arXiv:2603.06483v1 [math.NT] 6 Mar 2026

代数群的统一和积现象与 Bremner 猜想

JOSEPH HARRISON、AKSHAT MUDGAL、HARRY SCHMIDT

Abstract. 本文结合加性组合学与丢番图几何的方法，研究代数群中的广义和积现象。作为这一系列思想的应用，我们解决了 Bremner 关于椭圆曲线坐标中算术级数的猜想，以及文献中研究的其他若干推广问题。

我们还证明了在 $\mathbb{C}$ 上一般一维代数群 G 的统一 Bourgain–Chang型和积估计。利用这些思想，我们为 Bays–Breuillard 的一个问题提供了另一种解法。此外，在相同的背景下，我们针对小倍增的集合证明了一个 Elekes–Szab´o 型结果；当 G 不为 $\mathbb{G}_a$ 时，这改进了 Bays–Breuillard 先前的结果。我们还可以证明，此处的幂次节省在定量意义上是最优的。

我们结合了 David–Philippon、Laurent 和 Evertse–Schmidt–Schlickewei 在丢番图几何方面的深厚经典成果，以及 Gowers–Green–Manners–Tao 最近在整数上的弱多项式 Freiman–Ruzsa 猜想方面取得的突破性进展。

1. Introduction

数论中的许多问题都涉及两种不同算术结构之间的不相容。Bremner 在研究椭圆曲线有理点的坐标中等差数列的长度时，注意到了这一现象。这里，以等差数列为代表的加性结构与椭圆曲线上的群结构应当彼此不相关，这使他猜测，可能出现的等差数列长度应仅由曲线的秩决定。他与 Silverman 和 Tzanakis 合作的研究部分证实了这一猜想。

这一现象的另一个例子，是 Erdős–Szemerédi 提出的组合数论中著名的和积猜想。该猜想关注整数有限集在进行求和或求积运算时的扩张，这体现了加性结构与乘性结构之间的不相容性。对这类问题的研究进展，已在数论和调和分析中催生了各种应用。

这一现象的第三个例子涉及任意实数集在充分非退化的多项式映射下的扩张。Elekes– R´onyai [13] 和 Elekes–Szab´o [14], 最早研究了这一问题。自他们的工作以来，这一领域取得了长足进展，部分原因是它与组合几何中的问题以及

2020 数学主题分类。11B13, 11B25, 11B30,11G05。关键词和短语。代数群上的 Bourgain–Chang 和积结果、Bremner 猜想、Mordell–Lang、Freiman–Ruzsa定理、Elekes–Szab´o。

模型论中的课题有关。在本文中，我们统一这些乍看之下彼此迥异的主题，并证明了关于它们的有效定量结果。

我们首先转向 Bremner 提出的一个问题，该问题涉及椭圆曲线有理点坐标中等差数列可能长度的上界。若将加性结构替换为乘法结构，同样可以推测等比数列的长度应有上界，参见 Bremner–Ulas[6]的研究。另一个相关方向关注椭圆曲线有理点坐标中连续平方数序列的最长长度，参见 Kamel–Sadek [28]的研究。

作为本文所讨论方法的直接推论，我们证实了 Bremner 的猜想 [5,§5]如下的一般结果。

定理 1.1. 存在一个可有效计算的常数 $C \geq 1$，具有以下性质。设 E 是一个魏尔斯特拉斯形式的椭圆曲线

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}, \tag{1.1}$$

并令 r 为 $E(\mathbb{Q})$的秩。令 $X = \{x(P) \colon P \in E(\mathbb{Q})\}$ 以及 $Y = \{y(P) \colon P \in E(\mathbb{Q})\}$。令 A 为等差数列、等比数列，或形如.....的集合

$$\{u^2, (u+d)^2, (u+2d)^2, \ldots, (u+dl)^2\},$$

其中 u、$d \in \mathbb{Q}$和 $l \in \mathbb{N}$。若 $A \subseteq X$ 或 $A \subseteq Y$，则 $|A| \leq C^{1+r}$。

我们注意到，定理 1.1 中的常数 C 不依赖于 a, b；对于有界秩的椭圆曲线族，我们得到一个统一的界。迄今尚不清楚是否存在秩任意大的椭圆曲线。最近，人们发现了一条秩至少为 29 的椭圆曲线 [15, 16]。显然，椭圆曲线上的S-整点 [25, 定理 D.9.1] 所对应的西格尔定理意味着，在 $E(\mathbb{Q})$ 中不可能存在无限的等差数列、等比数列或平方数列。然而，该定理并未给出统一的界，即使对固定的椭圆曲线也是如此，因为需要求逆的素数个数取决于具体的数列。

对于等差数列，Garcia–Fritz 与 Pasten [21]证明了一个形如 C^{1+r}的界，其中 C 依赖于 E；但可以设想，倘若他们采用了 Mordell–Lang 猜想的统一版本（例如 [11]），其方法或许能导出一致界。然而，对于等比数列与连续平方数，即使允许依赖于 E，似乎也尚无此类一般界。我们证明了定理 1.1 的一个更一般版本（推论 2.2），它针对对应与有限秩群，并适用于大量类似序列。定理 1.1 也可以借助高维射影空间中一般型曲面上的有理点来表述。由此，我们确定了某些射影曲面的有理点的 Zariski闭包（见定理 A.1）。

现在我们转向和积现象。因此，给定有限集 $A, B \subseteq \mathbb{C}$，我们将和集与积集定义为

$$A + B = \{a + b : a \in A, b \in B\} \quad \text{and} \quad A \cdot B = \{ab : a \in A, b \in B\}.$$

人们通常认为，如果 $|A+A|$ 相对于 $|A|$较小，那么 A 应具有加法结构；如果 $|A \cdot A|$ 相对于 $|A|$较小，那么 A 应具有乘法结构。基于这两种结构不应同时存在的猜想，Erd˝os–Szemer´edi

[17] 猜想，对于任意有限集 $A \subseteq \mathbb{C}$，$A+A$ 或 $A \cdot A$ 的大小必定接近$|A|^2$。更一般地，记

$$gA = \{a_1 + \cdots + a_g : a_1, \ldots, a_g \in A\} \text{ and } A^{(g)} = \{a_1 \ldots a_g : a_1, \ldots, a_g \in A\},$$

对于任意 $g \in \mathbb{N}$，Erd˝os–Szemer´edi 猜想如下。

猜想1.2. 对于任意 $g \in \mathbb{N}$、任意 $\varepsilon > 0$ 以及任意集合 $A \subseteq \mathbb{C}$，应有

$$\max\{|gA|, |A^{(g)}|\} \gg_{g,\varepsilon} |A|^{g-\varepsilon}.$$

大量研究致力于这一猜想，主要关注 $g = 2$ 的情形。在这一背景下，Elekes [12] 和 Solymosi[41], 的研究颇具代表性，他们利用几何学洞见，为强和积估计给出了简短证明。目前已知的最佳结果来自 Cushman [10], 近期的一项工作，他运用关联几何和加法组合方法证明了

$$\max\{|2A|, |A^{(2)}|\} \gg_{\varepsilon} |A|^{\frac{4}{3}+\frac{10}{4407}-\varepsilon}$$

对于所有集合 $A \subseteq \mathbb{R}$ 以及所有 $\varepsilon > 0$，均成立。

可以将和积现象理解为两个非同源代数群之间结构的瓦解。事实上，可以令 $\mathbb{G}_m = (\mathbb{C}^*, \times)$ 和 $\mathbb{G}_a = (\mathbb{C}, +)$，并令 $\mathcal{C}$ 为这样的对应：其复点具有 (x, x) 的形式，其中 $x \in \mathbb{G}_m(\mathbb{C})$。关于代数群及其之间的对应，简要介绍见 §3。令 $\pi_1 : \mathcal{C} \to \mathbb{G}_m$ 和 $\pi_2 : \mathcal{C} \to \mathbb{G}_a$ 为标准投影映射。给定一个有限集$A \subseteq \mathbb{G}_m(\mathbb{C})$，记

$$\mathcal{C}(A) = \bigcup_{x \in A} \pi_2(\pi_1^{-1}(x)).$$

注意，$\mathcal{C}(A)$ 是 $\mathbb{G}_a(\mathbb{C})$ 的子集。现在，和积现象等价于以下说法：对于任意有限 $A \subseteq \mathbb{G}_m(\mathbb{C})$，$|A+A|$ 或 $|\mathcal{C}(A)+\mathcal{C}(A)|$ 必须远大于 $|A|$。

在一篇非常出色的论文中，Bays–Breuillard [1] 采用模型论方法，将这一系列思想推广到范围更广的代数群族。特别地，给定定义在 $\mathbb{C}$上的一维连通非同源代数群 G和 H，以及它们之间次数为 d 的某个代数对应 $\mathcal{C}$，Bays–Breuillard[1] 证明存在某个 $\delta = \delta(G, H, \mathcal{C}) > 0$，使得对于任意有限集 $A \subseteq G$，有

$$\max\{|A+A|, |\mathcal{C}(A)+\mathcal{C}(A)|\} \gg_{G,H,C} |A|^{1+\delta}. \tag{1.2}$$

与猜想1.2的 $g = 2$ 情形相比，对于要求无界扩张的情况，人们所知甚少；也就是说，给定任意实数 $k > 1$，希望找到某个 $1 \leq g \ll_k 1$，使得

$$\max\{|gA|, |A^{(g)}|\} \gg_k |A|^k \tag{1.3}$$

对所有有限集 $A \subseteq \mathbb{C}$均成立。当 $k \leq 2$时，关联几何方法似乎相当有效；但当 $k > 2$时，它们似乎无法给出任何结果。在一篇突破性论文中，Bourgain–Chang [3] 运用了复杂的调和分析技术以及一条

[1]Bays–Breuillard [1] 实际上证明了，对于非恒定有理映射 $f_1 : G \to \mathbb{C}$ 和 $f_2 : H \to \mathbb{C}$，以及所有有限集 $A \subseteq \mathbb{C}$，要么有 $|f_1^{-1}(A)+f_1^{-1}(A)| \geq c|A|^{1+\delta}$，要么有 $|f_2^{-1}(A)+f_2^{-1}(A)| \geq c|A|^{1+\delta}$，其中$c$，$\delta > 0$是依赖于 G，H，f_1和 f_2的常数。通过考虑由 $\{(x, y) \in G \times H : f_1(x) = f_2(y)\}$的一个不可约分支给出的对应，可以在对应的框架下表述这一结果。

巧妙的算术引理，证明了 (1.3) 对所有有限集 $A \subseteq \mathbb{Q}$均成立。随后，P´alv¨olgyi–Zhelezov [36], 对其工作进行了简化并在定量上加以改进， g 从而就该问题而言，关于 k 给出了目前已知的最佳界。这些思想后来通过将和集 gA 替换为加性结构的其他度量而得到推广。特别地，Hanson– Roche-Newton–Zhelezov [24] 证明了 (1.3) 的一个类似结果，其中和集 gA 被平移乘积集 $(A+1)^{(g)}$所替代。第二作者 [35],进一步将这一结果推广，证明了 (1.3) 的类似结果：先将 gA 替换为和集 $\varphi_1(A) + \cdots + \varphi_g(A)$，随后再替换为积集 $\varphi_1(A) \ldots \varphi_g(A)$，其中多项式 $\varphi_1, \ldots, \varphi_g \in \mathbb{Z}[x]$的次数均有界。

上述所有结果都在 [3, 36, 24, 35] 中关键性地利用了有关整数素因数分解的性质，因此无法推广到实数集合。事实上，该领域的一个重要问题是证明集合 $A \subseteq \mathbb{R}$ 的 (1.3)。在 Chang [7], 早期工作的基础上，第二作者 [34] 利用丢番图几何的结果，证明了在加性组合学中一个著名猜想成立的条件下，该条件成立；这个猜想称为关于 $\mathbb{Z}$ 的弱多项式 Freiman–Ruzsa 猜想。Gowers–Green–Manners–Tao [22] 的卓越工作如今已解决了这一猜想。

关于广义和积现象，我们的主要结果是在范围广泛得多的 $\mathbb{C}$上一维连通代数群中得到的 Bourgain–Chang 型无界扩张结果。

定理 1.3. 给定整数 $k \geq 1$ 与 $d \geq 2$，存在整数 $g \geq 1$ ，使得下列结论成立。设 G 与 H 为维数1的代数群，并设 $\mathcal{C}_1$、 $\cdots$、 $\mathcal{C}_g$ 为 G 与 H之间次数为 d 的对应。假设没有 $\mathcal{C}_i$ 是某个代数子群的平移，并假设 G不同构于 $\mathbb{G}_a$。则对所有有限非空集$A \subseteq G$，有

$$\max\{|gA|, |\mathcal{C}_1(A) + \cdots + \mathcal{C}_g(A)|\} \gg_{d,k} |A|^k.$$

取定 $G = \mathbb{G}_m$ 与 $H = \mathbb{G}_a$，我们令 $\mathcal{C}_i$ 由包含映射 $\mathbb{C}^* \hookrightarrow \mathbb{C}$的图给出。于是定理 1.3 的结论立即对任意有限集 $A \subseteq \mathbb{C}$推出(1.3)。类似地，取定 $G = \mathbb{G}_m$ 与 $H = \mathbb{G}_m$ 或 $\mathbb{G}_a$ ，并令 $\mathcal{C}_i$ 由 $G \times H$ 中$(x, \varphi_i(x))$的图给出，其中多项式 $\varphi_1, \ldots, \varphi_g$ 适当选取，便得到如下推论。

推论 1.4。 对于所有整数 $k \geq 2$，存在一个整数 $g \geq 2$ ，使得以下结论成立。对于任意次数至多为 d 的非恒定 φ_1，……， $\varphi_g \in \mathbb{C}[x]$ 以及任意有限集 $A \subseteq \mathbb{C}$，有

$$\max\{|A^{(g)}|, |\varphi_1(A) + \cdots + \varphi_g(A)|\} \gg_{d,k} |A|^k.$$

此外，如果对于 $1 \leq i \leq g$ ，每个 $\varphi_i(x)$ 都不具有对任何 $a \in \mathbb{C}$ 和任何 $n \in \mathbb{N}$ 形如 ax^n 的形式，那么我们还有

$$\max\{|A^{(g)}|, |\varphi_1(A) \ldots \varphi_g(A)|\} \gg_{d,k} |A|^k.$$

这在更一般的情形下定性地恢复了 [24, 35] 的结果：其中用 $A \subseteq \mathbb{C}$ 代替 $A \subseteq \mathbb{Q}$，并且多项式 φ_1，……， φ_g 可以具有复系数而非有理系数。关于我们方法的进一步应用，包括对 Bays–Breuillard 猜想的另一种证明，我们留待第 2 节讨论。

