arXiv:2512.15125v1 [math.CO] 17 Dec 2025

近似群中的阿贝尔结构与阿隆关于拉姆齐凯莱图的猜想

CARL SCHILDKRAUT

Abstract. Pyber 的一项结果指出，每个有限群 G 都包含一个阿贝尔子群，其阶在 $|G|$意义下具有准多项式规模。我们证明，在对 K仅施加适度限制的条件下，可解群的 K-近似子群也有类似结果。我们证明，若 A 是包含于某个可解群中的有限K-近似群，则存在某个阿贝尔群与 A^4相交，且交集中至少有 $\exp(\Omega(\log^{1/6}|A|/\log\ 2K))$ 个元素。对于不含大型交错子商的有限群中的近似子群，我们也证明了类似结果。此外，对于线性群中的近似子群，我们还得到了多项式界（而非准多项式界），适用于同一命题。

我们给出两个应用。首先，我们考察 Alon 的猜想：每个有限群G 都存在一个凯莱图，其团数和独立数均为 $O(\log|G|)$。Conlon、Fox、Pham 和 Yepremyan 最近证明，对于几乎所有正整数 N，阶为 N 的每个阿贝尔群都满足阿隆猜想。在他们结果的基础上，我们验证了几乎所有阶的群（不一定是阿贝尔群）都满足阿隆猜想。其次，借助 Kelley 和 Meka 关于 Roth 定理的最新突破，以及 Jaber、Liu、Lovett、Ostuni 和 Sawhney 关于角问题的最新突破，我们在（许多）非阿贝尔情形下，以准多项式界证明了 Roth 定理的一个“局部”版本。

1. Introduction

加性组合学中的许多问题都可以在非阿贝尔情形下提出，而在这种情形下，阿贝尔世界中的若干工具无法使用。当存在较小的阿贝尔结构时，考察这些结构往往能推动此类情形下的研究。最简单的一类论证是将一个群划分为某个阿贝尔子群的陪集，并在每个陪集中进行研究。这一由 Bergelson、McCutcheon 和 Zhang 提出的方法 [BMZ97, 推论 6.4], 已应用于算术组合学中的许多问题，包括 Roth 定理的非阿贝尔版本 [BMZ97, Sol13, San17] 和角问题 [Aus16, JLL$^+$25]，以及 Brown– Erd˝os–S´os 猜想 [Sol15, SW20, Lon20, NST20, Won20]。

要应用这类论证，需要在群中找到较大的阿贝尔子群。在一般（有限）群的情形下，可以借助 Pyber 的以下结果做到这一点。

定理 1.1 ([Pyb97，定理 1.1])。 存在一个绝对常数 $c > 0$，使得每个有限群 G 都含有一个阶至少为 $e^{c\sqrt{\log|G|}}$的阿贝尔子群。

在阿贝尔群的陪集中进行研究的策略，最适用于所关注的集合在环境群中较为稠密的情况。然而，我们往往需要理解有限群的稀疏子集，或无限群的子集的乘法结构。从非阿贝尔算术组合学的角度来看，尤其重要的是考察满足 A小三重积的集合，即乘积集 $A^3 := \{a_1a_2a_3 : a_1,\ a_2,\ a_3 \in A\}$ 本身不会大得太多的集合。（这类集合与研究已久的近似群密切相关。）关于这一概念的由来，以及研究这类集合在非阿贝尔情形中的诸多应用，读者可参阅 [Toi20，Shk21] 。

为此，我们的主要结果是将定理 1.1 推广到小三重积集（例如近似群）的以下两个结论。若集合 A 满足：当 $x \in A$时， $x^{-1} \in A$，则称其为对称。

Date: 2025年12月18日。

定理 1.2. 存在一个绝对常数 $c > 0$，使得以下结论成立。设 G是一个（不一定有限的）可解群，且 $A \subset G$ 是满足 $|A^3| \leq K|A|$ 的有限对称子集。那么存在某个交换集 $T \subset A^4$，满足

$$|T| \geq \exp\left(c\frac{\log^{1/6}|A|}{\log 2K}\right).$$

定理 1.3。存在绝对常数 $C, c > 0$，使得以下结论成立。设 G 是一个有限群，d 是一个正整数。假设 G 没有同构于交错群 交错群$_d$的子商。设 $A \subset G$ 是满足 $|A^3| \leq K|A|$的有限对称子集。那么存在某个交换集 $T \subset A^4$ 满足

$$|T| \geq \exp\left(\frac{c\log^{1/8}|A|}{\exp\big(C\log^2 d\log(1+\log d)\big)\cdot\log 2K}\right).$$

与定理 1.1 一样，定理 1.3 的证明依赖于有限单群分类。我们将有限单群分类的一个特定推论陈述为引理 2.7。

定理 1.2 和 1.3 可视为将定理 1.1 从群的情形推广到“近群”的情形。[2] 在结构最完善的情形下，即 $K = O(1)$（并且在定理 1.3 中，$d = O(1)$ 也成立），这两个结果还给出了交换子集在 $|A|$中的大小 $|T|$ 的准多项式依赖，尽管指数不同。从这个意义上说，定理 1.2 和 1.3 在定性上是最优的：由于定理 1.1 即使在可解情形 [Ol'78, BGH87], 下也是紧的，因此，即使 A 是真正的可解群，也不一定能找到一个大小超过关于 $|A|$ 的准多项式的交换集。

为展示定理 1.2 和 1.3 的用途，我们给出它们在非阿贝尔算术组合学中的两个应用。第一个应用也是本研究的主要动机：我们将解决阿隆关于拉姆齐凯莱图存在性的猜想在大多数情形下（从某种意义上说）。阿隆 [Alo95, Alo02]猜想，存在某个绝对常数 C，使得每个有限群 G都存在一个凯莱图，其中团或独立集的大小均不超过 $C\log|G|$；我们证实了这一点（见推论 1.8），适用于阶数几乎所有的群。我们的工作建立在 Conlon、Fox、Pham 和 Yepremyan [CFPY24]近期工作的基础上并将其推广：我们在保持相近定量强度的同时，从他们的许多结果中去除了阿贝尔条件。第二个应用是在许多非阿贝尔群中给出 Roth 定理的局部版本，其中包括不存在建模引理、因而无法将群的小子集转化为其他群的稠密子集的情形（见 [Gre08, HH12]）。例如，我们证明（见推论 1.11），在奇数阶群中，不含非平凡三项等差数列的集合至少具有准多项式倍增。这加强了 Freiman [Fre73] 在整数情形下的一个结果。

1.1. 应用：Ramsey 凯莱图。

Erd˝os 和塞凯赖什 [ES35],强化拉姆齐定理的一项经典结果指出，任何有 n 个顶点的图都必定包含一个团或一个独立集，其大小至少为 $\frac{1}{2}\log_2 n$。受此启发，如果一个有 n 个顶点的图不含大小超过 $C\log_2 n$ 的团或独立集，就称其为 C-拉姆齐图，其中 $C > 1/2$。Erd˝os [Erd47]证明，几乎所有图都是 2-拉姆齐图。然而，对于任何常数 C，目前都没有已知的 C-拉姆齐图的显式构造。

一类可用于寻找 C-拉姆齐图的图是凯莱图，它们是由有限群构造出的图。给定一个群 G 和一个对称子集 $S \subset G$，我们用 Cay(G, S) 表示顶点集为 G、边集为 $\{(x, y) : x^{-1}y \in S\}$ 的图。凯莱图为拉姆齐理论中的下界实例提供了丰富来源。基于凯莱图具有良好的拉姆齐理论性质这一想法，并受到其在编码理论中应用的启发，阿隆提出了以下猜想。

[1]交错群 *subquotient* 之 G 是 G的一个子群的商群。[2]定理 1.2 和 1.3 的结论中出现指数 4，不必为此担心。如果 A 具有小三重积，那么 A^4 不会比 A 本身大多少；我们稍后将看到（见引理 9.1），通过这两个定理得到的交换集 T 与 A 之间的关系足够密切，能够满足我们的需求。

猜想 1.4 （[Alo95], [Alo02, 猜想 4。1]）。存在某个绝对常数 $C > 0$，使得每个有限群都有一个 C-拉姆齐凯莱图。

关于猜想 1.4，阿隆和奥利茨基 [AO95] 证明，每个阶为 n 的群都有一个团数和独立数均为 $O(\log^2 n)$ 的凯莱图。最近，Conlon、Fox、Pham 和 Yepremyan [CFPY24] 将这一结果改进为 $O(\log\ n\log\log\ n)$。

若将讨论范围限定于特殊群类，还可以得到更多结论。最早的这类结果由 Green [Gre05], 给出，他证明了猜想 1.4 对循环群成立。Conlon、Fox、Pham 和 Yepremyan 证明了阿隆猜想对一个范围大得多的群族成立。他们沿此思路得到的最一般结果如下。

