)} \right|^4 \left| \sum_{a \in A} e^{2\pi i (ax + a^3 y)} \right|^4 dx\, dy \\ &\leq I_6(\mathbf{1}_A)^{2/3} I_{12}(\mathbf{1}_A)^{1/3}. \end{aligned}$$

由（3.4），

$$I_6(\mathbf{1}_A) \geq \#\{(a_1, a_2, a_3, c_1, c_2, c_3) \in A^6 : a_j = c_j,\ 1 \leq j \leq 3\} = |A|^3 > 0.$$

对角解表明 $I_6(\mathbf{1}_A) > 0$，因此我们可以重新整理前面的矩不等式，得到

$$I_{12}(\mathbf{1}_A) \geq \frac{I_8(\mathbf{1}_A)^3}{I_6(\mathbf{1}_A)^2}. \tag{4.1}$$

将（3.3）应用于十二阶矩可知，$I_{12}(\mathbf{1}_A)$ 统计满足$\sum_{j=1}^6 a_j = \sum_{j=1}^6 c_j$, $\sum_{j=1}^6 a_j^3 = \sum_{j=1}^6 c_j^3$的有序十二元组。将变量分成四个三元组，并将其与点

$$P_1 = (a_1+a_2+a_3,\ a_1^3+a_2^3+a_3^3), \quad P_2 = (a_4+a_5+a_6,\ a_4^3+a_5^3+a_6^3),$$
$$P_3 = (c_1+c_2+c_3,\ c_1^3+c_2^3+c_3^3), \quad P_4 = (c_4+c_5+c_6,\ c_4^3+c_5^3+c_6^3).$$

$$\left.\begin{aligned} \sum_{j=1}^6 a_j &= \sum_{j=1}^6 c_j \\ \sum_{j=1}^6 a_j^3 &= \sum_{j=1}^6 c_j^3 \end{aligned}\right\} \iff P_1 + P_2 = P_3 + P_4.$$

对于每个加法四元组，表示它的十二元组数量等于四个三元表示数的乘积。因此

$$I_{12}(\mathbf{1}_A)=\sum_{\substack{P_1,P_2,P_3,P_4\in\mathcal{T}\\ P_1+P_2=P_3+P_4}}\prod_{j=1}^{4}\#\{(a,b,c)\in A^3:(a+b+c,a^3+b^3+c^3)=P_j\}.$$

由（3.2），该乘积至多为（$N^{o(1)}$）$^4=N^{o(1)}$。利用（4.1）、（3.5中的六阶矩界以及假设 $I_8(\mathbf{1}_A)\ge N^{\theta}|A|^4$，我们得到

$$\begin{aligned}&\#\{(P_1,P_2,P_3,P_4)\in\mathcal{T}^4:P_1+P_2=P_3+P_4\}\\ &\quad\ge N^{-o(1)}I_{12}(\mathbf{1}_A)\ge N^{-o(1)}\frac{I_8(\mathbf{1}_A)^3}{|A|^6}\ge N^{3\theta-o(1)}|A|^6.\end{aligned}\tag{4.2}$$

利用（4.2）、$|\mathcal{T}|\le|A|^3$以及命题 2.2中对 $|A|$ 的上界，我们得到

$$\begin{aligned}\frac{|\mathcal{T}|^3}{\#\{(P_1,P_2,P_3,P_4)\in\mathcal{T}^4:P_1+P_2=P_3+P_4\}}&\le\frac{|A|^9}{N^{3\theta-o(1)}|A|^6}\\ &\le N^{3(1-\theta)-3\theta+o(1)}=N^{6(1/2-\theta)+o(1)}.\end{aligned}\tag{4.3}$$

Reiher–Schoen 定理 [14, 定理 1。2] 适用于阿贝尔群的任意非空有限子集。此处该群为 $\mathbb{Z}^2$，参数 K 是（4.3）左侧的比值，而误差参数为 $1/4$。该比值至少为一，因为加法四元组中的任意三个项都能确定第四项。该定理给出了一个同时满足以下两点的非空集合 $\Omega\subseteq\mathcal{T}$:

$$\begin{aligned}|\Omega|&\ge\frac{3}{4}\left(\frac{\#\{(P_1,P_2,P_3,P_4)\in\mathcal{T}^4:P_1+P_2=P_3+P_4\}}{|\mathcal{T}|}\right)^{1/2},\\ \frac{|\Omega-\Omega|}{|\Omega|}&\ll_{1/4}\left(\frac{|\mathcal{T}|^3}{\#\{(P_1,P_2,P_3,P_4)\in\mathcal{T}^4:P_1+P_2=P_3+P_4\}}\right)^4.\end{aligned}$$

第二个界中的隐常数仅依赖于固定的误差参数$1/4$。将 (4.2) 和 $|\mathcal{T}|\le|A|^3$ 代入 $|\Omega|$的界中，并在 $|\Omega-\Omega|/|\Omega|$的界中使用 (4.3), 得到

$$\begin{aligned}|\Omega|&\ge\tfrac{3}{4}\left(\frac{N^{3\theta-o(1)}|A|^6}{|A|^3}\right)^{1/2}\ge N^{3\theta/2-o(1)}|A|^{3/2},\\ \frac{|\Omega-\Omega|}{|\Omega|}&\ll\left(N^{6(1/2-\theta)+o(1)}\right)^4\le N^{24(1/2-\theta)+o(1)}.\end{aligned}\tag{4.4}$$

我们还需要对 $|3\Omega-3\Omega|$给出一个界。对于阿贝尔群中的有限非空子集 U,V 以及正整数 j,l, Pl¨unnecke–Ruzsa 不等式指出$|jV-lV|\le(|U+V|/|U|)^{j+l}|U|$ [13, 定理 1.2]。取 $U=-\Omega$ $V=\Omega$。于是$|U+V|=|\Omega-\Omega|$，且 $|U|=|\Omega|$。取 $j=l=3$ 并应用 (4.4)，得到

$$\frac{|3\Omega-3\Omega|}{|\Omega|}\le\left(\frac{|\Omega-\Omega|}{|\Omega|}\right)^6\le N^{144(1/2-\theta)+o(1)}.\tag{4.5}$$

接下来，我们选取 A中的元素，这些元素出现在 Ω 中各点的许多种表示中。$\Omega \subseteq \mathcal{T}$ 中的每个点至少有一种这样的表示，因此

$$\begin{aligned}&\sum_{a\in A}\#\{(u,v)\in A^2:(a+u+v,a^3+u^3+v^3)\in\Omega\}\\&=\sum_{P\in\Omega}\#\{(a,u,v)\in A^3:(a+u+v,a^3+u^3+v^3)=P\}\geq|\Omega|.\end{aligned}$$

丢弃伙伴对少于 $|\Omega|/(2|A|)$的元素 a 。这样至多丢弃$|A|\cdot|\Omega|/(2|A|)=|\Omega|/2$ 个三元组。因此，至少还剩下 $|\Omega|/2$ 个三元组。

选择在剩余三元组中出现次数最多的 $(u_0,\ v_0)\in A^2$ 。于是

$$\begin{aligned}\frac{|\Omega|}{2}&\leq\sum_{(u,v)\in A^2}\#\{a\in A:(a,u,v)\text{ remains}\}\\&\leq|A|^2\max_{(u,v)\in A^2}\#\{a\in A:(a,u,v)\text{ remains}\}\\&=|A|^2\#\{a\in A:(a,u_0,v_0)\text{ remains}\}.\end{aligned}$$

令 S 为它们第一坐标的集合：

$$S=\left\{a\in A:\begin{array}{l}(a+u_0+v_0,\,a^3+u_0^3+v_0^3)\in\Omega,\\ \#\{(u,v)\in A^2:(a+u+v,\,a^3+u^3+v^3)\in\Omega\}\geq\dfrac{|\Omega|}{2|A|}\end{array}\right\}.\tag{4.6}$$

使 $(u_0,\ v_0)$ 取到最大值的选择，结合 (4.6)，得到下面的第一个不等式。其余界由 (4.4) 和命题2.2) 得出。

$$\begin{aligned}&|S|\geq\frac{|\Omega|}{2|A|^2}\geq N^{3\theta/2-o(1)}|A|^{-1/2}\geq N^{3\theta/2-(1-\theta)/2-o(1)}=N^{2\theta-1/2-o(1)},\\&\frac{|A|}{|S|}\leq N^{(1-\theta)-(2\theta-1/2)+o(1)}=N^{3(1/2-\theta)+o(1)}.\end{aligned}\tag{4.7}$$

由 (4.6)，每个 $a,\ b\in S$ 都共享伙伴对 $(u_0,\ v_0)$。从 Ω 中减去对应的点，得到

$$\begin{aligned}(a-b,a^3-b^3)=&(a+u_0+v_0,\,a^3+u_0^3+v_0^3)\\&-(b+u_0+v_0,\,b^3+u_0^3+v_0^3)\in\Omega-\Omega.\end{aligned}\tag{4.8}$$

□

引理 4.2。设 A、θ 如引理 *4.1*中所述，并取 Ω S满足其结论。对于 N 充分大时，存在素数 $p\in[|S|/16,|S|/8]$ 和 $S'\subseteq S$，其中 $|S'|\geq 3|S|/4$，使得每个 $a\in S'$ 至少有 $|\Omega|/(4|A|)$ 个可容许伙伴对。若伙伴对 $(u,\ v)$ 对于 p 是可容许的，则称其为

$$p\nmid(u+v),\qquad\#\{n\in A:n\equiv w\pmod p\}\leq\frac{|A|}{|S|}\log^4(2N)\quad(w\in\{u,v\}).\tag{4.9}$$

证明。令 p 遍历 $[|S|/16,\,|S|/8]$中的素数，并记 $\sum_p 1$ 为它们的个数。由引理 4.1，$|S|\geq N^{2\theta-1/2-o(1)}$。由于 $2\theta-1/2>0$，所有这些素数都满足

$p \geq |S|/16 > 3$ 一旦 N 足够大。素数定理指出

$$\pi(x) := \#\{q \leq x : q \text{ is prime}\} \sim \frac{x}{\log x} \qquad (x \to \infty).$$

因此

$$\begin{aligned} \sum_p 1 &= \pi(|S|/8) - \pi(|S|/16) + \#\{q : q = |S|/16,\ q \text{ is prime}\} \\ &= \left(\frac{1}{8} - \frac{1}{16} + o(1)\right) \frac{|S|}{\log|S|} \sim \frac{|S|}{16\log|S|} \gg \frac{|S|}{\log(2N)} \qquad (|S| \leq N). \end{aligned} \tag{4.10}$$

设 j 是一个满足 $0 < |j| \leq 2N$ 的整数。其互不相同的素因子的乘积整除 $|j|$，且每个素数都至少为 2。因此

$$2^{\#\{p:p|j\}} \leq \prod_{p|j} p \leq |j| \leq 2N.$$

取对数并应用（4.10），可得

$$\#\{p : p \mid j\} \leq \log_2(2N) \ll \frac{\log^2(2N)}{|S|} \sum_p 1. \tag{4.11}$$

对每个 $w \in A$,

$$\begin{aligned} &\sum_p \#\{n \in A : n \equiv w \pmod p\} = \sum_{n\in A} \#\{p : p \mid (n-w)\} \\ &= \underbrace{\sum_p 1}_{n=w} + \sum_{n\in A\setminus\{w\}} \#\{p : p \mid (n-w)\} \\ &\overset{(4.11)}{\ll} \left(1 + (|A|-1)\frac{\log^2(2N)}{|S|}\right) \sum_p 1 \qquad (0 < |n-w| \leq N-1 \text{ if } n \neq w) \\ &\ll \frac{|A|}{|S|} \log^2(2N) \sum_p 1 \qquad (|S| \leq |A|). \end{aligned} \tag{4.12}$$

若 $\#\{n \in A : n \equiv w \text{(模 } p)\} > (|A|/|S|)$ 对数$^4(2N)$，则该素数对 $(|A|/|S|)$ 对数$^4(2N)$ 中的和贡献超过（4.12）。将该和除以阈值，得到

$$\begin{aligned} &\#\big\{p : \#\{n \in A : n \equiv w \pmod p\} > (|A|/|S|)\log^4(2N)\big\} \\ &\leq \frac{\sum_p \#\{n \in A : n \equiv w \pmod p\}}{(|A|/|S|)\log^4(2N)} \ll \frac{\sum_p 1}{\log^2(2N)}. \end{aligned} \tag{4.13}$$

一对 $(u、v)$ 不满足（4.9）当且仅当其至少有一个条件不成立。因此

$$\begin{aligned} &\{p : (u、v) \text{ 对 } p\} \text{ 而言不是可容许的} \\ &= \{p : p \mid (u+v)\} \\ &\cup \bigcup_{w\in\{u,v\}} \big\{p : \#\{n \in A : n \equiv w \pmod p\} > (|A|/|S|)\log^4(2N)\big\}. \end{aligned}$$