我们还研究多项式像集中的扩张问题，以及代数群中簇与离散盒的交问题。这与 Elekes–Szab´o 和 Elekes–R´onyai 型问题有关。我们简要介绍前者：给定 $n \geq 3$ 和

某个多项式 $P \in \mathbb{C}[x_1, \ldots, x_n]$，在什么情况下，对于任意有限非空集$A \subseteq \mathbb{C}$，都有

$$|\{(a_1, \ldots, a_n) \in A^n : P(a_1, \ldots, a_n) = 0\}| \ll |A|^{n-1-\eta} \tag{1.4}$$

对某个常数 $\eta > 0$成立? 此类刻画最早由Elekes–Szab´o [14],研究，此后相关研究大量涌现，部分原因在于它与多种组合几何问题 [38, 37, 42]以及模型论结果 [9, 1, 8]之间的联系。

在他们前述的工作中，Bays–Breuillard [1]针对这一问题引入了模型论方法，从而将上述结果推广到 $\mathbb{C}^n$中的不可约代数集。他们进一步指出，若限制于一类特殊的集合族 $A \subseteq \mathbb{C}$，则可以对更为广泛的簇得到形如(1.4)的幂次节省。特别地，在一维复连通代数群 G的设定下，他们证明：对任意不是子群之陪集的子簇 $\mathcal{V} \subseteq G^n$ ，存在仅依赖于 G 与 $\mathcal{V}$的常数 ε， $\eta > 0$，使得对任意满足 $|A + A| \leq |A|^{1+\varepsilon}$的有限集 $A \subseteq G$ ，都有

$$|A^n \cap \mathcal{V}| \ll_{G,\mathcal{V}} |A|^{\dim(\mathcal{V})-\eta}. \tag{1.5}$$

自然会问，在（1.5）中允许的 η 的最佳可能取值是多少。当 G 与 $\mathbb{G}_a$ 不同构时，我们解决这个问题。

定理 1.5. 设 G 是定义在 $\mathbb{C}$ 上、维数为 1 的连通代数群。假设 G 与 $\mathbb{G}_a$ 不同构。设 $A \subseteq G$ 是一个有限集，使得对某个 $K \geq 1$ 有 $|A + A| \leq K|A|$ 。那么，对于任意不可约子簇 $\mathcal{V} \subseteq G^g$，若它不是 G^g 的代数子群的平移，则有

$$|\mathcal{V} \cap A^g| \ll_{g,\deg(\mathcal{V})} K^C + |A|^{\dim(\mathcal{V})-1},$$

其中 $C > 0$ 是某个常数，仅取决于 $\deg(\mathcal{V})$ 和 g。

特别地，当 G 与 $\mathbb{G}_a$ 不同构，且 $\mathcal{V}$ 不是代数子群的平移时，存在某个 $\varepsilon > 0$，仅取决于 $\mathcal{V}$ 和 g，使得只要 $|A+A| \leq |A|^{1+\varepsilon}$，就有

$$|\mathcal{V} \cap A^g| \ll_{g,\deg(\mathcal{V})} |A|^{\dim(\mathcal{V})-1}.$$

我们进一步指出，这个上界的量级是正确的。

例 1.6。 设 $G = \mathbb{G}_m$ 和 $g = 3$。由多项式定义的簇 $\mathcal{V}$

$$P(X_1, X_2, X_3) = X_2X_3 - X_1 + 1 \tag{1.6}$$

包含代数子群 $X_2X_3 = 1, X_1 = 1$的平移 $X_2X_3 = \gamma, X_1 = \gamma + 1$，对任意 $\gamma \notin \{-1, 0\}$均成立。令

$$A = \{\gamma^i : -N \leq i \leq N\} \cup \{\gamma + 1\},$$

容易看出，对于所有 $N \geq 3$，我们都有 $|\mathcal{V} \cap A^3| \gg |A|$ 和 $|A \cdot A| \leq 3|A|$。然而， $\mathcal{V}$并不是代数子群的平移。

事实上，我们的方法还给出了更强的上界，该上界取决于包含在 $\mathcal{V}$ 中的代数子群的极大平移的最大维数，更多细节请参见 Theorem2.6。

我们还指出，尽管以往研究 Elekes–Szab´o 型问题的方法采用了组合几何方法或模型论，但我们的方法利用了 Mordell–Lang 与 S-单位型结果之间新颖的相互作用，并结合了加性组合学中涉及 Freiman–Ruzsa型结果的最新进展。

类似地，我们也可以考察多项式像集中的扩张。也就是说，给定某个多项式 $P \in \mathbb{C}[x_1, \dots, x_n]$ 和某个有限集 $A \subseteq \mathbb{C}$，集合

$$P(A, \dots, A) = \{P(a_1, \dots, a_n) : a_1, \dots, a_n \in A\}$$

是否显著大于 A。这一方向上的首个结果由 Elekes–R´onyai [13]给出，他们证明：要么 $P \in \mathbb{C}[x, y]$ 是退化的，即对于某些单变量多项式 f，g，h，有 $P = h(f(x) + g(y))$ 或 $P = h(f(x)g(y))$；要么对于每个有限集 $A \subseteq \mathbb{C}$，都有 $|P(A, A)| \gg |A|^{1+\eta}$，其中 $\eta > 0$ 为绝对常数。此后，人们对其进行了各种定量改进，也探索了如下情形：与前面一样，为了拓宽 P 的选择范围并获得更好的 η定量值，人们将集合限制在某个特殊族 A 中；关于相关的和-积型问题，参见 [1, 26, 34]以及 [24, 35] 。

我们在这一方向上的主要结果，是将上述结果显著推广到更广泛的代数群情形。为陈述这一结果，我们需要以下定义。

定义 1.7. 设 G 是定义在 $\mathbb{C}$ 上的一维连通代数群，$\mathcal{B}$ 是一个正维射影簇。设 $\pi_1 : G^g \times \mathcal{B} \to G^g$ 和 $\pi_2 : G^g \times \mathcal{B} \to \mathcal{B}$ 为典范投影映射。若存在一个正维连通代数群 $H \subseteq G^g$ 及一个真子簇 $\mathcal{W} \subsetneq G^g/H \times \mathcal{B}$，使得不可约子簇 $\mathcal{V} \subseteq G^g \times \mathcal{B}$ 满足

$$\mathcal{V} = \pi_H^{-1}(\mathcal{W}),$$

对于投影 π_H: $G^g \times \mathcal{B} \to G^g/H \times \mathcal{B}$。若 $\mathcal{V}$ 不是退化的，我们称 $\mathcal{V}$ 为非退化。

退化子簇的一个例子由方程 $P(X_1, X_2, X_3) = t$ 给出，其中 P 由（1.6）给出。定理 1.8 的陈述之后给出了一个非退化子簇的例子。

有了这些准备，我们将结果表述如下。

定理 1.8。设 G、$\mathcal{B}$、π_1 和 π_2 如定义 *1.7* 所述，且 G 与 $\mathbb{G}_a$ 不同构。设 $\mathcal{V} \subseteq G^g \times \mathcal{B}$ 是维数为 g、次数为 d 的非退化对象，并且 π_1 和 π_2 在 $\mathcal{V}$ 上的限制是支配的。设 $A \subseteq G$ 为有限非空集，且 $|A+A| \leq K|A|$。那么对于所有 $X \subseteq A$，我们有

$$|\pi_2((X^g \times \mathcal{B}) \cap \mathcal{V})| \gg_{d,g} \frac{|X|^g}{K^{O_{d,g}(1)}}. \tag{1.7}$$

作为例子，可以令 $G = \mathbb{G}_m, B = \mathbb{P}^1$，并将簇 $\mathcal{V}$ 定义为由方程 $P(x_1, \dots, x_g) = t$ 给出，其中 $P \in \mathbb{C}[x_1, \dots, x_g]$ 是某个多项式。若簇 $\mathcal{V}$ 是非退化的，则称 P关于 G^g 为非退化 。可以看出，这等价于：对任意选取的单项式$m_1, \dots, m_{g-1} \in \mathbb{C}[x_1, \dots, x_g]$ 以及任意 $F \in \mathbb{C}[y_1, \dots, y_{g-1}]$，都有 $P(\boldsymbol{x}) \neq F(m_1(\boldsymbol{x}) \dots, m_{g-1}(\boldsymbol{x}))$。在这种情况下，我们有

$$\pi_2((A^g \times \mathcal{B}) \cap \mathcal{V}) = P(A, \dots, A).$$

因此，(1.7) 意味着，对于任意满足 $|A\cdot A|\le K|A|$ 的有限集 $A\subseteq\mathbb{C}^*$，都有

$$|P(A,\dots,A)|\gg_{d,g}\frac{|A|^g}{K^{O_{d,g}(1)}}. \tag{1.8}$$

(1.8) 中的下界是在 [34] 中于 $\mathbb{Z}$ 上的弱 PFR 猜想条件下证明的。事实上，定理 1.8 可以看作是将 [34] 中的结果推广到 $\mathbb{C}$ 上一维代数群中的簇这一更为广泛的情形。

除了可应用于各种和-积型问题之外，这种退化性概念还有一个优点：它是最优的。具体而言，若多项式 P 在上述意义下是退化的，则由命题 1.2] 可知，对于任意满足 $|A\cdot A|\le K|A|$ 的有限 $A\subsetneq\mathbb{Z}$，都有

$$|P(A,\dots,A)|\ll_P K^{O_P(1)}|A|^{g-1}.$$

此外，(1.7) 中的下界几乎是最优的，因为除去 $K^{O_{d,g}(1)}$ 这些因子后，它与平凡上界 $|X|^g$ 相匹配。

请注意，在我们的一些结果中，包括定理 1.8，我们假设代数群 G 不与 $\mathbb{G}_a$ 同构。事实上，这是许多此类结果成立的必要条件。例如，当 $G=\mathbb{G}_a$ 时，定理 1.8 并不成立。

例 1.9. 设 $P(x,y,z)=xy+yz+zx$。可以证明，这个多项式相对于 $\mathbb{G}_a^3$ 是非退化的，参见附录 B。此外，集合 $A=\{1,2,\dots,N\}$ 是 $\mathbb{G}_a$ 的子集，且 $|A+A|\le 2|A|$。最后，$|P(A,A,A)|\ll N^2=|A|^2$，这表明在这种情况下，类似于 (1.8) 的结论并不成立。

值得一提的是，定理 1.8 可用于证明其对应结论：将条件“ A 具有较小的和集”替换为“ A 包含在一个秩较小的子群中”，参见定理 4.2。特别地，给定一个秩为 r 的子群 $\Gamma\subseteq G$ 和一个有限集 $Y\subseteq\Gamma$，定理 1.8 意味着必有

$$|\pi_2((Y^g\times\mathcal{B})\cap\mathcal{V})|\gg_{d,g}\frac{|Y|^g}{2^{O_{d,g}(r)}}. \tag{1.9}$$

事实上，令 Γ 由 γ_1、……、γ_r生成。现在，给定任意有限集 $Y\subseteq\Gamma$，我们可以找到某个 $L\in\mathbb{N}$，使得 $Y\subseteq A$，其中 $A=\{n_1\gamma_1+\cdots+n_r\gamma_r:\ |n_1|$、……、$|n_r|\le L\}$。此外，注意到 $|A+A|\le 2^r|A|$。现在我们可以应用定理 1.8 得到 (1.9)。此外，这意味着我们可以结合不等式 (1.9) 和命题 5.1，推导出定理 1.1 及其推广——推论 2.2。

证明我们的结果的一个重要步骤是，上述蕴含关系也可以大致逆转。我们通过结合 Gowers–Green–Manners–Tao [22] 最近对弱多项式 Freiman–Ruzsa 猜想的解决成果、各种加性组合技巧，以及代数群的有限子群生成元个数存在一致上界这一事实，来实现这种逆转；而后者是李理论的一个简单推论。

因此，只需在我们的集合位于有界秩子群中的情形下进行讨论即可。此处我们的关键结果之一是定理 4.2，其结论亦记录于 (1.9)。正是在这里，我们大量引入了来自丢番图几何的内容，包括利用 David–Philippon 给出的 Mordell–Lang 猜想的统一版本 [11] 以及 Evertse–Schlickewei–Schmidt 给出的S-单位界 [18]。

证明我们的和积结果（例如定理 1.3）所需的第三步，涉及证明一个辅助簇，该簇刻画了加性结构的移动

经由这些对应，在定义 1.7 的意义下是非退化的。这正是命题 5.1 的内容。对于可在第 5 节中找到的证明，我们在我们的代数群的切空间上进行研究。我们注意到，命题 5.1 与定理 4.2 相结合，可推出定理 1.3 的一个适当变体，该变体对包含于有限秩子群中的集合成立，见定理 2.1。后者已足以用于我们对 Bremner 猜想的应用。

作者们深信，此处显而易见的丢番图几何与加性组合学之间巧妙的互动似乎表明，代数群之间的对应为理解和积现象提供了一个非常合适的框架。看待这种互动的一种方式是，关于 $\mathbb{Z}$ 上的弱多项式 Freiman–Ruzsa 猜想只是一个关于 $\mathbb{Z}^r$中的加法的命题。后者可以通过秩为 r 的群以多种方式嵌入代数群。这与 $\mathbb{G}_a$，$\mathbb{G}_m$ 和椭圆曲线中隐含存在的代数结构相结合。最终，莫德尔–朗猜想告诉我们群的群运算如何与其扎里斯基拓扑相互作用。若记得同源所起的特殊作用，这一点就尤其令人信服，因为同源恰恰是同时保持代数结构和群结构的映射。任何并非代数子群平移的对应，在将有限集从一种群运算转移到另一种群运算时，都应当破坏其近似群结构。

概要。 我们将在 §2 中进一步介绍我们思想的一些应用。§3 将简要介绍代数群和对应，并记录 David–Philippon [11] 给出的 Mordell–Lang 猜想的统一版本以及 Evertse–Schlickewei–Schmidt [18] 的 S-单位界所带来的一些推论。§4 专用于证明定理 4.2，§5 中我们将证明命题 5.1。§6 将用于证明我们证明结果所需的加性组合结构性结果。最后，§7 将给出 §1 和 §2 中所有结果的证明。附录 A 中，我们将介绍一些结果在丢番图方程中的应用。此外，我们还将在附录 B 中简要讨论退化多项式的性质。

记号。 我们使用 Vinogradov 记号。因此，我们写 $X \ll_z Y$ 表示 $|X| \leq CY$，其中 $C > 0$ 是一个依赖于参数 z 的某个常数。我们写 $X = O(Y)$ 表示$X \ll Y$，并写 $X \asymp Y$ 表示 $X \ll Y \ll X$。我们常将有限集 A 和代数群 G 记作 $A \subseteq G$。在这种情况下，我们（通过记号滥用）将 A 视为由 A 中的点构成、且各点重数均为 1 的零维代数子簇。