定理 1.5 ([CFPY24，定理 4。6])。存在一个绝对常数 $C > 0$，使得以下结论成立：若 G 是一个阶为 N 的群，且有一个阿贝尔子群 H，其阶 ***(i)*** 至少为$N/(\log\ N)^{1/1000}$，并且 ***(ii)*** 与 6互素，那么 G 有一个 C-拉姆齐凯莱图。

虽然定理 1.5 以相当广泛的普遍性涵盖了阿贝尔群，但大多数非阿贝尔群（即使其阶与 6 互素）也没有足够大的阿贝尔子群，因而无法应用定理 1.5。针对猜想 1.4，我们的主要结果是将定理 1.5 扩展到完全非阿贝尔情形，具体如下。

定理 1.6. 设 N 是一个充分大的正整数，并假设 N 的由2 和3 的幂相乘得到的最大因子至多为 $\exp(\exp((\log\log\log\ N)^{1/3})))$。那么，每个阶为 N 的群 G 都有一个24000-***Ramsey*** 凯莱图。

我们指出定理 1.6 的以下两个推论，其中第二个通过去掉阿贝尔条件，推广了[CFPY24，推论 1.11] 。

推论 1.7. 猜想 *1.4* 对阶与6互素的群族成立。

推论 1.8。对于几乎所有[3] 整数 N，每个阶为 N 的群都有一个 24000-拉姆齐凯莱图。

现在我们简要谈谈我们的证明与 [CFPY24] 工作的不同之处。[CFPY24] 中给出的构造是随机的，但并非均匀随机。作者从一个精心构造的概率分布中选取凯莱图 $\Gamma := \mathrm{Cay}(G, S)$，使得 (1) 若 $|AA^{-1}|$ 相对于 $|A|$ 足够大，则 Γ 包含 A 作为团或独立集的可能性不高；(2) 若 $|AA^{-1}|$ 相对于 $|A|$ 足够小，则 Γ 确定性地 不可能将 A 作为团或独立集。只有第 (2) 部分在他们的工作中用到了阿贝尔性假设。在他们的构造中，可能构成团或独立集的集合会避开模式[4]$xy^{-1} = (zw^{-1})^2$的非平凡实例。在阿贝尔情形（以加法记号书写）下，这个方程变为 $x + 2w = y + 2z$，并且可以利用 Pl¨unnecke–Ruzsa 不等式和鸽巢原理找到解。在非阿贝尔情形下，用于将 $xy^{-1} = (zw^{-1})^2$ 化简为这种模式的操作并不成立。

我们在定理 1.6 中构造凯莱图的方法，是 [CFPY24] 中方法的自然非阿贝尔类比（特别是，它也是一种随机化构造）。利用定理 1.2 和 1.3，只需将重点限制在满足 $xy^{-1} = (zw^{-1})^2$ 的解上，其中 $\{x, y, z, w\}$ 全部位于某个阿贝尔子群的陪集中，我们便能得到他们第 (2) 部分的一个（略弱的）版本。在这样的陪集中，[CFPY24] 中的论证适用，因此很容易找到相关模式。

通过进一步推进我们的论证，我们得以得到定理 1.6 的如下加强版，从而精确确定哪些子群构成寻找拉姆齐凯莱图的障碍。

---

[3]这里“几乎所有”是指具有自然密度的意义。[4]为了便于阐述，我们稍微简化了情形；实际的模式是 $x_1y_1^{-1} = (x_2y_2^{-1})^2 = (x_3y_3^{-1})^4 = (x_4y_4^{-1})^8$。模式 $xy^{-1} = (zw^{-1})^2$ 满足许多与这里更复杂的模式相同的性质，因此可以将问题化简为研究诸如 $(\mathbb{Z}/5\mathbb{Z})^n$ 这样的模型情形中的这个较简单模式。

定理 1.9。 对所有充分大的 N，以下结论均成立。设 G 是一个阶为 N 的群，且 $r = \lfloor$指数函数$((\log\log\log N)^{1/3})\rfloor$。假设 G 既不含有

- 一个与 $(\mathbb{Z}/2\mathbb{Z})^r$ 或 $(\mathbb{Z}/3\mathbb{Z})^r$同构的子群，也不是
- 一个与 $\mathbb{Z}/L\mathbb{Z}$同构的子群，其中

$$L = \operatorname{lcm}\Big(1, 2, \dots, \Big\lfloor \exp\Big((\log\log N)^{1/27}\Big)\Big\rfloor\Big).$$

那么 G有一个24000-拉姆齐 *Cayley* 图 h.

1.2. **应用：无3项等差数列集合的增长**。Freiman 在其关于集合加法的专著中 [Fre73, Theorem 2.30] 给出了 Roth 关于三项等差数列的著名定理的以下推广：若 $A \subset \mathbb{Z}$ 不含非平凡的三项等差数列，则当 $|A|$ 增长时，$|A+A|/|A|$ 必定无界增长。Ruzsa [Ruz92] 将 Freiman 的结果加强为显式渐近式 $|A + A| \geq c|A|(\log|A|)^c$，其中 $c > 0$为某个常数。利用 Kelley 和 Meka 的最新突破 [KM 23],，这个结果可加强为如下结论：$|A+A|/|A|$ 至少以准多项式速度相对于$|A|$增长。（Schoen [Sch25], 曾指出这一点；他还将 Ruzsa 的结果推广到了更长等差数列的情形。）这一结论在受限和集的研究中有应用 [Sch02, HHP03],，也应用于离散几何中的各种问题 [Pac03, PW10, Dum19]。

将三项等差数列推广到非阿贝尔群，有两种不同的方式。第一种是模式 $\{x, xt, xt^2\}$，我们称之为平移型三项等差数列；第二种是方程 $xz = y^2$ 的一个解，我们称之为平均三项等差数列。平移型三项等差数列在左平移下保持不变，因此通常更容易处理。具体来说，“在阿贝尔群的陪集中进行研究”这一策略，会将平移型三项等差数列问题归结为在阿贝尔群中寻找三项等差数列（见[San17，定理 1.4], ，此处该观察归功于 Croot）；而对于平均三项等差数列问题，该策略则会将其归结为在阿贝尔群中寻找角形（见 [JLL+25，推论 1.6], ，此处该观察归功于 Fox）。相反，从多项式方法的角度来看，Petrov 的论证 [Pet24]表明，在有界指数的群中，平均三项等差数列或许更为自然。

作为定理 1.2 和 1.3 的第二个应用，我们将 Freiman 的结果推广到非阿贝尔群，得到准多项式界。

定理 1.10。 存在一个绝对常数 $c > 0$，使得以下结论成立。设 G 为一个群，且 $A \subset G$ 为一个不含非平凡平移三项等差数列的集合，即若 x、xy、$xy^2 \in A$，则 $y = 1$。[5] 假设以下任一条件成立：

(a) G 是可解群，或
(b) G 是一个不含 $(\mathbb{Z}/2\mathbb{Z})^d$ 作为子群的有限群，其中 $d = \Big\lfloor$指数函数$\Big(c\sqrt{\text{对数 对数}|A|\text{ 对数 }\underline{\text{对数 对数}|A|}}\Big)\Big\rfloor$。

Then

$$\frac{|AA^{-1}|}{|A|} \geq \exp\Big(c(\log|A|)^{1/1305}\Big).$$

如果 A 反而避免平均三项等差数列，即满足 $xz = y^2$ 且 $x \neq y$ 的解，那么在 G 满足相同条件的情况下，我们得到

$$\frac{|A^2|}{|A|} \geq \exp\Big(c(\log|A|)^{1/64809}\Big).$$

与阿贝尔情形不同，我们的论证并非直接通过在某个所在有限群中找到一个稠密的 A Freiman 同构副本来进行。事实上，对于小倍增的非阿贝尔集合，一般而言并不存在这样的“稠密模型”；参见 [Gre08，定理 1.2] 以及 [HH12，定理 1]。相反，我们首先运用定理 1.2 和 1.3，将问题化约为 A 的一个子集，该子集位于一个

[5]关于可能含有 2-挠的群中“三项等差数列”之“非平凡”定义，文献中的说法并不一致。遵循 [San17] （但例如不遵循 [Sol13], ）的做法，我们采取一种最小化的方法：只要一个等差数列中的元素不全相等，就将其归类为非平凡。特别地，在我们对“非平凡”平移型三项等差数列的定义中，我们允许 $xy^2 = x$ x, xy, xy^2。

