arXiv:2305.04038v1 [math.NT] 6 May 2023

素因子较少的整数的和-积问题

Brandon Hanson、Misha Rudnev、Ilya Shkredov 和 Dmitrii Zhelezov

ABSTRACT. E. Szemer´edi 曾提出，对于有限集 $A \subset \mathbb{Z}$，在所有相关整数的素因子数量有界这一约束下，能否改进 $\max\{|A+A|, |A\cdot A|\}$ 的估计？也就是说，每个 $a \in A$ 都满足 $\omega(a) \leq k$。本文通过证明该最大值的数量级为 $|A|^{\frac{5}{3}-o(1)}$（条件是 $k \leq (\log |A|)^{1-\varepsilon}$，其中 $\varepsilon > 0$），对 Szemer´edi 的问题给出了肯定回答。事实上，这一结论可由一项加法能量估计推出，而该估计除相差 $|A|^{o(1)}$ 量级的因子外已是最佳的。

1. INTRODUCTION

Erd˝os 和 Szemer´edi 在 [ES]中提出了和-积现象。

设 $1 < a_1 < \ldots < a_n$ 是一个整数序列。考虑形如以下形式的整数

$$a_i + a_j,\ a_i a_j : \qquad 1 \leq i \leq j \leq n\,. \tag{1}$$

人们很容易猜想，对于每个 $\epsilon > 0$，都存在一个 n_0，使得对于每个 $n \geq n_0$，形如 (1 的整数都有超过 $n^{2-\varepsilon}$ 个互不相同的).

用现代记法来说，我们关注和集与积集的大小。对于整数的子集 A，或更一般地，对于交换环，定义如下：

$$A + A = \{a + b : a, b \in A\},\ A \cdot A = \{ab : a, b \in A\}.$$

作为一种一般性启发，该猜想表明，除非 A 接近某个子环，否则 $A+A$ 或 $A\cdot A$ 会显著大于原集合。对于整数而言，后一种情况不可能发生，因为不存在非平凡的有限子环。有兴趣的读者可参阅[TV]，其中相当全面地探讨了和集及相关问题，也包括此前关于和-积问题的一些研究成果。

Erd˝os 和 Szemer´edi 接着给出了如下论述。

或许我们的猜想在 a's 为实数或复数时仍然成立。 $s.$

Erd˝os 和 Szemer´edi 最终证明了

$$\max\{|A+A|, |A\cdot A|\} \gg |A|^{1+c},$$

其中指数 c 可见等于 1 31，参见 [N]，；并且根据猜想，任何 $c < 1$ 都是可容许的，但需付出隐含常数的代价。

过去几十年来，和积现象得到了广泛研究。截至本文撰写时，实数情形的当前纪录为 [RSt]，而有限域中足够小的集合的当前纪录为 [MSt]（另见 [RSh]）。

和-积问题最初是针对有限整数集提出的，但多年来，涉及组合学和凸几何的诸多技巧一直是该领域的主要工具，而这些技巧同样适用于有限实数集。事实上，参见 [E], [So], and [HRNR]，其中介绍了有助于确立我们目前对实数范围内该问题理解的技巧。然而，只有在算术情形（在 $\mathbb{Z}$ 或许是 $\mathbb{Q}$上）下，人们才理解该问题的一个方面：具有较少不同乘积的集合的性质。事实上，在这种情形下，唯一分解和 p-进分析推动了相关研究取得进展，而实变方法尚未能达到同等成果。运用我们所指这些技巧的研究始于 [Ch]，随后有 [BC],，之后又在 [HRNZ1], [HRNZ2] 和 [PZ] 中得到了进一步阐述。特别是，当 A 由整数构成时，人们对满足 $A \cdot A$ 非常小的集合 A 有了深入得多的认识。或许受这类结果以及 $\{1, \dots, N\}$ 是和-积问题近极值例子的启发，E. Szemer´edi 曾询问排名第四的作者：当 A 由满足[1] $\omega(a) \leq k$的整数构成时，针对 A 的和积估计是否会有所改善；即使再施加非常严格的限制，例如 $k = 10$，是否仍会改善。这是一个自然的问题：如果类似初始区间 $A = \{1, \dots, N\}$ 的集合确实是最坏情形，那么平均而言就会有 $\omega(a) \leq \log\log |A|(1 + o(1))$；例如参见 [MV]。

即使在 $k = 1$ 的情况下，这个问题也已经暗示了某些微妙的现象。事实上，当 A 由不超过 N 的素数组成时，根据素数定理，这些素数的数量约为 $N/\log N$。当然有 $|A \cdot A| \gg |A|^2$，但 $|A + A| \ll |A| \log |A|$；更显著的情形是 A 为由素数组成的等差数列，其存在性正是 [GT], 中证明的 Green-Tao定理的内容，此时有 $|A+A| = 2|A| - 1$。因此，约束$k = 1$ 仍允许 A 在加法结构方面尽可能地复杂。另一方面，也可以对任意素数 p 取 $A = \{p, p^2, \dots, p^N\}$——请记住， ω 不考虑重数——于是 $|A+A| \gg |A|^2$，但 $|A \cdot A| = 2|A| - 1$，此时 A 的乘法结构达到最大。

不过，真正让这个问题显露出棘手之处的，正是 $k = 2$ 的情形。下面这个例子我们从 [BW] 得知，它就是我们所说的 Balog-Wooley 集。它不过是一个等比数列与一个等差数列的乘积：

$$\begin{aligned}
&\Gamma = \{r^m : 1 \leq m \leq M\},\\
&B = \{a + dn : 1 \leq n \leq N\},\\
&A = \Gamma \cdot B = \{r^m(a + dn) : 1 \leq m \leq M,\ 1 \leq n \leq N\}.
\end{aligned}$$

[1]这里， $\omega(a)$ 表示 a 的不同素因子的个数。

Balog 和 Wooley 选择了 $B = \{1, \dots, 2n^2\}$ 和 $\Gamma = \{1, 2, 4, \dots, 2^{n-1}\}$。（注意，为避免冲突，可以将生成 Γ 的素数 2 换成某个 $p > 2n^2$。）更一般地，可以考虑近似的 Balog-Wooley 集，其中 Γ 和 B 分别由等比数列和等差数列的近似形式替代；当然，也可以选择 r，并使 B 的所有元素都为素数，如 $k = 1$ 的情形所述。这些例子通过施加以下约束而获得其结构：

$$|\Gamma \cdot \Gamma| \leq K_\Gamma |\Gamma|, \ |B + B| \leq K_B |B|$$

其中 K_Γ 和 K_B 基本上可以任意小。这将迫使积集很小，因为

$$|A \cdot A| \leq |\Gamma \cdot \Gamma||B \cdot B| \leq K_\Gamma |\Gamma||B|^2 \leq (K_\Gamma |B|)|A|.$$

与此同时，这些集合也满足

$$E_+(A, A) \geq |\Gamma| E_+(B, B) \geq \frac{|\Gamma||B|^3}{K_B} = \frac{|A|^3}{K_B |\Gamma|^2},$$

其中，$E_+(X, Y)$ 表示加法能量

$$E_+(X, Y) = |\{(x_1, x_2, y_1, y_2) \in X \times X \times Y \times Y : x_1 + y_1 = x_2 + y_2\}|,$$

仅仅由于对角解

$$\gamma(b_1 + b_2) = \gamma(b_3 + b_4).$$

特别地，通过取 $|\Gamma|^2 = |B|$，A可以满足 $|A \cdot A| \ll |A|^{\frac{5}{3} - o(1)}$以及 $E_+(A, A) \gg |A|^{\frac{7}{3}}$，正如 Balog 和 Wooley 在他们的工作中所做的那样。他们进一步猜想，如果希望将 A 分解为两部分，其中一部分具有较小的加法能量，另一部分具有较小的乘性能量，那么指数 $\frac{7}{3} - o(1)$ 就是可能达到的最优指数。如果仅使用加法能量来预测$|A + A|$，例如通过标准的柯西-施瓦茨估计。

$$|A + A| E_+(A, A) \geq |A|^4,$$

那么只能推出 $|A + A| \gg |A|^{\frac{5}{3}}$。从这个例子中，我们可以观察到，即使 A 中的每个元素都只有两个素因子，也无法将结论中的指数提高到优于 $5\ 3$ 的程度。

$$\textit{There is a subset } \tilde{A} \subseteq A \textit{ for which } |A \cdot A| + \frac{|\tilde{A}|^4}{E_+(\tilde{A}, \tilde{A})} \gg |A|^{\frac{5}{3}},$$

如果素因子的数量增加到大约为 log log $|A|$，指数 $5\ 3$ 就会使另一个 $o(1)$ 损失。

事实上，我们证明的正是这一陈述，只差增长速度慢于 $|A|$ 的任意幂的项，并且是在素因子数量较少这一约束下。当然，A 的加法能量可能无法准确预测 $|A + A|$；事实上，Balog-Wooley 集并未违背 Erd˝os-Szemer´edi 猜想，而归根结底，该猜想仍然只是一个猜想。