致谢。 第二作者获得 Leverhulme 早期职业研究员奖学金资助 ECF-2025-148。

2. Further Applications

2.1. 广义 Bremner。

我们介绍定理 1.1 的一个推广版本，该版本适用于代数群之间的对应。我们首先记录对应的一个展开版本。

定理 2.1。 对于所有整数 $d \geq 1$ 和 $g \geq 2$，存在一个正的常数 $0 < c\,(d, g) < 1$，使其满足以下性质。设 $\mathcal{C}_1, \cdots, \mathcal{C}_g$ 是代数群 G 和 H 之间次数为 d 的对应，且这些代数群的维数为 *1*。假设没有一个 $\mathcal{C}_i$ 是代数子群的平移，并且

其中 G 不同构于加法群 $\mathbb{G}_a$。设 $\Gamma \subseteq G(\mathbb{C})$ 是一个有限秩为 r的子群。那么对于任意有限子集 $A \subseteq \Gamma$，有

$$|\mathcal{C}_1(A) + \cdots + \mathcal{C}_g(A)| \geq c(d,g)^{1+r}|A|^g.$$

我们注意到，该定理略有不对称，因为我们不能允许 G 与 $\mathbb{G}_a$ 同构。这确实是必要的，例如，对于 $\Gamma = \mathbb{Z}$、 $H = \mathbb{G}_m$ 和 Δ ，如上所述的对角线表明，如果去掉这一假设，就意味着 $\mathbb{Z}$ 中的任意集合都有很大的积集，而这显然不对。

还值得注意的是，固定数域 K 上的一条椭圆曲线 E 后，与它同源的 K 上的椭圆曲线只有有限多条，即使是在代数闭包上也是如此。这是 Faltings 著名定理 [19], 的推论；后来 Masser–W¨ustholz [31], 对此作了重大改进。该结果表明，即使固定一个数域，我们的定理也适用于种类繁多的非同源代数群。

给定 $k \in \mathbb{N}$，我们将秩为 k 的适当广义算术级数定义为如下形式的集合P：

$$P = \{P_0 + \ell_1 P_1 + \cdots + \ell_k P_k \ : \ 0 \leq \ell_i \leq L_i - 1\}, \tag{2.1}$$

其中 P_0、.....、 $P_k \in H$和 L_1、.....、 $L_k \geq 2$均为整数，且满足 $|P| = L_1 \ldots L_k$。这些集合在加性组合学和数论中发挥着关键作用，因为它们是一类重要的集合，具有加性结构。有了这些准备，我们现在证明关于 Bremner 猜想及相关问题的主要结果。

推论 2.2。 对所有整数 $d \geq 1$ ，存在一个常数 $D = D(d)$ ，使得以下性质成立。设 G 为 $\mathbb{G}_m$ 或一条椭圆曲线 E，且 $\mathcal{C}$ 是 G 与一个维数为 *1* 的代数群 H 之间次数不超过 d 的对应，并且不是某个代数子群的平移。则对任意秩为 r的子群 $\Gamma \subseteq G(\mathbb{C})$ ，在 $\mathcal{C}(\Gamma)$ 中的一个秩为 k 的适当广义算术级数 P 满足

$$|P| \leq D^{1+r}.$$

定理 1.1 可由上述结果直接推出，见 §7。推论 2.2 还给出了 [21, 定理 6.1] 的一个更一般且统一的版本。

我们的上界有一个优点：它完全不依赖于等差数列的秩 k 。此外，广义算术级数确实是一种严格更广泛的模式。例如，式（2.1）中所述的广义算术级数 P' 无法被少于 C^k 个等差数列覆盖，其中 $C > 1$是某个常数，但我们仍能得到形如 $|P'| \leq D^{1+r}$ 的统一上界，其中 $0 < D \ll_d 1$ 与 k无关。

2.2. 和积现象。 回到广义和积现象，Bays–Breuillard [1] 推测，他们在 (1.2) 中记录的结果里，指数 δ 应与 G 和 H无关。Chernikov–Peterzil–Starchenko [8]对这一模型论与关联几何框架作了重要推广，并以定量方式证实了 Bays–Breuillard 的推测。特别地，他们证明了 $\delta = 1/21$在 (1.2) 中是可取的。作为我们方法的一项应用，我们证明了 (1.2) 的一个非对称、统一版本，从而通过一套截然不同的技术证实了 Bays–Breuillard 的推测。

定理 2.3。 给定 $d \in \mathbb{N}$，存在某个常数 $D = D(d) > 0$，使得下述结论成立。设 $\delta > 0$，设 G 和 H 是维数为 *1* 的连通代数群，且G不同构于 $\mathbb{G}_a$；设 $\mathcal{C}$ 是 G与 H 之间的一个次数为$d \geq 2$ 的代数对应，且它不是某个代数子群的平移。那么，对于任意有限非空集$A \subseteq G$，以下情况至少有一种成立

$$|A + A| > |A|^{1+\delta} \quad or \quad |\mathcal{C}(A) + \mathcal{C}(A)| \geq D^{-1}|A|^{2-D\delta}. \tag{2.2}$$

事实上，定理 2.3 蕴含 $\delta = 1/(D + 1)$ 在 (1.2) 中是可接受的。虽然这一对 δ 的选择远小于 $1/21$，但我们结果的主要新意在于 (2.2) 中 $|A+A|$ 与 $|\mathcal{C}(A) + \mathcal{C}(A)|$ 的下界之间的不对称性。例如，如果我们令 $G = \mathbb{G}_m$ 和 $H = \mathbb{G}_a$，或令 $\mathbb{G}_m$ 以及对应关系 $\mathcal{C}$ 由某个适当多项式 $\varphi \in \mathbb{C}[x]$ 的图 $y = \varphi(x)$ 给出，就得到以下推论。

推论 2.4. 设 $A \subseteq \mathbb{C}$ 是一个有限集，$d \geq 1$ 是一个整数，设 $K \geq 1$，并且 $\varphi \in \mathbb{C}[x]$ 满足 度 $\varphi = d$。若 $|A \cdot A| \leq K|A|$，则

$$|\varphi(A) + \varphi(A)| \gg_d |A|^2/K^D \tag{2.3}$$

其中 $D > 0$ 是一个依赖于 d 的常数。此外，如果 φ（x）不是任何 $c \in \mathbb{C}$ 的形式 cx^d，那么我们还有

$$|\varphi(A) \cdot \varphi(A)| \gg_d |A|^2/K^D.$$

注意，在 (2.3) 中直接令 $\varphi = x$，便立即得到所谓的 $\mathbb{C}$ 上的弱 Erd˝os– Szemer´edi 猜想。Bourgain–Chang [3] 首先对集合 $A \subseteq \mathbb{Q}$ 证明了这一结论；Chang [7] 的工作则在弱 PFR 猜想 $\mathbb{Z}$ 成立的条件下，对集合 $A \subseteq \mathbb{R}$ 得到了这一结论。在 Chang 的工作基础上，并利用 Gowers–Green–Manners–Tao [22], 对 $\mathbb{Z}$ 上弱 PFR 猜想的解决，第二作者证明：对于任意满足 $|A \cdot A| \leq K|A|$ 的有限集 $A \subsetneq \mathbb{C}$，满足 $a_1 + a_2 = a_3 + a_4$ 的四元组 a_1，.....，$a_4 \in A$ 至多有 $|A|^2/K^{O(1)}$ 个，参见 [33, 命题 1.5]。由此立即可得 $|A + A| \geq |A|^2/K^{O(1)}$。

2.3. Elekes–Szab´o. 正如§1中所述，我们能够证明形如 $|\mathcal{V} \cap A^g|$ 的量的一个更一般的上界，这些量依赖于包含在 $\mathcal{V}$中的代数子群的平移的最大维数。为了对此加以阐述，我们给出如下定义。

定义 2.5. 对于不可约子簇 $\mathcal{V} \subseteq G^g$，我们将陪集亏量（记为余维($\mathcal{V}$)）定义为连通代数群 $H \subseteq G^g$的最大维数，使得对某个 $\gamma \in G^g(\mathbb{C})$有$\gamma + H \subseteq \mathcal{V}$。

据此，我们陈述我们的结果。

定理 2.6. 设 G 是 $\mathbb{C}$ 上的一个1维连通代数群，且不同构于 $\mathbb{G}_a$。设 $A \subseteq G$ 是一个有限集，使得对某个 $K \geq 1$有 $|A + A| \leq K|A|$ 。则对任意不可约子簇 $\mathcal{V} \subseteq G^g$，有

$$|\mathcal{V} \cap A^g| \ll_{g,\deg(\mathcal{V})} (K^C + |A|^{\mathrm{codef}(\mathcal{V})}),$$

其中常数 $C > 0$ 仅取决于$\deg(\mathcal{V})$ 和 g。

注意， $\mathcal{V}$ 可能被代数子群的平移覆盖，尽管 $\mathcal{V}$并非代数子群的平移。不过，定理 2.6 仍适用于此类簇。例如，对于 $g=3$，由 $X_1X_2^2X_3 - X_2X_3 - 1 = 0$ 定义的簇 $\mathcal{V}$不是陪集，但它被形如 $X_2X_3 = \gamma$， $X_1X_2 = (1+\gamma)/\gamma$（其中 $\gamma \in \mathbb{C}\setminus\{-1,0\}$）的陪集所覆盖。定理 2.6 可推出以下推论。

推论 2.7。对于任意 $d, g \geq 1$，存在 $\epsilon > 0$，使得对于次数至多为 d 的不可约簇$\mathcal{V} \subseteq G^g$，若 $|A+A| \leq |A|^{1+\epsilon}$ 且 余维$(\mathcal{V}) \geq 1$，则

$$|A^g \cap \mathcal{V}| \ll_{g,\deg(\mathcal{V})} |A|^{\operatorname{codef}(\mathcal{V})}. \tag{2.4}$$

最后，若 $\mathcal{V}$ 不包含正维陪集，则对于任意 $\epsilon > 0$，若 $|A+A| \leqq A|^{1+\epsilon}$，则

$$|\mathcal{V} \cap A^g| \ll_{g,\deg(\mathcal{V})} |A|^{C\epsilon},$$

其中 $C > 0$ 是一个常数，取决于 次数$(\mathcal{V})$ 和 g。

与定理 1.5 和例 1.6 的情形一样，可以证明定理 2.6 和不等式 2.4 中的上界是恰当的。

3. Setup

3.1. 代数群。我们将研究维数为 1 的 $\mathbb{C}$ 上的连通代数群。代数群（定义在 $\mathbb{C}$上）是一个代数簇 G，配有一个从$G \times G$到 G的态射，该态射在 G上诱导出群运算（$\mathbb{C}$）。例如，考虑由代数簇 $\mathbb{A}^1$ 及将 (x, y) 映射到 $x + y$的态射给出的代数群。我们将这个代数群称为加法群 $\mathbb{G}_a$。另一个例子是由代数簇 $\mathbb{A}^1 \setminus \{0\}$ 及将 (x, y) 映射到 xy的态射给出的代数群。我们将这个代数群称为乘法群 $\mathbb{G}_m$。第三个例子是定义在 $\mathbb{C}$ 上的椭圆曲线，配有其典范群运算 [40, III.2]。

以上三个例子都是定义在 $\mathbb{C}$上的一维连通代数群；事实上，可能的例子基本上也只有这些。为此，注意到 G 的解析化是一个复李群，因此具有指数映射

$$\exp_G : \mathbb{C} \to G(\mathbb{C}),$$

由于它是局部微分同胚，因此是解析且非恒定的 [30, 命题 20.8 (f)]。当 G 是交换的时，$\exp_G$ 是李群态射。相关内容见 [30, 练习 20-8] 或 Baker–Campbell–Hausdorff 公式。现在，利用复分析中的以下论证可知，$\exp_G$ 是满射且核离散。

命题 3.1。设 G 和 H 是维数为1的复李群。假设 H是连通的。从 G 到 H 的每个复李群态射，要么是平凡的，要么是满射且核离散。

证明。假设态射 f 不是平凡的。根据解析延拓的唯一性可知，核是离散的。由于 $\dim(G) = \dim(H) = 1$，开映射定理表明， f 的像 U 是开集。集合 U 也是 H的李子群。因此， H 是 U的陪集的不交并，其中每个陪集都是开集。由于 H 是连通的，至多只有一个陪集，即 $U = H$。□

因此， G 有三个选项，取决于 $\exp_G$ 的核。

（1）核是平凡的。在这种情况下， $G(\mathbb{C})$ 同构于复数的加法群 $\mathbb{C}$。（2）核是秩为一的格。在这种情况下， $G(\mathbb{C})$ 同构于复数的乘法群 $\mathbb{C}^*$。例如，切空间 $\mathbb{C}$上把 $\exp_G$ 的核映到格 $2\pi i\mathbb{Z}$ 的线性映射就是这样一个同构。（3）核是秩为二的格 Λ 。在这种情况下， $G(\mathbb{C})$ 同构于复环面 $\mathbb{C}/\Lambda$。借助经典魏尔斯特拉斯理论 [40, 命题 VI.3.6]可以证明， G 同构于一条椭圆曲线的复点群。

在每种情形下，通过将同构延拓到某个射影空间中 $G(\mathbb{C})$的闭包，并应用塞尔的 GAGA 定理，$G(\mathbb{C})$与 $\mathbb{C}, \mathbb{C}^*$ 或 $\mathbb{C}/\Lambda$ 之间的同构都可以提升为 G 与 $\mathbb{G}_a, \mathbb{G}_m$ 或椭圆曲线 E 之间的同构。

代数群的指数映射 $\exp_G$ 存在局部逆映射，记作 $\log_G$。注意，$\exp_{\mathbb{G}_a(\mathbb{C})} = \mathrm{id}_{\mathbb{C}}$ ，而 $\exp_{\mathbb{G}_m(\mathbb{C})}$ 是通常的指数函数 $\exp : \mathbb{C} \to \mathbb{C}^*$。此外，当 G 是通过其魏尔斯特拉斯形式嵌入 $\mathbb{P}^2$ 的椭圆曲线时，$\exp_G : \mathbb{C} \to G(\mathbb{C}) \subseteq \mathbb{P}^2(\mathbb{C})$ 满足

$$\exp_G(z) = (2\sigma(z)^3\wp(z) : \sigma(z)^3\wp'(z) : 2\sigma(z)^3)$$

对所有 $z \in \mathbb{C}$均成立，其中 $\wp$ 和 σ 分别表示与 $\exp_G$的核所给出的格相关联的经典魏尔斯特拉斯 $\wp$-函数和 σ-函数。

我们指出，这一维数为 1 的连通代数群分类可推广到特征零的任意代数闭域。这由 Barsotti–Chevalley–Rosenlicht 定理推出，参见 [32, 定理 10.25]。