阿贝尔群的陪集（或者在平均情形下，位于一个阿贝尔群的双陪集）中，然后借助阿贝尔领域中的结果，而这些结果确实需要建模引理。

我们指出，平移情形下的结论在定性意义上（而不仅仅是定量意义上）强于平均情形下的结论：由 Ruzsa 三角不等式，$|AA^{-1}|/|A|$ 的下界蕴含 $|A^2|/|A|$的下界，但反之则不成立。平移情形下，我们能够给出 $|AA^{-1}|$ 的下界，但平均情形下则不能，原因恰恰在于平移三项等差数列在左平移下保持不变。无论如何，Ruzsa 三角不等式给出了以下有趣的推论。

推论 1.11. 存在一个绝对常数 c，使得以下结论成立。设 G 是一个奇数阶有限群，[6] 且设 $A \subset G$。假设 A 不包含平移型3项等差数列，或者A 不包含平均3项等差数列。

$$\frac{|A^2|}{|A|} \geq \exp\Big(c(\log|A|)^{1/64809}\Big).$$

在证明定理 1.10 中平移型三项等差数列部分时，我们采用了上述 Kelley 和 Meka 在阿贝尔情形下的结果 [KM23] 。而在平均三项等差数列部分，我们采用了 Jaber、Liu、Lovett、Ostuni 和 Sawhney [JLL+25]近期对角问题作出的重大改进。

1.3. **矩阵群的近似子群**。 在证明定理 1.3 时，我们的大部分工作将在环境群 G 的合成列中进行。因此，我们需要运用有限单群分类，这使我们能够将许多问题归结为关于具有小倍增的线性群子集的问题。这类子集的结构已得到相当深入的研究，尤其是在求群上凯莱图的直径界这一背景下。我们关于线性群的工作虽借鉴了研究此类问题的方法，但完全是自成一体的。

我们关于线性群的主要结果如下，它与定理 1.2 相呼应。

定理 1.12. 存在一个绝对常数 $C > 0$，使得以下结论成立。设 $\mathbb{F}$ 是任意域，$d \geq 1$ 是任意整数，且 $A \subset$ 一般线性群$_d(\mathbb{F})$ 是某个 $K \geq 1$ 的 K-近似群。设

$$M(d) := \exp\big(C \log^2 d \cdot \log(1 + \log d)\big) = e^{\log^{2+o(1)}(d)}$$

是一个准多项式 函数，定义在 d 上。那么存在某个阿贝尔子群 $H \leq$一般线性群$_d(\mathbb{F})$，使得

$$|A^2 \cap H| \geq \frac{1}{(2K)^{Cd^9}} |A^2|^{1/M(d)}.$$

定理 1.12 表述中的 $\log(1+\log d)$ 项源于以下命题，该命题本身也可能具有独立的研究价值。

命题 1.13. 设 $d \geq 8000$，$\mathbb{F}$ 是代数闭域，且 $A \subset$一般线性群$_d(\mathbb{F})$ 是一个K-近似子群。以下结论至少有一项成立：

- （不太不规则的元素）存在 a 的某个元素，其最大维数特征子空间的余维数至少为600^{d}双对数 d。
- （由良性子群控制）存在两个子空间 $V_1 \subset V_2 \subset \mathbb{F}^d$，其维数 $V_2 > \frac{9d}{10}$ 和维数 $V_1 < \frac{d}{10}$，至少有$(2K)^{-2d^6}|A^2|$个 a A^2 的元素满足以下性质：存在某个 $\lambda \in \mathbb{F}$，使得$(a-\lambda)V_2 \subset V_1$。

除了第一个条件中一个 $O(1/\log\log d)$ 因子之外，命题 1.13 已是最优的：满足（$a - \lambda$）$V_2 \subset V_1$（对某个 λ）的可逆算子 a 构成一般线性群 $\mathrm{GL}_d(\mathbb{F})$ 的一个子群，且该子群的每个元素

[6]要从定理 1.10 推出这个推论，要么需要结合费特–汤普森定理使用陈述 (a)，要么使用依赖于有限单群分类的陈述 (b)。因此，前一种方法更为初等；事实上，如果完整推导，其给出的定量界会比我们在此写出的略好。

都有维数至少为 $4d/5$ 的 λ-特征子空间。因此，“由性质良好的子群控制”这一条件确实构成了一种障碍，使得 A 无法拥有一个没有大特征子空间的元素。

现在，我们来讨论我们的工作与此前关于线性群近似子群的研究之间的关系。此处的讨论仅限于结果之间的关系；若要深入了解相关方法，请参见第5.2节。

Babai 的一个猜想 [BS92]指出，阶为N的单群上的每个连通凯莱图，其直径均为 $(\log\ N)^{O(1)}$；换言之，若 G 是一个阶为 N的单群，且 $A \subset G$ 生成G，那么对于某个 $D =$，有 $A^D = G$ $(\log\ N)^{O(1)}$。为解决这一猜想所做的大量工作，例如有界秩情形的解决 [Hel08, Hel11, BGT11, PS16] ，都着眼于各种群的“乘积定理”：大致来说，这类定理的形式是“若 $A \subset G$ 生成 A，则要么$A^3 = G$ ，要么 A^3 远大于 A。”这一结论远强于我们的需求（假设还额外满足 A生成某个性质良好的线性群），但所有这类研究中，对秩的定量依赖往往都相当糟糕。近期的定量改进 [BDH24], 以及“高秩”情形下的研究 [HS14, HMPQ19], ，证明了对非常大的迭代乘积集成立的扩张结果，而不只是形如“A^3 远大于A”的结论。尽管这些结果对直径界颇有用处，但对我们所研究的情形帮助不大。

此外，已有一些有趣的工作 [EMPS25] 致力于在线性群的近似子群分类方面取得进展（沿着 Breuillard、Green 和 Tao 的结构定理 [BGT12]的思路），且不对它们所生成的群作任何假设。我们认为， [EMPS25]的结果似乎可以推出定理 1.12 的一个弱化版本，其中允许函数 $M(d)$以任意快的速度增长。相关地，如果愿意在 A^m 而非 A^2 中寻找不太不规则的元素，其中某个 m大致为指数级，那么类似于 [BDH24 命题 6.2] 的论证可以给出命题 1.13 的一个更强版本。

在这项工作中，我们力求优化对环境线性群的秩的定量依赖。这使得我们在阿隆猜想上的应用（见定理 1.6）能够达到与 [CFPY24] 在阿贝尔情形中的应用相当的普适性。

1.4. **结构安排**。 在第2节中，我们介绍一些定义、记号和预备结果，这些内容对我们会有用。

第3节概述定理 1.2 和 1.3 的证明，其中许多细节留待第 4 节展开。

第 5 至第 8 节讨论矩阵群的近似子群；我们在此证明定理 1.12 和命题 1.13。

在第9节中，我们将结果应用于 Roth型问题，并证明定理 1.10；在第10节中，我们将结果应用于 Ramsey Cayley 图的存在性，并证明定理 1.6 和定理 1.9。定理 1.9 和 1.10 都需要阿贝尔加性组合学中的一些结果，我们会在需要时陈述这些结果，并在第 11 节中证明。对于只关注将定理 1.2 和 1.3 应用于三项等差数列或阿隆猜想的读者来说，相关内容仅见第9至第11节。

第 12 节包含一些总结性评论和猜想。最后，一些纯粹的群论结果的证明留待附录给出。

2. Preliminaries

我们将需要一些关于群的性质和相关定义（大多是标准的） .

2.1. **群与群的子集**。 对于一个群 G 和一个子集 $S \subset G$，我们用 $S \leq G$ 表示 S 是 G 的子群，用 $S \trianglelefteq G$ 表示 S 是 G的正规子群。我们用$\langle S\rangle$ 表示由 S生成的 G 的子群。 G 的子群的商群称为G的子商 。

对于群 G，我们用 1_G 表示 G 的单位元，用 $Z(G)$ 表示 G 的中心。对于子群 $H_1, H_2 \leq G$，我们用 $[H_1, H_2]$ 表示由换位子集合生成的群

$\{h_1h_2h_1^{-1}h_2^{-1}\colon\ h_1 \in H_1, h_2 \in H_2\}$。对于元素 $g \in G$，我们记

$$C_G(g) := \{h \in G : gh = hg\}$$
$$\mathrm{Conj}_G(g) := \{hgh^{-1} : h \in G\}$$

分别表示 g 在 G 中的中心化子和共轭类。对于 $S \subset G$，我们也用 $C_G(S)$ 表示交集 $\bigcap_{g\in S} C_G(g)$。在所有记号中，只要上下文清楚，我们通常省略指明群的下标。