我们的主定理如下。

定理 1.1。设 ε 为满足 $0 < \varepsilon < 1/6$ 的实数，并设 $k \in \mathbb{N}$ 为正整数。假设 A 是满足对每个 $a \in A$ 均有 $\omega(a) \le k$，且满足 $(\log |A|)^{1-6\varepsilon} \ge k$ 的充分大的有限整数集。那么，存在一个子集 $\tilde{A} \subseteq A$，使得

$$|\tilde{A}| \ge \frac{|A|}{k!(2\log|A|)^k}$$

and

$$|A \cdot A| + \frac{|\tilde{A}|^4}{E_+(\tilde{A},\tilde{A})} \ge |A|^{\frac{5}{3}} \exp(-C(\log|A|)^{1-\varepsilon}),$$

其中 $C > 0$ 是某个绝对常数。

特别地，我们得到以下和积估计。

推论 1.2. 设 A 是一个有限整数集，且 ε 和 k 是满足定理 1.1 条件的参数。则，

$$\max\{|A+A|, |A \cdot A|\} \gg_{\varepsilon,k} |A|^{\frac{5}{3}-o(1)}.$$

如上所述，指数 $\frac{5}{3}$ 并非巧合，因为我们的方法首先证明了 Balog-Wooley 集基本上是最坏的情形。正是由于这种方法，即针对 A 的加法能量进行研究，我们未能证明完全的二次增长。

我们还注意到，据我们所知，大多数和积估计都将能量与“相反集合”的基数并置。Solymosi [So], 的论文标题就明确体现了这一点，该论文证明了不等式

$$E_\times(A,A) \ll |A+A|^2 \log|A|,$$

其中，乘性能量 $E_\times(A,A)$ 的定义与加法能量类似，只是以乘法代替加法。特别地，这意味着，若 $|A+A| \le K_+|A|$，且加法倍增常数 K_+ 足够小，那么 $E^\times(A,A)$ 仅略高于其平凡下界 $|A|^2$，因此 $|A \cdot A|$ 几乎是 $|A|^2$，从而证明了 Erd˝os-Szemer´edi 关于实数（甚至复数）的猜想在端点 $K_+ \approx 1$ 处的一个特例；另见 [KR]。

另一方面，令 $K_\times = |A \cdot A|/|A|$ 表示乘法加倍常数，P´alv˝olgyi 和第四位作者 [PZ] 证明，对于有限集 $A \subset \mathbb{Z}$ 和 $\varepsilon \in (0, 1/2)$，存在一个子集 $\tilde{A} \subseteq A$，使得 $|\tilde{A}| \ge |A|^{1-\varepsilon}$ 以及

$$E_+(\tilde{A},\tilde{A}) \le K_\times^{\frac{4}{\varepsilon}} |A|^{2+4\varepsilon}.$$

该定理为 Bourgain 和 Chang [BC] 的研究带来了新的认识，并改进了他们的结果。它还解决了 Erd˝os-Szemer´edi 猜想的端点情形 $K_\times \approx 1$.[2] 在这里，可以通过积集得到加法能量估计，而这能够很好地预测

[2]目前只有整数（以及由伸缩不变性可知的有理数）满足这一结论；对于实数，已知的最佳结果要弱得多 [MRSS]。

$|A+A|$。然而，在远离端点的情形下，鉴于 Balog-Wooley 例子，直接应用柯西-施瓦茨不等式，将加法能量的上界转化为和集的下界，代价过高。

就本文的结果而言，它们的源头是以下这个初等引理，该引理说明了少素因子假设的强大作用。

引理 1.3. 设 A 和 B 是有限整数集，满足对 $a \in A$ 有 $\omega(a) \leq k$，并且对 $b \in B$ 有 $\omega(b) \leq l$。那么，任意元素 $q \in A \cdot B$ 至多有 2^{k+l} 个解满足 $q = ab$，其中 $a \in A$、$b \in B$ 且 $\gcd(a,b) = 1$。

证明。事实上，$\omega(q) \leq k+l$，而满足 $\gcd(a,b) = 1$ 的分解 $q = ab$ 等价于从整除 q 的素数中选取某个子集。这样的子集共有 $2^{\omega(q)}$ 个。□

定理 1.1 的证明分为三个步骤。首先，我们为少素因子整数集建立一个近似结构定理，即第 2 节的定理 4.2。正是这一结构定理告诉我们，（广义的）Balog-Wooley 集从本质上说是最坏的情形。引理 1.3 将与结构定理结合起来，对所得分解的纤维提供一致控制。

接下来需要用到的是一个 Littlewood-Paley 型定理，它能让我们相当高效地估计 Balog-Wooley 型集合的加法能量。我们的定理 5.1 是 Chang 在 [Ch] 中提出的关键引理 6 的加强版（另见下文引理 3.3）。这一引理也是后续论文 [BC], [HRNZ1], [HRNZ2], [PZ] 中相关进展的基础。该引理的结论足以满足上述论文的目标；这些论文研究的是小乘积集的端点情形。若要超越端点情形，则需要更强的结果。

定理 5.1 可由 Burkholder 的鞅 Littlewood-Paley 定理 [Bu] 推出。这种方法顺理成章，因为随机化（即鞅变换）为迭代 Littlewood-Paley 分解提供了一条途径，而若从这一角度看，Chang 引理本身就是一种鞅差分方法。在本项目进行期间，我们通过一本精彩的著作 [P]，发现，Gundy 和 Varopoulos 早已注意到了我们所需的这类结果 [GV]。我们推测，该定理以推论 5.2 的形式出现在第 3 节中，或可在这一领域有更多应用。

证明的最后一个部分是对来自低秩群的数乘集上的加法能量进行平均后，给出一个上界。当秩为 1 时，我们给出所需估计的一个初等证明，参见第 4 节的定理 6.1；而对于更一般的情形，我们则借助更复杂的数学工具，即 [RNZ]，中的引理 2.1，该引理依赖于超越数理论中的一个相当强的子空间定理版本。我们很想知道，定理 6.1 中的简单方法能否推广到一般情形。

因此，我们的方法将基础组合数学和初等数论与调和分析和超越数理论中的现代工具相结合，而这些工具恰好与我们的研究完美契合。人们自然会想，这在多大程度上只是巧合。

在正式开始证明之前，我们先在第 3 节中给出一个更简单的论证；该论证仍足以达到指数 $3/2$。

Acknowledgements

作者感谢海尔布隆数学研究所（HIMR）资助于2022年5月至6月举办的加性结构测试重点研究小组活动，本项目正是在此次活动中启动的；同时感谢位于林茨的约翰·拉东研究所（RICAM）为活动提供场地及额外资助。我们特别感谢 Oleksiy Klurman 共同组织该重点研究小组，并感谢 Oliver Roche-Newton 主办此次活动。Brandon Hanson 得到美国国家科学基金会奖项2135200的支持。Dmitrii Zhelezov 得到奥地利科学基金 FWF项目P 34180 的支持。

2. Notation

渐近记号：对于非负量 X 和 Y，$X \ll Y$ 或 $X = O(Y)$ 都表示存在某个绝对常数 $C > 0$，使得 $X \le CY$；而 $X = o(Y)$ 表示 $X/Y \to 0$。隐含常数 C 对参数的依赖关系以下标表示，例如 $X \ll_{\alpha,\,\beta} Y$ 或 $X = O_{\alpha,\,\beta}(Y)$ 表示对于某个 $C(\alpha,\beta) > 0$，有 $X \le CY$。符号 $X \approx Y$ 意在表示 $X \ll Y \ll X$。

数论记号：我们用字母 p 表示素数，因此算术基本定理指出，对于整数 n

$$n = \prod_p p^{v_p(n)},$$

该乘积遍历互不相同的素数，其中 $v_p(n)$ 表示 n 的 p-进赋值（即 n 的唯一分解中 p 的指数）。由于除有限多个 p 外，$v_p(n) = 0$，因此该乘积隐含地是有限的。对于满足 $v_p(n) > 0$ 的那些 p，我们记作 $p|n$，并令 $\omega(n)$ 表示此类 p 的数量。我们用 $\gcd(m,n) = \prod_p p^{\min(v_p(m),\,v_p(n))}$ 表示 m 和 n 的最大公因数。如果 $P = \{p_1,\dots,p_r\}$ 是素数集，我们可以固定其顺序，将其写成一个 r 元组 $\mathbf{p} = (p_1,\dots,p_r)$；于是，对于一个由整数构成的 r 元组 $\mathbf{v} = (v_1,\dots,v_r)$，我们记作 $\mathbf{p}^{\mathbf{v}} = p_1^{v_1}\cdots p_r^{v_r}$。我们将 $\langle P\rangle = \{\mathbf{p}^{\mathbf{v}} : \mathbf{v} \in \mathbb{Z}^r\}$ 记作由 P 中的素数生成的 $\mathbb{Q}^\times$ 的乘法子群，并将 $\langle P\rangle_+$ 记作包含那些满足对 P 中每个素数都有 $v_p(n) \ge 0$ 的元素 $n \in \langle P\rangle$ 的乘法半群。