若 G 是一个代数群，则称 G 的闭子簇为代数子群，若它本身是一个代数群且具有相同的群运算。特别地，我们要求代数子群是闭的，但不要求不可约。

给定代数群 G 和 H，从 G 到 H 的态射是底层簇之间的态射，并且还会诱导一个从 $G(\mathbb{C})$ 到 $H(\mathbb{C})$ 的群同态。例如，从 $\mathbb{G}_m$ 到 $\mathbb{G}_m$ 的每个态射，都是将 x 映到某个 $n \in \mathbb{Z}$ 的 x^n 。此外，从 $\mathbb{G}_m$ 到 $\mathbb{G}_a$ 的每个态射都是平凡的；也就是说，它将 x 映到 0。代数群态射的核是一个代数子群。此外，如果 $\dim(G) = \dim(H) = 1$，那么从 G 到 H 的任何代数群态射要么是平凡的，要么是满射且核有限。这由命题 3.1 得出，因为核在解析拓扑中是离散的，在 Zariski 拓扑中是闭的。满射且核有限的代数群态射称为同源。此外， G 和 H 称为同源 ，若存在一个从 G 到 H 的同源。因此，任何维数为 1 的代数群态射要么是平凡的，要么是同源。若两个维数为 1 的连通代数群同源，则它们要么同构，要么都是椭圆曲线。我们将用到以下关于复代数群的著名事实。

引理 3.2。设 G、H 是一维复连通代数群，且 $\mathcal{C} \subsetneq G \times H$ 是一个代数对应。假设存在一维向量空间 $V \subsetneq \mathbb{C}^2$、$b \in \mathbb{C}^2$ 以及一个非空开集 $U \subseteq \mathbb{C}^2$，使得 $U \cap (V + b)$ 非空，并且

$$\exp_{G\times H}(U \cap (V + b)) \subseteq \mathcal{C}(\mathbb{C}).$$

则 $\mathcal{C}$ 是某个代数群的平移。

我们将给出证明，以方便读者阅读。

证明。 我们可以通过 $\mathcal{C}$ $P = \exp_{G\times H}(b)$ 进行平移，从而假设 $b = 0$ 和 U 是单位元的一个邻域。现在 $\exp_{G\times H}(U \cap V) \subseteq \mathcal{C}(\mathbb{C})$。存在一个非空开集 $U' \subseteq U$，使得对于所有 $x \in U'$，$U + x \cap U$都是非空的。因此 $\exp(U') \subsetneq \mathrm{Stab}(\mathcal{C}) = \{P \in \mathcal{C}(\mathbb{C});\ P + \mathcal{C} = \mathcal{C}\}$。由于稳定子 Stab 是一个代数簇且 $\mathcal{C}$ 不可约$\mathcal{C} = \mathrm{Stab}(\mathcal{C})$。我们还注意到，稳定子是一个群，因而是$G \times H$ 的代数子群。□

3.2. **次数**。给定一个代数群 G 及其子簇 $\mathcal{V}$（属于 G），我们常常需要定义 $\mathcal{V}$ 的次数。值得一提的是，我们所讨论的簇始终是纯维的，否则我们会讨论 Zariski闭集。为了定义 $\mathcal{V}$ 的次数，我们需要一个从 G 到射影空间 $\mathbb{P}^n$ 的映射，其中 $n \in \mathbb{N}$。此类映射由线丛参数化。

因此，设 G 是一个维数为 1 的代数群。如果 G 是 $\mathbb{G}_a$ 或 $\mathbb{G}_m$，我们固定一个典范开浸入 $G \to \mathbb{P}^1$。在这种情况下， G 在 $\mathbb{P}^1$ 中的 Zariski闭包 G 满足 $G = \mathbb{P}^1$。我们用 L_G 表示 $\mathbb{P}^1$ 上的线丛 $O_{\mathbb{P}^1}(1)$。如果 G 是椭圆曲线，则令 L_G 为充足线丛 $O_G(O)$，其中 O 是 E 的单位元。此外，对于椭圆曲线，我们有 $G = G$。

在代数群的乘积 $G_1 \times \cdots \times G_g$ 上，我们将始终使用线丛

$$L = (\pi_1^* L_{G_1}) \otimes \cdots \otimes (\pi_g^* L_{G_g}),$$

其中，对于每个 $i \in \{1, \ldots, g\}$，映射

$$\pi_i : \overline{G_1} \times \cdots \times \overline{G_g} \to \overline{G_i}$$

是投影态射，而 π_i^* 是线丛上的拉回态射 s.

固定线丛 L 后， $G_1 \times \cdots \times G_g$ 中维数为 n 的（拟射影）子簇 $\mathcal{V}$ 的次数 $\deg_L(\mathcal{V})$ 为相交积

$$\deg_L(\mathcal{V}) = c_1(L)^n \cdot [V],$$

其中， $c_1(L)$ 是 L 的第一陈类。相交积和陈类的定义见 [20, 第 2 章。5]一种所需工具较少的观点是， L 的某个倍数是极丰富的，并给出到射影空间的一个嵌入。于是， $\mathcal{V}$ 的次数就是该嵌入像的次数。

注3.3。如果 G 是 $\mathbb{G}_a$ 或 $\mathbb{G}_m$，且 $\mathcal{V}$ 是由单个多项式定义的超曲面，那么上述定义与多项式次数的直观定义颇为相似。具体来说，令 $X_1, \ldots X_g$ 表示 G^g 的笛卡尔坐标，我们将超曲面 $\mathcal{V}$ 视为由某个多项式定义的 $\mathbb{A}^g$ 的子簇

$$f_{\mathcal{V}} = \sum_{\boldsymbol{\lambda} \in A} c(\boldsymbol{\lambda}) X^{\boldsymbol{\lambda}},$$

其中， A 是 $\mathbb{Z}^g_{\geq 0}$的某个有限非空子集， $c(\boldsymbol{\lambda}) \neq 0$ 对所有 $\boldsymbol{\lambda} \in E$都成立，且 $X^{\boldsymbol{\lambda}} = X_1^{\lambda_1} \ldots X_g^{\lambda_g}$。事实证明，$\deg_L(\mathcal{V}) = j_1 + \cdots + j_g$；其中，对于每个 $1 \leq i \leq k$，数 j_i 是满足存在单项式 $X^{\boldsymbol{\lambda}}$且$\boldsymbol{\lambda} \in E$、并且该单项式可被 X_i^j 整除的最大非负整数 j 。这可能严格大于多项式通常的总次数，后者定义为系数非零的单项式的最大次数。

3.3. **对应 对应**。 我们首先准确阐述对应这一概念。

定义 3.4. 设 X 和 Y 为不可约曲线。 $\mathcal{C}$ 是 X 与 Y 之间的一个对应，它是一个不可约曲线 $\mathcal{C} \subseteq X \times Y$，且典范投影 $\pi_X \colon \mathcal{C} \to X$ 和 $\pi_Y \colon \mathcal{C} \to Y$ 均为支配映射。此外，对于任意集合 $A \subseteq X(\mathbb{C})$, 我们定义

$$\mathcal{C}(A) = \{\pi_Y(\pi_X^{-1}(x)) : x \in A\} = \pi_Y(\mathcal{C} \cap (A \times Y)).$$

这里回顾一下，若对于每个 $x \in X$，集合 $\pi_X^{-1}(x) = \{z \in \mathcal{C}(\mathbb{C}) : \pi_X(z) = x\}$ 都是有限的，则投影 π_X 是有限的。由于涉及的曲线均不可约，这等价于 π_X 是支配映射。我们回顾一下，若 $\pi_X(\mathcal{C}(\mathbb{C}))$ 在 X 中稠密，则投影 π_X 是支配映射。注意，此处我们利用了这样一个事实： $\pi_X(\mathcal{C}(\mathbb{C}))$ 要么是有限集、空集，要么是余有限集；对于任意稠密集 $A \subseteq X(\mathbb{C})$，这一点并不成立。

若 $A \subseteq X(\mathbb{C})$ 是有限集，则根据我们对 X, Y 和 $\mathcal{C}$ 维数的假设， $\mathcal{C}(A)$ 也有限。若 d_X 和 d_Y 分别是投影映射 π_X 和 π_Y 的次数，由于 $X, Y, \mathcal{C}$ 是不可约代数曲线， d_X, d_Y 等于纤维的最大基数。因此 $|\mathcal{C}(A)| \leq d_X|A|$ ，并且

$$\frac{1}{d_Y}|A| \leq |\mathcal{C}(A)|$$

若 A 属于 π_Y 的像。特别地，当π_Y 为满射时，下界对所有有限集 A 都成立。

设 L_X 和 L_Y 分别是射影簇 X 和 Y 上的线丛，并令$L = \pi_X^* L_X \otimes \pi_Y^* L_Y$。若 $\mathcal{C}$ 是 X 与 Y 之间的对应，则

$$\deg_L(\mathcal{C}) = \deg_{L_X}((\pi_X)_*[\mathcal{C}]) + \deg_{L_Y}((\pi_Y)_*[\mathcal{C}]) = d_X \deg_{L_X}(X) + d_Y \deg_{L_Y}(Y)$$

根据投影公式。因此，若 L_X 和 L_Y 充足，则

$$|\mathcal{C}(A)| \asymp_{\deg_L(\mathcal{C})} |A|$$

对所有有限集 A 都成立。特别地，这在我们上文第 3.2 节所述的预备知识中成立。

我们将研究代数群之间的对应。如果代数群 G 和 H 之间存在一个对应，且该对应是某个代数群的平移，那么 G 和 H 同源。现在给出两个直观的例子。

例 3.5。 我们可以固定一个有理映射 $\varphi : X \to Y$ ，它在某个开集$U \subseteq X$ 上有定义，然后将 $\mathcal{C}$ 视为 φ 的图的扎里斯基闭包。引言中讨论的 Bremner 问题涉及这样的情形： X 是魏尔斯特拉斯形式为 $y^2 = x^3 + ax + b$, $U = X \setminus \{O\}$ 的椭圆曲线， X 是去掉其无穷远点后的曲线， $Y = \mathbb{G}_a$，且$\varphi(x, y) = x$。如果 $A \subseteq U(\mathbb{C})$ 是有限集，那么 $\mathcal{C}(A)$ 就是 A 中各点所对应的所有 x 坐标构成的集合。

例 3.6. 设 φ 是次数为 $d \geq 1$的多项式。我们可以考虑 $\mathbb{G}_m \times \mathbb{G}_m$ 之间的一个对应，其复点由 $\{(x, \varphi(x)) : x \in \mathbb{G}_m(\mathbb{C})\}$给出。可以看出，该对应的次数为 $d + 1$。此外， $\mathcal{C}$ 是代数子群的平移，当且仅当 φ 具有如下形式： cx^d ，其中 $c \in \mathbb{C}$。这正是我们用来从定理 1.3 推导推论 1.4 的对应。

3.4. **Mordell–Lang 猜想与 S-单位方程**。 我们在此回顾 Laurent、David–Philippon 和 Evertse–Schlickewei–Schmidt 关于 Mordell–Lang 猜想的深刻结果。

定理 3.7. [11, 29, 18] 对任意正整数 d、g，存在常数 $C = C(d, g) \in \mathbb{N}$，具有如下性质。设 G 为椭圆曲线或 $\mathbb{G}_m$。令 $\mathcal{V} \subseteq G^g$ 为次数为 d的代数簇，且 $\mathcal{V}^{co}$ 为

$$\mathcal{V}^{co} = \mathcal{V} \setminus \bigcup_{R+B \subset \mathcal{V}, \dim(B)>0} (R + B),$$

其中 R 遍历 t 过 G^g 中的点，且 B 遍历连通代数子群。则 en

$$|\mathcal{V}^{co} \cap \Gamma| \leq C^{1+r}$$

对任意子群 $\Gamma \subseteq G^g(\mathbb{C})$，其秩为 r。更一般地，有

$$\mathcal{V} \cap \Gamma = \bigcup_{i=1}^{C^{1+r}} (\gamma_i + H_i) \cap \Gamma,$$

其中 γ_1、……、$\gamma_{C^{1+r}}$ 是 Γ 的元素，而 H_1、……、$H_{C^{1+r}}$ 是 G^g 的连通子群，其次数以上界 d 的函数为界。

证明。对于 $G = \mathbb{G}_m$，我们首先证明第一部分。直接由 [11, 29, 18] 得出 $Q_k \in \mathbb{C}[X_1, \ldots, X_g]$，使得 $\mathcal{V}$ 是它们的公共零点集。它们的次数由 $\mathcal{V}$ 的次数界定，而 Q_i 中非零单项式的数量由 deg(Q_i)^g 界定，其中 $i = 1$、……、g。如果有一个点 $\gamma \in \mathcal{V} \cap \Gamma$，那么 $Q_i(\gamma) = 0$，$i = 1$、……、k；如果 $\gamma \in \mathcal{V}^{co}$，那么至少存在一个 i，使得 Q_i 中的单项式在 γ 处取值时不存在和为零的子和。这由 Laurent [29] 的证明可得。对于所有 i [18]，$Q_i(\gamma) = 0$ 中不存在和为零的子和的解的数量由 c(deg(Q_i) g)$^{1+r}$ 界定。这就得到了第一个断言。

对于一般性表述，我们沿用 Laurent [29] 的证明。包含于 $\mathcal{V}$ 中的每个极大代数群，都对应于其定义方程支撑的一个划分。因此，它们的数量和次数仅由 $\mathcal{V}$ 的次数决定。对于由一个划分给出的每个代数子群，Laurent 构造了一个映射，将交点数量的计数转化为 S 单位方程的问题，从而可以应用 [18] 中的主定理。

最后，每个 H_i 的次数由 d 控制这一事实，可由 [2, 引理 2] 中的论证推出。□

注意，即使 $\mathcal{V}$ 不是陪集，$\mathcal{V}^{co}$ 也可能为空。一个简单的例子是曲线 $\mathcal{C}$ 的乘积 $\mathcal{C} \times \mathbb{G}_m \subseteq \mathbb{G}_m^3$，它被形如 $\{P\} \times \mathbb{G}_m$ 的陪集覆盖。

4. 投影笛卡尔积

本节的主要目标是证明定理 4.2，该定理描述了簇的某些投影的扩张性质。

因此，设 G为 $\mathbb{C}$上某个一维连通代数群，且不同构于 $\mathbb{G}_a$，并设 $\mathcal{B}$ 为正维数的射影簇。设 π_1：$G^g \times \mathcal{B} \to G^g$ 与π_2：$G^g \times \mathcal{B} \to \mathcal{B}$ 为典范投影映射。我们回顾定义 1.7 中所述的退化簇概念。