定义 2.1（次正规列与正规列）。给定一个群 G，若子群序列 $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = \{1\}$ 中的每个子群都正规于前一个子群，则称其为**次正规列**。若每个 G_i 实际上都正规于 G，则称该列为**正规列**。无论哪种情况，我们都称相应的商群为

$$G_0/G_1, G_1/G_2, \ldots, G_{s-1}/G_s$$

该列的**连续商群**。

从一个群中可以构造出两种特别重要的列。

定义 2.2（导出列）。给定一个群 G，其**导出列** $G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots$ 定义为 $G^{(0)} = G$ 和 $G^{(i+1)} = [G^{(i)}, G^{(i)}]$。假设 G 的导出列最终稳定，并令 s 为使 $G^{(s)} = G^{(s+1)}$ 成立的最小值。若 $G^{(s)}$ 是平凡群，则称 G 是**可解的**，其**导出长度**为 s。此时，导出列是 G 的正规列。

定义 2.3（合成列）。如果一个群非平凡且没有真正规子群，则称它为**单群**。给定一个群 G，G 的**合成列**是一个次正规列 $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = \{1\}$，其中每个连续商群都是单群。单群 G_i/G_{i+1} 称为 G 的**合成因子**。

每个有限群都有合成列，有些无限群也有合成列。“合成因子”这一术语由 Jordan–H¨older 定理所证明；该定理指出，（当 G 有合成列时）群 G 的每个合成列都有相同的合成因子，且各因子的重数也相同。我们还在此指出，有限群 G 可解，当且仅当它的所有合成因子都是阿贝尔群。（注意，唯一的阿贝尔有限单群是素数 p 对应的 $\mathbb{Z}/p\mathbb{Z}$。）

如果在合成列的定义中加入条件，要求每个 G_i 都是 G 的正规子群，那么得到的就是**主列**。

定义 2.4（主列）。给定一个群 G，G 的**主列**是一个正规列 $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = \{1\}$，其中对每个 i，满足 $G_i \geq N \geq G_{i+1}$ 的 G 的正规子群 N 仅有 G_i 和 G_{i+1}。

我们将使用主列与合成列之间的以下关系。

引理 2.5（见 [Hup67，定理 I.9.12 和 I.11。7]）。每个有限群 G 都存在主列。此外，有限群 G 的任意主列 $G_0 \trianglerighteq \cdots \trianglerighteq G_s$ 中，商群 G_i/G_{i+1} 均为同构单群的直积，且其中每个单群都是 G 的合成因子。

我们还需要一些由有限单群分类推出的事实。首先给出以下非标准定义。

定义 2.6. 设 G 是一个群。G 的**合成秩**是满足以下条件的最小正整数 d：G 的每个合成因子 S 都能嵌入到某个域 $\mathbb{F}$ 上的一般线性群 $\mathrm{GL}_d(\mathbb{F})$ 中（该域可能取决于 S）。如果 G 没有合成列，或者 G 的某个合成因子无法嵌入任何一般线性群 $\mathrm{GL}_d(\mathbb{F})$，则将 G 的合成秩定义为 ∞。

例如，可解群的合成秩为 **1**，因为对于每个素数 p，$\mathbb{Z}/p\mathbb{Z}$ 嵌入一般线性群 $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$。下面的引理部分是有限单群分类的推论。从定性角度看，它表明，具有较大合成秩等价于具有作为子商的大交错群。

引理 2.7。 存在一个绝对常数 $C > 0$，使得以下结论成立。设 d 为一个正整数，G 为一个有限群。

(1) 如果 G 拥有一个同构于交错群$_d$的子商，那么 G 的合成秩至少为 $d/7 - 1$。*(2)* 如果 G 不拥有任何同构于交错群$_d$的子商，那么 G的合成秩至多为 Cd^2。

引理 2.7 的证明推迟到附录 A。对于我们的一些应用，还需要另一个纯粹的群论引理。这个引理基本上可由 Thompson 的结果（见 [Hup67，定理 III.12.3]）和 Mann [Man71，定理 B]，，以及一些将问题化归到 p-群情形的简单引理推出（这些引理在引理 2.7(1) 的证明中也很有用）。我们在附录 A 中给出推导。

引理 2.8。 设 p 为素数，d 为正整数。每个含有同构于$(\mathbb{Z}/p\mathbb{Z})^{2d^2}$ 的子商的有限群，都有一个同构于$(\mathbb{Z}/p\mathbb{Z})^d$的子群。

2.2. **算术组合学**。 现在我们介绍一些更专用于算术组合学的记号和术语。给定一个群 G 和子集 A，$B \subset G$，我们用 $AB := \{ab : a \in A,\ b \in B\}$ 表示由 A 中的一个元素与 B中的一个元素相乘所得的乘积构成的集合。对于正整数k，我们用 $A^k := \{a_1 a_2 \cdots a_k : a_1, \ldots, a_k \in A\}$ 表示 A的第 k 次迭代乘积集，并用$A^{-1} := \{a^{-1} : a \in A\}$ 表示由 A中元素的逆元构成的集合。当环境群是阿贝尔群时，我们有时会使用相应的加法记号（$A + B$、kA和 $-A$）；这种用法仅限于第 11 节。

加性组合学中的一些工具无需修改即可应用于非阿贝尔情形。其中两个工具是 Ruzsa 三角不等式和覆盖引理（例如参见 [Toi20，引理 2.3.4 和 2.4.4]）。

L引理 2.9（Ruzsa 三角不等式）。 对于任意三个有限集合 A、B、$C \subset G$，我们有 ve

$$|A||B^{-1}C| \leq |AB||AC|.$$

引理 2.10（Ruzsa 覆盖引理）。 设 A、$B \subset G$ 是有限集合。存在一个集合 $Y \subset G$，其大小至多为 $|AB|/|B|$，且满足 $A \subset YBB^{-1}$。

最后，我们需要引入无关集的概念，这对于构造定理 1.2 和 1.3 结论中所描述的集合至关重要。无关集通常只在阿贝尔群中定义；我们在任意群中的所有无关集都包含于阿贝尔子群中。

定义 2.11。 设 G 是一个群，$D = \{h_1, \ldots, h_m\} \subset G$ 是一个两两可交换子集（也就是说，D 中任意两个元素都交换；这等价于 $\langle D \rangle \leq G$ 是 G 的阿贝尔子群）。我们称 D 为无关的，如果对于任意不全为零的 ε_1、……、$\varepsilon_m \in \{-1, 0, 1\}$，有

$$h_1^{\varepsilon_1} h_2^{\varepsilon_2} \cdots h_m^{\varepsilon_m} \neq 1.$$

这等价于 2^m 子集乘积 $h_1^{\delta_1} \cdots h_m^{\delta_m}$对于 $(\delta_1, \ldots, \delta_m) \in \{0, 1\}^m$的互异性。给定一个无关集 $D = \{h_1, \ldots, h_m\}$，我们记

$$\langle D \rangle_{\pm} := \left\{ h_1^{\varepsilon_1} h_2^{\varepsilon_2} \cdots h_m^{\varepsilon_m} : (\varepsilon_1, \ldots, \varepsilon_m) \in \{-1, 0, 1\}^m \right\}.$$

2.3. **近似群**。 我们已用小三重积集陈述定理 1.2 和 1.3。这些集合与结构更丰富（且研究较为深入）的近似群密切相关。

定义 2.12. 设 $K \geq 1$ 为一个参数。群 G 的子集 A 若满足 $A = A^{-1}$，则称为对称；若还满足 $1 \in A$，则称为含单位元的。若 A 含单位元，且存在一个大小至多为 K 的子集 $X \subset G$ 使得 $A^2 \subset XA$，则称 A 为一个 K-近似群。

K-近似群的迭代乘积集具有极佳的性质。特别是，如果 A 是一个近似群，且 $k \geq j$ 是正整数，那么 $A^k \subset X^{k-j} A^j$，因此 $|A^k| \leq K^{k-j} |A^j|$。我们还需要了解一些（不一定是阿贝尔的）近似群的其他性质。以下事实出自 Tointon 的著作 [Toi20]，我们将反复用到；它指出，近似群与子群的交具有良好的性质。

引理 2.13 ([Toi20，命题 2.6 的特殊情形。5])。设 G 是一个群，且 H 是 G 的任意子群（不一定是正规子群）。若 $A \subset G$ 是任意一个 K-近似子群，则 $A^2 \cap H$ 是一个 K^3-近似群。此外，对于任意 $k \geq 2$，都有 $|A^k \cap H| \leq K^{k-1}|A^2 \cap H|$。

我们还需要 Tao 的以下结果，它指出，小的集合 $A \subset G$ （满足 AA^{-1} ）受一个性质良好的中心化集合“控制”。

引理 2.14 ([Tao08，命题 4。5])。若 $|AA^{-1}| \leq K|A|$，则存在一个中心化集合 $B \subset A^{-1}A$，满足 $|B| \geq |A|/(2K)$，且对每个正整数 n，都有 $|AB^nA^{-1}| \leq 2^nK^{2n+1}|B|$。[7]