加性组合记号：对于复数的子集 A和 B，我们记

$$A + B = \{a + b : a \in A,\ b \in B\}$$

和集记作，

$$A \cdot B = \{a + b : a \in A,\ b \in B\}$$

对于积集，以及

$$t + A = \{t + a : a \in A\},\ d \cdot A = \{da : a \in A\}$$

分别表示将 A 平移 $t \in \mathbb{C}$ 以及将 A 伸缩 $d \in \mathbb{C}$。这些量

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

and

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

分别表示 A 和 B的加法能量与乘法能量。

图论记号：若 X 和 Y是集合，我们将 $G \subseteq X \times Y$称为二分图。当然，它也是一个有向图，但我们不强调这一点。进一步地，对于子集 $X' \subseteq X$、 $Y' \subseteq Y$，定义

$$N_{Y'}(x) = \{y \in Y' : (x, y) \in G\},\ N_{X'}(y) = \{x \in X' : (x, y) \in G\},$$

分别称为 x和 y在 Y'和 X'中的邻居。基数 $|N_Y(x)|$和$|N_X(y)|$ 分别是 x 和 y的度。

分析记号：我们将 $\mathbb{T} = \mathbb{R}/\mathbb{Z} = [0, 1)$ 视为环面，并在 $\mathbb{T}$上的足够光滑函数空间赋予 L^q-范数

$$\|f\|_{L^q} = \left(\int_0^1 |f(t)|^q dt\right)^{1/q}$$

对于 $q \geq 1$ 和内积

$$\langle f, g\rangle = \int_0^1 f(t)\overline{g(t)}dt.$$

一个形如 $f\colon \mathbb{T} \to \mathbb{C}$ 的函数

$$f(t) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)e(nt)$$

称为傅里叶级数。其中，函数 $e(nt) = e^{2\pi int}$ 是

$\widehat{\ }$ $\widecheck{\ }\mathbb{Z}$ 上的标准特征，系数 $f(n)$ 是 f 的第 n 个傅里叶系数。如果对于有限个 n， $f(n)$ 均不为零，则称 f 为三角多项式。

3. A simple argument yielding exponent $3/2$

本节首先介绍一个相当简单的结构定理，以帮助读者初步了解一般问题。最终采用的并不是这个版本的结构定理，不过它的证明相当简单，也展示了一般的策略。

引理 3.1. 假设 $G \subseteq X \times Y$。若对每个 $x \in X$, $|N_Y(x)| \leq k$，则存在一个大小至多为 $2k^2$ 的子集$Y' \subseteq Y$，使得至少有 $|X|^2/2$ 个数对 $(x, x') \in X$ 满足$N_Y(x) \cap N_Y(x') \subseteq Y'$。

证明。事实上，令 $Y' = \{y \in Y\colon |N_X(y)| \geq |X|/2k\}$。那么

$$|Y'| \leq \frac{2k}{|X|} \sum_{y \in Y} |N_X(y)| = \frac{2k}{|X|} \sum_{x \in X} |N_Y(x)| \leq 2k^2.$$

令 $Y'' = Y \setminus Y'$，并观察到

$$\sum_{x,x' \in X} |N_{Y''}(x) \cap N_{Y''}(x')| = \sum_{y \in Y''} |N_X(y)|^2 \leq \frac{|X|}{2k} \sum_{x \in X} |N_Y(x)| \leq \frac{|X|^2}{2},$$

因此，至多一半的点对（x, x'）$\in X \times X$ 在 Y'之外有共同邻点。 □

推论 3.2. 设 A 是一个有限整数集，使得对于 $a \in A$, $\omega(a) \leq k$。那么存在一个至多包含 $r \leq 2k^2$ 个素数的集合 $P = \{p_1, \ldots, p_r\}$，使得

$$A = \bigcup_{\boldsymbol{v} \in \mathbb{N}_0^r} \boldsymbol{p}^{\boldsymbol{v}} \cdot B_{\boldsymbol{v}}$$

其中， $B_{\boldsymbol{v}}$是一个与 $p_1 p_2 \cdots p_r$ 互素的整数集合，并且满足

$$\sum_{\boldsymbol{v}, \boldsymbol{v}'} |\{(b, b') \in B_{\boldsymbol{v}} \times B_{\boldsymbol{v}'} : \gcd(b, b') = 1\}| \geq \frac{|A|^2}{2}.$$

证明。设 $X = A$ 和 $Y = \{p\colon\ p|a$，其中 $a \in A\}$，并设 $G = \{(a, p) \in X \times Y\colon\ p|a\}$。应用引理 3.1，我们得到 P，满足 $|P| = r \leq 2k^2$，使得对于至少一半的所有对 (a, a') $\in A \times A$，同时整除 a 和 a' 的所有素数都属于 P。每个 $a \in A$ 分解为

$$a = b_a \prod_{p \in P} p^{v_p(a)}$$

其中 b_a 与每个 $p \in P$ 互素，因此我们根据赋值 $v_p(a)$ 将 A 划分，其中 $p \in P$，于是得到

$$A = \bigcup_{\boldsymbol{v} \in \mathbb{N}_0^r} \boldsymbol{p}^{\boldsymbol{v}} \cdot B_{\boldsymbol{v}}$$

对于某些有限整数集 $B_{\boldsymbol{v}}$，它们与每个 $p \in P$ 互素。此外，若 (a, a') 是一对满足所有公共素因子都属于 P 的元素，则 b_a 与 $b_{a'}$ 互素。□

这样，我们从任意一组 A 整数中提取出一种伪乘积结构——其中一个因子来自低秩乘法群，另一个因子则是乘法独立的，因为其纤维两两互素。固定 $\mathbf{v}_1$，并注意到这些集合

$$\boldsymbol{p}^{\boldsymbol{v}_1} B_{\boldsymbol{v}_1} \cdot \boldsymbol{p}^{\boldsymbol{v}_2} B_{\boldsymbol{v}_2} = \boldsymbol{p}^{\boldsymbol{v}_1 + \boldsymbol{v}_2} B_{\boldsymbol{v}_1} \cdot B_{\boldsymbol{v}_2}$$

随着 $\mathbf{v}_2$的变化彼此不相交，因为它们按指数 $\mathbf{v}_1+\mathbf{v}_2$分层。现在假设有 $M(\mathbf{v}_1, \mathbf{v}_2)$ 对 $(b_1, b_2) \in B_{\boldsymbol{v}_1} \times B_{\boldsymbol{v}_2}$互素。那么，

$$\sum_{\boldsymbol{v}_1} \sum_{\substack{\boldsymbol{v}_2 \\ |B_{\boldsymbol{v}_1}| \geq |B_{\boldsymbol{v}_2}|}} M(\boldsymbol{v}_1, \boldsymbol{v}_2) \geq \frac{1}{2} \sum_{\boldsymbol{v}_1, \boldsymbol{v}_2} M(\boldsymbol{v}_1, \boldsymbol{v}_2) \geq \frac{|A|^2}{4},$$

由推论 3.2 的结论得出。但是

$$\sum_{\boldsymbol{v}_1} |B_{\boldsymbol{v}_1}| \sum_{\substack{\boldsymbol{v}_2 \\ |B_{\boldsymbol{v}_2}| \leq |B_{\boldsymbol{v}_1}|}} \frac{M(\boldsymbol{v}_1, \boldsymbol{v}_2)}{|B_{\boldsymbol{v}_1}|} \leq |A| \max_{\boldsymbol{v}_1} \frac{1}{|B_{\boldsymbol{v}_1}|} \sum_{\substack{\boldsymbol{v}_2 \\ |B_{\boldsymbol{v}_2}| \leq |B_{\boldsymbol{v}_1}|}} M(\boldsymbol{v}_1, \boldsymbol{v}_2),$$

因此，对于某个 $\mathbf{v}_1$，的取值，我们有

$$\sum_{\substack{\boldsymbol{v}_2 \\ |B_{\boldsymbol{v}_2}| \leq |B_{\boldsymbol{v}_1}|}} M(\boldsymbol{v}_1, \boldsymbol{v}_2) \geq \frac{|A||B_{\boldsymbol{v}_1}|}{4}.$$

令 $V' = \{\mathbf{v}_2 : \ |B_{\boldsymbol{v}_2}| \leq |B_{\boldsymbol{v}_1}|\}$且

$$A' = \bigcup_{\boldsymbol{v}_2 \in V'} \boldsymbol{p}^{\boldsymbol{v}_2} \cdot B_{\boldsymbol{v}_2},$$

使得

$$|A'| \geq \sum_{\boldsymbol{v}_2 \in V'} |B_{\boldsymbol{v}_2}| \geq \sum_{\boldsymbol{v}_2 \in V'} \frac{M(\boldsymbol{v}_1, \boldsymbol{v}_2)}{|B_{\boldsymbol{v}_1}|} \geq \frac{|A|}{4}.$$

进一步注意到，根据引理 1.3，在互素数对上，映射 $(b_1, b_2) \ \mapsto \ b_1 b_2$ 至多是 4^k-对一的，因此

$$(2) \qquad |A \cdot A| \geq |\boldsymbol{p}^{\boldsymbol{v}_1} B_{\boldsymbol{v}_1} \cdot A'| \geq \sum_{\boldsymbol{v}_2 \in V'} |\boldsymbol{p}^{\boldsymbol{v}_1 + \boldsymbol{v}_2} B_{\boldsymbol{v}_1} \cdot B_{\boldsymbol{v}_2}| \geq \frac{1}{4^k} \sum_{\boldsymbol{v}_2 \in V'} M(\boldsymbol{v}_1, \boldsymbol{v}_2) \geq \frac{|A||B_{\boldsymbol{v}_1}|}{4^{k+1}}.$$