定义 4.1. 我们称不可约子簇 $\mathcal{V} \subseteq G^g \times \mathcal{B}$ 退化，如果存在正维数的连通代数群 $H \subseteq G^g$ 以及真子簇 $\mathcal{W} \subseteq G^g/H \times \mathcal{B}$，使得

$$\mathcal{V} = \pi_H^{-1}(\mathcal{W}),$$

对于投影 π_H： $G^g \times \mathcal{B} \to G^g/H \times \mathcal{B}$。如果 $\mathcal{V}$不是退化的，我们称 $\mathcal{V}$为非退化。

有了这一点，我们现在陈述定理 1.8 关于位于低秩子群中的集合的版本。

定理 4.2。设 $\mathcal{V} \subseteq G^g \times \mathcal{B}$ 是维数为 g 的非退化子簇，使得π_1 和 π_2 限制在 $\mathcal{V}$ 上时是支配的。设 $\Gamma \subseteq G(\mathbb{C})$ 是秩为 r 的子群。那么对于任意有限集 $A \subseteq \Gamma$，我们有

$$|\pi_2((A^g \times \mathcal{B}) \cap \mathcal{V})| \geq c(g, \deg(\mathcal{V}))^{1+r}|A|^g,$$

其中常数 $c = c(g,\ \deg(\mathcal{V})) > 0$ 仅取决于 g 和$\deg(\mathcal{V})$。

为了证明定理 4.2，我们需要以下引理。

引理 4.3。设 $\mathcal{V} \subseteq G^g \times \mathcal{B}$ 是一个维数为 g 的非退化子簇，并设映射 π_1 和 π_2 均为支配映射。那么存在一个适当的扎里斯基闭集 $Z \subseteq G^g$，使得如果存在一个正维子群 $H \subseteq G^g$，且 $(P, Q) \in (G^g \times \mathcal{B})(\mathbb{C})$ 满足

$$\{(P + T, Q) : T \in H(\mathbb{C})\} \subseteq \mathcal{V}, \tag{4.1}$$

那么 $P + H \subseteq Z$。此外，Z 的各个分支的次数及其数量均有界，该界仅取决于 g、$\deg(\mathcal{V})$。

证明。我们先固定一个维数为 k 的连通代数子群 H，并证明所有满足 $(P + H) \times \{Q\} \subseteq \mathcal{V}$ 的 P（其中某个 Q）都包含在一个扎里斯基闭集中 Z_H，而该集合仅取决于 H。取这些集合 Z_H 的并，即可证明此引理。令 p_H 为商映射 π_H： $G^g \times \mathcal{B} \to (G^g/H) \times \mathcal{B}$ 在 $\mathcal{V}$ 上的限制。由切瓦莱定理[23, 定理 1.3。1] 集合

$$Z^H = \{y \in \mathcal{V}(\mathbb{C}) : \dim(p_H^{-1}(p_H(y))) \geq k\}$$

是闭的。因此，如果 $(P + H) \times \{Q\} \subseteq \mathcal{V}$，那么 $(P + H) \times \{Q\} \subseteq p_H^{-1}(p_H(P, Q))$，从而 $(P, Q) \in Z^H$。

由于 $\mathcal{B}$ 是射影的，投影 π_1： $G^g \times \mathcal{B} \to G^g$ 是闭映射 [39, 定理 1.11]。因此，$Z_H = \pi_1(Z^H)$ 在 G^g 中是闭的。若 $Z_H = G^g$，则 Z^H 的维数为 g，因此等于 $\mathcal{V}$。此外，根据投影公式，Z_H 的次数不超过 Z^H 的次数。因此，只需证明 Z^H 不等于 $\mathcal{V}$，并且 Z^H 的次数可由 g 和 $\deg(\mathcal{V})$ 界定。

我们首先证明 $Z^H \neq \mathcal{V}$，因此，假设 $Z^H = \mathcal{V}$。然后考虑 $\mathcal{W}$，即 $\pi_H(\mathcal{V})$和 $Z' = \pi_H^{-1}(\mathcal{W})$的Zariski闭包；它是 $G^g \times \mathcal{B}$ 的一个包含 $\mathcal{V}$的子簇。首先，$\mathcal{W}$ 是不可约的，因为 $\mathcal{V}$ 是不可约的。由于 H 是连通的，π_H的纤维是不可约的，因此 [39, 定理1.26] 推出 Z' 是不可约的。由于 $\pi_H(\mathcal{V})$是可构造的，它包含 U，后者在 $\mathcal{W}$中是Zariski开（稠密）的。因此我们有 $Z' = \pi_H^{-1}(U) \cup \mathcal{E}$，其中 $\mathcal{E}$是不可约子簇 $E = \pi_H^{-1}(E')$的有限并，E' 遍历 $\mathcal{W} \setminus U$的所有不可约分支。根据纤维维数定理，对于所有 E，$\dim(E) < \dim(Z')$。由于 $\pi_H^{-1}(U) \subset \mathcal{V}$，我们得到 $Z' \subseteq \mathcal{V} \cup \mathcal{E}$，并且维数

计数表明，$\dim(\mathcal{V}) = \dim(Z')$。由于 $\mathcal{V}$ 和 Z' 都是不可约的 $\mathcal{V} = Z'$。这意味着

$$\mathcal{V} = \pi_H^{-1}(\mathcal{W})$$

因此， $\mathcal{V}$ 是退化的。这与我们对 $\mathcal{V}$ 的假设矛盾。

现在我们将证明， Z^H 的次数可由 g 和 $\deg(\mathcal{V})$ 控制。对于 $g \geq 1$，定义 $\exp_{G^g}$ 为 G^g 在单位元处的指数映射，并令 $\mathcal{F}$ 为 $\exp_G$ 的一个适当选取的基本域。将 $\exp_G$ 限制在 $\mathcal{F}$ 上所得的图，是一个复杂度由绝对常数（可有效计算）控制的子 Pfaffian 集，参见 Jones 与第三作者的工作[27]。每个代数群 H 都对应一个向量空间 T_H，使得 $\exp_{G^g}(T_H) = H$。接下来我们考虑集合

$$T^H = \{\gamma \in \mathcal{F}^g : \text{there exists } b \in \mathcal{B}(\mathbb{C}) \text{ such that } \exp_{G^g}(\gamma + T_H) \subseteq \mathcal{V} \cap (G^g \times \{b\})\},$$

这是一个复杂度为 c_{comp} 的子 Pfaffian 集，其中 c_{comp} 仅取决于 $\deg(\mathcal{V})$。接下来有 $Z^H = \exp_{G^g}(T^H)$，其复杂度同样有界，并且它是一个闭代数簇。 Z^H 的复杂度控制着它的次数，因此我们也证明了这一断言。

最后，假设 $P + H$ 是包含在纤维 $\mathcal{V}_Q = \pi_2^{-1}(Q) \cap \mathcal{V}$中的极大平移。注意，根据贝祖定理，$\deg(\mathcal{V}_Q) \ll_g \deg(\mathcal{V})$。由 Bombieri–Zannier [2,引理 2], 的论证可知，若 H 是出现在 $\mathcal{V}_Q$的某个极大平移中的代数子群，则 H属于一个有限集 $\{H_1, \ldots, H_\ell\}$，其中 $\ell \ll_{g,\ \deg(\mathcal{V})} 1$。取$Z = Z_{H_1} \cup \cdots \cup Z_{H_\ell}$即可证明该引理。□

为证明定理 4.2，我们将引理 4.1 与一致莫德尔–朗猜想（定理 3.7）给出的估计结合起来。为了控制引理 4.1 中闭集 Z 的贡献，我们需要以下 Schwartz–Zippel 型估计。

引理 4.4. 设 $Z \subseteq G^g$ 是一个代数子簇。那么对于任意有限集 $A \subseteq G(\mathbb{C})$

$$|Z \cap A^g| \ll_{g,\deg(Z)} |A|^{\dim(Z)}.$$

证明。 我们对维数使用归纳法来证明。由于可以逐个分量进行论证，因此不妨设 Z 不可约。我们还可以将 Z 在 G^g中的闭包 Z 代替 Z 。如果 $\dim(Z) = 0$，则结论显然成立。因此假设 $\dim(Z) \geq 1$。我们可以选取一个因子 GinG^g ，使得从 Z 到 G 的投影是满射。不失一般性，不妨设这是第一个因子。于是交集 $Z \cap (\{a\} \times G^{g-1})$的维数等于 $\dim(Z) - 1$。根据贝祖定理

$$\deg(\overline{Z} \cap (\{a\} \times \overline{G}^{g-1})) \leq \deg(Z)\deg(\overline{G}^{g-1}) \ll_g \deg(Z).$$

由归纳法可得

$$|Z \cap A^g| \leq \sum_{a \in A} |A^g \cap (\{a\} \times \overline{G}^{g-1}) \cap \overline{Z}| \ll_{g,\deg(Z)} |A||A|^{\dim(Z)-1}. \quad \square$$

现在我们可以证明定理 4.2 了。

定理 *4.2* 的证明。由于 $\mathcal{V}$ 是非退化的，包含在纤维 $\mathcal{V}_Q = \pi_2^{-1}(Q) \cap \mathcal{V}$中的陪集包含在一个不依赖于 Q的闭集 $Z \subseteq \mathcal{V}$ 中。这就是引理 4.1。我们令$A' = A^g \setminus Z(\mathbb{C})$，根据引理 4.4， $|Z \cap A^g| \ll_{\deg(\mathcal{V})} |A|^{g-1}$。由于投影 π_1 从$\mathcal{V}$ 到 G^g 是支配的，且 $\mathcal{B}$ 是射影的， π_1 实际上是满射，因为它是闭的 [39]。

因此，对于每个点 $a \in A'$，都存在一个点 $b \in B$，使得 $(a,\ b) \in (A' \times \mathcal{B}) \cap \mathcal{V}$。另一方面，由定理 3.7 可知，对于每个 $b \in \mathcal{B}(\mathbb{C})$，有

$$|(A' \times \{b\}) \cap \mathcal{V}| \leq c(r, g, \deg(\mathcal{V}))^{r+1}$$

因此，像 $\pi_2((A^g \times \mathcal{B}) \cap \mathcal{V})$ 至少包含

$$c(r, g, \deg(\mathcal{V}))^{-1-r}(|A|^g - c'|A|^{g-1})$$

个元素，其中常数 $c' > 0$ 仅取决于 $\deg(\mathcal{V})$ 和 g，由此完成定理 4.2 的证明。□

5. Correspondences and cosets

本节构造一个簇 $\mathcal{V}_{\text{sum}}$，使得 $\pi_2((A^g \times H) \cap \mathcal{V}_{\text{sum}})$ 大致等于和集 $\mathcal{C}_1(A) + \cdots + \mathcal{C}_g(A)$，其中 $\mathcal{C}_1, \ldots, \mathcal{C}_g$ 是代数群 G 和 H 之间的对应。我们希望将定理 4.2 应用于 $\mathcal{V}_{\text{sum}}$，因此本节专门证明该簇是非退化的，含义见定义 1.7。

现在设 G 和 H 是维数为 1 的连通代数群，且 G 与 $\mathbb{G}_a$ 不同构。我们按照第 3.2 节开头所述将 H 紧化。因此，H 要么是 $\mathbb{P}^1$，要么是椭圆曲线，具体取决于 H 是否与 $\mathbb{G}_a$ 同构，$\mathbb{G}_m$ 还是与椭圆曲线同构。我们还考虑 H 上的 g 重和映射

$$p_{\text{sum}} : H^g \to H$$
$$(Q_1, \ldots, Q_g) \mapsto Q_1 + \cdots + Q_g,$$

其图 $\Gamma(p_{\text{sum}}) \subseteq H^g \times H$，以及其在 H^{g+1} 中的闭包 $\Gamma(\overline{p_{\text{sum}}})$。

设 $\mathcal{C}_1$，……，$\mathcal{C}_g \subseteq \overline{G \times H}$ 为对应，且它们都不是代数子群的平移。我们设

$$\mathcal{V}^* = \{(P_1, \ldots, P_g, Q_1, \ldots, Q_{g+1}) : (Q_1, \ldots, Q_{g+1}) \in \overline{\Gamma(p_{\text{sum}})}, (P_i, Q_i) \in \mathcal{C}_i\},$$

这是一个不可约簇。根据 [39, 定理 1.11]，投影 $\pi_{G^g \times H} \colon G^g \times H^{g+1} \to G^g \times H$ 到 G^g 以及 H^{g+1} 的最后一个坐标都是闭映射。我们设

$$\mathcal{V}_{\text{sum}} = \pi_{G^g \times \overline{H}}(\mathcal{V}^*) \tag{5.1}$$

这是一个不可约簇，因为它是一个不可约簇在闭映射下的像。因此，第 4 节中射影簇 $\mathcal{B}$ 所起的作用由 H 承担。

本节的主要目标是证明以下结果。

命题 5.1. 簇 $\mathcal{V}_{\text{sum}} \subseteq G^g \times H$ 是非退化的，维数为 g。投影 $\pi_1 : \mathcal{V}_{\text{sum}} \to \overline{G^g}$ 是满射，而投影 $\pi_2 : \mathcal{V}_{\text{sum}} \to H$ 是支配的。

由于我们只研究复代数群，因此将证明一个关于代数群切空间之间的全纯映射的引理。

引理 5.2。 设 $U = U_1 \times \cdots \times U_g$ 是 $\mathbb{C}^g$ 的一个开集，且 $f_i : \ U_i \to \mathbb{C}$ 是 $1 \leq i \leq g$ 上的非恒定全纯函数。假设存在一个维数为 1 的向量空间 $W \subseteq \mathbb{C}^g$，使得对任意 $b \in \mathbb{C}^g$，$(f_1, \ldots, f_g)$ 限制在 $(W + b) \cap U$ 上满足

$$f_1(z_1) + \cdots + f_g(z_g) \equiv const.$$

于是至少存在一个 $j \in \{1, \ldots, g\}$，使得 f_j 是仿射线性的。

证明。 在可能置换坐标之后，我们可以将任意陪集 $W+b$ 用

$$(b_1,\dots,b_{g-k},z,a_1z+c_1,\dots,a_{k-1}z+c_{k-1})$$

其中 $k\geq 1$ 是整数， a_1、……、 $a_{k-1}\in\mathbb{C}^*$ 取决于 W 和 b_1、……、 b_{g-k}， c_1、……、 c_{k-1} 取决于 $W+b$。我们可以假设 $k\neq 1$，因为否则 f_g 是常数。我们应用可逆线性变换

$$L:\mathbb{C}^{g-k}\times\mathbb{C}\times\mathbb{C}^{k-1}\to\mathbb{C}^{g-k}\times\mathbb{C}\times\mathbb{C}^{k-1}$$
$$L(\underline{z},z,\underline{w})=(\underline{z},z,w_1-a_1z,\cdots,w_{k-1}-a_{k-1}z)$$