我们需要一个依赖于以下定义的引理。给定两个群 G 和 G'、一个中心化子集 $A \subset G$ 以及一个整数 $\ell \geq 2$，中心化 Freiman ℓ-同态 ϕ: $A \to G'$ 是满足 $\phi(1_G) = 1_{G'}$ 的映射；并且，若 $x_1, \dots, x_\ell, y_1, \dots, y_\ell \in A$ 满足 $x_1 \cdots x_\ell = y_1 \cdots y_\ell$，则 $\phi(x_1) \cdots \phi(x_\ell) = \phi(y_1) \cdots \phi(y_\ell)$。我们记录该定义的两个性质：首先，任何中心化 Freiman ℓ-同态对每个 $x \in A$ 都满足 $\phi(x^{-1}) = \phi(x)^{-1}$；其次，任何群同态在限制到任意中心化集合时，都是任意 ℓ 的中心化 Freiman ℓ-同态。

下面的引理说明，以恰当的方式来看，近似群之间的 Freiman 同态的纤维彼此不会相差太大。在我们几乎所有对该引理的应用中，ϕ 都将是到 G的某个商群上的投影。

引理 2.15. 设 G是一个群，且 A 是 G中的一个 K-近似子群。设 G' 是一个群，并设 ϕ: $A^6 \to G'$ 是一个映射，其在 A^2上限制为含单位元的 *Freiman* 3-同态。那么，对每个子集 $S \subset G'$，

$$K^{-4}\frac{|A^2 \cap \phi^{-1}(S)|}{|A^2|} \leq \frac{|\phi(A^2) \cap S|}{|\phi(A^2)|} \leq \frac{|A^6 \cap \phi^{-1}(S)|}{|A^2|}.$$

证明。选取 $t \in \phi(A^2)$，使 $|A^2 \cap \phi^{-1}(t)|$最大。对每个 $s \in \phi(A^2)$，选取满足 $s = \phi(a_sb_s)$ 的元素 $a_s, b_s \in A$。对于任意这样的 s，以及任意满足 $\phi(a') = t$的 $a' \in A^2$，利用关于 ϕ的假设可得

$$\phi((a_tb_t)^{-1}a'(a_sb_s)) = \phi(a_tb_t)^{-1}\phi(a')\phi(a_sb_s) = t^{-1}ts = s.$$

我们得出，对于每个 $s \in \phi(A^2)$，

$$|A^6 \cap \phi^{-1}(s)| \geq |(a_tb_t)^{-1}A^2a_sb_s \cap \phi^{-1}(s)| \geq |A^2 \cap \phi^{-1}(t)| \geq \frac{|A^2|}{|\phi(A^2)|}, \tag{2.1}$$

其中，最后一个不等式源于我们对 t 的选择。对所有 $s \in \phi(A^2) \cap S$ 求和（2.1），即可得到我们所述的第二个不等式。为证明第一个不等式，我们对所有 $s \in \phi(A^2)$ 求和，从而得到

$$|A^6| \geq \sum_{s \in \phi(A^2)} |A^6 \cap \phi^{-1}(s)| \geq |\phi(A^2)| \cdot |A^2 \cap \phi^{-1}(t)|.$$

因此，

$$\frac{|A^2 \cap \phi^{-1}(S)|}{|A^6|} = \frac{1}{|A^6|}\sum_{s \in \phi(A^2) \cap S} |A^2 \cap \phi^{-1}(s)| \leq \frac{|A^2 \cap \phi^{-1}(t)|}{|A^6|} \cdot |\phi(A^2) \cap S| \leq \frac{|\phi(A^2) \cap S|}{|\phi(A^2)|}.$$

不等式 $|A^6| \leq K^4|A^2|$ 完成了证明。 □

我们还需要的最后一个结果是 Sanders 的以下命题，它与 Croot 和 Sisask 的一个“几乎周期性”引理有关。如果 $A \subset G$ 是一个具有小倍增的中心化集合，那么该结果允许我们找到一个包含于 A^4 中的大型迭代乘积集。

命题 2.16 ([San12, 命题 4.1])。存在一个绝对常数 $C \geq 1$，使得以下结论成立。设 G 是任意一个群，$A \subset G$ 满足 $|AA^{-1}| \leq K|A|$，且 $t \geq 1$ 是一个参数。那么存在某个含单位元的集合 $S \subset G$，使得

[7]该结果按此处的表述，相比 [Tao08]，中的版本多包含两个条件，即 $B \subset A^{-1}A$ 以及 $1 \in B$。这两个条件都可以从证明中轻易看出。

(1) $|S| \geq$ 指数函数$(-Ct^2(\log 2K)^2)|A|$
和 *(2)* $S^t \subset A^{-1}AA^{-1}A$。

为了证明定理 1.12 和命题 1.13，我们需要引入一些与矩阵群和线性代数相关的记号。我们将推迟到需要用到这些记号之前再介绍，见第 6.1 节。

2.4. **渐近记号**。如果存在某个绝对常数 C，使得当所有相关参数都充分大时，$|f| \leq Cg$，我们记作 $f = O(g)$，或等价地记作 $f \lesssim g$ 或 $g = \Omega(f)$。当 $f = O(g)$ 和 $g = O(f)$ 同时成立时，我们记作 $f = \Theta(g)$。在论证中出现渐近记号时，所有隐藏常数都是绝对的，与任何参数无关。在讨论某个论证的上下文中，我们偶尔会写出类似 $O_d(1)$ 的表达式，表示“由 d的某个函数所界定，且与其他任何参数无关”。

3. Our approach, and a toy problem

本节将介绍我们证明定理 1.2 和 1.3 所采用的方法。我们从一个玩具问题开始：给定一个有限可解群 G，它必定包含多大的阿贝尔子群?

在一般有限群的情形下，这个问题可追溯到 Erd˝os 和 Straus [ES76], ，他们最先给出了 $(1-o1)\log|G|$ 的下界。（更早以前，Miller 已证明，有限的 p-群 G含有一个阶为 $\exp(\Omega(\sqrt{\log|G|}))$ [Mil98] 的阿贝尔子群。）Pyber [Pyb97] 基本上解决了这个问题（见定理 1.1），他给出了适用于一般有限G 的 $\exp(\Omega(\sqrt{\log|G|}))$ 下界。即使在 G 为二步幂零的特殊情形下，这个下界也无法改进 [Ol'78, BGH87]。

我们给出定理 1.1 的一个弱版本的不同证明，部分基于[Mil98], 中的论证；该论证为有限可解群 G 的最大阿贝尔子群的大小建立了一个准多项式下界。随后，我们将把这一论证推广到近似群，从第 3.2 节开始。

3.1. 可解群中的阿贝尔子群。

命题 3.1 （ [Pyb97，定理 1]的弱版本）。任意有限可解群 G，若其阶为 n，则包含一个阶至少为

$$\exp\left(\frac{1}{2}\log^{1/3} n\right).$$

我们给出的命题 3.1 的证明是证明定理 1.2 的起点，因此也是证明更一般的定理 1.3 的起点。此证明中的每一个要素都可以迁移到近似子群的情形，唯独以下事实例外。

事实 3.2。设 G 是一个群。若 H 是 G 的子群且 $h \in G \setminus H$，则 $\frac{|\langle H, h\rangle|}{|H|} \geq 2$。

我们希望在近似群中应用事实 3.2，而不是在真正的群中应用；但事实 3.2 在近似群中不一定成立。为了解决这一问题，我们采用无关集的概念；关于此修正的详细说明，请参见第 3.2 节。

命题 3.1 的证明通过以下引理进行（参见引理 3.6）。

引理 3.3。设 G 是一个群，N 是 G 的正规子群，且 I 是 $Z(G)$ 的子群。假设 $I \lneq G$，且 G/N 是阿贝尔的。那么存在一个正整数 m 和一个阿贝尔子群$I \leq I' \leq G$，它是通过向 I 添加 m 个元素生成的，并满足 $|I'|/|I| \geq 2^m$ 且

$$|G| \leq |N|^m |I'|.$$

证明。设 $h_1, \ldots, h_m \in G$ 是 G 中元素的一个极大列表，使得 $h_1, \ldots, h_m$ 两两可交换，且

$$I \lneq \langle I, h_1\rangle \lneq \cdots \lneq \langle I, h_1, h_2, \ldots, h_m\rangle.$$