如果 $B_{\boldsymbol{v}_1}$ 足够大，这是一个很好的估计。否则，我们必须借助加法增长。我们从上述 Chang 引理开始；在我们所需的特殊情形下，无需进行傅里叶分析。

引理 3.3（Chang）。设 A 是一个有限整数集，其分解形式为

$$A = \bigcup_{\boldsymbol{v} \in \mathbb{N}_0^r} \boldsymbol{p}^{\boldsymbol{v}} B_{\boldsymbol{v}},$$

其中每个 $B_{\boldsymbol{v}}$ 都是与 p_1、……、p_r 互素的有限整数集。则

$$E_+(A, A)^{1/2} \ll_r \sum_{\boldsymbol{v}} E_+(B_{\boldsymbol{v}}, B_{\boldsymbol{v}})^{1/2}.$$

特别地，

$$E_+(A, A) \ll_r |A|^2 \max_{\boldsymbol{v}} |B_{\boldsymbol{v}}|.$$

证明。为方便起见，将 A 替换为 $A \cup -A$，从而假设 $A = -A$。令 $p = p_1$。考虑方程

$$a_1 - a_2 = a_3 - a_4$$

变量取自 A。假设，在所有 $v_p(a_i)$中， a_1 的 p进赋值 $v_p(a_1)$最小。那么，将 $a_1 = a_2 + a_3 - a_4$ 模 $p^{v_p(a_1)+1}$约化后可知，方程中的另一项必须具有相同的 p进赋值；经过重新排列，代价仅为一个常数因子，该项就是 a_2。

由此可得

$$E_+(A,A) \ll \sum_v E(p^v B_v, A) \ll \sum_v E_+(B_v, B_v)^{1/2} E_+(A,A)^{1/2},$$

由柯西–施瓦茨不等式（应用于加法能量）并约去 p^v。整理后，对 $\{p_1, \dots, p_r\}$中的每个素数应用所得估计，可得

$$E_+(A,A)^{1/2} \ll_r \sum_{\boldsymbol{v}} E(B_{\boldsymbol{v}}, B_{\boldsymbol{v}})^{1/2}.$$

最后一个结论由应用平凡估计

$$E_+(B_{\boldsymbol{v}}, B_{\boldsymbol{v}}) \le |B_{\boldsymbol{v}}|^3$$

于每个加数得出，因此

$$E_+(A,A)^{1/2} \ll_r \max_{\boldsymbol{v}} |B_{\boldsymbol{v}}|^{1/2} \sum_{\boldsymbol{v}} |B_{\boldsymbol{v}}| = \max_{\boldsymbol{v}} |B_{\boldsymbol{v}}|^{1/2} |A|.$$

□

将 Chang 引理应用于上文的集合 A'，可得

$$|A + A| \ge |A' + A'| \gg_k \frac{|A'|^2}{|B_{\boldsymbol{v}_1}|} \gg \frac{|A|^2}{|B_{\boldsymbol{v}_1}|}.$$

结合 (2)，我们得到指数为 $3/2$ 的和积估计。此外，通过追踪 Chang 引理证明中的依赖关系可知，隐含常数关于 r 至多呈单指数增长，而 r 至多为 $2k^2$。

4. A refined structure theorem

我们精细化后的结构定理在思想上与推论 3.2 类似，但我们将力求使纤维 $B_{\boldsymbol{v}}$ 相同。一般来说，这样的断言过于理想化，但可以通过用一个具有结构的集合覆盖子集 $A \subseteq A$ 而使其成立。最终，我们将估计 A的加法能量；加法能量在集合上具有单调性，因此覆盖便足够了。至于 A的乘法结构，在我们的情形中，我们需要相对于 A的对偶分解进行正则化，具体如下述引理所述。

引理 4.1（迭代引理）。设 A 是一个具有性质$\omega(a) \le k$的有限整数集，其中 $a \in A$。令 p_1、……、p_j为互不相同的素数，并设 A分解为

$$A = \bigcup_{b \in B} b \cdot \Gamma_b,$$

对于某个由与 $p_1 \cdots p_j$ 互素的整数构成的集合 B，以及集合 $\Gamma_b \subseteq \langle p_1、\ldots\ldots、p_j \rangle_+$。那么下列情况之一成立：

(1) 要么 $|B| \le 2k$，要么至少一半的数对 $(a, a') \in A \times A$ 满足 $\gcd(a, a') \in \langle p_1、\ldots\ldots、p_j \rangle$；

(2) 存在一个素数 p_{j+1}，它不同于 $p_1、\ldots\ldots、p_j$，以及一个大小为

$$|\tilde{A}| \ge \frac{|A|}{2(k-j)\log_2 |A|},$$

且具有如下形式

$$\tilde{A} = \bigcup_{b \in \tilde{B}} b \cdot \tilde{\Gamma}_b$$

~ ~对于某个由与 $p_1 \cdots p_{j+1}$ 互素的整数构成的集合 B，以及集合 $\Gamma_b \subseteq \langle p_1、\ldots\ldots、p_{j+1} \rangle_+$，其大小~满足 $L \le |\Gamma_b| \le 2L$，其中某个 $L \ge 1$。

Proof. 令 P_A 表示整除 A 中某个元素的素数集，并令 t

$$P = P_A \setminus \{p_1, \ldots, p_j\}.$$

考虑二分图

$$G = \{(a, p) \in A \times P : p | a\}$$

并注意到 $\gcd(a, a') \notin \langle p_1, \ldots, p_j \rangle$ 当且仅当 a和 a'在 P中有一个共同邻居。现在，用 $N_P(a)$表示 a在 P中的邻居，我们有 $|N_P(a)| \le k - j$，因为每个a至多有 k个素因子，其中 j 个是 $p_1, \ldots, p_j$。因此，用 $N_A(p)$表示 p在 A中的邻居，通过双重计数我们得到

$$(k-j)|A| \ge \sum_{a \in A} |N_P(a)| = \sum_{p \in P} |N_A(p)| \ge \frac{1}{\max_p |N_A(p)|} \sum_{p \in P} |N_A(p)|^2.$$

若（1）不成立且 $|B| > 2k$，则上面的最右侧求和至少为 $|A|^2/2$，因此存在某个 $p_{j+1} \in P$，使得 $|N_A(p_{j+1})| \ge |A|/2(k-j)$。令 $A' = N_A(p_{j+1})$，于是 A' 可进一步分解（通过提出适当次幂的 p_{j+1}），得到

$$A' = \bigcup_{b' \in B'} b' \cdot \tilde{\Gamma}_{b'}$$

其中

$$B' = \{p_{j+1}^{-v_{j+1}(b)} b : b \in B,\ p_{j+1} | b\},$$

其中，$v_{j+1}(b)$ 是 b 的 p_{j+1}-进赋值。

现在我们使用二进制鸽巢法:

$$\frac{|A|}{2(k-j)} \le \sum_{b' \in B'} |\tilde{\Gamma}_{b'}| \le \sum_{l \le \log_2 |A|} 2^l |B'_l|$$

其中

$$B'_l = \{b' \in B' : 2^l \le |\tilde{\Gamma}_{b'}| < 2^{l+1}\}.$$

因此，取一个使 l 的加数达到最大值的值，并令 $L = 2^l$ 和 $\tilde{B} = B'_l$，我们~得到某个形如以下形式的子集 $A \subseteq A'$

$$\tilde{A} = \bigcup_{b \in \tilde{B}} b \cdot \tilde{\Gamma}_b$$

其大小至少为 $|\tilde{A}| \ge 2^{\frac{|A|}{(k-j)\log_2 |A|}}$，且具有如下性质：每个纤维 $\tilde{\Gamma}_b$的大小均属于 $[L, 2L]$。□

定理 4.2. 假设 A 是一个有限整数集，使得对 $a \in A$ 和$|A \cdot A| \le K|A|$有 $\omega(a) \le k$ 。那么存在一个至多含有 $r \le k$ 个素数的集合 $P = \{p_1, \dots, p_r\}$，以及一个大小至少为 $|A|/(2^k k!(\log_2 |A|)^k)$ 的集合$\tilde{A} \subseteq A$，并具有如下结构分解

$$\tilde{A} = \bigcup_{v \in V} \boldsymbol{p}^{\boldsymbol{v}} \cdot B_{\boldsymbol{v}} = \bigcup_{b \in B} b \cdot \Gamma_b,$$

其中每个集合 $B_{\boldsymbol{v}}$都是一个与 $p_1 \cdots p_r$互素的有限整数集，$B = \bigcup_{v \in V} B_{\boldsymbol{v}}$满足 $|B| \le 4^{k+2} K|A|/|\tilde{A}|$；且每个集合 Γ_b都是 $\langle p_1, \dots, p_r \rangle$ 的子集，其大小为 $L \le |\Gamma_b| \le 2L$，其中 L取适当的值。