凡是使 $(u,\ v)$ 不可容许的素数，至少属于右侧集合中的一个。因此，将这些集合的大小相加，即可得到这类素数数量的上界

。由于 $2 \le u+v \le 2N$，(4.11) 给出 $\#\{p: \ p \mid (u+v)\} \ll (\log^2(2N)/|S|)\sum_p 1$。对于剩余类条件，将 (4.13) 对 $w \in \{u,v\}$ 求和：

$$\begin{aligned}&\sum_{w\in\{u,v\}} \#\big\{p : \#\{n\in A : n \equiv w \pmod p\} > (|A|/|S|)\log^4(2N)\big\}\\ &\le \sum_{w\in\{u,v\}} \frac{\sum_p \#\{n\in A : n\equiv w \pmod p\}}{(|A|/|S|)\log^4(2N)} \ll \frac{\#\{u,v\}}{\log^2(2N)}\sum_p 1.\end{aligned}$$

由于 $\#\{u,v\} \le 2$，w 至多有两个取值。结合这些估计，我们得到 $\#\{p: \ (u, \ v)$ 对于 $p\}$ 而言不是可容许的

$$\begin{aligned}&\le \#\{p : p \mid (u+v)\}\\ &\quad + \sum_{w\in\{u,v\}} \#\big\{p : \#\{n\in A : n\equiv w \pmod p\} > (|A|/|S|)\log^4(2N)\big\}\\ &\ll \left(\frac{\log^2(2N)}{|S|} + \frac{2}{\log^2(2N)}\right)\sum_p 1 = o(1)\sum_p 1.\end{aligned} \tag{4.14}$$

最终的 o（1）由引理 $|S|$ 4.1 中的下界得到。该下界关于（u, v）$\in A^2$是一致的。

固定 $a \in S$。对其配对求和，交换两个有限和的次序，得到

$$\begin{aligned}&\sum_p \#\{(u,v)\in A^2 : (u,v) \text{ partners } a \text{ and is inadmissible for } p\}\\ &= \sum_{\substack{(u,v)\in A^2\\ (a+u+v,a^3+u^3+v^3)\in\Omega}} \#\{p : (u,v) \text{ is not admissible for } p\}\\ &\le o(1)\Big(\sum_p 1\Big)\#\{(u,v)\in A^2 : (a+u+v, a^3+u^3+v^3)\in\Omega\}.\end{aligned} \tag{4.15}$$

如果 a 的伙伴对中有超过一半对于素数 p是不合容的，那么其贡献超过伙伴对总数的一半。将求和限制在这些素数上，得到

$$\begin{aligned}&\tfrac{1}{2}\#\{(u,v)\in A^2 : (a+u+v, a^3+u^3+v^3)\in\Omega\}\\ &\qquad \times \#\left\{p : \begin{smallmatrix}\text{more than half of the pairs for } a\\ \text{are inadmissible for } p\end{smallmatrix}\right\}\\ &\le \sum_{\substack{p:\text{ more than half of the pairs for } a\\ \text{are inadmissible for } p}} \#\left\{(u,v)\in A^2 : \begin{smallmatrix}(u,v) \text{ partners } a,\\ (u,v) \text{ is inadmissible for } p\end{smallmatrix}\right\}\\ &\le \sum_p \#\{(u,v)\in A^2 : (u,v) \text{ partners } a \text{ and is inadmissible for } p\}.\end{aligned}$$

根据假设，a 至少有 $|\Omega|/(2|A|) > 0$ 个伙伴对。应用（4.15并除以伙伴对总数的一半，得到

(4.16) $\#\{p: \text{对于 } a, \text{超过一半的数对对于 } p\} \le o(1)\sum 1_p$是不合容的

对4.16) 求和 $a \in S$ 可得，对于充分大的 N,

$$\sum \#\{a \in S: \text{ 其数对中超过一半是不合容的，对于 } p\}_p = \sum_{a\in S} \#\{p: \ a \text{ 的数对中超过一半是不合容的，对于 } p\} < \frac{|S|}{4}\sum_p 1.$$

因此，至少存在一个素数 p，使得少于 $|S|/4$ 个元素 $a \in S$ 对应的配对中，超过一半是不合容的。固定这个素数。保留配对中至少一半可容许的元素，并记

$$S' = \{a \in S : \text{at least half of its partner pairs are admissible for } p\}.$$

B由 p 的选取以及配对数下界的假设可知,

$$\begin{aligned} &|S'| \geq \frac{3}{4}|S|, \\ &\#\{(u,v) \in A^2 : (u,v) \text{ is an admissible partner pair of } a\} \geq \frac{|\Omega|}{4|A|} \quad (a \in S'). \end{aligned} \tag{4.17}$$

□

命题 *2.5*。设 $13/27 < \theta < 1/2$，且令 N 充分大。若非空集合$A \subseteq \{1,\dots,N\}$满足 $I_8(\mathbf{1}_A) \geq N^\theta |A|^4$，则存在一个素数 p、一个尺度 $X = 2^j$（其中 j 为非负整数）以及一个非空集合

$$E \subseteq \left\{ \left(\frac{a-b}{p}, \frac{a^3-b^3}{p}\right) : \begin{array}{l} a,b \in A,\ a>b,\ p \mid (a-b), \\ X \leq (a-b)/p < 2X \end{array} \right\}$$

使得

$$|E| \geq N^{2\theta - 1/2 - o(1)}.$$

对于每个整数 $1 \leq H \leq X$，将 $[X, 2X)$ 划分为

$$I_j = [X + jH,\ \min\{X + (j+1)H,\ 2X\}), \qquad j = 0, \dots, \lceil X/H \rceil - 1.$$

如果 h_0 是使 $\#\{(h,k) \in E: h \in I_j\}$ 最大化的某个区间的左端点，那么非空集

$$B = \{(h,k) \in E : h_0 \leq h < h_0 + H\}$$

满足

$$\frac{|B-B|}{|B|} \leq N^{153(1/2-\theta)+o(1)}.$$

p, X, E 的选取与 H 无关，并且该界关于 H 以及最大化区间的选取是一致的。

命题 *2.5*的证明。根据引理 S，选取 $(u_0,\ v_0)$，由引理 4.1，于是 p，S' 由引理 4.2。对于这个素数 p，对 S' 的剩余类计数并应用柯西–施瓦茨不等式，可得

$$\sum_{j=0}^{p-1} \#\{a \in S' : a \equiv j \pmod p\} = |S'|, \quad \sum_{j=0}^{p-1} \big(\#\{a \in S' : a \equiv j \pmod p\}\big)^2 \geq \frac{|S'|^2}{p}.$$

一对 $(a,\ b)$ 满足 $p \mid (a-b)$，当且仅当两个元素属于同一个剩余类。因此

$$\#\{(a,b) \in (S')^2 : p \mid (a-b)\} = \sum_{j=0}^{p-1} \big(\#\{a \in S' : a \equiv j \pmod p\}\big)^2.$$

对角点对为（$a,\ a$），每个 $a \in S'$ 对应一个。移除这些 $|S'|$ 对后，交换坐标将剩余情形 $a > b$ 和 $a < b$ 配对：

$$\{(a,b) \in (S')^2 : a > b,\ p \mid (a-b)\} \longrightarrow \{(a,b) \in (S')^2 : a < b,\ p \mid (a-b)\},$$
$$(a,b) \longmapsto (b,a).$$

该映射保持整除条件，因为 $p \mid (a-b) \iff p \mid (b-a)$，且应用两次后会返回原数对。因此，恰好一半的非对角点对具有 $a > b$。于是

$$\begin{aligned}
&\#\{(a,b) \in (S')^2 : a > b,\ p \mid (a-b)\} \\
&= \frac{1}{2}\left(\sum_{j=0}^{p-1} \big(\#\{a \in S' : a \equiv j \pmod p\}\big)^2 - |S'|\right) \\
&\geq \frac{1}{2}\left(\frac{|S'|^2}{p} - |S'|\right) \geq \frac{1}{2}\left(\frac{(3|S|/4)^2}{|S|/8} - |S|\right) = \frac{7}{4}|S|.
\end{aligned}$$

在最后一个不等式中，我们使用了 $p \leq |S|/8$ 和 $3|S|/4 \leq |S'| \leq |S|$（见4.17）以及 $S' \subseteq S$。引理3.1 说明，一个弦点能够唯一确定其端点。因此映射

$$(a,b) \longmapsto \left(\frac{a-b}{p}, \frac{a^3-b^3}{p}\right) \qquad (a,b \in S',\ a > b,\ p \mid (a-b))$$

是单射的。

由于

$$\{1,\dots,N\} \subseteq \bigcup_{j=0}^{\lfloor \log_2 N \rfloor} [2^j, 2^{j+1}),$$

抽屉原理给出了一个尺度 $X = 2^j$，使得集合

$$E = \left\{ \left(\frac{a-b}{p}, \frac{a^3-b^3}{p}\right) : \begin{array}{l} a,b \in S',\ a > b,\ p \mid (a-b), \\ X \leq (a-b)/p < 2X \end{array} \right\}$$

满足下面的第一个不等式。第二个不等式由（4.7）得出。

$$|E| \geq \frac{7|S|}{4(1+\lfloor \log_2 N \rfloor)} \geq N^{2\theta - 1/2 - o(1)}. \tag{4.18}$$

保持 p、X、E 不变。现在我们对水平坐标进行局部化。对于任意整数 $1 \leq H \leq X$，将 $[X, 2X)$ 划分为半开区间

$$I_j = [X + jH,\ \min\{X + (j+1)H,\ 2X\}), \qquad j = 0,\dots,\lceil X/H \rceil - 1.$$

在每个区间 I_j 中，我们统计满足 $h \in I_j$ 的点，即

$$(h,k) = \left(\frac{a-b}{p}, \frac{a^3-b^3}{p}\right) \in E, \qquad a,b \in S', \quad a > b, \quad p \mid (a-b).$$

选择一个包含 E 中最多点的区间 I_j，并将其左端点记为 h_0。由于对于每个 $(h,k)\in E$，都有 $h<2X$，该区间内的点构成集合

$$B=\{(h,k)\in E: h_0\le h<h_0+H\},\qquad |B|=\max_j \#\{(h,k)\in E: h\in I_j\}.$$

利用

$$|E|=\sum_j \#\{(h,k)\in E: h\in I_j\}\le \lceil X/H\rceil\,|B|\le (2X/H)|B|$$

我们得到

$$h_0\ge X,\qquad |B|\ge \frac{H}{2X}|E|. \tag{4.19}$$

从空集开始，每次选取一个点 $z=(h,\ k)\in E$。在每一步中，要求其水平坐标与此前选取的每个坐标之差都大于 $2H$。当无法再添加点时停止。由于 E 是有限集，该过程必然停止。将所得集合记为 $T\subseteq E$；于是

$$|c_1-c_1'|>2H\qquad \big(c=(c_1,c_2),\ c'=(c_1',c_2')\in T,\ c\ne c'\big). \tag{4.20}$$

设 $z=(h,\ k)\in E\setminus T$。如果对每个 $c=(c_1,\ c_2)\in T$，都有 $|h-c_1|>2H$，那么我们就可以添加 z，这与停止规则矛盾。因此，存在某个 $c\in T$ 满足 $|h-c_1|\le 2H$。对于 $z\in T$，取 $c=z$。这就证明了覆盖

$$E=\bigcup_{c=(c_1,c_2)\in T}\{(h,k)\in E: c_1-2H\le h\le c_1+2H\}.$$

固定 $c=(c_1,\ c_2)\in T$。我们估算这个中心覆盖了 E 中多少个点。由于 $c_1\in[X,2X)$，区间 $[c_1-2H,c_1+2H]$ 至少与一个 I_j 相交。设 j_- 和 j_+ 分别是它所相交区间的最小和最大指标。这些指标连续：

$$I_{j_-},\ I_{j_-+1},\ \dots,\ I_{j_+}.$$

取 $x_-\in I_{j_-}\cap[c_1-2H,c_1+2H]$ 和 $x_+\in I_{j_+}\cap[c_1-2H,c_1+2H]$。对于 $j_-<j<j_+$，区间 I_j 并非可能缩短的最终区间，因为 $j<\lceil X/H\rceil-1$。此外，

$$c_1-2H\le x_-<X+jH<X+(j+1)H\le x_+\le c_1+2H.$$

因此，每个满足 $j_-<j<j_+$ 的区间 $I_j=[X+jH,X+(j+1)H)$ 都包含在 $[c_1-2H,c_1+2H]$ 内，且长度为 H。这些区间两两不相交。若 $j_+-j_-\ge 2$，它们的总长度至多为 $4H$：

$$(j_+-j_--1)H=\sum_{j_-<j<j_+} H\le (c_1+2H)-(c_1-2H)=4H.$$

计入 I_{j_-} 和 I_{j_+} 后，总共有 $j_+-j_-+1\le 6$ 个区间。若 $j_+-j_-\le 1$，则至多有两个。根据 B的选取，每个区间至多包含 $|B|$ 个点，因此

$$\begin{aligned}\#\{(h,k)\in E:|h-c_1|\le 2H\}&\le \sum_{j=j_-}^{j_+}\#\{(h,k)\in E: h\in I_j\}\\&\le (j_+-j_-+1)|B|\le 6|B|.\end{aligned}$$