（存在这样的元素 h_1，因为 $I \leq Z(G)$，而 $I \lneq G$，所以我们有 $m \geq 1$。）定义函数 ϕ: $G \to N^m$，使得

$$\phi\colon x \mapsto (xh_1x^{-1}h_1^{-1}, \ldots, xh_mx^{-1}h_m^{-1}).$$

（由于 G/N 是阿贝尔的，此映射将 G 映到 N^m。）若 $x,\ y \in G$ 满足 $\phi(x) = \phi(y)$，则 $y^{-1}x$ 与 $h_1, \ldots, h_m$ 交换。因此，根据 m 的极大性，必有 $y^{-1}x \in \langle I, h_1, \ldots, h_m\rangle$。我们得出，$\phi$ 的纤维恰好是 $\langle I, h_1, \ldots, h_m\rangle$ 的左陪集。这意味着

$$|G| \le |N|^m |\langle I, h_1, \ldots, h_m\rangle|.$$

令 $I' = \langle I, h_1, \ldots, h_m\rangle$ 并使用事实 3.2，即可得到结果。 □

现在，我们给出命题 3.1 证明的其余部分。这里介绍的思路将在引理 3.7 的证明中再次出现。

命题 *3.1* 的证明。令 s 为 G的导出长度，并令

$$G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(s)} = \{1\}$$

为 G的导出列。我们迭代地构造 G 的阿贝尔子群 I。我们将定义一个阿贝尔群序列 $\{1\} =: I_0 \subset I_1 \subset \cdots \subset I_\ell$，以及一个辅助正整数序列 $m_0, m_1, \ldots, m_{\ell-1}$（$\ell$是该过程终止时的指标，不预先选定）。对于每个 j，在定义 I_j时，令 $H_j := C_G(I_j)$。我们依次对每个 $j \ge 0$ 重复以下过程:

(i) 如果 $I_j = H_j$，也就是说，如果 I_j 是其自身的中心化子，则终止该过程。(ii) 取满足 $H_j \cap G^{(i)} \not\subset I_j$ 的极大 i；这样的 i 存在，因为 $I_j \lneq H_j$。(iii) 对群 $H_j \cap G^{(i)}$、正规子群 $H_j \cap G^{(i+1)}$ 和阿贝尔子群 $I_j \le Z(H_j \cap G^{(i)})$ 应用引理 3.3，得到一个正整数 m 和一个阿贝尔子群$I' \le H_j \cap G^{(i)}$。令 $m_j := m$ 和 $I_{j+1} := I'$。

我们断言

$$\frac{|H_j|}{|H_{j+1}|} \le |H_j \cap G^{(i)}|^{m_j} \le |I_j|^{m_j^2} |I_{j+1}|^{m_j} \tag{3.1}$$

事实上，取满足 $I' = \langle I_j, h_1, \ldots, h_{m_j}\rangle$的 $h_1, \ldots, h_{m_j} \in H_j \cap G^{(i)}$，并定义映射 σ: $H_j \to (H_j \cap G^{(i)})^{m_j}$ 为

$$\sigma\colon x \mapsto (xh_1x^{-1}, \ldots, xh_{m_j}x^{-1}).$$

由于 $G^{(i)}$ 是 G的正规子群，我们有 $H_j \cap G^{(i)}$ 是 H_j的正规子群，因此对每个 $x \in H_j$和每个 $1 \le k \le m_j$，都有 $xh_kx^{-1} \in H_j \cap G^{(i)}$。若 $\sigma(x) = \sigma(y)$，则 $y^{-1}x$与 h_1、……、h_{m_j}交换。这意味着 $y^{-1}x \in C_G(I_{j+1}) = H_{j+1}$。由此得到 (3.1) 的第一个不等式。对于第二个不等式，根据引理 3.3 以及我们在步骤 (ii) 中对 i 的选择，还有

$$|H_j \cap G^{(i)}| \le |H_j \cap G^{(i+1)}|^{m_j} |I_{j+1}| \le |I_j|^{m_j} |I_{j+1}|. \tag{3.2}$$

由 (3.2) 即得 (3.1) 的第二个不等式。

剩下的只是简单的计算。由于 $I_\ell = H_\ell$，我们有

$$n = |G| = |H_0| = \frac{|H_0|}{|H_\ell|} \cdot \frac{|I_\ell|}{|I_0|} = \prod_{j=0}^{\ell-1} \left(\frac{|H_j|}{|H_{j+1}|} \cdot \frac{|I_{j+1}|}{|I_j|} \right).$$

利用 (3.1)，得到

$$n \le \prod_{j=0}^{\ell-1} |I_j|^{m_j^2 - 1} |I_{j+1}|^{m_j + 1} \le \prod_{j=0}^{\ell} |I_\ell|^{m_j^2 + m_j} \le |I_\ell|^{2(m_0 + \cdots + m_{\ell-1})^2}.$$

取对数并利用

$$|I_\ell| = \prod_{j=0}^{\ell-1} \frac{|I_{j+1}|}{|I_j|} \ge 2^{m_0 + \cdots + m_{\ell-1}}$$

得到

$$\log_2 n \le 2(m_0 + \cdots + m_{\ell-1})^2 \log_2 |I_\ell| \le 2(\log_2 |I_\ell|)^3.$$

结论由此得出。 □

注 3.4. 命题 3.1 证明末尾所用的界相当粗略。然而，仅凭 (3.1) 和界 $|I_{j+1}|/|I_j| \leq 2^{m_j}$，无法得到一个界超过 $\exp(O(\log^{1/3} n))$ 的命题 3.1 版本。考虑 $\ell = 2$ 和 $m_0 = m_1$ 的可能性即可看出这一点。

现在，我们对上述证明作一些评论，希望借此阐明我们的论证结构。命题 3.1 的证明首先写出环境群 G 的一个正规列，然后沿着该正规列逐步构造一个阿贝尔子群。在每次迭代中，我们会谨慎地选择该正规列中的一个步骤，尽可能多地找出可以加入阿贝尔群的元素，随后将注意力转向迄今构造出的群的中心化子。只要我们知道在每次迭代中应当如何恰当地选择正规列中的步骤，这一过程就可以在群的任意子集 A 中进行。由此得到的渐近结果（尤其是 (3.1) 的类似命题，以及引理 3.3 中关于 $|I'|/|I|$ 的下界）取决于子集 A 的性质是否良好。进一步阐述这一观察，将引出定理 1.2 的证明。

将这一方法扩展到非可解群时，一个关键观察是可以重复进行这一迭代。假设我们有一个群，其正规列中的连续商群未必是阿贝尔群。如果我们知道如何从连续商群中选取两两交换的元素，就可以采用与证明命题 3.1 相同的论证，只需将引理 3.3 替换为一种任意的（可能更复杂的）寻找两两交换元素的方法。[8] 我们将在下文的定义 3.5 中形式化地描述这类方法的概念。

3.2. **对近似群的适配**。现在，我们运用命题 3.1 的证明策略，为近似子群证明相应的结果。正如命题 3.1 的证明先证明关于阿贝尔商群的一个结论，再将其逐步推广到可解群一样，我们对定理 1.2 和 1.3 的证明也将反复逐步推广关于属于某些类别的商群的结论。为此，我们引入以下定义。

定义 3.5。令 $R \geq 1$ 和 $\beta \in (0, 1]$ 为参数。若群的一个对子群封闭的类 $\mathscr{G}$ 是 (R, β)-可交换的，则称其满足以下条件。

令 Γ 为一个群，令 $G \leq \Gamma$，并令 $N \trianglelefteq G$。设 A 是 Γ 的一个 K-近似子群，且 S 是 Γ 的一个含单位元的子集。假设 $G/N \in \mathscr{G}$ 和 $A^4 \cap N \subset S \subset C_\Gamma(G)$。那么集合 $A^4 \cap G$ 包含一个两两交换的无关子集 D，满足 $\langle D \rangle_\pm \cap S = \{1\}$，并且

$$|D| \geq (\beta \log_3 |A^2 \cap G|)^{1/R} - \log_3(3K|S|).$$

在陈述定义 3.5 满足的一些性质之前，我们先作一点说明（引理 3.9 的陈述和证明将具体体现这一点）。定义 3.5 提供了找到大小关于 $|A|$ 呈多对数级的两两交换的独立集的方法，而不是找到大小关于 $|A|$ 呈准多项式级的交换集（定理 1.2 和 1.3 需要后者）。这是因为前面提到的事实 3.2 在近似群情形下不再成立。我们将通过每次添加少数几个元素来构造交换集。如果不对所添加的元素施加额外限制，我们无法保证这些元素能使我们的交换子集在 A 的有界次幂中扩张得快于线性速度。（在真正的子群情形下，事实 3.2 保证每加入一个新元素，交换集的大小至少翻倍。）我们通过施加限制来避开这一问题：要求交换集在每一步都保持无关。实施这一条件不会带来太大代价，而且之后能让我们将一个多对数级大小的集合扩充为一个准多项式级大小的集合：我们可以取该无关集的各个子集所对应的乘积组成的集合。还有一个问题：我们需要有足够多这样的乘积落在 A^4 中。为此，我们先将 Sanders 的结果——命题 2.16——应用于集合 A。这样做会使“三重乘积