证明。以 $A_0 = B_0 = A$、$j = 0$ 和每个 $\Gamma_b = \{1\}$ 为起点，反复应用迭代引理，直到满足结论 (1)。我们得到一列互不相同的素数 $p_1, \dots, p_r$，一列集合 $A_0 \supseteq \cdots \supseteq A_r$，使得 $p_1 \cdots p_i$ 整除 A_i 中的每个元素；以及~个整数集合 $B_1, \dots, B_r$，使得 B_i 与 $p_1 \cdots p_i$ 互素。这里 $A_{i+1} = A_i$、$B_{i+1} = B_i$ 是引理结论 (2) 中的记号。由于 $p_1 \cdots p_i$ 整除 A_i 中的每个元素，且 B_i 与 $p_1 \cdots p_i$ 互素，因此对于 $b \in B_i$，有 $\omega(b) \le k - i$。所以，经过 k 次迭代后，结论 (1) 必定成立，从而 $r \le k$。

~我们设定 $B = B_r$ 和 $A = A_r$，于是得到

$$\tilde{A} = \bigcup_{b \in B} b \cdot \Gamma_b$$

对某些集合 $\Gamma_b \subseteq \langle p_1, \dots, p_{j+1} \rangle_+$，其大小满足 $L \le |\Gamma_b| \le 2L$，其中某个 $L \ge 1$。我们还有如下估计

$$|\tilde{A}| \ge \frac{|A|}{2^k k! (\log_2 |A|)^k}.$$

To ~为了得到定理中所述的 A 另一种形式，考虑分解 n

$$\tilde{A} = \bigcup_{\boldsymbol{v} \in V} \boldsymbol{p}^{\boldsymbol{v}} B_{\boldsymbol{v}}$$

˜其中 p = $(p_1, \dots, p_r)$, $V = \{(v_{p_1}(a) \dots, v_{p_r}(a)) : a \in A\}$ 且

$$B_{\boldsymbol{v}} = \{b \in B : \boldsymbol{p}^{\boldsymbol{v}} \in \Gamma_b\}.$$

˜现在我们估计 $|B|$。此时，$A = \bigcup_{b\in B} b \cdot \Gamma_b$ 的并集互不相交，因此有

$$\tilde{A} \cdot \tilde{A} = \bigcup_{q\in B\cdot B} q \cdot \bigcup_{bb'=q} \Gamma_b \cdot \Gamma_{b'},$$

其中外层并集也互不相交。事实上， B 和 $B \cdot B$分别由关于群 $\langle p_1$、.....、 $p_r\rangle$的陪集 ˜ ˜ ˜代表元组成，而 A和 $A \cdot A$ 分别对应这些群。因此，由平凡估计 $|\Gamma_b \cdot \Gamma_{b'}| \geq L$ 可知

$$K|A| \geq |\tilde{A} \cdot \tilde{A}| \geq |B \cdot B|L \geq \frac{|B \cdot B||\tilde{A}|}{2|B|}.$$

假设 b、$b' \in B$满足：存在一对 $(a, a') \in (b \cdot \Gamma_b) \times (b' \cdot \Gamma_{b'})$，使得最大公约数$(a, a') \in \langle p_1$, ..., $p_r\rangle$。那么必有最大公约数$(b, b') = 1$，因此

$$|\{(b, b') \in B \times B : \gcd(b, b') = 1\}| \geq \frac{1}{4L^2}|\{(a, a') \in \tilde{A} \times \tilde{A} : \gcd(a, a') \in \langle p_1, \dots, p_r\rangle\}|.$$

由于迭代只能在条件 (1) 成立时终止，因此要么 $|B| \leq 2k$，这比所要求的结论更强；要么上面的右端至少为$|\tilde{A}|^2/8L^2$。在后一种情况下，引理 1.3 告诉我们

$$|B \cdot B| \geq \frac{|\tilde{A}|^2}{8L^2 4^k} \geq \frac{|B|^2}{8 \cdot 4^k},$$

因此，

$$K|A| \geq \frac{|B||\tilde{A}|}{4^{k+2}}.$$

□

5. Fourier Analysis

Chang 估计，引理 3.3，可以描述为对由有限素数集生成的乘法群子集中 $\Lambda(q)$ 常数的估计（通常称为 S-单位）。然而，在某些情况下，该估计略显粗糙，这是应用 H¨older 不等式的结果，而这种应用有时效率不高。我们证明中的下一个要素是沿着一个倍数序列进行 Littlewood-Paley 分解的平方函数估计。本节的最终目标是证明以下定理。

ˆ定理 5.1. 设 p = $(p_1, \dots, p_r)$ 是一个由互不相同的素数组成的 r-元组，并设 $f(t)$ $= \sum_{a\in A} f(a)e(at)$ 是一个三角多项式，其傅里叶系数支撑在一个形如 A 的集合中

$$A = \bigcup_{\boldsymbol{v}\in V} \boldsymbol{p}^{\boldsymbol{v}} B_{\boldsymbol{v}},$$

其中每个集合 $B_{\boldsymbol{v}}$ 都是由与 $p_1 \cdots p_r$ 互素的整数构成的集合。定义

$$f_{\boldsymbol{v}}(t) = \sum_{b \in B_{\boldsymbol{v}}} \widehat{f}(\boldsymbol{p}^{\boldsymbol{v}} b) e(\boldsymbol{p}^{\boldsymbol{v}} b t).$$

那么对于任意满足 $1 < q < \infty$ 的 q，都存在一个常数 $C_q > 0$，使得

$$\|f\|_{L^q} \leq C_q^r \left\| \left(\sum_{\boldsymbol{v}} |f_{\boldsymbol{v}}|^2 \right)^{1/2} \right\|_{L^q}.$$

至少当 $r = 1$ 时，这一结果可以相当直接地由 Burkholder鞅Littlewood-Paley定理推出。[EG], [P], 和 [St] 都有易于阅读的阐述。事实上，Gundy 和 Varapoulos 此前已在 [GV] 中指出，上述结论可以作为 Burkholder定理 的推论。熟悉此类平方函数估计的专家可以跳过本节剩余部分；下面我们将介绍证明中的一些要点。我们作此阐述，部分是为了使内容完整，尽管我们并不证明 Burkholder定理；同时也是为了将所需的事实汇集于同一来源之中（这些内容也可在 [EG] 的不同部分找到）。除了将这些事实专门用于当前应用之外，我们不主张有任何原创性。

$\widehat{}$应用定理 5.1，并取 $q = 4$ 和 $f = \mathbf{1}_A$，我们得到 Chang 能量估计的如下改进。

推论 5.2。设 $A \subseteq \mathbb{Z}$ 是一个形如.....的有限集。

$$A = \bigcup_{\boldsymbol{v} \in V} \boldsymbol{p}^{\boldsymbol{v}} B_{\boldsymbol{v}}.$$

那么存在一个常数 $C > 0$

$$E(A, A) \leq C^r \sum_{\boldsymbol{v}, \boldsymbol{v}' \in V} E(\boldsymbol{p}^{\boldsymbol{v}} B_{\boldsymbol{v}}, \boldsymbol{p}^{\boldsymbol{v}'} B_{\boldsymbol{v}'}).$$

推论 5.2 与柯西-施瓦茨不等式结合后，可以恢复 Chang 的原始估计。然而，我们将在下一节看到，对于许多对 $(\mathbf{v}_1, \mathbf{v}_2)$，我们得到的结果远优于平凡的能量估计。

如上所述，为了证明定理 5.1，我们将使用 Burkholder 关于鞅变换的不等式。具体而言，我们将使用以下结果，它给出了在 p-进尺度上为常数的乘子的范数界。下文中，我们记♀♀♀♀♀♀

$$f_\varepsilon(t) = \sum_{n \in \mathbb{Z}} \varepsilon(n) \widehat{f}(n) e(nt).$$

定理 5.3. 设 p 是一个素数，并假设 q 满足 $1 < q < \infty$。设 $\varepsilon : \mathbb{Z} \to \{-1, 1\}$是一个函数，使得 $\varepsilon(n)$仅依赖于 $v_p(n)$。那么存在一个绝对常数 C_q，它仅依赖于 q，使得

$$\|f\|_{L^q} \leq C_q \|f_\varepsilon\|_{L^q}.$$

可以将 ε 视为随机选取，但需满足它在 p-进尺度上为常数这一约束。于是，通过欣钦不等式可知，上述乘子定理等价于定理 5.1 中引用的平方函数估计（在 $r=1$的情形下）。先介绍一些记号：对于 $\mathbb{Z}$的一个划分 $\mathcal{P}$，记

$$(S_{\mathcal{P}}f)(t)=\left(\sum_{P\in\mathcal{P}}\left|\sum_{n\in P}\widehat{f}(n)e(nt)\right|^2\right)^{1/2}.$$

引理 5.4. 设 $\mathcal{P}$ 是 $\mathbb{Z}$的一个划分。那么以下条件等价：　　t:

(1) 对任意 $q>1$，存在常数 c_q 和 C_q，使得对任意三角多项式f,

$$c_q\|f\|_{L^q}\le\|S_{\mathcal{P}}f\|_{L^q}\le C_q\|f\|_{L^q},$$

(2) 对任意 $q>1$，存在常数 C_q，使得对任意三角多项式 f和任意函数 ε：$\mathbb{Z}\to\{-1,1\}$（该函数在 $\mathcal{P}$的各部分上为常数），都有

$$\|f\|_{L^q}\le C_q\,\|f_\varepsilon\|_{L^q}.$$

证明。设

$$f_\varepsilon(t)=\sum_n\varepsilon(n)\widehat{f}(n)e(nt).$$

那么，假设引理中的条件 (1) 成立，

$$\|f\|_{L^q}\le\frac{1}{c_q}\,\|S_{\mathcal{P}}f\|_{L^q}=\frac{1}{c_q}\,\|S_{\mathcal{P}}f_\varepsilon\|_{L^q}\le\frac{C_q}{c_q}\|f_\varepsilon\|_{L^q}.$$

反过来，若假设引理中的条件 (2) 成立，则我们可以写成 $f=(f_\varepsilon)_\varepsilon$，因此得到反向不等式

$$\|f_\varepsilon\|_{L^q}^q\le C_q^q\|f\|_{L^q}^q$$

成立，并对所有 ε 的选择取期望，

$$C_q^q\|f\|_{L^q}^q\ge\mathbb{E}_\varepsilon\|f_\varepsilon\|_{L^q}^q=\int_0^1\mathbb{E}_\varepsilon\left|\sum_{P\in\mathcal{P}}\varepsilon(P)\sum_{n\in P}\widehat{f}(n)e(nt)\right|^q dt.$$

We g由欣钦不等式（例如，参见 [MS] 的引理 5.5）可得 th　　at

$$\mathbb{E}_\varepsilon\left|\sum_{P\in\mathcal{P}}\varepsilon(P)\sum_{n\in P}\widehat{f}(n)e(nt)\right|^q\ge c_q'\left(\sum_{P\in\mathcal{P}}\left|\sum_{n\in P}\widehat{f}(n)e(nt)\right|^2\right)^{q/2}=c_q'(S_{\mathcal{P}}f)^q,$$

这就通过对 $t\in[0,1]$ 积分，证明了不等式 (1) 中的第二个不等式。

为证明条款 (1) 中的第一个不等式，我们运用对偶性。令 q' 为 q 的对偶指数，并取一个三角多项式 g，使得 $\|g\|_{L^{q'}}=1$。根据正交性和三角不等式，

$$|\langle f,g\rangle|\le\int_0^1\sum_{P\in\mathcal{P}}\left|\sum_{n\in P}\widehat{f}(n)e(nt)\right|\left|\sum_{n\in P}\widehat{g}(n)e(nt)\right|dt.$$

根据柯西-施瓦茨不等式，右侧至多为

$$\langle S_{\mathcal{P}} f, S_{\mathcal{P}} g\rangle \le \|S_{\mathcal{P}} f\|_{L^q} \|S_{\mathcal{P}} g\|_{L^{q'}} \le C_{q'} \|S_{\mathcal{P}} f\|_{L^q}$$

其中在最后一个估计中，我们对 g 应用了 Hölder 不等式以及条款 (1) 中的第二个不等式。□

这里我们指出，利用上述证明的最后一部分，通常只需证明 (1) 中的第二个不等式，进而可由对偶性推出第一个不等式。

引入乘子表述的原因在于，它非常适合迭代，从而使我们能够证明以下结果。

引理 5.5。设 $q \ge 1$，并设 $\mathcal{P}_1$ 和 $\mathcal{P}_2$ 是 $\mathbb{Z}$ 的两个划分，使得对任意三角多项式 f，

$$\left\|S_{\mathcal{P}_j} f\right\|_{L^q} \le C_q(\mathcal{P}_j) \|f\|_{L^q}\,, \qquad j = 1, 2\,.$$

那么，若 $\mathcal{P} = \{P_1 \cap P_2 :\ P_1 \in \mathcal{P}_1,\ P_2 \in \mathcal{P}_2\}$，存在常数 $C_q(\mathcal{P})$，使得

$$\|S_{\mathcal{P}} f\|_{L^q} \le C_q(\mathcal{P}) \|f\|_{L^q}$$

证明。首先假设 $q \ge 2$。设 $\varepsilon :\ \mathbb{Z} \to \{-1, 1\}$ 是一个在 $\mathcal{P}_2$ 的各部分上为常数的函数，并设 f 是一个三角多项式。根据假设和引理 5.4，存在正常数 C，使得

$$\|f_\varepsilon\|_{L^q} \le C\|f\|_{L^q},$$

由此

$$\|S_{\mathcal{P}_1} f_\varepsilon\|_{L^q} \le C_q(\mathcal{P}_1)\|f_\varepsilon\|_{L^q} \le C_q(\mathcal{P}_1)C\|f\|_{L^q}.$$

Now

$$(S_{\mathcal{P}_1} f_\varepsilon(t))^2 = \sum_{P_1 \in \mathcal{P}_1} \sum_{n,m \in P_1} \varepsilon(n)\varepsilon(m)\widehat{f}(n)\overline{\widehat{f}(m)} e((n-m)t),$$

并对 ε 取期望，得到

$$\mathbb{E}_\varepsilon((S_{\mathcal{P}_1} f_\varepsilon(t))^2) = \sum_{P_1 \in \mathcal{P}_1} \sum_{P_2, P_2' \in \mathcal{P}_2} \sum_{\substack{n,m \in P_1 \\ n \in P_2, m \in P_2'}} \mathbb{E}_\varepsilon(\varepsilon(n)\varepsilon(m))\widehat{f}(n)\overline{\widehat{f}(m)} e((n-m)t).$$

除非 $P_2 = P_2'$，否则该期望为零；在 $P_2 = P_2'$ 的情况下，期望为 1，因此

$$\mathbb{E}_\varepsilon((S_{\mathcal{P}_1} f_\varepsilon(t))^2) = \sum_{P_1 \in \mathcal{P}_1} \sum_{P_2 \in \mathcal{P}_2} \sum_{n,m \in P_1 \cap P_2} \widehat{f}(n)\overline{\widehat{f}(m)} e((n-m)t) = (S_{\mathcal{P}} f(t))^2.$$

将两边提升至 $q/2$ 次方，得到

$$(S_{\mathcal{P}} f(t))^q = (\mathbb{E}_\varepsilon((S_{\mathcal{P}_1} f_\varepsilon(t))^2)^{q/2} \le \mathbb{E}_\varepsilon((S_{\mathcal{P}_1} f_\varepsilon(t))^q)$$

由詹森不等式，并对 t 积分可得

$$\|S_{\mathcal{P}} f\|_{L^q}^q \le (C_{\mathcal{P}_1} C)^q \|f\|_{L^q}^q,$$

这正是所需的。

为了得到 $1 \le q < 2$ 的结论，我们使用对偶性和随机乘子表述。事实上，设 $q' \ge 2$ 是与 q 共轭的指数，设 $\varepsilon : \mathbb{Z} \to \{-1, 1\}$ 是一个在 $\mathcal{P}$ 的各部分上为常数的函数，并设 g 是一个满足 $\|g\|_{L^{q'}} = 1$ 的三角多项式。那么根据帕塞瓦尔恒等式和 H¨older 不等式,

$$|\langle f_\varepsilon, g\rangle| = |\langle f, g_\varepsilon\rangle| \le \|f\|_{L^q}\|g_\varepsilon\|_{L^{q'}} \le C_{q'}(\mathcal{P})\|f\|_{L^q}$$

这表明对于任意 ε， $\|f_\varepsilon\|_{L^q} \le C_q\|f\|_{L^q}$： $\mathbb{Z} \to \{-1, 1\}$ 在 $\mathcal{P}$ 的各部分上为常数，因此 $S_{\mathcal{P}}$ 的有界性可由引理 5.4 得出。□

定理 5.1 的证明。对于每个满足 $1 \le i \le r$ 的素数 p_i，我们将 $\mathbb{Z}$ 划分为 p_i-进尺度，并与之关联划分 $\mathcal{P}_i$。由定理 5.3 和引理 5.4 可知，对于每个满足$1 \le i \le r$的素数 p_i，存在常数 C_q 使得 $\|S_{\mathcal{P}_i} f\|_{L^q} \le C_q\|f\|_{L^q}$。由对偶性，只需证明划分 $\mathcal{P}_i$ 的公共细化给出有界的平方函数。这又可由引理 5.5 应用 $r - 1$ 次得到。□

6. Energy estimates with Dilates

本节中，我们将证明：在秩有界的乘法群（或其陪集）中，差的数量的估计。当秩为一时，可以用初等方法得到这样的结果，如下列定理所述。除非 $k = 2$，否则我们不会用到该定理（不过，正如开篇所讨论的，这个特例本身已经相当非平凡）；但我们仍将其列出，因为无需借助更为高深的结果来证明我们的结论，或许本身也有一定价值。

定理 6.1. 设 B 是一个满足 $|B| \ge 2$ 的正整数有限集， p 是一个素数， n 是一个非零整数。定义

$$X_p(B, n) = \{(b_1, b_2) \in B \times B : b_1 - b_2 = np^v \text{ for some } v \in \mathbb{Z}_{\ge 0}\}.$$