以 $c \in T$ 为中心的集合覆盖了 E。对它们的界求和，并利用（4.18），我们得到

$$|E| \le 6|T||B|, \qquad |T||B| \ge \frac{|E|}{6} \ge |S|N^{-o(1)}. \tag{4.21}$$

根据 E 的定义，每个 $z=(h,k) \in E$ 都来自一对 $a,b \in S'$。引理3.1中的端点唯一性保证了这对点的唯一性。其端点满足

$$a > b, \qquad p \mid (a-b), \qquad h = \frac{a-b}{p}, \quad k = \frac{a^3-b^3}{p}.$$

对于中心 $c=(c_1,c_2) \in T \subseteq E$，将这些端点记为 $a_c > b_c$。于是

$$pc = (pc_1, pc_2) = (a_c - b_c,\ a_c^3 - b_c^3).$$

由于 $S' \subseteq S$，(4.6) 给出 $(x+u_0+v_0,\ x^3+u_0^3+v_0^3) \in \Omega$，对每个 $x \in S'$ 均成立。将此结果用于$x=a$ 和 $x=b$，并如 (4.8) 中那样相减：

$$\begin{aligned} pz = (a-b,\ a^3-b^3) &= (a+u_0+v_0,\ a^3+u_0^3+v_0^3) \\ &\quad - (b+u_0+v_0,\ b^3+u_0^3+v_0^3) \in \Omega - \Omega. \end{aligned}$$

对于 $w \in B-B$，取 $z,z' \in B \subseteq E$，使得 $w=z-z'$。将 z 的端点记为 $a>b$，并将 z' 的端点记为 $a'>b'$。将 (4.8) 应用于 pz 和 pz'，并将正项和负项分组，得到

$$\begin{aligned} pw = pz - pz' &= (a+u_0+v_0,\ a^3+u_0^3+v_0^3) + (b'+u_0+v_0,\ b'^3+u_0^3+v_0^3) \\ &\quad - (b+u_0+v_0,\ b^3+u_0^3+v_0^3) - (a'+u_0+v_0,\ a'^3+u_0^3+v_0^3) \\ &\in 2\Omega - 2\Omega. \end{aligned} \tag{4.22}$$

固定中心 $c \in T$ 以及 a_c的一个可容许伙伴对 $(u,\ v)$。我们按其和及立方和模 p 对这类数对分组。记 ρ为剩余类的有序数对

$$\rho_1 := (u+v) + p\mathbb{Z}, \qquad \rho_2 := (u^3+v^3) + p\mathbb{Z},$$
$$\rho := (\rho_1, \rho_2) \in (\mathbb{Z}/p\mathbb{Z})^2.$$

条件 $\rho_1 = 0$ 等价于 $u+v \equiv 0$ (模 p)。由 (4.9) 中的可容许性可得$p \nmid (u+v)$，因此 $\rho_1 \neq 0$。利用 $(u+v)^3 - u^3 - v^3 = 3uv(u+v)$，得到 $3uv\rho_1 \equiv \rho_1^3 - \rho_2$(模 p)。由于 $p>3$，我们可以在 $\mathbb{Z}/p\mathbb{Z}$中除以 $3\rho_1$。因此

$$uv \equiv \frac{\rho_1^3 - \rho_2}{3\rho_1} \pmod p.$$

系数取自 $\mathbb{Z}/p\mathbb{Z}$且未定元为 Z时，得到

$$(Z-u)(Z-v) = Z^2 - (u+v)Z + uv = Z^2 - \rho_1 Z + \frac{\rho_1^3 - \rho_2}{3\rho_1}.$$

一旦 ρ 确定，二次多项式也随之确定。它的根至多给出两个有序剩余类对：根不同时有两种排列，根相同时有一种排列。对于每一组有序剩余类，(4.9) 至多允许 $(|A|/|S|)\log^4(2N)$ 个整数值分别对应于 u 和 v。因此，对所有中心而言，具有此 ρ的不同有序整数对 (u,v) 总数至多为

$$2\left(\frac{|A|}{|S|}\log^4(2N)\right)^2. \tag{4.23}$$

对于每个出现的 ρ，在这些剩余类中选取一个整数对 (u_ρ, v_ρ)，使其作为可接受伙伴对对应尽可能多的中心。因此，它使

$$\#\{c \in T : (u_\rho, v_\rho) \text{ is an admissible partner pair of } a_c\}.$$

称一个中心 c 在此集合中计数，且与 ρ相容。为每个 ρ选择一个整数对之前，(4.17)给出了三元组(c, u, v)的如下计数:

$$\sum_{c\in T} \#\{(u,v) \in A^2 : (u,v) \text{ is an admissible partner pair of } a_c\} \geq \frac{|T||\Omega|}{4|A|}. \tag{4.24}$$

按 ρ对三元组分组，再按整数对(u, v)分组。在ρ, u, v固定的组内，各中心 c互不相同。整数对(u_ρ, v_ρ)所在的 ρ组中的中心数至少达到平均数。将每组中的三元组计数除以界(4.23)，然后对 ρ 求和并使用(4.24)，得到

$$\begin{aligned} \#\{(\rho, c) : c \in T \text{ is compatible with } \rho\} &\geq \frac{|T||\Omega|}{4|A|} \frac{1}{2\big((|A|/|S|)\log^4(2N)\big)^2} \\ &\geq N^{-o(1)} \frac{|T||\Omega||S|^2}{|A|^3}. \end{aligned} \tag{4.25}$$

对于每个相容的(ρ, c)以及每个 $w \in B - B$，关联整数点

$$(u_\rho + v_\rho,\ u_\rho^3 + v_\rho^3) + p(c + w). \tag{4.26}$$

由于 $pc = (a_c - b_c, a_c^3 - b_c^3)$，我们有

$$\begin{aligned} &(u_\rho + v_\rho, u_\rho^3 + v_\rho^3) + pc \\ &\quad = (a_c + u_\rho + v_\rho,\ a_c^3 + u_\rho^3 + v_\rho^3) \\ &\qquad - (b_c + u_0 + v_0,\ b_c^3 + u_0^3 + v_0^3) + (u_0 + v_0,\ u_0^3 + v_0^3). \end{aligned}$$

相容性给出了 Ω 中涉及 a_c的点。包含关系 $b_c \in S' \subseteq S$ 给出了涉及 b_c的点，而(4.22)给出了关于 pw的条件:

$$\begin{gathered} (a_c + u_\rho + v_\rho, a_c^3 + u_\rho^3 + v_\rho^3) \in \Omega, \\ (b_c + u_0 + v_0, b_c^3 + u_0^3 + v_0^3) \in \Omega, \qquad pw \in 2\Omega - 2\Omega. \end{gathered}$$

因此，由（4.26）构造的每个点都属于

$$(u_0 + v_0,\ u_0^3 + v_0^3) + (3\Omega - 3\Omega).$$

我们断言（4.26）中的映射是单射。设（ρ，c，w）和（ρ'，c'，w'）对应同一个点。先对 p取模即可确定 ρ，随后所选的整数对便唯一确定:

$$\begin{aligned} &(u_\rho + v_\rho, u_\rho^3 + v_\rho^3) + p(c + w) \\ &\quad = (u_{\rho'} + v_{\rho'}, u_{\rho'}^3 + v_{\rho'}^3) + p(c' + w') \\ &\implies \quad \rho = \rho' \quad \implies \quad (u_\rho, v_\rho) = (u_{\rho'}, v_{\rho'}) \\ &\implies \quad c + w = c' + w'. \end{aligned}$$

由于 w，$w' \in B - B$ 以及 $B \subseteq [h_0, h_0 + H] \times \mathbb{Z}$，

$$|c_1 - c_1'| = |w_1' - w_1| \leq |w_1'| + |w_1| \leq 2H.$$

由（4.20），T 中的不同中心的水平坐标相距超过 $2H$。因此$c = c'$，进而 $w = w'$。这证明了单射性。由于平移不会改变集合的大小，我们得到

$$\#\{(\rho, c) : c \in T \text{ is compatible with } \rho\}\,|B - B| \le |3\Omega - 3\Omega|. \tag{4.27}$$

将 (4.25) 代入 (4.27)，再除以 $|B|$，得到下面的第一行。对于第二行，利用 (4.21) 对 $|T||B|$作界。对于最后一行，利用 (4.5) 和 (4.7)。

$$\begin{aligned}\frac{|B-B|}{|B|} &\le N^{o(1)}\frac{|3\Omega-3\Omega|}{|\Omega|}\frac{|A|^3}{|T||B||S|^2}\\ &\le N^{o(1)}\frac{|3\Omega-3\Omega|}{|\Omega|}\left(\frac{|A|}{|S|}\right)^3\\ &\le N^{(144+3\cdot3)(1/2-\theta)+o(1)} = N^{153(1/2-\theta)+o(1)}.\end{aligned} \tag{4.28}$$

我们先选取 p，X，E，然后再选取 H。该论证适用于每个整数 $1 \le H \le X$以及包含 E 中点数最多的每个区间，并且具有相同的一致界。这就证明了命题2.5。□

命题 *2.6*。设 $1/2 - 1/1550 < \theta < 1/2$，并设 N 充分大。假设一个非空集合 $A \subseteq \{1, \dots, N\}$满足 $I_8(\mathbf{1}_A) \ge N^\theta |A|^4$。设 p，X，E如命题2.5中所述。则

$$X \ge N^{1/2-155(1/2-\theta)-o(1)}.$$

当 N 足够大时，该整数

$$H = \lfloor XN^{-2/5} \rfloor$$

满足 s $1 \le H \le XN^{-2/5}$。在此宽度下，集合 B 在命题 2.5 中选取，满足

$$|B| \ge N^{2\theta-9/10-o(1)}.$$

其水平坐标位于 $[h_0, h_0 + H]$ 中，其中 $h_0 \ge X$，并且

$$B \subseteq \left\{\left(\frac{a-b}{p}, \frac{a^3-b^3}{p}\right) : a, b \in A,\ a > b,\ p \mid (a-b)\right\}.$$

F对于同一集合 B，命题2.5中的差集估计仍然成立 .

命题 *2.6* 的证明。由于 $1/2 - 1/1550 > 13/27$，命题 2.5 适用。固定p、X、E，如该命题中所述。我们首先从下方估计 X。对于每个整数 $1 \le H \le X$，选择包含最多点的区间可得到集合 B，其满足（4.28）。取 $H = X$。于是只有一个区间，$[X, 2X)$，因此 $B = E$ 且

$$|E - E|/|E| \le N^{153(1/2-\theta)+o(1)}.$$

共有 X 个可能的水平坐标，且 $\sum_{h=X}^{2X-1} \#\{k : (h,\ k) \in E\} = |E|$。因此，柯西–施瓦茨不等式给出了同一列中数对数量的下界。

按垂直差 t 对这些数对进行分组，得到

$$\begin{aligned}\frac{|E|^2}{X} &\le \sum_{h=X}^{2X-1}\big(\#\{k:(h,k)\in E\}\big)^2\\ &= |E| + \sum_{\substack{t\neq 0\\ (0,t)\in E-E}} \#\{(h,k)\in E:(h,k+t)\in E\}\\ &\le |E| + N^{o(1)}|E-E|.\end{aligned}$$

这里，纵坐标相等的数对贡献 $|E|$。对于每个非零 t，引理 3.1通过 (3.1，将数对的数量界定为 $N^{o(1)}$。具体而言，

$$\begin{gathered}\#\{((h,k),(h,k'))\in E^2 : k'=k\} = |E|,\\ \#\{(h,k)\in E:(h,k+t)\in E\}\le N^{o(1)} \qquad (t\neq 0),\\ \#\{t\neq 0:(0,t)\in E-E\}\le |E-E|.\end{gathered}$$

将 列计数除以 $|E|>0$，然后结合 (4.18) 和 (4.28)，取 $B=E$。由此得到

$$\begin{aligned}X &\ge \frac{|E|}{1+N^{o(1)}|E-E|/|E|}\\ &\ge N^{2\theta-1/2-153(1/2-\theta)-o(1)} = N^{1/2-155(1/2-\theta)-o(1)}.\end{aligned} \tag{4.29}$$

由于 $\theta > 1/2 - 1/1550$,

$$\frac{1}{2} - 155\left(\frac{1}{2}-\theta\right) > \frac{1}{2} - \frac{155}{1550} = \frac{2}{5}.$$

由 (4.29)， $XN^{-2/5}\ge N^{1/10-155(1/2-\theta)-o(1)}$。固定指数 $1/10-155(1/2-\theta)$ 为正，因此 $XN^{-2/5}\to\infty$。现在我们可以取 $H=\lfloor XN^{-2/5}\rfloor$。当 N足够大，使得 $XN^{-2/5}\ge 2$ 时，

$$1\le \tfrac{1}{2}XN^{-2/5}\le XN^{-2/5}-1\le H\le XN^{-2/5}\le X.$$

在此宽度下，选取一个包含 E中最多点的区间，并令B 由这些点组成。界（4.19）和（4.18）给出

$$|B|\ge \frac{H}{2X}|E|\ge \tfrac{1}{4}N^{-2/5}|E|\ge N^{2\theta-1/2-2/5-o(1)} = N^{2\theta-9/10-o(1)}.$$