[8]如果我们只知道如何处理可解群，这并不能帮助我们，因为任何具有正规列且其连续商群均为可解群的群实际上都是可解群。然而，借助定理 1.12，我们将能够转而处理连续商群中适当选取的阿贝尔子群，并在这些子群中使用命题 3.1。

常数" K 增大为某个更大的 L，从而得到一个 L-近似群 B，满足 $B^t \subset A^4$，其中 t 足够大。将定义 3.5 的条件应用于 B 而非 A，然后考虑由所得两两交换的独立集中的元素构成的乘积集合，就能得到我们的结果。

我们将证明，$(R,\ \beta)$-可交换这一概念具有以下四个性质。

引理 3.6 (阿贝尔群是可交换的)。 阿贝尔群的类 $\mathscr{A}(2,\ 1/3)$-可交换。

引理 3.7 (具有可交换连续商群的群是可交换的)。 设 $\mathscr{H}$ 是任意一个对群的子群封闭的类，并令 $\mathscr{G}$ 表示由那些具有有限正规列且所有连续商群都属于 $\mathscr{H}$ 的群构成的类。假设 $\mathscr{H}$ 是$(R,\ \beta)$-可交换的。那么 $\mathscr{G}$ 是$(R+1,\ \beta')$-可交换的，其中 $\beta' = \min(\beta,\ 1\,10)$。

引理 3.8 (具有足够多可交换子群的群是可交换的)。 设 $\mathscr{H}$ 是任意一个对群的子群封闭的类。设 C、$\varepsilon > 0$ 为参数，并设 $\mathscr{G}$ 是一个对群的子群封闭的类；对于其中的群，若 $G \in \mathscr{G}$ 且 $A \subset G$ 是一个 K-近似群，则存在一个子群 $H \leq G$ 满足 $H \in \mathscr{H}$，并且

$$|A^2 \cap H| \geq \frac{1}{(2K)^C}|A^2|^{\varepsilon}.$$

设 $\mathscr{H}$是（$R,\ \beta$）-可交换的。那么，$\mathscr{G}$与 $\beta' = \beta\varepsilon/$（$3C+12$）是（$R,\ \beta'$）-可交换的 .

引理 3.9 （可交换群的近似子群具有大的阿贝尔子结构）。存在一个绝对常数 $c > 0$，使得以下结论成立。设 $\mathscr{G}$ 是一个对群的子群封闭的类，并且是（$R,\ \beta$）-可交换的；设 $G \in \mathscr{G}$，且设 $A \subset G$ 是满足 $|A^3| \leq K|A|$ 的有限对称子集。那么存在某个阿贝尔子群 H，它是 G 的子群，并满足

$$|A^4 \cap H| \geq \exp\left(c\frac{(\beta \log|A|)^{1/(2R)}}{\log 2K}\right)$$

我们将在第 4 节中证明引理 3.6 至 3.9。现在，我们先对这些引理的证明作一些简要说明。引理 3.6 和 3.7 可被视为我们在命题 3.1 的证明中所使用的两个主要要素的推广，而我们将给出的这些引理的证明将与命题 3.1 的证明相似。引理 3.8 的证明主要涉及展开定义并使用引理 2.15。如前所述，引理 3.9 的证明涉及将可交换性条件应用于通过应用命题 2.16 得到的一个近似子群。

3.3. **定理 1.2 和 1.3 的证明**。最后，我们利用引理 3.6 至 3.9 给出定理 1.2 和 1.3 的证明。证明定理 1.3 时，还需要假设定理 1.12 成立。

引理 3.10。*(1)* 可解群的类 $\mathscr{S}$ 是$(3, 1/10)$-可交换的。
(2) 对每个 $r \geq 1$，合成秩至多为 r 的群的类 $\mathscr{G}_r$ 对某个$(4, \beta_r)$-可交换

$$\beta_r \geq e^{-O(\log^2 r \log\log r)}.$$

证明。回顾引理 3.6，阿贝尔群的类 $\mathscr{A}$ 是 $(2, 1/3)$-可交换的。任意可解群 G 的导出列是一个正规列，其中所有相邻商群均为阿贝尔群。因此，(1) 由引理 3.6 和引理 3.7 得出。

对于 (2)，令 $\mathscr{L}_r$ 表示可作为某个域 $\mathbb{F}$ 上的 $\mathrm{GL}_r(\mathbb{F})$ 的子群出现的群类，并令 $\mathscr{L}'_r$ 表示可作为某个域 $\mathbb{F}$上的 $\mathrm{GL}_r(\mathbb{F}) \times \cdots \times \mathrm{GL}_r(\mathbb{F})$ 的某个直积的子群出现的群类。采用定理 1.12 中的记号，记

$$\varepsilon_r := \frac{1}{M(r)} = e^{-O(\log^2 r \log\log r)} \quad \text{and} \quad C_r := Cr^9$$

因此，对于任意域 $\mathbb{F}$ 上的 $\mathrm{GL}_r(\mathbb{F})$ 中的每个 K-近似子群，都存在某个阿贝尔子群 $H \subset \mathrm{GL}_d(\mathbb{F})$，使得

$$|A^2 \cap H| \geq \frac{1}{(2K)^{C_r}}|A^2|^{\varepsilon_r}.$$

由引理 3.8 和引理 3.6，即阿贝尔群是 $(2,1/3)$-可交换的这一事实，我们得出 $\mathscr{L}_r$ 是 $(2,\beta_r)$-可交换的

$$\beta_r := \frac{(1/3)\varepsilon_r}{3C_r+12} = \frac{\varepsilon_r}{9C_r+36}.$$

接下来，我们考虑类 $\mathscr{L}_r'$。任取 $G\in\mathscr{L}_r'$，并写作 $G\subset H_1\times\cdots\times H_m$，其中 m 是某个正整数，且 $H_1\cong\cdots\cong H_m\cong \mathrm{GL}_r(\mathbb{F})$，其中 $\mathbb{F}$ 是某个域。对每个 $0\le i\le m$，定义

$$G_i = G\cap(\{1\}\times\cdots\times\{1\}\times H_{i+1}\times\cdots\times H_m).$$

每个 G_i 都是 G 的正规子群，因此 $G=G_0\trianglerighteq G_1\trianglerighteq\cdots\trianglerighteq G_m=\{1\}$ 是 G 的有限长度正规列 m。此外，该列中的每个连续商群 G_{i-1}/G_i 都通过到 H_i 因子的投影映射，自然嵌入到 $H_i\cong\mathrm{GL}_r(\mathbb{F})$ 中。由此可得，任意 $G\in\mathscr{L}_r'$ 都有一个有限长度的正规列，其中所有连续商群都属于 $\mathscr{L}_r$。因此，引理 3.7 表明 $\mathscr{L}_r'$ 是 $(3,\ \beta_r)$-可交换的（因为 $\beta_r<1/10$）。

最后，根据引理 2.5，$\mathscr{G}_r$ 中的每个群都存在一个正规列，其中每个连续商群都包含于某个域 $\mathbb{F}$ 上的 $\mathrm{GL}_r(\mathbb{F})\times\cdots\times\mathrm{GL}_r(\mathbb{F})$ 的乘积中；特别是，每个连续商群都属于 $\mathscr{L}_r'$。最后再应用一次引理 3.7，可得 $\mathscr{G}_r$ 是 $(4,\ \beta_r)$-可交换的。定理 1.12 给出的关于 ε_r 和 C_r 的渐近估计表明，$\beta_r=\exp(-O(\log^2 r\log\log r))$，这正是所需结论。□

在建立了相关概念和定义之后，定理 1.2 由引理 3.9 和引理 3.10(1) 推出。

*假设引理 3.6 至 3.9，证明定理 1.2。*设 G 是一个可解群，$A\subset G$ 是满足 $|A^3|\le K|A|$ 的对称子集。根据引理 3.10(1)，G 属于一个 $(3,\ 1/10)$-可交换族。因此，引理 3.9 表明，存在一个阿贝尔子群 $H\le G$，满足

$$|A^4\cap H|\ge\exp\left(\Omega\left(\frac{\log^{1/6}|A|}{\log 2K}\right)\right).$$ □