则 $|X_p(B, n)| \le 1 + 4|B| \log_2 |B|$。

证明。设 p 是一个固定的素数。将 B 规范化如下会比较方便。首先，若 p 整除 n，则写作 $n = p^v n'$，其中 $\gcd(n', p) = 1$。于是 $X_p(B, n) \subseteq X_p(B, n')$，因此不妨假设 $\gcd(n, p) = 1$。其次，若 B 中的元素都属于模 p^{r_0} 的同一个同余类，其中 $r_0 > 0$，则可以用 $B - \min B$ 替换 B（或用 B 中的任意其他元素替换），而不影响 $|X_p(B)|$。这样一来， $B - \min B$ 中的元素都是 p^{r_0} 的倍数；又因为 p 不整除 n，所以可将 $|X_p(B, n)|$ 上界为 $|X_p(p^{-r_0}B, n)|$。因此还可以进一步假设， B 中的元素并非全都模 p 同余。

我们对 $|B|$进行归纳法。当 $|B| = 2$时，设 $B = \{b, b'\}$ 是一个集合，且 p 是一个素数。那么 $b - b' = p^r n$ 至多有一个 r取值，因此 $|X_p(B)| \le 1$ 由此得证17

基本情形。F 对于更大的 B，我们对 b （模 p）的取值进行分类。为此，我们写出

$$B_u = \{b \in B : b \equiv u \pmod p\}$$

并令 $\mu(u) = \frac{|B_u|}{|B|}$ 为相应的概率测度。给定 $b \equiv u \pmod p$，我们要么有 $b - b' = n$，此时 $b' \equiv u - n \pmod p$，而这类解至多贡献

$$\begin{aligned}\sum_{u \pmod p} \min\{|B_u|, |B_{u-n}|\} &= |B| \sum_{u \pmod p} \min\{\mu(u), \mu(n-u)\} \\ &\le |B| \sum_{u \pmod p} \min\{\mu(u), 1-\mu(u)\} \\ &= |B| \min\{1, 2 - 2\mu(u_{\max})\}\end{aligned}$$

个解，其中 $u_{\max}$ 是使 $\mu(u)$ 取值最大的剩余类。否则，对某个 $r > 0$ 有 $b - b' = p^r n$，此时 b 和 b' 模 p同余。因此

$$|X_p(B, n)| \le \sum_{u \pmod p} |X_p(B_u, n)| + |B| \min\{1, 2 - 2\mu(u_{\max})\}.$$

由于根据我们的归一化有 $B_u \ne B$，我们应用归纳法并得到

$$|X_p(B_u, n)| \le |B_u|(1 + 4\log_2 |B_u|) = \mu(u)|B|(1 + 4\log_2 |B|) - 4\mu(u)|B| \log(1/\mu(u)).$$

综上所述，

$$|X_p(B, n)| \le |B|(1 + 4\log_2 |B|) - 4|B|(H(\mu) - \frac{1}{4}\min\{1, 2 - 2\mu(u_{\max})\}).$$

Here

$$H(\mu) = \sum_{u \pmod p} \mu(u) \log_2 \frac{1}{\mu(u)}$$

是测度 μ的熵。我们断言

$$H(\mu) - \frac{1}{4}\min\{1, 2 - 2\mu(u_{\max})\}) \ge 0.$$

事实上，若 $\mu(u_{\max}) \le 1/2^{1/4}$ 则 $H(\mu) \ge 1/4$；否则，根据不等式

$$\frac{1-x}{2} \le \log_2 \frac{1}{x},$$

我们有

$$\frac{1 - \mu(u_{\max})}{2} \le \log_2 \frac{1}{\mu(u_{\max})} = \sum_{u \pmod p} \mu(u) \log_2 \left(\frac{1}{\mu(u_{\max})}\right) \le \sum_{u \pmod p} \mu(u) \log_2 \left(\frac{1}{\mu(u)}\right).$$

□

上述论证或许可以推广到高秩情形 $r > 1$。不过，我们可以直接借助一些关于 S-单位方程的强大工具来解决这个问题。下面的论证采用了关于乘法群中线性方程的一个定量估计，该估计取自 [AV], ，并改进了 [ESS]的工作。

定理 6.2（S-单位界）。设 $S = \{p_1, \dots, p_r\}$ 是一个有理素数集合，令$\Gamma = \langle S \rangle$ 为它们生成的乘法群。对于固定的 $a_1, \dots, a_l \in \mathbb{C}^\times$,

$$\left| \left\{ \gamma_1, \dots, \gamma_l \in \Gamma : \sum_{1 \le i \le l}^{*} a_i \gamma_i = 1 \right\} \right| \le (8l)^{4l^2 + lr + 1},$$

其中，记号 $\sum^*$ 表示非退化性，具体而言，对于非空真子集 $I \subset \{1, \dots, l\}$，有 $\sum_{i \in I} a_i \gamma_i \neq 0$ 。

我们需要这一估计来证明以下应用，该应用取自 [RNZ], （参见其中的引理 2.1）。我们给出证明，以便明确说明定量细节。我们引用有理数情形的结果，不过它适用范围要广泛得多。

引理 6.3（ [RNZ] 的引理 2.1）。设 $0 < \varepsilon < \frac{1}{6}$ 。对于任意充分大的有理数集合 B，以及由 r 个有理素数生成的乘法群 $\Gamma \subseteq \mathbb{C}^\times$ ，若满足 $r \le (\log |B|)^{1-6\varepsilon}$，则有以下估计

$$|\{(b_1, b_2) \in B \times B : b_1 - b_2 \in \Gamma\}| \le |B| \exp((\log |B|)^{1-\varepsilon}).$$

证明。为简化记号，令 $|B| = n$；如有必要，将 -1 并入 Γ 。考虑顶点集 B上的无向图 G ，其边为满足 $b_1 - b_2 \in \Gamma$的那些 $\{b_1, b_2\}$。用 $nf(n)$ 表示边数，其中 $f(n)$ 是某个函数。可以假设 $f(n)$ 单调递增且大于 $(\log n)^r$，否则便无须证明。

令 $d = f(n)/2$。我们首先通过反复移除度小于d的顶点来剪枝 G ，并在每一步之后更新各顶点的度（但不改变阈值 d），以反映任何顶点的移除。由于至多有 n个顶点可被移除，这一过程至多经过 n 步便会终止；终止时，我们移除的边不会超过 $n \cdot f(n)/2$ 条。如有必要，我们将 G 重新定义为剪枝图，其中每个顶点的度至少为 $f(n)/2$

固定一个顶点 b_0，并考虑 G中一条从 b_0出发、长度为 l 的非退化路径。路径 $b_0, b_1, \dots, b_l$ 对应于伸缩和

$$(b_1 - b_0) + (b_2 - b_1) + \ldots + (b_l - b_{l-1}) = \gamma_1 + \gamma_2 + \ldots + \gamma_l,$$

如果右侧的任何子和都不为零，我们就称该路径为非退化路径。给定一条长度为 l的非退化路径，我们至少可以向其追加 $f(n)/2 - (2^l - 1)$条边，从而得到一条长度为 $l+1$的非退化路径。事实上，可能导致退化的边只有 $2^l - 1$ 条。因此，通过归纳法可知，长度为 l 的非退化路径至少有 $f(n)^l/4^l$条，前提是 $f(n) \ge 2^{l+2}$。

因此， $f(n)^{l-1}/(4^{l-1}n)$与某个其他元素 $b \in B$之间至少有 b_0 条非退化路径，因此，在追加一条边 $b - b_1$后，从 b_0到某个 $b_1 \in B$的路径数为 $f(n)^l/(4^l n)$

到上述路径上。另一方面，对于此路径数，定理 6.2 给出了上界，只需为 $1 \le i \le l$选择 $a_i = 1/(b_1 - b_0)$。取对数，并假设$r \ge 2$ 和（比如） $l \ge 100$，即可将上界简化为

$$l \log f(n) \le l^{\frac{11}{2}} r + \log n$$

选择 $l \approx \left(\frac{\log n}{r}\right)^{\frac{2}{11}}$使右端各项达到平衡后，我们得到

$$\log f(n) \ll r^{\frac{2}{11}} (\log n)^{\frac{9}{11}},$$

结合引理陈述中假设的关于 r 的界，即完成证明。□

注意，在引理 6.3 中，条件 $b_1 - b_2 \in \Gamma$ 可以通过将 B放大，把它替换为陪集归属条件 $b_1 - b_2 \in u \cdot \Gamma$。

7. 定理 1.1 的证明

设 A 是一个有限整数集，使得对每个 $a \in A$，都有 $\omega(a) \le k$。必要时取一个子集并按 -1 放大，我们可以假设 $A \subset \mathbb{N}$，代价是一个常数因子。令 $K = |A \cdot A|/|A|$，并应用定理 4.2，得到一个集合以及一个大小为 $A \subseteq A$ 的集合

$$|\tilde{A}| \ge \frac{|A|}{2^k k! (\log_2 |A|)^k} \ge \frac{|A|}{(\log |A|)^{3k}}, \tag{3}$$