对于同一个 B，估计式（4.28）仍然成立。其水平坐标位于 $[h_0,h_0+H]$ 中，其中 $h_0\ge X$，且所有端点都位于 A 中。这就证明了该命题。 □

5. Integer chords and the reduction to indicator functions

命题 5.1。 固定一个整数 $r \geq 2$ 和一个实数 $\kappa \geq 1$。令 $N \geq 2$，并令$B \subseteq \mathbb{Z}^2$非空，其中每个点（h， k）都满足 $1 \leq h \leq N^{\kappa}$， $|k| \leq N^{\kappa}$， $h \mid k$。记 $B - B = \{z - z' : z,\ z' \in B\}$。如果所有水平坐标都位于 $[h_0, h_0 + H]$中，其中 $1 \leq H \leq X \leq h_0$，那么对于每个 $\varepsilon > 0$，存在一个常数$C_{\kappa,\ r,\ \varepsilon} \geq 1$，其仅取决于 κ， r， ε，使得

$$
\begin{aligned}
|B| \leq C_{\kappa,r,\varepsilon} N^{\varepsilon} \Bigg(& \max_{q \in \mathbb{Z}} \#\{(h,k) \in B : k = qh\} \\
& + \max_{t \in \mathbb{Z} \setminus \{0\}} \#\{(h,k) \in B : (h, k+t) \in B\} \\
& + (H/X)^r \max_{(h,k) \in B} \left| \frac{k}{h} \right| \Bigg) \left(\frac{|B - B|}{|B|} \right)^{2^r - 1}.
\end{aligned} \tag{5.1}
$$

B中的有序加法立方体由一个基点（h， k）和 r 个方向（s_i， t_i） $\in \mathbb{Z}^2$ 组成，并满足

$$
\left(h + \sum_{i \in J} s_i,\ k + \sum_{i \in J} t_i \right) \in B \qquad \big(J \subseteq \{1, \ldots, r\}\big).
$$

我们约定空和为零，并允许零方向和重复顶点。方向固定后，如果所有这些顶点都位于 B 中，则称（h， k）为可容许的。在每个可容许基点处，考虑

$$
\ell(h,k) = \sum_{J \subseteq \{1,\ldots,r\}} (-1)^{r - |J|} \frac{k + \sum_{i \in J} t_i}{h + \sum_{i \in J} s_i}. \tag{5.2}
$$

比较 ℓ（h， k）和 ℓ（h'， k'）时，我们始终固定方向。

引理 5.2。 在命题 *5.1*的假设下，固定 r 个方向，并在可容许基点上使用 (5.2)。 的值均为整数，且不同值的数量至多为

$$
1 + \left\lfloor 2(H/X)^r \max_{(x,y) \in B} |y/x| \right\rfloor.
$$

证明。 每个顶点都属于 B，因此其水平坐标整除其垂直坐标。特别地，

$$
\frac{k + \sum_{i \in J} t_i}{h + \sum_{i \in J} s_i} \in \mathbb{Z} \quad (\forall J) \quad \Longrightarrow \quad \ell(h,k) \in \mathbb{Z}.
$$

We 首先界定 $\ell(h,\ k)$ 的变化范围。从有限等比级数恒等式开始

$$
(1 - x) \sum_{j=0}^{r-1} x^j = \sum_{j=0}^{r-1} (x^j - x^{j+1}) = 1 - x^r.
$$

代入 $x = 1 - h/(h_0 + H/2)$ 得

$$
1 = \frac{h}{h_0 + H/2} \sum_{j=0}^{r-1} \left(1 - \frac{h}{h_0 + H/2} \right)^j + \left(1 - \frac{h}{h_0 + H/2} \right)^r.
$$

等式两边乘以 k/h 得

$$\frac{k}{h} = \frac{k}{h_0 + H/2} \sum_{j=0}^{r-1} \left(1 - \frac{h}{h_0 + H/2}\right)^j + \frac{k}{h} \left(1 - \frac{h}{h_0 + H/2}\right)^r. \tag{5.3}$$

由于

$$h_0 \le h \le h_0 + H \quad \Longrightarrow \quad -H/2 \le h - (h_0 + H/2) \le H/2$$

我们得到

$$\left|1 - \frac{h}{h_0 + H/2}\right| = \frac{|h - (h_0 + H/2)|}{h_0 + H/2} \le \frac{H/2}{h_0 + H/2} = \frac{H}{2h_0 + H}.$$

每个顶点的水平坐标都位于同一个区间内，因此此界对所有顶点都成立。

展开式 k/h 的第一项是关于 h, k 的多项式:

$$\frac{k}{h_0 + H/2} \sum_{j=0}^{r-1} \left(1 - \frac{h}{h_0 + H/2}\right)^j = \sum_{j=0}^{r-1} \sum_{a=0}^{j} \binom{j}{a} \frac{(-1)^a h^a k}{(h_0 + H/2)^{a+1}}.$$

$$0 \le a \le j \le r-1 \quad \Longrightarrow \quad \deg(h^a k) = a + 1 \le r,$$
$$a + 1 = r \iff a = j = r - 1.$$

对于函数 G，记 $\Delta_{(s,t)} G(h,k) = G(h+s, k+t) - G(h,k)$。对于单项式，二项式定理给出

$$\Delta_{(s,t)}(h^a k^b) = \sum_{\substack{0 \le i \le a,\ 0 \le j \le b \\ (i,j) \ne (a,b)}} \binom{a}{i} \binom{b}{j} h^i k^j s^{a-i} t^{b-j}.$$

$$(i,j) \ne (a,b) \quad \Longrightarrow \quad i + j \le a + b - 1 \quad \Longrightarrow \quad \deg \Delta_{(s,t)} G \le \deg G - 1$$

这里的次数比较仅针对非零多项式进行。逐项展开这些差值可得

$$\Delta_{(s_r,t_r)} \cdots \Delta_{(s_1,t_1)} G(h,k) = \sum_{J \subseteq \{1,\dots,r\}} (-1)^{r-|J|} G\left(h + \sum_{i \in J} s_i,\ k + \sum_{i \in J} t_i\right). \tag{5.4}$$

对于在积分点邻域内属于 C^r 类的 G，微积分基本定理将每个差表示为一个积分。应用 r 次链式法则可得

$$\begin{aligned} &\Delta_{(s_r,t_r)} \cdots \Delta_{(s_1,t_1)} G(h,k) \\ &\quad = \int_{[0,1]^r} \left[\prod_{i=1}^{r} (s_i \partial_h + t_i \partial_k) G\right] \left(h + \sum_{i=1}^{r} s_i y_i,\ k + \sum_{i=1}^{r} t_i y_i\right) dy_1 \cdots dy_r. \end{aligned} \tag{5.5}$$

这里， ∂_h， ∂_k 分别表示关于 h， k 的偏微分。对于 $0 \le a \le r-1$,

$$\prod_{i=1}^{r}(s_i\partial_h + t_i\partial_k)(h^a k) = \left(\prod_{i=1}^{r} s_i\right)\partial_h^r(h^a k) + \sum_{i=1}^{r} t_i \prod_{\substack{1\le j\le r\\ j\neq i}} s_j\, \partial_h^{r-1}(h^a)$$
$$= \begin{cases} 0, & a < r-1, \\ (r-1)!\displaystyle\sum_{i=1}^{r} t_i \prod_{\substack{1\le j\le r\\ j\neq i}} s_j, & a = r-1. \end{cases}$$

由（5.5）可知，只有 $h^{r-1}k$ 在（5.3）的多项式部分中的项有贡献。利用二项式展开中的系数可得

$$\Delta_{(s_r,t_r)}\cdots\Delta_{(s_1,t_1)}\left[\frac{k}{h_0+H/2}\sum_{j=0}^{r-1}\left(1-\frac{h}{h_0+H/2}\right)^j\right]$$
$$= \frac{(-1)^{r-1}(r-1)!}{(h_0+H/2)^r}\sum_{i=1}^{r} t_i \prod_{\substack{1\le j\le r\\ j\neq i}} s_j.$$

此表达式仅取决于方向。因此，在两个交错和（5.2）之差中，多项式项相消，留下（5.3）中的余项。

对于任意顶点（u， v） $\in B$，余式满足

$$\left|\frac{v}{u}\left(1-\frac{u}{h_0+H/2}\right)^r\right| \le \left(\frac{H}{2h_0+H}\right)^r \max_{(x,y)\in B}\left|\frac{y}{x}\right|. \tag{5.6}$$

由此，三角不等式给出

$$|\ell(h',k') - \ell(h,k)| \le \sum_{J\subseteq\{1,\dots,r\}}\left|\frac{k'+\sum_{i\in J}t_i}{h'+\sum_{i\in J}s_i}\right|\left|1-\frac{h'+\sum_{i\in J}s_i}{h_0+H/2}\right|^r$$
$$+\sum_{J\subseteq\{1,\dots,r\}}\left|\frac{k+\sum_{i\in J}t_i}{h+\sum_{i\in J}s_i}\right|\left|1-\frac{h+\sum_{i\in J}s_i}{h_0+H/2}\right|^r.$$

将（5.6）应用于每一项。对于每个子集 J，都有一项，即使某些顶点重合也是如此。由于

$$\#\{J : J\subseteq\{1,\dots,r\}\} = \sum_{j=0}^{r}\binom{r}{j} = 2^r, \qquad 2h_0+H \ge 2X$$

我们得到

$$\begin{aligned} |\ell(h',k') - \ell(h,k)| &\le 2^{r+1}\left(\frac{H}{2h_0+H}\right)^r \max_{(x,y)\in B}\left|\frac{y}{x}\right| \\ &= 2\left(\frac{2H}{2h_0+H}\right)^r \max_{(x,y)\in B}\left|\frac{y}{x}\right| \\ &\le 2(H/X)^r \max_{(x,y)\in B}\left|\frac{y}{x}\right|. \end{aligned} \tag{5.7}$$

假设至少存在一个可容许基点，并将 $\ell(h,k)$ 的不同整数值列为 $\ell_1 < \cdots < \ell_m$。相邻值至少相差 1，因此

$$\ell_i \in \mathbb{Z}, \qquad \ell_{i+1} - \ell_i \geq 1, \qquad m - 1 \leq \sum_{i=1}^{m-1} (\ell_{i+1} - \ell_i) = \ell_m - \ell_1$$

结合（5.7），我们得到

$$\begin{aligned} & m - 1 \leq 2(H/X)^r \max_{(x,y)\in B} |y/x|, \\ & m \leq 1 + \left\lfloor 2(H/X)^r \max_{(x,y)\in B} |y/x| \right\rfloor, \\ & 2(H/X)^r \max_{(x,y)\in B} |y/x| < 1 \quad \Longrightarrow \quad m = 1. \end{aligned} \tag{5.8}$$

若不存在可容许基点，则没有层级需要计数。若只有一层，其值可能取决于方向；它不一定为零。□

引理 5.3. 设 $B \subseteq \mathbb{Z}^2$ 为有限非空集合，并记 $C_j(B)$ 为 B 中有序的 j 维加性立方体的数量，其中包括重复顶点。对每个整数$r \geq 1$,

$$C_r(B) \geq |B|^{r+1} \left(\frac{|B|}{|B - B|} \right)^{2^r - r - 1}.$$

证明. 令 $C_0(B) = |B|$。对于固定的 j 个方向，两个可容许基点 z，z' 通过添加方向 $z' - z$构成一个（$j+1$）维立方体。反过来，每个这样的立方体都给出这两个基点。因此

$$C_{j+1}(B) = \sum_{(s_1,t_1),\ldots,(s_j,t_j)\in B-B} \left(\# \left\{ z \in B : \begin{array}{l} z + \sum_{i\in J}(s_i,t_i) \in B \\ \text{for every } J \subseteq \{1,\ldots,j\} \end{array} \right\} \right)^2.$$

j 个方向至多有 $|B-B|^j$ 种选择。由柯西–施瓦茨不等式可得下列第一个不等式，其余各行给出了归纳步骤：

$$\begin{aligned} & C_{j+1}(B) \geq \frac{C_j(B)^2}{|B-B|^j}, \\ & C_j(B) \geq |B|^{j+1} \left(\frac{|B|}{|B-B|} \right)^{2^j - j - 1} \\ & \quad \Longrightarrow \; C_{j+1}(B) \geq |B|^{j+2} \left(\frac{|B|}{|B-B|} \right)^{2(2^j - j - 1) + j}, \\ & 2(2^j - j - 1) + j = 2^{j+1} - (j+1) - 1. \end{aligned}$$

从 $C_0(B) = |B|$ 出发，归纳可得

$$C_r(B) \geq |B|^{r+1} \left(\frac{|B|}{|B-B|} \right)^{2^r - r - 1}. \tag{5.9}$$

□

命题 5.1的证明。 常数 C 仅取决于其下标中的参数，并可能随行递增。引理 5.2对每组方向给出（5.8）。我们通过统计基点和方向的数量来界定立方体的数量。接下来统计满足 $s_1 \cdots s_r \neq 0$ 的立方体。反转最后一个方向会交换它的两个相对的面：

$$\begin{aligned}&\big((h,k);(s_1,t_1),\dots,(s_r,t_r)\big)\\&\quad\longleftrightarrow \big((h+s_r,k+t_r);(s_1,t_1),\dots,(-s_r,-t_r)\big),\qquad s_r<0 \longleftrightarrow s_r>0.\end{aligned}$$