~ ~ ~到 U参数化，则开集 $L(U)$ 包含一个积集 $U=U_1\times\cdots\times U_g$。对 z 取全导数，我们得到

$$\partial_{z_{g-k+1}}f_{g-k+1}(z)+a_1\partial_{z_{g-k+2}}f_{g-k+2}(a_1z+c_1)+\cdots+a_{k-1}\partial_{z_g}f_g(a_{k-1}z+c_{k-1})=0,$$

~对所有 $(b_1,\dots,b_{g-k},z,c_1,\dots,c_{k-1})\in U$. 成立。由于 $k\geq 2$，我们可以固定任意

$$(z_0,c_{1,0},\dots,c_{k-2,0})\in\tilde{U}_{g-k+1}\times\cdots\times\tilde{U}_{g-1}$$

从而发现 f_g 是仿射线性的。 □

推论 5.3. 令 $U_1\times\cdots\times U_g$ 为 $\mathbb{C}^g$ 的一个开集，且 $f_i\colon\ U_i\to\mathbb{C}$ 为全纯非常数函数 $i=1,\dots,g$。假设存在一个维数为k 的向量空间 $V\subsetneq\mathbb{C}^g$，使得对任意 $b\in\mathbb{C}^g$，$(f_1,\dots,f_g)$ 限制在 $(V+b)\cap U$ 上满足

$$f_1(z_1)+\cdots+f_g(z_g)\equiv const.$$

那么，对于至少一个 $j\in\{1,\dots,g\}$， f_j 是仿射线性的。

证明。我们可以用一维向量空间 L 的平移覆盖 V，因此 V 的任意平移都包含 L的一个平移。因此，推论 5.3 可由引理 5.2 推出。□

命题 5.1 的证明。令 $\mathcal{V}^o$ 为由满足以下条件的点 $(P_1,\dots,P_g,Q)\in G^g\times H$构成的簇：存在 $(P_i,Q_i)\in\mathcal{C}_i\cap(G\times H(\mathbb{C}))$，其中 $Q_1+\cdots+Q_g=Q$。注意， $\mathcal{V}^o$ 在 $\mathcal{V}_{\mathrm{sum}}$中是开集。除有限多个 $P\in G(\mathbb{C})$ 外，均存在 $Q\in H(\mathbb{C})$，使得对于 $i=1,\dots,g$，$(P,Q)\in\mathcal{C}_i(\mathbb{C})$。因此， π_1 是支配映射，并且根据 [39, 定理 1.11]，它是满射。此外，对于$Q\in H(\mathbb{C})$，我们可以找到 $(Q_1,\dots,Q_g)\in H(\mathbb{C})$，使得 $Q_1+\cdots+Q_g=Q$。由此可知， π_2 是支配映射。现在假设 $\mathcal{V}_{\mathrm{sum}}$ 是退化的，也就是说，存在一个正维数的连通代数群 $H'\subseteq G^g$，以及一个真子簇 $\mathcal{W}\subseteq(G^g/H')\times H$，使得 —

$$\mathcal{V}_{\mathrm{sum}}=\pi_{H'}^{-1}(\mathcal{W}),\tag{5.2}$$

对于投影 $\pi_{H'}\colon\ G^g\times H\to(\overline{G}^g/H')\times H$。

现在，设 s_1、……、 s_g 是开集 $U\subseteq G(\mathbb{C})$ 上以 $H(\mathbb{C})$ 为目标的解析函数，使得 s_i 的图与 $\mathcal{C}_i(\mathbb{C})$ 在 $U\times H(\mathbb{C})$ 上的限制相重合。根据 (5.2)，和 $\sum_{i=1}^g s_i$（其中求和于 H 中）沿着 $H'+P$ 对所有 $P\in G^g(\mathbb{C})$ 都是常数。在必要时缩小U，以确保其单连通，我们通过设定 $f_i=\exp_H\circ s_i\circ\log_G$、 $i=1$、……、 g，将这些函数提升为从 G 的切空间到 H 的切空间的函数。现在令 V 为 H'的切空间，并回忆和 $\sum_{i=1}^g s_i$ 沿着 H'的平移保持常数，我们由此推出 f_1、……、 f_g 满足推论 5.3 的条件。因此， f_i 中至少有一个是仿射线性的。引理 3.2 意味着，至少有一个 $\mathcal{C}_i$ 是某个代数子群的平移，这与我们关于这些对应的假设相矛盾，从而证明得证。□

6. Freiman–type structural theorems

对于本节及下一节，给定一个 1 维连通代数群 H 和某个有限非空集 $A \subsetneq H$，我们将 **rk(**A**)** 定义为满足以下条件的最小整数 $r \geq 1$： 存在 ξ_1、……、$\xi_r \in H$，使得

$$A \subseteq \{n_1\xi_1 + \cdots + n_r\xi_r : n_1, \ldots, n_r \in \mathbb{Z}\}.$$

本节的主要目的是证明以下结构性结果 lt.

引理 6.1. 设 H 是一个维数为1的连通代数群， $A \subseteq H$ 是一个有限非空集， $n \geq 2$ 是一个整数，且 $|nA| \leq K|A|$ 对某个 $K > 1$成立。那么存在某个整数 $1 \leq d$ 以及某个子集 $A' \subseteq A$，使得

$$d \ll 1 + \frac{\log(4K)}{\log n} \quad and \quad |A'| \gg \frac{|A|}{K^{\frac{C\log 2}{\log n}}} \quad and \quad \mathrm{rk}(A') \leq d,$$

其中 $C > 0$ 是某个绝对常数。

我们将首先证明这一结果的 $n = 2$ 版本。

引理 6.2。 设 H 是一个维数为1的连通代数群，设 $A \subseteq H$ 是一个有限非空集，使得 $|A + A| \leq K|A|$ 对某个 $K > 1$成立。那么存在某个整数$1 \leq d \leq C\log(400K)$，以及某个子集 $A' \subseteq A$，使得 $|A'| \geq |A|/(100K)^{C'}$，且 $\mathrm{rk}(A') \leq d$，其中 $C = 140$ 且 $C' = 110$。

为了证明引理 6.2，我们需要用到 Gowers–Green–Manners–Tao 关于在 $\mathbb{Z}$上解决弱多项式 Freiman–Ruzsa 猜想的一个非常漂亮的结果 [22, 定理 **1**。3]

引理 6.3。 设 D 是一个正整数，设 $A \subsetneq \mathbb{Z}^D$ 是一个有限非空集，使得$|A + A| \leq K|A|$ 对某个 $K > 1$成立。那么存在某个整数 $1 \leq d \leq C\log(4K)$、某些元素 $\boldsymbol{x}_1$、……、$\boldsymbol{x}_d \in \mathbb{Z}^D$ 以及某个子集 $A' \subseteq A$，使得 $|A'| \geq |A|/K^{C'}$ 并且

$$A' \subseteq \{n_1\boldsymbol{x}_1 + \cdots + n_d\boldsymbol{x}_d : n_1, \ldots, n_d \in \mathbb{Z}\},$$

其中 $C = 140$ 且 $C' = 110$。

我们还将需要下面这条简单引理。

引理 6.4. 设 H 是维数为 1 的连通代数群，设 $A \subsetneq H$ 是有限非空集。则由 S 生成的子群同构于 $\mathbb{Z}^D \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ 的某个子群，其中 D 为某个非负整数，且 n、$m \in \mathbb{N}$为某些量。

证明。 当 $H = (\mathbb{C}, +)$ 时这成立，因为 $(\mathbb{C}, +)$ 的任意有限生成子群都对某个 $D \in \mathbb{N}$同构于 $\mathbb{Z}^D$。当 $H = (\mathbb{C}^*, \cdot)$ 时，这一点稍显不平凡，但有一个标准事实：$(\mathbb{C}^*, \cdot)$ 的任意有限生成子群都同构于 $\mathbb{Z}^D \times \mathbb{Z}/N\mathbb{Z}$，其中 D 为某个非负整数，且 $N \in \mathbb{N}$为某个量。最后，当 H 是 $\mathbb{C}$上的某条椭圆曲线时，我们可以利用第 3.1 节中提到的事实，即 H 同构于 $\mathbb{C}/L$，其中 L 是 $\mathbb{C}$中某个秩为二的格，从而推出 H 的任意有限生成子群都同构于 $\mathbb{Z}^D \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ 的某个子群，其中 D 为某个非负整数，且 n， $m \in \mathbb{N}$为某些量。 □

现在我们可以证明引理 6.2 了

引理 *6.2* 的证明。令 Γ 为由 S生成的子群。我们可以利用引理 6.4，将 Γ 视为 $\mathbb{Z}^l \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ 的子群，其中 $n,\ m \geq 1$ 是一些整数，$l \geq 0.$ 是某个整数。现在，对于任意 $0 \leq i,\ j \leq 9$，定义

$$A_i = \{x \in \mathbb{Z} : in/10 \leq x < (i+1)n/10\} \pmod{n}$$

and

$$B_j = \{x \in \mathbb{Z} : jm/10 \leq x < (j+1)m/10\} \pmod{m}.$$

因此 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = \cup_{0\leq i,\ j\leq 9}(A_i \times B_j)$。此外，对每个$0 \leq i,\ j \leq 9$，令 $S_{i,\ j} = S \cap ($ $\mathbb{Z}^l \times A_i \times B_j)$。由于

$$\sum_{0\leq i,j\leq 9} |S_{i,j}| = |S|,$$

根据鸽巢原理，存在某些 $0 \leq i,\ j \leq 9$ 使得 $|S_{i,\ j}| \geq |S|/100$。

令 $\pi\colon \mathbb{Z}^l \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}^{l+2}$ 为满足下式的映射

$$\pi(\boldsymbol{x}, a \pmod{n}, b \pmod{m}) = (\boldsymbol{x}, a, b)$$

对所有 $\boldsymbol{x} \in \mathbb{Z}^l$、 $a \in \{0, 1, \ldots, n-1\}$ 和 $b \in \{0, 1, \ldots, m-1\}$均成立。现在我们声称，对于任意 $s_1,\ s_2,\ s_3,\ s_4 \in S_{i,\ j}$，有

$$\pi(s_1) + \pi(s_2) = \pi(s_3) + \pi(s_4) \text{ if and only if } s_1 + s_2 = s_3 + s_4. \tag{6.1}$$

为了解释这一点，首先注意到，由于 π^{-1} 只是投影映射，只需验证右边的等式能够推出左边的等式。写作

$$s_l = (\boldsymbol{x}_l, a_l \pmod{n}, b_l \pmod{m})$$

对于每个 $1 \leq l \leq 4$，我们看到 $s_1 + s_2 = s_3 + s_4$ 蕴含

$$a_1 + a_2 - a_3 - a_4 \equiv 0 \pmod{n} \text{ and } b_1 + b_2 - b_3 - b_4 \equiv 0 \pmod{m}.$$

由于 $in/10 \leq a_1,\ a_2,\ a_3,\ a_4 <$ $(i+1)n/10$，我们看到

$$a_1 + a_2 - a_3 - a_4 \in [-n/5, n/5] \cap \mathbb{Z}.$$

上述同余条件现在要求 $a_1 + a_2 = a_3 + a_4$。类似的论证可得 $b_1 + b_2 = b_3 + b_4$。

因此，写作 $S_1 = \pi(S_{i,\ j})$，(6.1) 中的等价关系意味着

$$|S_1 + S_1| = |S_{i,j} + S_{i,j}| \leq |S + S| \leq K|S| \leq 100K|S_{i,j}| = 100K|S_1|$$

由于 $S_1 \subseteq \mathbb{Z}^{l+2}$，现在可以应用引理 6.3，找到某个子集 $S_1' \subseteq S_1$ ，使得$|S_1'| \geq |S_1|/(100K)$ $^{C'}$ 并且

$$S_1' \subset \{n_1\boldsymbol{x}_1 + \cdots + n_d\boldsymbol{x}_d : n_1, \ldots, n_d \in \mathbb{Z}\},$$

其中 $\boldsymbol{x}_1$，*.....*， $\boldsymbol{x}_d \in \mathbb{Z}^{l+2}$ 是一些元素，且 $1 \leq d \leq C\log(400K)$ 是某个整数。这意味着

$$\pi^{-1}(S_1') \subset \{n_1\pi^{-1}(\boldsymbol{x}_1) + \cdots + n_d\pi_1^{-1}(\boldsymbol{x}_d) : n_1, \ldots, n_d \in \mathbb{Z}\}.$$

令 $S' = \pi^{-1}(S_1')$，即可完成引理 6.2 的证明。 □

现在我们给出引理 6.1 的证明。

引理 *6.1* 的证明。由于 $n \geq 2$，我们有 $|2S| \leq |nS|$，因此，只要 $2 \leq n \leq 16$，就可以应用引理 6.1，并调整 Vinogradov 记号中的隐含常数，从而得到所需结果。因此，我们假设 $n > 16$；在这种情况下，令 $k = \lfloor (\log n)/(\log 2) \rfloor$，可得 $k \geq 4$。现在，由于 $|2^k S| \leq |nS| \leq K|S|$，我们得到

$$K \geq \frac{|2^k S|}{|S|} = \prod_{1 \leq j \leq k} \frac{|2^j S|}{|2^{j-1} S|},$$

因此，存在某个 $1 \leq j \leq k$ 使得

$$|2^j S| = |2^{j-1} S + 2^{j-1} S| \leq K^{1/k} |2^{j-1} S|. \tag{6.2}$$

对集合 $2^{j-1}S$ 应用引理 6.2，我们得到存在某个集合 $X \subseteq 2^{j-1}S$ 使得

$$|X| \gg \frac{|2^{j-1} S|}{K^{C/k}} \quad \text{and} \quad X \subseteq \{n_1 \xi_1 + \cdots + n_d \xi_d : n_1, \ldots, n_d \in \mathbb{Z}\}, \tag{6.3}$$

对于某个

$$d \ll 1 + \frac{\log(4K)}{k}$$

以及某些点 ξ_1、……、$\xi_d \in H$。

因此，只需证明 S 存在一个大子集，该子集包含于集合 $-X$ 的某个平移中。为此，注意到

$$|X||S| = \sum_{y \in X+S} |(y - X) \cap S| \leq |X + S| \max_{y \in X+S} |(y - X) \cap S|.$$

因此，只需证明

$$\frac{|X + S|}{|X|} \ll K^{C'/k},$$

对某个绝对常数 $C' > 0$。为了看出这一点，我们将 $X \subseteq 2^{j-1}S$这一事实与 (6.2) 和 (6.3) 结合起来，从而得到

$$\frac{|X + S|}{|X|} \leq \frac{|2^{j-1} S + 2^{j-1} S|}{|X|} \ll K^{C/k} \frac{|2^j S|}{|2^{j-1} S|} \ll K^{(C+1)/k}.$$

至此，引理 6.1 的证明结束。 □

我们简要指出，类似于 Freiman 逆定理的结构结果常常与覆盖结果配合使用。其中一个这样的结果称为 Ruzsa 覆盖引理。

引理 6.5. 设 G 为阿贝尔群，设 A、$B \subseteq G$ 为非空集合，使得 $|A+B| \leq K|B|$。则存在某个非空集合 $X \subseteq A$，使得 $|X| \leq K$ 且 $A \subseteq X + B - B$.