根据对 k所假设的界，并具有如下结构

$$\tilde{A} = \bigcup_{\boldsymbol{v} \in V} \boldsymbol{p}^{\boldsymbol{v}} \cdot B_{\boldsymbol{v}} = \bigcup_{b \in B} b \cdot \Gamma_b,$$

其中每个 $B_{\boldsymbol{v}}$都是一个与 $p_1 \cdots p_r$互素的有限整数集，且它们的并集$B = \bigcup_{\boldsymbol{v} \in V} B_{\boldsymbol{v}}$满足

$$|B| \le \frac{4^{k+2} K |A|}{|\tilde{A}|}, \tag{4}$$

而每个 Γ_b都是 $\Gamma = \langle p_1、\ \ldots\ldots、\ p_r \rangle$ 的子集，其大小满足 $L \le |\Gamma_b| \le 2L$，其中 L取适当值。

现在我们估计 A的加法能量。为此，不妨假设 $A = -A$，代价是一个常数。由推论 5.2，我们有

$$E(\tilde{A}, \tilde{A}) \le C^k \sum_{\boldsymbol{v}_1, \boldsymbol{v}_2 \in V} E(\boldsymbol{p}^{\boldsymbol{v}_1} B_{\boldsymbol{v}_1}, \boldsymbol{p}^{\boldsymbol{v}_2} B_{\boldsymbol{v}_2}).$$

上面的和统计了 A 中满足方程

$$a_1 - a_2 = a_3 - a_4,$$

其中，对于某些 $b_1、\ b_2 \in B_{\boldsymbol{v}_1}$，有 $a_1 = b_1 \mathrm{p}^{\boldsymbol{v}_1}、\ a_2 = b_2 \mathrm{p}^{\boldsymbol{v}_1}$；对于某些$b_3、\ b_4 \in B_{\boldsymbol{v}_2}$，有 $a_3 = \mathrm{p}^{\boldsymbol{v}_2} b_3、\ a_4 = \mathrm{p}^{\boldsymbol{v}_2} b_4$。换句话说，我们已将问题化归为能量方程左右两侧出现的指数均为重复指数的情形。

现在令 $\gamma = \mathrm{p}^{v_1}$ 和 $\gamma' = \mathrm{p}^{v_2}$，于是我们只需计算下式的解的数量

$$b_1 - b_2 = \gamma^{-1}\gamma'(b_3 - b_4), \tag{5}$$

其中现在有 b_1、. . .、$b_4 \in B$、$\gamma \in \Gamma_{b_1} \cap \Gamma_{b_2}$ 和 $\gamma' \in \Gamma_{b_3} \cap \Gamma_{b_4}$。满足 $b_3 = b_4$ 的解仅对应于 $\tilde{A}$ 中能量方程的平凡解，而这类解至多有 $|\tilde{A}|^2$ 个。对于其余解，固定 b_3、b_4 和 γ'，然后注意到，根据引理 6.3，方程 (5) 的解至多有 $O(|B| \exp((\log |B|)^{1-\varepsilon}))$ 个。$|B|$ 至多有 b_4 种选择，而至多有

$$\sum_{b \in B} |\Gamma_b| = |\tilde{A}|$$

对 (b_3, γ') 这一对有若干种选择。综合以上所有结果，我们得到

$$E(\tilde{A}, \tilde{A}) \ll C^k(|\tilde{A}|^2 + |\tilde{A}||B|^2 \exp((\log |B|)^{1-\varepsilon})) \ll C^k \left(|\tilde{A}|^2 + K^2|\tilde{A}| \exp(2(\log |A|)^{1-\varepsilon})\right)$$

˜，其中代入了由 (4) 和 (3) 得到的 $|B|$ 和 $|A|$ 的相应界。如果量 $C^k|\tilde{A}|^2$ 占主导，则我们已经证明了比所需更多的结论。否则，根据界 (3)，只需证明

$$K|A| + \frac{|A|^3}{K^2} \gg |A|^{\frac{5}{3}}$$

wh这是显然的，因为当 $K \approx |A|^{2/3}$ 时，左侧大小达到最小值。

References

[AV] F. Amoroso 和 E. Viada，《环面子簇上的小点》。《杜克数学杂志》150（2009），第 3 期，407–442。[BW] A. Balog 和 T. D. Wooley，《低能量分解定理》。《季刊数学杂志》68（2017），第 1 期，207–226。[BC] J. Bourgain 和 M.-C. Chang，《关于整数的 k 重和集与积集的大小》。《美国数学会杂志》17（2004），第 2 期，473–497。[Bu] D. L. Burkholder，《鞅变换》。《数学统计年刊》37（1966），1494–1504。[Ch] M.-C. Chang，《Erd ˝os-Szemer ´edi 关于和集与积集的问题》。《数学年刊》（第 2 辑）157（2003），第 3 期，939–957。[EG] R. E. Edwards 和 G. I. Gaudry，《Littlewood-Paley 理论与乘子理论》。《数学及其边界领域成果》，第 90 卷。Springer-Verlag，柏林—纽约，1977。ix+212 页。[E] G. Elekes，《关于和与积的数量》。《算术学报》81（1997），第 4 期，365–367。[ES] P. Erd ˝os 和 E. Szemer ´edi，《关于整数的和与积》。《纯数学研究》，213–218，Birkh ¨auser，巴塞尔，1983。[ESS] J. H. Evertse、H. P. Schlickewei 和 W. M. Schmidt，《乘法群中元素所满足的线性方程》。《数学年刊》（第 2 辑）155（2002），第 3 期，807–836。[GT] B. Green 和 T. Tao，《素数包含任意长的等差数列》。《数学年刊》（第 2 辑）167（2008），第 2 期，481–547。[GV] R. F. Gundy 和 N. Th. Varopoulos，《调和分析中出现的一个鞅》。《阿克数学》14（1976），第 2 期，179–187。[HRNR] B. Hanson、O. Roche-Newton 和 M. Rudnev，《高阶凸性与迭代和集》。《组合数学》42（2022），第 1 期，71–85。[HRNZ1] B. Hanson、O. Roche-Newton 和 D. Zhelezov，《带平移的迭代积集》。《Mathematika》65（2019），第 4 期，831–850。

[HRNZ2] B. Hanson、O. Roche-Newton 和 D. Zhelezov，《带平移的迭代积集（II）》。《代数与数论》14（2020），第 8 期，2239–2260。[KR] S. V. Konyagin 和 M. Rudnev，《关于新的和积型估计》。《SIAM 离散数学杂志》27（2013），第 2 期，973–990。[MSt] A. Mohammadi 和 S. Stevens，《在有限域和-积问题中达到 $5/4$ 指数》。《国际数学研究通知》2023，第 4 期（2023）：3516–3532。[MV] H. L. Montgomery 和 R. C. Vaughan，《乘法数论。I. 经典理论》。剑桥高等数学研究丛书，第 97 卷。剑桥大学出版社，剑桥，2007。xviii+552页。[MRSS] B. Murphy、M. Rudnev、I. Shkredov 和 Yu. Shteinikov，《关于少积多和问题》。《波尔多数论杂志》31（2019），第 3 期，573–602。[MS] C. Muscalu 和 W. Schlag，《经典与多线性调和分析》。第 I 卷。剑桥高等数学研究丛书，第 137 卷。剑桥大学出版社，剑桥，2013。[N] M. B. Nathanson，《关于整数的和与积》。《美国数学会会刊》125（1997），第 1 期，9–16。[PZ] D. P´alv´olgyi 和 D. Zhelezov，《查询复杂度与多项式 Freiman-Ruzsa 猜想》。《数学进展》392（2021），论文编号 108043，18 页。[P] G. Pisier，《Banach 空间中的鞅》。剑桥高等数学研究丛书，第 155 卷。剑桥大学出版社，剑桥，2016。xxviii+561页。[RNZ] O. Roche-Newton 和 D. Zhelezov，《和集乘法能量的上界与极值和积问题》。《莫斯科组合与数论杂志》5（2015），第 1–2 期，52–69。[RSh] M. Rudnev 和 I. D. Shkredov，《$\mathrm{SL}_2(\mathbb{F}_p)$、仿射群中的增长率及和积型推论》。《Mathematika》68（2022），第 3 期，738–783。[RSt] M. Rudnev 和 S. Stevens，《和-积问题最新进展》。《剑桥哲学会数学会刊》173（2022），第 2 期，411–430。[So] J. Solymosi，《用和集给出乘法能量上界》。《数学进展》222（2009），第 2 期，402–408。[St] E. M. Stein，《与 Littlewood-Paley 理论相关的调和分析主题》。《数学年刊研究丛书》，第 63 号，普林斯顿大学出版社，普林斯顿，新泽西州；东京大学出版社，东京，1970。viii+146 页。[TV] T. Tao 和 V. Vu，《加法组合学》。剑桥高等数学研究丛书，第 105 卷。剑桥大学出版社，剑桥，2006。xviii+512 页。

University of Maine, Orono, Maine, U.S.A.电子邮箱：brandon.w.hanson@gmail.com
School of Mathematics, University of Bristol, Bristol BS8 1UG, U.K.电子邮箱：misharudnev@gmail.com 电子邮箱：ilya.shkredov@gmail.com
Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria电子邮箱：dzhelezov@gmail.com