因此，只需计数满足 $s_r > 0$ 的立方体，再将结果加倍即可。固定方向和层 ℓ_0。

由（5.4）和（5.5），取 $G(h,\ k) = 1/h$ 以及 $h = x$ 可得

$$\begin{aligned}\sum_{J\subseteq\{1,\dots,r\}} \frac{(-1)^{r-|J|}}{x+\sum_{i\in J} s_i} &= (-1)^r r! \left(\prod_{i=1}^r s_i\right)\\ &\quad\cdot \int_{[0,1]^r} \left(x+\sum_{i=1}^r s_i y_i\right)^{-r-1} dy_1\cdots dy_r.\end{aligned} \tag{5.10}$$

只要在整个 $[0,1]^r$ 上都有 $x + \sum_i s_i y_i > 0$，该恒等式就成立。对于可容许基点，仿射函数 $h + \sum_i s_i y_i$ 在 $[0,1]^r$ 上的最小值在某个顶点处取得。因此

$$h+\sum_{i=1}^r s_i y_i \geq h+\sum_{s_i<0} s_i = \min_{J\subseteq\{1,\dots,r\}} \left(h+\sum_{i\in J} s_i\right) \geq h_0 > 0.$$

在（5.2）中，k 的系数是（5.10）的左端，其中 $x = h$。积分为正且 $s_1 \cdots s_r \neq 0$，因此该系数非零。于是可以解出 $\ell(h,\ k) = \ell_0$ 关于k:

$$\sum_J \frac{(-1)^{r-|J|}}{h+\sum_{i\in J} s_i} \neq 0, \qquad \ell(h,k)=\ell_0 \quad\Longrightarrow\quad k=\frac{P(h)}{Q(h)},$$

其中

$$\frac{P(x)}{Q(x)} = \frac{\ell_0 - \displaystyle\sum_{J\subseteq\{1,\dots,r\}} (-1)^{r-|J|} \frac{\sum_{i\in J} t_i}{x+\sum_{i\in J} s_i}}{\displaystyle\sum_{J\subseteq\{1,\dots,r\}} \frac{(-1)^{r-|J|}}{x+\sum_{i\in J} s_i}}. \tag{5.11}$$

约分并选择 $P,\ Q \in \mathbb{Z}[x]$ 在 $\mathbb{Q}[x]$中的互素表示，使其所有系数的最大公约数等于 1。如果该分式恒为零，则取 P =0，Q = 1。在每个可容许基点处，$Q(h) \neq 0$。顶点处的坐标界与（5.2）一起给出

$$|s_i|, |t_i| \leq 2N^\kappa, \qquad |\ell_0| \leq 2^r N^\kappa.$$

为了界定 P、Q的次数和系数，首先将（5.11）中的分子和分母分别乘以乘积

$$\prod_{J\subseteq\{1,\dots,r\}}\left(x+\sum_{i\in J}s_i\right).$$

按重数计入重复因子。所得整系数多项式的次数至多为 2^r，其系数的绝对值至多为 $N^{C_{\kappa,\,r}}$。为说明约分后仍保持这种形式的界，使用高斯引理和以下估计。若 $G(x)=\sum_{j=0}^{m}c_jx^j=c_m\prod_{i=1}^{m}(x-\alpha_i)$ 是非常数，且非零多项式 $U(x)=\sum u_jx^j\in\mathbb{Z}[x]$ 整除 G 于 $\mathbb{Z}[x]$，则

$$|\alpha_i|\le 1+\max_{j<m}|c_j/c_m|,\qquad |\text{leading coefficient of } U|\le|c_m|,$$
$$\max_j|u_j|\le 2^m|c_m|\left(1+\max_i|\alpha_i|\right)^m.$$

由此可知，P，Q 的次数至多为 2^r，且所有系数的绝对值均不超过 $N^{C_{\kappa,\,r}}$。

现在根据 Q和 ℓ_0，分三种情况讨论。

首先设 $\deg Q\ge 1$。由于 P，Q 互素，由结式恒等式可得 U，$V\in\mathbb{Z}[x]$，使得

$$\begin{aligned}&UP+VQ=\operatorname{Res}(P,Q)\neq 0,\\ &P(h)=kQ(h)\quad\Longrightarrow\quad \operatorname{Res}(P,Q)=Q(h)\big(kU(h)+V(h)\big),\\ &Q(h)\mid\operatorname{Res}(P,Q),\qquad 0<|\operatorname{Res}(P,Q)|\le N^{C_{\kappa,r}}.\end{aligned}$$

结式是 Sylvester 矩阵的行列式，因此，次数和系数的界给出了最后一个不等式。用 $\tau(m)$ 表示 $m\ge 1$ 的正因子数量。我们使用因子界

$$\tau(m)\le C_\beta m^\beta\quad(\beta>0).$$

共有 $2\tau(|\operatorname{Res}(P,Q)|)$ 个可能的非零带符号因子 v。对于每一个这样的因子，$Q(h)=v$至多有 $\deg Q$ 个解。因此

$$\begin{aligned}&\#\{h\in\mathbb{Z}:Q(h)\neq 0,\ Q(h)\mid\operatorname{Res}(P,Q)\}\\ &\qquad\le 2(\deg Q)\tau(|\operatorname{Res}(P,Q)|)\le C_{\kappa,r,\varepsilon}N^{\varepsilon}.\end{aligned}$$

每个这样的 h 至多确定一个值 $k=P(h)/Q(h)$，从而得到可容许基点数量的相同界。

接下来假设 Q 是一个非零常数，并且 $\ell_0=0$。当 $x\to+\infty$时，我们比较（5.10）的分子和分母。根据（5.10），

$$\lim_{x\to+\infty}x^{r+1}\sum_{J\subseteq\{1,\dots,r\}}\frac{(-1)^{r-|J|}}{x+\sum_{i\in J}s_i}=(-1)^r r!\prod_{i=1}^{r}s_i\neq 0.\tag{5.12}$$

对于分子，首先收集包含每个 t_i的项：

$$\sum_{J\subseteq\{1,\dots,r\}} (-1)^{r-|J|}\frac{\sum_{i\in J} t_i}{x+\sum_{i\in J} s_i} = \sum_{i=1}^{r} t_i \sum_{J\subseteq\{1,\dots,r\}\setminus\{i\}} \frac{(-1)^{r-1-|J|}}{x+s_i+\sum_{j\in J} s_j}.$$

对每个内层求和应用阶数为 $(r-1)$ 的 (5.10) 形式。当 $x > 2\sum_i |s_i|$时，这给出

$$\left|\sum_{J\subseteq\{1,\dots,r\}} (-1)^{r-|J|}\frac{\sum_{i\in J} t_i}{x+\sum_{i\in J} s_i}\right| \le \frac{2^r(r-1)!}{x^r}\sum_{i=1}^{r}|t_i|\prod_{\substack{1\le j\le r\\ j\ne i}}|s_j|. \tag{5.13}$$

由（5.12）和（5.13），（5.11）中的分母的阶为 x^{-r-1}，其分子在O（x^{-r}）时为 $\ell_0 = 0$。由于 Q 为常数，我们得到

$$\ell_0 = 0, \quad Q \text{ is constant} \quad\Longrightarrow\quad \lim_{x\to+\infty}\frac{P(x)}{x^2} = 0 \quad\Longrightarrow\quad P = 0 \text{ or } \deg P \le 1.$$

At an 可容许基点， $h \mid k$。结合 P（h）$= Qk$ 由（5.11），这给出 s

$$h \mid k, \quad P(h) = Qk \quad\Longrightarrow\quad h \mid P(h) \quad\Longrightarrow\quad h \mid P(0).$$

如果 $P(0) \neq 0$，我们可以统计 h 的可能正值，通过

$$\#\{h \ge 1 : h \mid P(0)\} = \tau(|P(0)|) \le C_{\kappa,r,\varepsilon}N^{\varepsilon}.$$

若 $P(0) = 0$，则多项式 P 是线性多项式或零多项式，并且

$$P(h) = P'(0)h, \qquad k = \frac{P'(0)}{Q}h, \qquad \frac{P'(0)}{Q} = \frac{k}{h} \in \mathbb{Z},$$

因此，所有可容许基点都位于一条经过原点、斜率为整数的直线上。其数量至多为

$$\max_{q\in\mathbb{Z}} \#\{(h,k) \in B : k = qh\}.$$

对于固定方向，这一项只在层 $\ell_0 = 0$ 出现。

最后，假设 Q 是一个非零常数，且 $\ell_0 \neq 0$。在5.12和5.13中使用5.11，此时分子趋于 ℓ_0，于是得到

$$\deg P = r+1, \qquad \frac{P(x)}{Q} = \sum_{j=0}^{r+1} a_j x^j, \qquad a_{r+1} = \frac{(-1)^r\ell_0}{r!\prod_{i=1}^{r} s_i} \neq 0. \tag{5.14}$$

取自 $P(h) \equiv Qk$，其中5.11，并在每个顶点处应用整除条件。对于每个 $J \subseteq \{1,\dots,r\}$，

$$h+\sum_{i\in J} s_i \mid k+\sum_{i\in J} t_i$$
$$\Longrightarrow\ h+\sum_{i\in J} s_i \mid P(h)+Q\sum_{i\in J} t_i,$$
$$P(h)+Q\sum_{i\in J} t_i \equiv P\left(-\sum_{i\in J} s_i\right)+Q\sum_{i\in J} t_i \pmod{h+\sum_{i\in J} s_i}.$$

因此，

$$h+\sum_{i\in J} s_i \ \Big|\ P\left(-\sum_{i\in J} s_i\right)+Q\sum_{i\in J} t_i \qquad \big(J\subseteq\{1,\dots,r\}\big). \tag{5.15}$$

右侧的表达式与 h无关：它是除以$x+\sum_{i\in J} s_i$后的余式。其大小满足

$$\left|P\left(-\sum_{i\in J} s_i\right)+Q\sum_{i\in J} t_i\right| \le N^{C_{\kappa,r}}.$$

若对某个 J，(5.15) 使 $h+\sum_{i\in J} s_i$ 成为某个固定的非零整数的正因子。每种选择都确定了 h，从而 k。因此

$$\#\{\text{admissible base points}\} \le \tau\left(\left|P\left(-\sum_{i\in J} s_i\right)+Q\sum_{i\in J} t_i\right|\right) \le C_{\kappa,r,\varepsilon}N^{\varepsilon}.$$

剩下的情况是所有这些余式都为零，且 Q 为常数并且 $\ell_0 \neq 0$。此时

$$\frac{P(-\sum_{i\in J} s_i)}{Q} = -\sum_{i\in J} t_i \qquad \big(J\subseteq\{1,\dots,r\}\big). \tag{5.16}$$

在这种情况下，我们固定基点和前 $r-1$ 个方向，并计算最后一个方向的可能取值。

我们将使用多项式的有限差分恒等式。取 $m \ge 1$ 和 $G(x) = b_{m+1}x^{m+1}+b_m x^m+\cdots$。由于

$$G^{(m)}(x) = (m+1)!b_{m+1}x + m!b_m, \qquad \int_{[0,1]^m} y_i\,dy_1\cdots dy_m = \frac{1}{2},$$

在一个变量中应用（（5.5），步长为 $-s_1$，……，$-s_m$ 可得

$$\begin{aligned}
&\sum_{J\subseteq\{1,\dots,m\}}(-1)^{m-|J|}G\left(-\sum_{i\in J}s_i\right)\\
&=(-1)^m\left(\prod_{i=1}^m s_i\right)\int_{[0,1]^m}G^{(m)}\left(-\sum_{i=1}^m s_iy_i\right)\,dy_1\cdots dy_m\\
&=(-1)^m m!\left(\prod_{i=1}^m s_i\right)\left(b_m-\frac{m+1}{2}\,b_{m+1}\sum_{i=1}^m s_i\right).
\end{aligned}\tag{5.17}$$

应用（5.17），令 $m=r$ 和 $G=P/Q$，利用（5.16）和 $r\geq 2$ 可得

$$\begin{aligned}
\sum_J(-1)^{r-|J|}\frac{P(-\sum_{i\in J}s_i)}{Q}&=-\sum_{i=1}^r t_i\sum_{J\subseteq\{1,\dots,r\}\setminus\{i\}}(-1)^{r-1-|J|}\\
&=-\sum_{i=1}^r t_i(1-1)^{r-1}=0.
\end{aligned}$$

将这个零值代入（5.17）得到

$$\begin{aligned}
0&=(-1)^r r!\left(\prod_{i=1}^r s_i\right)\left(a_r-\frac{r+1}{2}a_{r+1}\sum_{i=1}^r s_i\right),\\
\Longrightarrow\quad a_r&=\frac{r+1}{2}\,a_{r+1}\sum_{i=1}^r s_i.
\end{aligned}\tag{5.18}$$