这立即与引理 6.2 结合，从而得到如下结果。

引理 6.6。 设 H 是一个维数为1的连通代数群，设 $A \subseteq H$ 是一个有限非空集，使得 $|A + A| \leq K|A|$ 对某个 $K > 1$成立。那么存在某个整数$1 \leq d \leq C \log(400K)$，某个有限子集 $T \subsetneq H$，满足$\mathrm{rk}(T) = d$，以及某个非空$X \subseteq H$，使得

$$|X| \leq (100K)^{C'+1} \quad and \quad A \subseteq X + T,$$

其中 $C = 140$ 和 $C' = 110$。

7. Proofs of main results

本节将给出 §1 和 §2 中提及的所有结果的证明。我们首先由推论 2.2 推导出定理 1.1。

定理 *1.1* 的证明。令 G 为魏尔斯特拉斯形式（1.1）中的一条椭圆曲线，$H = \mathbb{G}_a$和 $\mathcal{C}$ 为由（x、y、x）给出的对应关系，我们可以应用推论 2.2 得到定理 1.1 的第一部分。对 $H = \mathbb{G}_m$ 进行类似处理，即可得到关于等比数列的所需结论。令 $\mathcal{C}$ 等于（x、y、z）$x =$（$u + z$），我们得到连续平方数的界。此外，例如取 $z^2 = x$，我们还可以对某些高亏格曲线中等差数列的长度给出界。□

现在我们将结合定理 2.1 和引理 6.1 来证明定理 1.3。

定理 *1.3* 的证明。设 $k \geq 1$ 和 $d \geq 2$ 为整数，且 $g \in \mathbb{N}$ 相对于 d, k 足够大。我们还可以假设 $|gA| \leq |A|^k$，否则结论显然成立。在这种情况下，我们可以应用引理 6.1，找到某些 $\xi_1, \ldots, \xi_r \in G$ 以及某个 $A' \subseteq A$，使得 $r \ll k \log |A|/\log g$，并且

$$|A'| \gg |A|^{1-Ck/\log g} \quad \text{and} \quad A' \subseteq \{n_1\xi_1 + \cdots + n_d\xi_d : n_1, \ldots, n_d \in \mathbb{Z}\}.$$

后一个条件意味着由 A' 生成的子群的秩至多为 r，因此我们可以应用定理 2.1，推出

$$\begin{aligned} |\mathcal{C}_1(A) + \cdots + \mathcal{C}_g(A)| &\geq |\mathcal{C}_1(A') + \cdots + \mathcal{C}_{2k}(A')| \\ &\geq c(d,2k)^{-1-r}|A'|^{2k} \\ &\gg_k c(d,2k)^{-1}|A|^{-\frac{k\log c(d,2k)}{\log g}}|A'|^{2k} \\ &\gg_{k,d} |A|^{2k-\frac{2Ck^2}{\log g}-\frac{k\log c(2k,d)}{\log g}}. \end{aligned}$$

选取足够大的 g，以确保

$$\frac{2Ck^2}{\log g} < k/2 \quad \text{and} \quad \frac{k\log c(d,2k)}{\log g} < k/2 \quad \text{and} \quad 2k < g,$$

我们得到

$$|\mathcal{C}_1(A) + \cdots + \mathcal{C}_g(A)| \geq |\mathcal{C}_1(A) + \cdots + \mathcal{C}_{2k}(A)| \gg_{k,d} |A|^k.$$

这就完成了定理 1.3 的证明。□

定理 1.5 是定理 2.6 的一个特例。事实上，若 $\mathcal{V}$ 是 G^g 的一个不可约子簇，且它不是某个子群的陪集，那么有显然的不等式 $\operatorname{codef}(\mathcal{V}) \leq \dim(\mathcal{V}) - 1$。因此，我们现在证明定理 1.8。

定理 *1.8* 的证明。由于 $|A + A| \leq K|A|$，我们可以应用引理 6.6，推得 $A \subseteq Y + T$，其中 T包含于 H的一个子群 Γ 中，该子群的秩为 $d \ll \log K$，且 $Y \subset H$满足 $|Y| \leq K^{O(1)}$。现在，由于 $X \subseteq A$，这意味着 X 也包含于某个子群 Γ的至多 $K^{O(1)}$ 个平移中。根据鸽巢原理，我们可以找到某个 $X' \subseteq X$，满足 $|X'| \geq |X|/K^{O(1)}$，使得 X' 包含于 Γ的一个平移中，因此，X' 包含于

i秩为 $d+1$的一个子群中。现在应用定理 4.2，我们可以推得

$$|\pi_2((X^g \times \mathcal{B}) \cap \mathcal{V})| \geq |\pi_2((X'^g \times \mathcal{B}) \cap \mathcal{V})| \geq \frac{|X'|^g}{C^{2+d}}$$
$$\geq \frac{|X|^g}{K^{O(g)} 2^{C' \log K}} \gg \frac{|X|^g}{K^{C''}}$$

其中 C、C'、$C'' > 0$ 是仅依赖于 g、$\deg(\mathcal{V})$ 的常数。 □

接下来，我们证明定理 2.1。

定理 *2.1* 的证明。我们考虑式 (5.1) 中描述的簇 $\mathcal{V}_{\mathrm{sum}}$，并注意到对于任意有限集 $A \subset G$，集合

$$\pi_2((A^g \times \overline{H}) \cap \mathcal{V}_{\mathrm{sum}}) = \mathcal{C}_1(A) + \cdots + \mathcal{C}_g(A).$$

命题 5.1 表明，该簇 $\mathcal{V}_{\mathrm{sum}}$ 是非退化的，维数为 g，且投影 π_1 到 G^g 是满射，而 π_2 到 H 在 $\mathcal{V}$ 上的限制是支配的。因此，我们可以应用引理 4.2 推得

$$|\mathcal{C}_1(A) + \cdots + \mathcal{C}_g(A)| \geq c(g, \deg(V))^{1+r} |A|^g. \qquad \square$$

现在我们将由定理 2.1 推出推论 2.2。

推论 *2.2* 的证明。 在整个证明中，设 $C_1, C_2, C_3 > 0$ 为仅依赖于 d的正常数。假设 A 是 $\mathcal{C}(\Gamma)$中秩为 k的广义算术级数，其中 $k \in \mathbb{N}$为某个量。我们将首先证明，对某个常数 $0 < C \ll_d 1$，有 $k \leq C^{1+r}$。为看出这一点，设

$$P' = \{P_0 + \ell_1 P_1 + \cdots + \ell_k P_\ell : 0 \leq \ell_i \leq 1\}. \tag{7.1}$$

由于 $L_1, \ldots, L_k \geq 2$，我们得到 $P' \subseteq P$。由于 P是适当的，我们得到 P'也是适当的，因此有

$$|P' + P'| \leq 3^k = |P'|^{\frac{\log 3}{\log 2}}.$$

对 P' 应用定理 2.1，我们得到

$$|P'|^2 C_1^{-1-r} \ll |P' + P'| \ll |P'|^{\frac{\log 3}{\log 2}},$$

由此得 $2^k = |P'| \leq C_2^{1+r}$。现在，我们考虑集合 P，并利用前面关于 $|P'|$ 的上界来看出

$$|P + P| \leq (2L_1 - 1) \ldots (2L_k - 1) \leq 2^k L_1 \ldots L_k = 2^k |P| \leq C_2^{1+r} |P|.$$

现在我们可以应用定理 2.1 推出

$$C_1^{-1-r} |P|^2 \leq |P + P| \leq C_2^{1+r} |P|,$$

因此，我们得到了所需的结论 $|P| \leq C_3^{1+r}$。 □

现在考虑定理 2.3。与定理 1.3 的证明类似，我们将结合定理 2.1 和引理 6.1 得出该结论。

定理 *2.3* 的证明。设 $A \subseteq G$ 是一个有限非空集。我们可以假设 $|A+A| \leq |A|^{1+\delta}$，否则结论显然成立。在这种情况下，我们应用引理 6.2，得到ξ_1，……，$\xi_r \in G$，使得

$$r \leq 140(\delta \log |A| + \log 400)$$

以及满足以下条件的某个子集 $A' \subseteq A$

$$|A'| \geq \frac{|A|}{(100|A|^{\delta})^{110}} \text{ and } A' \subseteq \{n_1\xi_1 + \cdots + n_r\xi_r : n_1, \ldots, n_r \in \mathbb{Z}\}.$$

后一个条件意味着 A' 包含于一个秩为 $\leq r$ 的子群中，因此我们可以应用定理 2.1，推出

$$\begin{aligned} |\mathcal{C}(A') + \mathcal{C}(A')| &\geq c(d,2)^{-(r+1)}|A'|^2 \\ &\geq c|A|^{2-\delta(140\log c(d,2)+220)}. \end{aligned}$$

结合以下事实：$|\mathcal{C}(A) + \mathcal{C}(A)| \geq |\mathcal{C}(A') + \mathcal{C}(A')|$，即可得到所声称的估计。□

我们通过结合定理 3.7 和引理 6.6 来证明定理 2.6。

定理 *2.6* 的证明。由于 $\mathcal{V}$ 不是陪集，对于每个秩为 r的子群 Γ ，都有等式

$$\mathcal{V} \cap \Gamma = \bigcup_{i=1}^{S} (\gamma_i + H_i) \cap \Gamma,$$

其中， H_i 是连通子群，其次数由$\mathcal{V}$的次数控制； $S \leq c^{1+r}$，其中 $c = c(\deg(\mathcal{V}) \ g) > 0$ 是一个常数，见定理 3.7。

由于 $|A + A| \leq K|A|$，存在 $1 \leq d \leq C\log(400K)$，以及某个有限子集 $T \subsetneq G$，使得 $\mathrm{rk}(T) = d$且存在某个非空子集 $X \subsetneq G$，满足 $|X| \leq (100K)^{C'+1}$，并且 $A \subseteq X+T$，其中 $C = 140$, $C' = 110$，见引理 6.6。我们推得， A^g 包含于某个有限子集 T_g （其秩为 gd ）的平移集与一个基数为 $(100K)^{gC'+g}$ 的集合 X_g 之和中。令 Γ_A为由 T_g中的元素生成的群。注意， Γ_A 的秩 r 满足

$$r \leq gd \ll g\log(100K).$$

设 $x \in X_g$。由定理 3.7 可知， $\gamma \in (\mathcal{V} - x) \cap \Gamma_A$ 要么属于一个次数由 $\mathcal{V}$ 的次数控制的陪集，要么属于一个基数为 c^{1+r} 的集合。对于固定的 x ，陪集的数量由 c^{1+gr} 控制，因此将引理 4.4 应用于包含在 $\mathcal{V}$ 中的每个陪集，即可得到所需的界。□

Appendix A. Diophantine equations

我们证明，与 Bremner 猜想相关的结果对莫德尔–朗猜想具有一些推论。粗略地说，David–Philippon 定理和 Evertse– Schmidt–Schlickewei 定理对簇上落在有限生成群中的点的数量给出了非常一致的界。然而，它们通常无法为这些点的高度提供有效界。对于椭圆曲线而言，情况在很大程度上甚至更为严峻。坐标属于某个数域的椭圆曲线上的点构成一个有限生成群，但目前尚无确定其生成元的算法。从数量估计转到莫德尔–朗猜想的（部分）有效版本是直接的。例如，对于给定的曲线 C ，若有界 t 给出了有理点 $C(K)$ 的数量（其中 K 为某个数域），我们很容易说明， $C^{t+1}(K)$ 上的有理点位于由令某些坐标彼此相等而得到的真子簇的有限并中。然而，这与实际确定 $C^{t+1}(K)$ 的扎里斯基闭包仍相距甚远。我们的工作并未一般性地解决这一问题，但固定一个数域 K，并允许椭圆曲线的幂具有很高的

维数，我们可以构造出大族曲面，并确定其有理点的扎里斯基闭包。下文中，我们令 E 为魏尔斯特拉斯形式下由下式给出的椭圆曲线

$$y^2 = x^3 + ax + b,$$

其中 a，$b \in K$，K 是一个数域。设 r 为 $E(K)$ 的秩。当且仅当元组 $(a_1, a_2, \ldots, a_t)$ 是 $\mathbb{A}^t$ 中由方程定义的平面 P 上的一个点时，它构成一个等差数列

$$Z_{j+2} - 2Z_{j+1} + Z_j = 0. \tag{A.1}$$

对于 $j \in \{1, \ldots, t-2\}$。

现在考虑由方程定义的 $(\mathbb{A}^2)^t \times \mathbb{A}^t$ 的子簇

$$Y_j^2 - X_j^3 - aX_j - b = 0$$

对于 $j \in \{1, \ldots, t\}$ 和

$$Z_{j+2} - 2Z_{j+1} + Z_j = 0$$

对于 $j \in \{1, \ldots, t-2\}$。这样的簇不过是 t 个仿射椭圆曲线副本的乘积 $U^t \times P$

$$U : y^2 = x^3 + ax + b$$

与平面 P 相交，因此维数为 $t+2$。该簇上的点对应于椭圆曲线上的 t 元组点和 t 项等差数列，两者之间没有任何关系。

最后，我们施加代数关系

$$P_i(X_i, Y_i, Z_i) = 0, \quad i = 1, \ldots, t$$

使椭圆曲线上的点与等差数列的各项满足关系。因此，我们还要求 $P_i \notin K[X_i, Y_i] \cup K[Z_i]$ 不可约，从而使它们诱导出一个对应。例如，可以取

$$P_i(X_i, Y_i, Z_i) = X_i - Z_i^2, \quad i = 1, \ldots, t,$$

这编码了这样的条件：U 上各点的 x 坐标应为某个等差数列中各项的平方。这些新关系 P_i 各使维数减少一，因为它们只涉及变量 (X_i, Y_i, Z_i)。因此，由 t 个新关系定义的 $U^t \times P$ 子簇是一个曲面 S_A。类似的构造也适用于二次方程

$$Z_{j+1}Z_1 = Z_jZ_2, \quad j = 2, \ldots, t-1. \tag{A.2}$$

我们得到一个簇 $U^t \times Q$，施加由 P_i 给出的代数条件后，得到一个曲面 S_G。我们将由附加方程 $Z_1 = Z_2$ 给出的子簇记为 $D \subsetneq S_A$，S_B。因此，D 上的点对应于退化的等差数列或等比数列。