再次应用（5.17），令 $m=r-1$，并取下方的多项式 G。对于可容许基点和 $J\subseteq\{1,\dots,r-1\}$，顶点条件给出 $h+\sum_{i\in J}s_i\geq h_0>0$。因此，分母 $-\sum_{i\in J}s_i-h$ 非零。利用（5.11）和（5.16）计算 G:

$$\begin{aligned}
G(x)&=\frac{P(x)-P(h)}{Q(x-h)}=a_{r+1}x^r+(a_r+ha_{r+1})x^{r-1}+\cdots,\\
G\left(-\sum_{i\in J}s_i\right)&=\frac{-\sum_{i\in J}t_i-k}{-\sum_{i\in J}s_i-h}=\frac{k+\sum_{i\in J}t_i}{h+\sum_{i\in J}s_i}\quad\big(J\subseteq\{1,\dots,r-1\}\big).
\end{aligned}$$

公式（5.17）给出

$$\begin{aligned}
&\sum_{J\subseteq\{1,\dots,r-1\}}(-1)^{r-1-|J|}\frac{k+\sum_{i\in J}t_i}{h+\sum_{i\in J}s_i}\\
&=(-1)^{r-1}(r-1)!\left(\prod_{i=1}^{r-1}s_i\right)\left(a_r+ha_{r+1}-\frac{r}{2}\,a_{r+1}\sum_{i=1}^{r-1}s_i\right).
\end{aligned}$$

将 a_r 代入（5.18）以及将 a_{r+1} 代入（5.14）。约去后，我们得到

$$\begin{aligned}&\ell_0\left(2h+\sum_{i=1}^{r-1}s_i+(r+1)s_r\right)\\&\quad=-2rs_r\sum_{J\subseteq\{1,\dots,r-1\}}(-1)^{r-1-|J|}\frac{k+\sum_{i\in J}t_i}{h+\sum_{i\in J}s_i}.\end{aligned}\tag{5.19}$$

基面所有顶点处的斜率都是整数。其两个相对顶点的水平坐标给出下面的第一个界，而（5.19）给出第二个蕴含：

$$\begin{aligned}&2h_0\le h+\left(h+\sum_{i=1}^{r-1}s_i\right)=2h+\sum_{i=1}^{r-1}s_i\le 2N^{\kappa},\\&s_r>0,\ \ell_0\neq 0\quad\Longrightarrow\quad\sum_{J\subseteq\{1,\dots,r-1\}}(-1)^{r-1-|J|}\frac{k+\sum_{i\in J}t_i}{h+\sum_{i\in J}s_i}\neq 0.\end{aligned}$$

将（5.19）乘以 $r+1$，并对 $2h+\sum_{i=1}^{r-1}s_i+(r+1)s_r$取模。这得到

$$\begin{aligned}&2r\left(2h+\sum_{i=1}^{r-1}s_i\right)\sum_{J\subseteq\{1,\dots,r-1\}}(-1)^{r-1-|J|}\frac{k+\sum_{i\in J}t_i}{h+\sum_{i\in J}s_i}\\&\quad\equiv 0\pmod{2h+\sum_{i=1}^{r-1}s_i+(r+1)s_r}.\end{aligned}\tag{5.20}$$

左侧的整数仅取决于固定的基点和前 $r-1$ 个方向。它非零且满足

$$\begin{aligned}0<&\left|2r\left(2h+\sum_{i=1}^{r-1}s_i\right)\sum_{J\subseteq\{1,\dots,r-1\}}(-1)^{r-1-|J|}\frac{k+\sum_{i\in J}t_i}{h+\sum_{i\in J}s_i}\right|\\&\le 2r\cdot 2N^{\kappa}\cdot 2^{r-1}N^{\kappa}=2^{r+1}rN^{2\kappa}.\end{aligned}$$

该和 $2h+\sum_{i=1}^{r-1}s_i$至少为 $2h_0>0$，我们正在计算满足 $s_r>0$的立方体。因此 $2h+\sum_{i=1}^{r-1}s_i+(r+1)s_r>0$，而（5.20）使其成为固定整数的一个正因子。它随 s_r严格递增，因此由因子界可得

$$\#\{\text{possible values of } s_r\}\le C_{\kappa,r,\varepsilon}N^{\varepsilon}.$$

一旦 s_r 确定，（5.19）就确定了 ℓ_0。为确定 t_r，取其在（5.2）中的系数，并使用（$r-1$）阶形式的（5.10）：

$$\begin{aligned}\text{coefficient of } t_r &= \sum_{J\subseteq\{1,\dots,r-1\}} \frac{(-1)^{r-1-|J|}}{h+s_r+\sum_{i\in J} s_i} \\ &= (-1)^{r-1}(r-1)!\left(\prod_{i=1}^{r-1} s_i\right) \\ &\quad\cdot \int_{[0,1]^{r-1}} \left(h+s_r+\sum_{i=1}^{r-1} s_i y_i\right)^{-r} dy_1\cdots dy_{r-1} \neq 0.\end{aligned}$$

该系数非零，因此 t_r 可以唯一确定。基点和前 $r-1$ 个单步顶点至多有 $|B|^r$ 种选择；这些选择确定整个基面。因此

$$\#\{\text{ordered base faces}\} \le |B|^r, \qquad \#\{\text{cubes in this case}\} \le C_{\kappa,r,\varepsilon} N^{\varepsilon} |B|^r.$$

我们仍需计算水平步为零的立方体数量。如果某个完整方向为零，例如 $(s_i,\ t_i) = (0,\ 0)$，则选择其位置、基点以及其余的单步顶点。这些选择确定该立方体，因此

$$\#\{\text{cubes with a zero direction}\} \le r|B|^r.$$

如果没有方向为零，但某个 $s_i = 0$，那么 $t_i \neq 0$。每个可容许基点都给出一对具有这个非零垂直差的点：

$$\begin{aligned}&t_i \neq 0, \qquad (h,k),(h,k+t_i)\in B,\\ &\#\{\text{个关于这些方向的可容许基点}\}\\ &\quad\le \#\{(h,k)\in B : (h,k+t_i)\in B\}\\ &\quad\le \max_{t\in\mathbb{Z}\setminus\{0\}} \#\{(h,k)\in B : (h,k+t)\in B\}.\end{aligned}$$

对于上界，将前述计数对各个方向求和，并使用5.8）来界定每个方向元组的层级数量：

$$\begin{aligned}C_r(B) \ &\le C_{\kappa,r,\varepsilon} N^{\varepsilon}|B|^r \\ &\quad + 2|B-B|^r \max_{q\in\mathbb{Z}} \#\{(h,k)\in B : k = qh\} \\ &\quad + |B-B|^r \max_{t\in\mathbb{Z}\setminus\{0\}} \#\{(h,k)\in B : (h,k+t)\in B\} \\ &\quad + C_{\kappa,r,\varepsilon} N^{\varepsilon}|B-B|^r \left(1 + 2(H/X)^r \max_{(h,k)\in B}\left|\frac{k}{h}\right|\right).\end{aligned} \tag{5.21}$$

为合并这些项，使用

$$\begin{aligned}\#\{\text{direction tuples}\} \le |B-B|^r, \qquad |B|^r \le |B-B|^r,\\ 1 \le \max_{q\in\mathbb{Z}} \#\{(h,k)\in B : k = qh\},\\ (2^r - r - 1) + r = 2^r - 1.\end{aligned}$$

比较上界（5.21）与下界（5.9）。除以 $|B|^r$ 并乘以 $(|B-B|/|B|)^{2^r-r-1}$。所得不等式为（5.1）。□

注记 5.4。（5.1）中的三项分别对应于

过原点直线上的点 $(h,k)\in B,\ k=qh$,固定的非零垂直位移 (h,k),$(h,k+t)\in B,\ t\neq 0$,整数层级 $|\ell(h',k')-\ell(h,k)|\le 2(H/X)^r$ 最大值 $\max_{(x,y)\in B}|y/x|$.

如果每个垂直列最多包含一个点，就不会出现非零垂直差，第二项也随之消失。当 $r=2$，(5.19) 可写为

$$\ell_0(2h+s_1+3s_2)=-4s_2\left(\frac{k+t_1}{h+s_1}-\frac{k}{h}\right).$$

括号中的表达式是基边两个端点处斜率之差。对于 $r\ge 3$，对应的表达式是基面上的 $r-1$ 阶交替差分。

命题 5.5。固定整数 $N\ge 2,\ p\ge 1$，并令 $f\in\mathbb{Z}[x]$ 的次数为 $d\ge 3$。曲线 $(n,f(n))$ 上一条从 $(b,f(b))$ 指向 $(a,f(a))$ 且经 p 归一化的弦，给出整数点

$$(h,k)=\left(\frac{a-b}{p},\frac{f(a)-f(b)}{p}\right),\qquad a,b\in\mathbb{Z},\quad 1\le b<a\le N,\quad p\mid a-b.$$

令 B 为这些归一化弦点的任意子集。记 $\tau(m)$ 为正整数 m 的正因子个数。对于每个非零整数 t,

$$\#\{(h,k)\in B:(h,k+t)\in B\}\le 2(d-2)\tau(|t|)^2.$$

因此，对于每个 $\eta>0$，该计数至多为 $C_{f,\,\eta}N^{\eta}$，并且关于 t，p，B 一致成立。

对于 $f(x)=x^3$，这就是引理 3.1 的垂直差界。

证明。记 $f(x)=\sum_{j=0}^{d}c_jx^j$，其中 $c_j\in\mathbb{Z}$ 且 $c_d\neq 0$。我们首先计算可能的水平坐标。由于 f 具有整数系数，

$$a-b\mid f(a)-f(b)\quad\Longrightarrow\quad h\mid k,$$
$$(h,k),(h,k+t)\in B\quad\Longrightarrow\quad h\mid t\quad\Longrightarrow\quad\#\{\text{possible values of } h\}\le\tau(|t|).$$

对于一对 $(h,\ k)$，$(h,\ k+t)$，将较小的端点记为 b 和 $b+w$。两条弦的水平增量均为 ph，因此其端点坐标分别为 $(b+ph,\ b)$ 和 $(b+w+ph,\ b+w)$。利用二项式定理展开得

$$\begin{aligned}\frac{f(b+ph)-f(b)}{p}&=\sum_{j=1}^{d}c_j\sum_{i=1}^{j}\binom{j}{i}p^{i-1}h^ib^{j-i}\\&=dc_dh\,b^{d-1}+\cdots\in\mathbb{Z}[b],\\\frac{f(b+w+ph)-f(b+w)-f(b+ph)+f(b)}{p}&=t.\end{aligned}$$

表达式 $(f(b+ph)-f(b))/p$ 是关于 b 的整系数多项式。它在 $b+w$ 和 b 处的值之差是 w 的倍数。它们的差为 t，因此

$$t\neq 0\quad\Longrightarrow\quad w\neq 0,\quad w\mid t,\quad\#\{\text{possible values of } w\}\le 2\tau(|t|).$$

一旦固定了 h, w，这个差的首项为

$$\frac{f(b+w+ph)-f(b+w)-f(b+ph)+f(b)}{p}$$
$$= d(d-1)c_d hw\, b^{d-2} + \cdots, \qquad d(d-1)c_d hw \neq 0.$$

因此，右端为 t 的方程关于 b 的次数恰为 $d-2$，且至多有 $d-2$ 个解。每组选取 h、w、b都确定了 k，所以

$$\begin{aligned}
&\#\{(h,k) \in B : (h,k+t) \in B\} \\
&\leq \#\{\text{endpoint data } (h,w,b) \text{ satisfying these conditions}\} \\
&\leq \tau(|t|) \cdot 2\tau(|t|) \cdot (d-2) \\
&= 2(d-2)\tau(|t|)^2.
\end{aligned}$$

如果某个数对出现，其垂直差满足 $1 \leq |t| \leq C_f N^d$。因子界给出

$$1 \leq |t| \leq C_f N^d \quad \Longrightarrow \quad 2(d-2)\tau(|t|)^2 \leq C_{f,\eta} N^{\eta}. \qquad \square$$

注记 5.6。

$$a-b = ph, \qquad f(a)-f(b) = pk, \qquad \frac{k}{h} = \frac{f(a)-f(b)}{a-b}.$$

具有相同水平坐标 h 的点来自具有相同水平增量 ph 的弦。我们统计不同的点 (h,k)；其中若干点可能位于同一垂直列中。

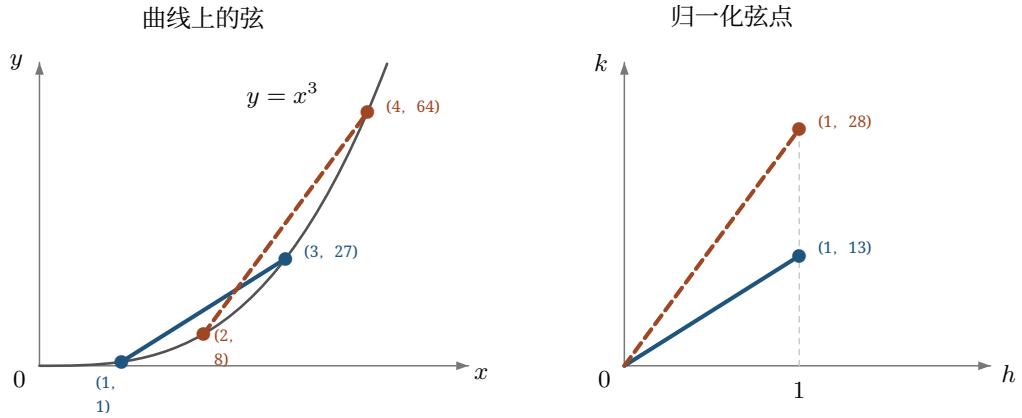

FIGURE 1. 对于 $d=3$ 和 $p=2$，这两条弦给出点 (1,13) 和 (1,28)。它们的差为 (0,15)，因此对 $t=15$ 贡献一个有序对。

命题 5.7。对于每个整数 $d \geq 3$ 和每个正整数 q，令 $\omega(q)$ 表示 q 的不同素因子个数。那么

$$\#\left\{(a,b) \in \mathbb{Z}^2 : 1 \leq b < a,\ \frac{a^d - b^d}{a-b} = q\right\} \leq 2\tau(q) d^{\omega(q)}.$$

特别地，如果 $N \geq 2$ 是整数且 $1 \leq q \leq dN^{d-1}$，那么对每个 $\varepsilon > 0$，左侧至多为 $C_{d,\varepsilon} N^{\varepsilon}$，并且对 N，q一致成立。

证明。 固定 q。我们先约去公因子 a, b:

$$g=\gcd(a,b),\qquad a=gu,\quad b=gv,\qquad u>v\ge 1,\quad \gcd(u,v)=1,$$

$$q=g^{d-1}\sum_{j=0}^{d-1}u^{d-1-j}v^{j}\quad\Longrightarrow\quad g^{d-1}\mid q,\quad \#\{\text{possible values of } g\}\le\tau(q).$$

对每个可能的 g，使用模数

$$m=\frac{q}{g^{d-1}}=u^{d-1}+u^{d-2}v+\cdots+v^{d-1}>u^{d-1}.$$

由于

$$m\equiv u^{d-1}\pmod v,\qquad \gcd(v,m)=\gcd(v,u^{d-1})=1,$$
$$u^d-v^d=m(u-v)\quad\Longrightarrow\quad (uv^{-1})^d\equiv 1\pmod m,$$

其中 v^{-1} 表示模 m 下 v 的乘法逆元。因此，每个可容许的数对（u, v）都通过映射给出 $z^d=1$ 的一个根

$$(u,v)\longmapsto uv^{-1}\pmod m\in\{z\in(\mathbb{Z}/m\mathbb{Z})^\times : z^d=1\}.$$

此映射是单射。事实上，若 $uv^{-1}\equiv u'(v')^{-1}$（模 m），则

$$m\mid uv'-u'v,\qquad 0<v<u<m^{1/(d-1)},\quad 0<v'<u'<m^{1/(d-1)},$$
$$|uv'-u'v|<uu'<m^{2/(d-1)}\le m\qquad (d\ge 3),$$
$$uv'-u'v=0\quad\Longrightarrow\quad \frac{u}{v}=\frac{u'}{v'}\quad\Longrightarrow\quad (u,v)=(u',v').$$

最后一步中，相等的分式已经约至最简，因为 $\gcd(u,\ v)=\gcd(u',\ v')=1$。

接下来要计算这些根的数量。模素数幂的单位群结构 [8, 第 4 章第 1] 节给出，对于素数 π 和 $e\ge 1$,

$$\#\{z \bmod \pi^e : z^d\equiv 1\pmod{\pi^e}\}$$
$$=\begin{cases}\gcd(d,\pi^{e-1}(\pi-1))\le d, & \pi>2,\\ 1, & \pi=2,\ e=1,\\ \gcd(d,2)\le 2, & \pi=2,\ e=2,\\ \gcd(d,2)\gcd(d,2^{e-2})\le 2d, & \pi=2,\ e\ge 3.\end{cases}$$

中国剩余定理将各素数幂对应的计数合并起来:

$$\#\{z \bmod m : z^d\equiv 1\pmod m\}=\prod_{\pi^e\| m}\#\{z \bmod \pi^e : z^d\equiv 1\pmod{\pi^e}\}$$
$$\le 2d^{\omega(m)}\le 2d^{\omega(q)}.$$

这里 $\pi^e\parallel m$ 表示 $\pi^e\mid m$ 和 $\pi^{e+1}\nmid m$。g 至多有 $\tau(q)$ 种选择，因此求和可得

$$\#\{(a,b):1\le b<a,\ (a^d-b^d)/(a-b)=q\}\le\tau(q)\cdot 2d^{\omega(q)}.$$

最后，因子界也能控制因子 $d^{\omega(q)}$:

$$2^{\omega(q)} \le \tau(q), \qquad d^{\omega(q)} \le \tau(q)^{\log_2 d},$$
$$2\tau(q)d^{\omega(q)} \le 2\tau(q)^{1+\log_2 d} \le C_{d,\varepsilon} q^{\varepsilon/(d-1)} \le C_{d,\varepsilon} N^{\varepsilon} \qquad (q \le dN^{d-1}).$$

□

注记 5.8。 对于固定的 p,

$$\#\{(h,k) \in B : k = qh\} \le \#\{(a,b) : 1 \le b < a,\ (a^d - b^d)/(a-b) = q\}.$$

现在我们可以估计命题 5.1 中的两个计数项。命题 5.7给出了过原点直线上的点的数量界，而命题 5.5给出了垂直差固定且非零的数对数量界。代入这些估计即可得到下一个结果。

命题 5.9。 设 $N \ge 2$, $d \ge 3$, $r \ge 1$, $p \ge 1$为整数，且 B 是任意一个非空子集

$$\left\{ \left(\frac{a-b}{p}, \frac{a^d - b^d}{p} \right) : a, b \in \mathbb{Z},\ 1 \le b < a \le N,\ p \mid a-b \right\}.$$

若 B 的所有水平坐标都属于 $[h_0, h_0 + H]$，其中 $1 \le H \le X \le h_0$，则对每个 $\varepsilon > 0$，存在一个常数$C_{d,\ r,\ \varepsilon} \ge 1$，它仅依赖于 d，r，ε，使得

$$|B| \le C_{d,r,\varepsilon} N^{\varepsilon} \big(1 + N^{d-1}(H/X)^r\big) \left(\frac{|B-B|}{|B|} \right)^{2^r - 1}. \tag{5.22}$$

特别地，若 $H \le XN^{-(d-1)/r}$，则对每个 $\varepsilon > 0$,

$$|B-B| \ge \frac{1}{C_{d,r,\varepsilon}} N^{-\varepsilon} |B|^{1+1/(2^r-1)}. \tag{5.23}$$

证明。 对于每个弦点（h，k）$\in B$,

$$\frac{k}{h} = \frac{a^d - b^d}{a-b} = \sum_{j=0}^{d-1} a^{d-1-j} b^j. \tag{5.24}$$

$$h \mid k, \qquad 1 \le h \le N, \qquad |k| \le N^d, \qquad 1 \le k/h \le dN^{d-1}.$$

首先假设 $r \ge 2$。由（5.24）中的斜率范围，我们可以应用命题 5.7，而命题 5.5 适用于竖直差。这就得到

$$\max_{q \in \mathbb{Z}} \#\{(h,k) \in B : k = qh\} \le C_{d,\eta} N^{\eta},$$
$$\max_{t \in \mathbb{Z}\setminus\{0\}} \#\{(h,k) \in B : (h, k+t) \in B\} \le C_{d,\eta} N^{\eta}.$$

在（5.1）中，取 $\kappa = d$，并令幂损失为 $\varepsilon/2$。在两处计数中都使用 $\eta = \varepsilon/2$，并用（5.24）作为最大斜率。这便得到

$$|B| \le C_{d,r,\varepsilon/2} N^{\varepsilon/2} \big(2C_{d,\varepsilon/2} N^{\varepsilon/2} + dN^{d-1}(H/X)^r\big) \left(\frac{|B-B|}{|B|} \right)^{2^r-1}$$
$$\le C_{d,r,\varepsilon} N^{\varepsilon} \big(1 + N^{d-1}(H/X)^r\big) \left(\frac{|B-B|}{|B|} \right)^{2^r-1}.$$

对于 $r=1$，至多有 $H+1$ 个整数水平坐标。应用柯西–施瓦茨不等式，然后对每个非零垂直差使用命题5.5：

$$\begin{aligned}\frac{|B|^2}{H+1} &\le \sum_{h\in[h_0,h_0+H]\cap\mathbb{Z}} \big(\#\{k:(h,k)\in B\}\big)^2 \\ &= |B| + \sum_{\substack{t\neq 0\\(0,t)\in B-B}} \#\{(h,k)\in B : (h,k+t)\in B\} \\ &\le |B| + C_{d,\eta}N^{\eta}|B-B| \le C_{d,\eta}N^{\eta}|B-B|.\end{aligned}$$

此外，

$$X \le h_0 \le N, \qquad N^{d-1}H/X \ge H, \qquad H+1 \le 1+N^{d-1}H/X,$$

将前述计数除以 $|B|$，再乘以 $H+1$，并取 $\eta=\varepsilon$。关于$H+1$ 的界给出（5.22），其中 $r=1$。

为得到差集下界，假设 $H \le XN^{-(d-1)/r}$。那么

$$1+N^{d-1}(H/X)^r \le 2.$$

A将（5.22）应用于幂损失（2^r-1）ε，并取2^r-1次方根。由此得到

$$\begin{aligned}|B| &\le 2C_{d,r,(2^r-1)\varepsilon}N^{(2^r-1)\varepsilon}\left(\frac{|B-B|}{|B|}\right)^{2^r-1}, \\ \frac{|B-B|}{|B|} &\ge \big(2C_{d,r,(2^r-1)\varepsilon}\big)^{-1/(2^r-1)}N^{-\varepsilon}|B|^{1/(2^r-1)}.\end{aligned}$$

将固定因子吸收到常数中，得到（5.23）。 □

注记 5.10。 在（5.23）中，增大差分阶数可以得到更宽的水平区间，并给出更小的扩张指数：

$$XN^{-(d-1)/(r+1)} \ge XN^{-(d-1)/r}, \qquad \frac{1}{2^{r+1}-1} < \frac{1}{2^r-1}.$$

将（5.24）和（5.23）专门化为 $d=3,\quad r=5$ 可得

$$\max_{(h,k)\in B} k/h \le 3N^2, \qquad 2^5-1=31,$$

$$H \le XN^{-2/5} \quad\Longrightarrow\quad |B-B| \ge \frac{1}{C_{3,5,\varepsilon}}N^{-\varepsilon}|B|^{32/31}.$$

对于三次应用，设 $\delta = 1/2-\theta$。推导（4.29）时仅使用了命题2.5，从而得到

$$XN^{-2/r} \ge N^{1/2-2/r-155\delta-o(1)}.$$

为了使该下界的指数为正，对于 $\delta>0$ 充分小时，我们需要$1/2-2/r>0$，因此 $r\ge 5$。当指数为正时，取 $H=\lfloor XN^{-2/r}\rfloor$。方程（4.19）和（4.18）于是给出

$$|B| \ge N^{1/2-2/r-2\delta-o(1)}.$$

将 5.23 中关于 $|B-B|$ 的下界除以 $|B|$，并与 4.28 中关于 $|B-B|/|B|$ 的上界进行比较。提升至（2^r-1）次幂后，只要

$$\delta < \frac{1/2-2/r}{153(2^r-1)+2}. \tag{5.25}$$

此条件还保证 $1/2-2/r-155\delta>0$，因为 $153(2^r-1)+2>155$ 对于 $r\geq 5$。对于 $r\geq 5$，将 r 增加 1 会使式 (5.25) 中的分子乘以

$$\frac{1/2-2/(r+1)}{1/2-2/r} = 1+\frac{4}{(r+1)(r-4)} \leq \frac{5}{3},$$

而分母则增加一倍以上。因此，在这项比较中，最大的阈值出现在 $r=5$。它在 $r=5$ 处为 $1/47450$，在 $r=6$处为 $1/57846$。

注记5.11。若 $f(x)=\sum_{j=0}^{d} c_j x^j \in \mathbb{Z}[x]$，且 $d\geq 3$，则

$$\left|\frac{f(a)-f(b)}{a-b}\right| \leq \sum_{j=1}^{d}|c_j|\sum_{i=0}^{j-1} a^{j-1-i}b^i \leq \left(\sum_{j=1}^{d} j|c_j|\right) N^{d-1}.$$

因此，同样的论证适用于 f；若对每个 $\eta>0$ 和 $N\geq 2$，都有

$$\max_{q\in\mathbb{Z}} \#\{(a,b)\in\mathbb{Z}^2 : 1\leq b<a\leq N,\ f(a)-f(b)=q(a-b)\} \leq C_{f,\eta}N^{\eta}.$$