这多少有些技术性，但对于 $P_i = Z_i - X_i$ 有理点 $S_A(K)$ 对应于 $E(K)$ 中长度为 t 的等差数列；同理，$S_G(K)$ 对应于等比数列。不难看出（我们将在下一段给出详细说明），这些曲面 S_A，S_B 因此是一般型。莫德尔–朗猜想预言，$S_A(K)$ $S_B(K)$ 的扎里斯基闭包由有限个椭圆曲线和点组成。

这意味着椭圆曲线上长度为 3 的等差数列或等比数列只有有限多个。

在此设定下，推论 2.2 给出了一个更为精确的版本，它恰好预测了有理点的分布，尽管这是针对依赖于 K 的 t。

定理 A.1. 对每个 d、$r \geq 0$，存在可有效计算的 t，使得$S_A(K) = S_B(K) = D(K)$。

簇 D 要么是空集，要么是椭圆曲线 E 的副本的有限并。我们可将 $\mathbb{A}^{3t}$ 嵌入 $\mathbb{P}^{3t}$，经由

$$(X_1, Y_1 \ldots, X_t, Y_t, Z_1, \ldots, Z_t) \hookrightarrow [X_1, Y_1, \ldots, X_t, Y_t, Z_1, \ldots, Z_t, 1]$$

并且 S_A 的扎里斯基闭包 $\overline{S_A}$ 是一个射影曲面。设 $d_1, \ldots, d_t$ 为次数$P_1, \ldots, P_t$，并且若 S_A 是光滑的，则 S_A 的典范类的次数为

$$d_1 + \cdots + d_t + t - 3,$$

参见 [25, 例 5.1.1]。因此，S_A 是一般型。类似的论证也适用于 S_G。

Appendix B. Degenerate polynomials

设 G，$\mathcal{B}$，π，π_2如定义 1.7 所述。我们称 $P \in \mathbb{C}[x_1, \ldots, x_g]$ 相对于 $\mathbb{G}^g$ 是退化的，当且仅当由方程 $P(x_1, \ldots, x_g) = t$ 定义的簇 $\mathcal{V} \subseteq \mathbb{G}_a^g \times \mathcal{B}$ 是退化的。本节简要讨论几种可能的方法，用于检验给定的多项式 $P \in \mathbb{C}[x_1, \ldots, x_g]$ 在 $G = \mathbb{G}_a$ 或 $G = \mathbb{G}_m$时是否相对于 G^g 退化。对于后一种情况，第二作者 [34]证明了多项式

$$\sum_{\boldsymbol{\alpha} \in E} c_{\boldsymbol{\alpha}} x_1^{\alpha_1} \ldots x_g^{\alpha_g},$$

其中 $E \subseteq \mathbb{C}^g$ 是有限非空集，且对所有 $\boldsymbol{\alpha} \in E$，$c_{\boldsymbol{\alpha}} \neq 0$，当且仅当 $\{\sum_{\boldsymbol{\alpha} \in E} z_{\boldsymbol{\alpha}} \cdot \boldsymbol{\alpha} : \ z_{\boldsymbol{\alpha}} \in \mathbb{C}\} = \mathbb{C}^g$ 时，$E \subseteq \mathbb{C}^g$ 是非退化的。

现在我们将给出一个判据，用于检验多项式 $P \in \mathbb{C}[x_1, \ldots, x_g]$ 是否关于 $\mathbb{G}_a^g$非退化。

引理 B.1. 如果 $P \in \mathbb{C}[x_1, \ldots, x_g]$ 关于 $\mathbb{G}_a^g$退化，那么存在非零的 $\boldsymbol{v} \in \mathbb{C}^g$，使得恒等式

$$\boldsymbol{v} \cdot ((\nabla P)(x_1, \ldots, x_g)) = 0$$

成立。

证明。设 $\mathcal{V}$ 由簇 $P(\boldsymbol{x}) = t$给出，其中，按照记号滥用的惯例，我们记$\boldsymbol{x} = (x_1, \ldots, x_g)$。由于 $G = \mathbb{G}_a$且 $\mathcal{V}$退化，可以推得

$$P(\boldsymbol{x}) = F(L_1, \ldots, L_k)$$

对于某个 $0 \leq k < g$以及某些线性形式 $L_1, \ldots, L_k \in \mathbb{C}[x_1, \ldots, x_g]$和某个 $F \in \mathbb{C}[y_1, \ldots, y_k]$。由于 $k < g$，存在某个非零的 $\boldsymbol{v} = (v_1, \ldots, v_g) \in \mathbb{C}^g$，使得恒等式

$$L_i(\boldsymbol{x}) = L_i(\boldsymbol{x} + t \cdot \boldsymbol{v})$$

对所有 $1 \leq i \leq k$ 和所有 $t \in \mathbb{R}$ 均成立。这里 $t \cdot \boldsymbol{v} = (tv_1, \ldots, tv_g)$。特别地，我们得到单位元

$$P(\boldsymbol{x}) = P(\boldsymbol{x} + t \cdot \boldsymbol{v}).$$

对 t 求导，得到

$$0 = \sum_{j=1}^{k} \left(\frac{\partial F}{\partial y_j} \right) (L_1(\boldsymbol{x} + t \cdot \boldsymbol{v}), \ldots, L_k(\boldsymbol{x} + t \cdot \boldsymbol{v})) \cdot \sum_{l=1}^{g} \left(\frac{\partial L_j}{\partial x_l} \right) (\boldsymbol{x} + t \cdot \boldsymbol{v}) \cdot v_l$$

对所有 $t \in \mathbb{R}$。令 $t = 0$ 并重新排列求和后，我们得到

$$0 = \sum_{l=1}^{g} v_l \left(\sum_{j=1}^{k} \left(\frac{\partial F}{\partial y_j} \right) (L_1(\boldsymbol{x}), \ldots, L_k(\boldsymbol{x})) \cdot \left(\frac{\partial L_j}{\partial x_l} \right) (\boldsymbol{x}) \right) = \boldsymbol{v} \cdot ((\nabla P)(\boldsymbol{x})). \qquad \square$$

我们将用此证明多项式 $P(x,\ y,\ z) = xy + yz + zx$ 关于 $\mathbb{G}_a^3$是非退化的。事实上，若 P 关于 $\mathbb{G}_a^3$是退化的，那么由引理 B.1可知，存在某个非零的 $\boldsymbol{v} = (v_1,\ v_2,\ v_3) \in \mathbb{C}^3$ 使得恒等式

$$\boldsymbol{v} \cdot ((\nabla P)(x, y, z)) = v_1(y + z) + v_2(x + y) + v_3(z + x) = 0$$

成立。特别地，这意味着

$$v_1 + v_2 = v_2 + v_3 = v_3 + v_1 = 0,$$

也就是说，$v_1 = v_2 = v_3 = 0$。这与 $\boldsymbol{v}$ 非零的假设矛盾，因此，P必定关于 $\mathbb{G}_a^3$是非退化的。

References

1. Martin Bays 和 Emmanuel Breuillard，源自 Elekes-Szab{o} 问题的射影几何，比萨高等师范学校科学年刊，第4辑，第54卷（2021年），第3期，627–681页。MR 4311096 2. E. Bombieri 和 U. Zannier，阿贝尔簇子簇上代数点的高度，比萨高等师范学校科学年刊，第4辑，第23卷（1996年），第4期，779–792页（英文）。3. Jean Bourgain 和 Mei-Chu 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年），第2期，473–497页。MR 2051619 4. A. Bremner、J. H. Silverman 和 N. Tzanakis，$y^2 = x(x^2 - n^2)$ 上等差数列中的整点，数论杂志80（2000年），第2期，187–208页（英文）。5. Andrew Bremner，关于椭圆曲线上的等差数列，实验数学8（1999年），第4期，409–413页。MR 1737236 6. Andrew Bremner 和 Maciej Ulas，某些超椭圆曲线上的等比数列中的有理点，德布勒森数学出版物82（2013年），第3–4期，669–683页（英文）。7. Mei-Chu Chang，多项式 Freiman-Ruzsa 猜想的一些推论，巴黎科学院数学报告347（2009），第11–12期，583–588页。MR 2532910 8. Artem Chernikov、Ya'acov Peterzil 和 Sergei Starchenko，稳定与 o-极小超图的模型论 Elekes-Szab{o} 定理，杜克数学杂志173（2024年），第3期，419–512页。MR 4729440 9. Artem Chernikov 和 Sergei Starchenko，强极小情形下的模型论 Elekes-Szab{o} 定理，数学逻辑杂志21（2021年），第2期，论文编号2150004，20页。MR 4290493 10. Adam Cushman，关于和积问题与凸和集问题的一则注记，arXiv:2512.13849。11. Sinnou David 和 Patrice Philippon，椭圆曲线幂的子簇的规范化高度下界，国际数学研究论文 IMRP（2007年），第3期，文章编号rpm006，113页。MR 2355454 12. Gy¨orgy Elekes，关于和与积的数量，算术学报81（1997年），第4期，365–367页。MR 1472816 13. Gy¨orgy Elekes 和 Lajos R´onyai，关于多项式与有理函数的一个组合问题，J. Combin. Theory Ser. A 89（2000年），第1期，1–20页。MR 1736139 14. Gy¨orgy Elekes 和 Endre Szab´o，如何找到群？（以及如何在 Erd ¨os 几何中使用它们？），组合数学32（2012年），第5期，537–571页。MR 3004808 15. N. D. Elkies 和 Z. Klagsbrun，$\mathbb{Z}^{29}$ in $E(\mathbb{Q})$，数论邮件列表服务器档案，2024年。

16. Noam D. Elkies 和 Zev Klagsbrun，具有有理挠的椭圆曲线的新秩记录，ANTS XIV：第十四届算法数论研讨会论文集，新西兰奥克兰，线上会议，2020年6月29日至7月4日，加利福尼亚州伯克利：Mathematical Sciences Publishers（MSP），2020年，第233–250页（英文）。17. Paul Erd˝os 和 E. Szemer´edi，关于整数的和与积，《纯数学研究》，P. Tur´an 纪念文集，213–218页（1983）。1983年。18. J.-H. Evertse、H. P. Schlickewei 和 W. M. Schmidt，位于乘法群中的变量所满足的线性方程，数学年刊，第2辑，第155卷（2002年），第3期，807–836页（英文）。19. G. Faltings，数域上阿贝尔簇的有限性定理，Invent. Math. 73（1983年），第3期，349–366页。MR 718935 20. William Fulton，交理论，第2版，第2卷，数学与其边缘领域，第3辑，柏林：Springer，1998年（英文）。21. Natalia Garcia-Fritz 和 Hector Pasten，具有长等差数列的椭圆曲线具有较大秩，国际数学研究论文集 IMRN（2021年），第10期，7394–7432页。MR 4259152 22. W. T. Gowers、Ben Green、Freddie Manners 和 Terence Tao，关于 Marton 的一个猜想，数学年刊，第2辑，第201卷（2025年），第2期，515–549页。MR 4880432´ ´23. A. Grothendieck，《代数几何要素IV：概形与概形态射的局部研究》（第四部分）。与 J. Dieudonné 合作撰写，法国高等科学研究院数学出版物32（1967年），1–361页（法文）。24. Brandon Hanson、Oliver Roche-Newton 和 Dmitrii Zhelezov，关于带平移的迭代积集，II，《代数与数论》14（2020年），第8期，2239–2260页。MR 4172707 25. Marc Hindry 和 Joseph H. Silverman，《丢番图几何：导论》，数学研究生教材，第201卷，纽约州纽约：Springer，2000年（英文）。26. Yifan Jing、Souktik Roy 和 Chieu-Minh Tran，半代数方法与广义和积现象，离散分析（2022年），论文编号18，23页。MR 4527758 27. Gareth Jones 和 Harry Schmidt，Weierstrass 椭圆函数的 Pfaff 定义，《数学年鉴》 379 （ 2021 年），第 1–2 期，825–864页。MR 4211105 28. Mohamed Kamel 和 Mohammad Sadek，四次椭圆曲线上的连续平方数序列，Funct. Approximatio, Comment. Math. 60（2019年），第2期，245–252页（英文）。29. Michel Laurent，指数型丢番图方程，Invent. Math. 78（1984年），第2期，299–327页。MR 767195 30. John M. Lee，《光滑流形导论》，第2次修订版，数学研究生教材，第218卷，纽约州纽约：Springer，2013年（英文）。31. D. W. Masser 和 G. W¨ustholz，椭圆曲线上的同源估计，Invent. Math. 100（1990年），第1期，1–24页（英文）。32. J. S. Milne，《代数群：域上有限型群概形理论》，剑桥高等数学研究，第170卷，剑桥：剑桥大学出版社，2017年（英文）。33. Akshat Mudgal，关于任意矩阵集中的交换对，arXiv:2411.10404。34. ，关于少积集的集合的 Elekes-R´onyai 定理，国际数学研究论文集 IMRN（2024年），第13期，10410–10424页。MR 4770374 35. ，多项式与积的无界扩张，《数学年鉴》390（2024年），第1期，381–415页。MR 4800917 36. D¨om¨ot¨or P´alv¨olgyi 和 Dmitrii Zhelezov，查询复杂度与多项式 Freiman-Ruzsa 猜想，Adv. Math. 392（2021年），论文编号108043，18页。MR 4319771 37. Orit E. Raz、Micha Sharir 和 Frank De Zeeuw，笛卡尔积上消失的多项式：重新审视 Elekes-Szab{o} 定理，杜克数学杂志165（2016年），第18期，3517–3566页。MR 3577370 38. Orit E. Raz、Micha Sharir 和 J´ozsef Solymosi，网格上消失的多项式：重新审视 Elekes-R´onyai 问题，美国数学杂志138（2016年），第4期，1029–1065页。MR 3538150 39. Igor R. Shafarevich，《基本代数几何1：射影空间中的簇》，由 Miles Reid 从俄文翻译，第3版，柏林：Springer，2013年（英文）。40. Joseph H. Silverman，《椭圆曲线算术》，第2版，数学研究生教材，第106卷，纽约州纽约：Springer，2009年（英文）。

41. J´ozsef Solymosi，通过和集界定乘法能量，Adv. Math.**222** （2009），第 2 期，402–408。MR 2538014 42. Jozsef Solymosi 和 Joshua Zahl，利用邻近性改进的 *Elekes-Szab´o* 类型估计，J. Combin. Theory Ser. A **2024年**，论文编号 105813，9 页。MR 4638826

Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL,United Kingdom电子邮箱: joseph.s.harrison@warwick.ac.uk电子邮箱: Akshat.Mudgal@warwick.ac.uk电子邮箱: Harry.Schmidt@warwick.ac.uk