对于 $r\geq 2$，将此假设与命题5.5 结合，并将两个估计代入命题5.1。这给出 5.22) 和 (5.23)，其中 f，常数可能依赖于 f。

对于 $r=1$，对至多 $H+1$ 个整数水平坐标应用柯西–施瓦茨不等式，得到

$$\begin{aligned}\frac{|B|^2}{H+1} &\leq \sum_{h\in[h_0,h_0+H]\cap\mathbb{Z}} \big(\#\{k:(h,k)\in B\}\big)^2 \\ &= |B| + \sum_{\substack{t\neq 0\\(0,t)\in B-B}} \#\{(h,k)\in B : (h,k+t)\in B\} \\ &\ll_{f,\varepsilon} N^{\varepsilon}|B-B|,\end{aligned}$$

其中对角线项的贡献为 $|B|\leq|B-B|$，命题 5.5 将每一项界定为 $t\neq 0$。由于 $X\leq h_0\leq N$，我们得到如下形式的（5.22）：

$$|B| \ll_{f,\varepsilon} N^{\varepsilon}(H+1)\frac{|B-B|}{|B|} \leq N^{\varepsilon}\left(1+N^{d-1}\frac{H}{X}\right)\frac{|B-B|}{|B|}.$$

对于 $f(n)=\lambda n^d+\mu n+\nu$，其中 λ，μ，$\nu\in\mathbb{Z}$ 以及 $\lambda\neq 0$，我们可以直接从单项式情形转移界：

$$\begin{aligned}&\left(\frac{a-b}{p},\frac{f(a)-f(b)}{p}\right) = (h,\lambda k+\mu h),\\ &(h,\lambda k+\mu h)=(h',\lambda k'+\mu h') \quad\Longrightarrow\quad h=h',\ k=k',\\ &(h,\lambda k+\mu h)-(h',\lambda k'+\mu h')\\ &\qquad = (h-h',\lambda(k-k')+\mu(h-h')).\end{aligned}$$

映射 $(h,k)\mapsto(h,\lambda k+\mu h)$ 是可加且单射的。它保持点集及其差集的大小，因此可得相同的估计。

注记 5.12. 限制 $d\geq 3$ 是必要的。对于 $d=2$，命题 5.9 对每个差分阶数 $r\geq 2$都不成立。为说明这一点，取 $m\geq 1$ 并设

$$N=16m^2,\quad p=2,\quad h_0=X=N/4,\quad H=m,$$
$$a=N/2+h,\quad b=N/2-h,\quad N/4\leq h\leq N/4+m,\quad h\in\mathbb{Z},$$
$$1\leq b<a\leq N,\qquad a+b=N,\qquad \left(\frac{a-b}{2},\frac{a^2-b^2}{2}\right)=(h,Nh).$$
$$B=\{(h,Nh):h\in[X,X+H]\cap\mathbb{Z}\},$$
$$|B|=m+1,\quad |B-B|=2m+1,$$
$$H=XN^{-1/2},\qquad N(H/X)^2=1,\qquad \frac{|B-B|}{|B|}<2.$$

若 (5.22) 对 $d=r=2$成立，则

$$m+1\leq 2C_{2,2,\varepsilon}(16m^2)^{\varepsilon}\left(\frac{2m+1}{m+1}\right)^3\leq 16C_{2,2,\varepsilon}(16m^2)^{\varepsilon}.$$

取 $\varepsilon=1/4$ 得

$$m+1\leq 32C_{2,2,1/4}\sqrt{m}\quad\Longrightarrow\quad\sqrt{m}\leq 32C_{2,2,1/4},$$

这不可能，因为 $m\to\infty$。对每个固定的 $r>2$，同一个例子给出

$$N(H/X)^r=N^{1-r/2}\leq 1\quad\Longrightarrow\quad m+1\leq 2^{2^r}C_{2,r,\varepsilon}(16m^2)^{\varepsilon},$$

再取 $\varepsilon=1/4$，当 $m\to\infty$时便再次得到矛盾。这个例子还说明了为什么命题 5.1 要计入过原点直线上的点的数量:

$$\max_q\#\{(h,k)\in B:k=qh\}=|B|,$$
$$\max_{t\neq 0}\#\{(h,k)\in B:(h,k+t)\in B\}=0.$$

允许一列中有多个点，也能为 $r=1$ 构造一个反例。保留N，p，X，但取

$$H=1,\qquad a=b+N/2,\qquad b=1,\dots,N/2,$$
$$B=\left\{\left(\frac{N}{4},\frac{N}{4}\left(2b+\frac{N}{2}\right)\right):1\leq b\leq N/2\right\},$$
$$|B|=N/2,\qquad |B-B|=2|B|-1,\qquad NH/X=4.$$

若（5.22）对 $d=2$，$r=1$成立，则

$$N/2\leq 10C_{2,1,\varepsilon}N^{\varepsilon}\quad\Longrightarrow\quad N^{3/4}\leq 20C_{2,1,1/4}\quad(\varepsilon=1/4),$$

这不可能，因为 $N\to\infty$。对于这个集合，

$$\#\{(h,k)\in B:(h,k+N/2)\in B\}=|B|-1,$$

因此，当 $d=2$时，固定非零垂直差的计数也可能很大。 N 命题 5.5 中关于任意小的 $d\geq 3$ 的界要求。

命题 *2.8*。 设 $N \geq 2$ 和 $p \geq 1$ 为整数，设 B 为以下整数弦点集合的任意非空子集，

$$B \subseteq \left\{ \left(\frac{a-b}{p}, \frac{a^3-b^3}{p} \right) : a, b \in \mathbb{Z},\ 1 \leq b < a \leq N,\ p \mid (a-b) \right\}.$$

设有 $1 \leq H \leq X \leq h_0$。如果 B 的所有水平坐标都位于 $[h_0, h_0 + H]$ 和 $H \leq XN^{-2/5}$ 中，那么，对于每个 $\eta > 0$，存在一个常数 $C_\eta > 0$，该常数仅取决于 η，使得

$$\frac{|B-B|}{|B|} \geq C_\eta N^{-\eta} |B|^{1/31}.$$

命题的证明 *2.8*。 现在，我们将单项式估计专门应用于三次弦。取 $d = 3$ 和 $r = 5$ 于命题 5.9。于是

$$2^r - 1 = 31, \qquad H \leq XN^{-(d-1)/r} = XN^{-2/5}.$$

应用（5.22），其中 $\varepsilon = 31\eta$。对 H 的条件将括号中的因子限制在 2 以内，从而得到

$$\begin{aligned} |B| &\leq C_{3,5,31\eta} N^{31\eta} \big(1 + N^2 (H/X)^5\big) \left(\frac{|B-B|}{|B|} \right)^{31} \\ &\leq 2C_{3,5,31\eta} N^{31\eta} \left(\frac{|B-B|}{|B|} \right)^{31}. \end{aligned}$$

取 31 次方根并重新排列，得到

$$\frac{|B-B|}{|B|} \geq (2C_{3,5,31\eta})^{-1/31} N^{-\eta} |B|^{1/31}.$$

因子 $(2C_{3,\ 5,\ 31\eta})^{-1/31}$ 为正，且仅取决于 η。将其记为 C_η 即可证明该命题。 □

命题 *2.1*。 固定 $N \geq 1$。如果 $D > 0$ 满足 $I_8(\mathbf{1}_A) \leq D|A|^4$ 对每个 $A \subseteq \{1, \ldots, N\}$ 都成立，那么对于所有复系数 b_1，……，b_N，

$$I_8(b) \leq D(1 + \log N)^4 \left(\sum_{n=1}^{N} |b_n|^2 \right)^4.$$

命题的证明 *2.1*。 首先固定一个集合 A，并为每个元素指定一个模为 1 的系数。展开八阶矩并应用（3.3），得到的八元组与（2.3）中的相同。每个系数乘积的绝对值均为 1，因此由三角不等式，该矩的上界为 $I_8(\mathbf{1}_A) \leq D|A|^4$。对于一般系数，将每个模 $|b_n|$表示为区间 $0 \leq t < |b_n|$的长度。于是

$$\begin{aligned} &\sum_{n=1}^{N} b_n \exp\big(2\pi i(nx + n^3 y)\big) \\ &\quad = \int_0^\infty \sum_{\substack{1 \leq n \leq N \\ |b_n| > t}} \frac{b_n}{|b_n|} \exp\big(2\pi i(nx + n^3 y)\big)\, dt. \end{aligned}$$

条件 $|b_n| > t \geq 0$ 排除了 $b_n = 0$，因此该公式中的每个商都有定义。应用闵可夫斯基积分不等式，以及模为 1 的系数所满足的界：

$$I_8(b)^{1/8} \leq D^{1/8} \int_0^\infty \big(\#\{n \in \{1,\dots,N\} : |b_n| > t\}\big)^{1/2}\, dt.$$

通过选取一个置换 σ 使得 $|b_{\sigma(1)}| \geq \cdots \geq |b_{\sigma(N)}|$，将各项的大小排序。用$\sqrt{m} = \sum_{j=1}^{m}($ $\sqrt{j} - \sqrt{j-1})$将被积函数写成有限和。将该和与积分交换，即得到下面的第一个等式。随后应用柯西–施瓦茨不等式可得

$$\begin{aligned}
&\int_0^\infty \big(\#\{n : |b_n| > t\}\big)^{1/2}\, dt \\
&= \sum_{j=1}^{N} |b_{\sigma(j)}|(\sqrt{j} - \sqrt{j-1}) \\
&\leq \left(\sum_{n=1}^{N} |b_n|^2\right)^{1/2} \left(\sum_{j=1}^{N} (\sqrt{j} - \sqrt{j-1})^2\right)^{1/2} \\
&\leq \left(\sum_{n=1}^{N} |b_n|^2\right)^{1/2} \left(\sum_{j=1}^{N} \frac{1}{j}\right)^{1/2} \leq (1+\log N)^{1/2} \left(\sum_{n=1}^{N} |b_n|^2\right)^{1/2}.
\end{aligned}$$

对于最后两个不等式，我们用到了

$$(\sqrt{j} - \sqrt{j-1})^2 = (\sqrt{j} + \sqrt{j-1})^{-2} \leq \frac{1}{j}, \qquad \sum_{j=1}^{N} \frac{1}{j} \leq 1 + \int_1^N \frac{dt}{t} = 1 + \log N.$$

将两边提升至八次方，即可证明（2.1）。 □

致谢。在准备本手稿期间，作者使用 GPT 提供协助。作者对论文中的数学论证及最终内容负责。

References

1. Jean Bourgain, *Fourier transform restriction phenomena for certain lattice subsets and applications to nonlinear evolution equations. II. the KdV-equation* **3** 1993 3, 209 ，《几何与泛函分析》（），第 – 卷 262。2. Jean Bourgain, Ciprian Demeter 和 Larry Guth, *Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three* 2 **184** 2016 2, 633 682 ，《数学年刊》（） （），第 – 期。3. G. H. Hardy 和 E. M. Wright, *An introduction to the theory of numbers*, 第六版，牛津大学出版社，2008 年，由 D. R. Heath-Brown 和 J. H. Silverman 修订。4. Yi Hu 和 Xiaochun Li, *Discrete Fourier restriction associated with KdV equations*, 《分析与偏微分方程》**6** （2013），第 4 期，859–892。5. , *Discrete Fourier restriction associated with Schrödinger equations*, 《伊比利亚数学评论》**30** （2014），第 4 期，1281–1300。6. , *Local well-posedness of periodic fifth-order KdV-type equations*, 《几何分析杂志》**25** （2015），第 2 期，709–739。7. Kevin Hughes 和 Trevor D. Wooley, *Discrete restriction for (x, x^3) and related topics*, 《国际数学研究通知》**2022** （2022），第 20 期，15612–15631。

8. Kenneth Ireland 和 Michael Rosen, *A classical introduction to modern number theory*, 第二版, 数学研究生教材, 第 84 卷, Springer, 纽约, 1990。9. XUDONG LAI 和 Yong Ding, *A note on the discrete Fourier restriction problem*, 《美国数学学会会刊》**146** (2018), 第 9 期, 3839–3846。10. Xiaochun Li, *A remark on the mean value inequalities related to Waring's problem*, 预印本, 2023。11. , *A Stein–Tomas type estimate and a decoupling inequality*, 预印本, 2023。12. , *A ~~remark~~ on Stein–Tomas type restriction theorems*, 《数学学报（英文版）》**41** (2025), 第 1 期, 122–130。13. Giorgis Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, 《组合数学》**32** (2012), 第 6 期, 721–733。14. Christian Reiher 和 Tomasz Schoen, *Note on the theorem of Balog, Szemerédi, and Gowers*, 《组合数学》**44** (2024), 第 3 期, 691–698。15. Trevor D. Wooley, *Mean value estimates for odd cubic Weyl sums*, 《伦敦数学学会会刊》**47** (2015), 第 6 期, 946–957】【。

Xudong Lai: Institute for Advanced Study in Mathematics, Harbin Institute of Tech-nology, Harbin 150001, China; Zhengzhou Advanced Research Institute, Harbin Institute of Technology, Zhengzhou 450000, China*Email address*: xudonglai@hit.edu.cn xudonglai@mail.bnu.edu.cn

Hongxu Wu: Institute for Advanced Study in Mathematics, Harbin Institute of Technology, Harbin, 150001, China*Email address*: 2022110278@stu.hit.edu.cn