相应地，定理 1.3 可由引理 3.9 和引理 3.10(2) 推出。

*假设引理 3.6 至 3.9 和定理 1.12，证明定理 1.3。*设 G 是一个有限群，并假设 G 没有与交错群 A_d 同构的子商。设 $A\subset G$ 是满足 $|A^3|\le K|A|$ 的有限对称子集。由引理 2.7，G 的合成秩至多为 $r=O(d^2)$。由引理 3.10(2)（其证明中我们用到了定理 1.12），群 G 属于一个 $(4,\ \beta)$-可交换族，其中 $\beta=\beta_r=\exp(-O(\log^2 d\log\log\ d))$ 的定义与引理 3.10(2) 中相同。因此，由引理 3.9 可知，存在某个阿贝尔子群 $H\le G$ 满足

$$|A^4\cap H|\ge\exp\left(\Omega\left(\beta^{1/8}\frac{\log^{1/8}|A|}{\log 2K}\right)\right)\ge\exp\left(\Omega\left(\frac{\log^{1/8}|A|}{\exp(O(\log^2 d\log\log d))\cdot\log 2K}\right)\right).$$ □

4. Proofs of (R,β)-commutability properties

本节中，我们证明引理 3.6 至 3.9。

我们先证明引理 3.6，即阿贝尔群是 $(2,\ 1/3)$-可交换的。其证明与引理 3.3 的证明非常相似：我们取一个极大的“新”两两交换元素集合，并利用这些元素进行共轭来推导出相应的界。

*引理 3.6 的证明。*设 Γ 是一个群，设 $G\le\Gamma$，并设 $N\trianglelefteq G$ 满足 G/N 是阿贝尔的。设 A 是 Γ 的一个 K-近似子群，满足 $n:=|A^2\cap G|$，并设 $S\supset A^4\cap N$。我们将证明，$A^4\cap G$ 包含一个两两交换的无关子集 D，满足 $\langle D\rangle_\pm\cap S=\{1\}$ 和

$$|D|\ge\sqrt{\frac{\log_3 n}{3}}-\log_3(3K|S|).$$

设 $D = \{h_1, \dots, h_m\}$ 是 $A^4 \cap G$ 的一个极大子集，该子集两两交换、无关，并满足 $\langle D\rangle_{\pm} \cap S = \{1\}$。定义 ϕ 在 $A^2 \cap G$ 上的映射如下：

$$\phi(a) = (ah_1a^{-1}h_1^{-1}, \dots, ah_ma^{-1}h_m^{-1}).$$

由于 G/N是阿贝尔的，$[G,G] \subset N$。因此，ϕ的像包含于$(A^{12} \cap N) \times \cdots \times (A^{12} \cap N)$中。另一方面，如果 $\phi(a) = \phi(b)$，那么 $b^{-1}a$ 与每个 h_i都可交换。因此，对于 ϕ的任意纤维 Y，集合 $Y^{-1}Y \subset A^4 \cap G$ 中的每个元素都与 D中的每个元素可交换。因此，D 的极大性意味着，对于每个 $x \in Y^{-1}Y$，以下情况必有其一：(a) $x \in D$；(b) $D \cup \{x\}$ 不是无关的；或(c) $\langle D \cup \{x\}\rangle_{\pm} \cap S$包含 G的某个非单位元。这些情况中的任一种都意味着存在某个 $y \in \langle D\rangle_{\pm}$ 和某个 $s \in S$，使得 $xy = s$。这意味着

$$|Y| \le |Y^{-1}Y| \le |S\langle D\rangle_{\pm}^{-1}| \le |S| \cdot |\langle D\rangle_{\pm}| = 3^m|S|.$$

由此可得

$$n = |A^2 \cap G| = \sum_{t \in \operatorname{im}\phi} |\phi^{-1}(t)| \le 3^m|S| \cdot |\operatorname{im}\phi| \le (3 \cdot |A^{12} \cap N|)^m|S|.$$

若 $m = 0$，则由上述内容可知 $|S| \ge n$，结论显然成立。否则，由于 A 是一个 K-近似群，引理 2.13 给出不等式 $|A^{12} \cap N| \le K^{11}|A^2 \cap N| \le K^{11}|S|$。这意味着 $n \le (3K^{11}|S|)^m|S| \le (3K|S|)^{11m}$；等价地，

$$|D| = m \ge \frac{\log_3 n}{11(\log_3(3K|S|))}.$$

应用不等式 $\frac{x}{11y} \ge \sqrt{\frac{x}{3}} - y$，将关于 m的这个下界转化为所需的形式 . □

接下来，我们证明引理 3.7。设 $\mathscr{H}$是一个 (R,β)-可交换群类。设 Γ 是一个含有子群 G 的群，并设 $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = N$是一个正规列，其中对每个 $0 \le i < s$都有 $G_i/G_{i+1} \in \mathscr{H}$；该正规列由将 $G/N \in \mathscr{G}$ 的此类正规列提升至 G而得。设 $A \subset \Gamma$ 是一个K-近似子群，并设 S是 Γ的一个含单位元的子集，满足 $A^4 \cap N \subset S \subset C_\Gamma(G)$。回顾一下，我们必须找到 $A^4 \cap G$ 的某个两两交换的无关子集 D，使其满足 $\langle D\rangle_{\pm} \cap S = \{1\}$ 并且

$$|D| \ge \left(\min\left(\beta, \frac{1}{10}\right)\log_3|A^2 \cap G|\right)^{1/(R+1)} - \log_3(3K|S|). \tag{4.1}$$

证明与真正的群情形下命题 3.1 的证明颇为相似。我们将归纳地构造集合 D，每一步都尽可能深入级数$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = N$，将元素添加到 D 中。利用 $\mathscr{H}$的$(R$、$\beta)$-可交换性，并考察新元素所诱导的共轭作用，即可在每一步得到所需的界。

引理 *3.7* 的证明。我们迭代地构造这样的集合 D。初始化 $D_0 = \emptyset$。每当我们定义D_j时，也同时定义 $S_j := \langle D_j\rangle_{\pm}S$ 和 $H_j := \bigcap_{x \in D_j} C_G(x) \le G$。我们保持以下性质：对每个 j，集合 D_j 两两交换、无关，并满足 $\langle D_j\rangle_{\pm} \cap S = \{1\}$。由于 $S \subset C_\Gamma(G)$且 S_j 由 $D_j \cup S$生成，因此对每个 j，S_j 都含单位元且包含于 $C_\Gamma(H_j)$。

假设我们已经构造出某个 D_j（因此也构造出了 H_j和 S_j）。若 $A^4 \cap H_j \subset S_j$，则终止该过程；令 ℓ 为这种情况发生时的指数。（我们将在后续论证中证明，该过程最终会终止。）否则，由于

$$A^4 \cap H_j \cap G_0 = A^4 \cap H_j \not\subset S_j,$$
$$A^4 \cap H_j \cap G_s \subset A^4 \cap N \subset S \subset S_j,$$

存在某个指数 $i \in [0,s)$，使得 $A^k \cap H_j \cap G_i \not\subset S_j$ 且 $A^k \cap H_j \cap G_{i+1} \subset S_j$。由于 $G_i/G_{i+1} \in \mathscr{H}$ 且 $\mathscr{H}$对子群封闭，我们有 $(H_j \cap G_i)/(H_j \cap G_{i+1}) \in \mathscr{H}$。令 D' 为满足条件 $\langle D'\rangle_{\pm} \cap S_j = \{1\}$ 的 $A^4 \cap H_j \cap G_i$ 的最大规模两两交换的无关子集。

一方面，我们有 $|D'| \ge 1$；由于 S_j 是含单位元的，我们可以将 D' 取为非空集合 $(A^4 \cap H_j \cap G_i) \setminus S_j$ 中任意元素所组成的单元素集合。另一方面，我们可以应用以下事实

即 $\mathscr{H}$ 对 Γ 的子商 $(H_j \cap G_i)/(H_j \cap G_{i+1})$ 是 (R,β)-可交换的；利用近似群 A 和包含 $A^4 \cap H_j \cap G_{i+1}$ 的含单位元集合 $S_j \subset C_\Gamma(H_j) \subset C_\Gamma(H_j \cap G_i)$，可以找到满足以下条件的某个此类集合 D'

$$|D'| \geq (\beta \log_3 |A^2 \cap H_j \cap G_i|)^{1/R} - \log_3(3K|S_j|). \tag{4.2}$$

令 $D_{j+1} := D_j \sqcup D'$。由于 $D' \subset A^4 \cap H_j$， D' 的每个元素都与 D_j的每个元素两两交换。由于 D_j 和 D' 是交换集，这意味着 D_{j+1} 也是如此。现在，由于 D' 是两两交换且无关的，并且 $\langle D' \rangle_\pm \cap \langle D_j \rangle_\pm S = \{1\}$，我们有 $D_{j+1} = D_j \sqcup D'$ 无关且 $\langle D_{j+1} \rangle_\pm \cap S = \{1\}$。事实 $|D'| \geq 1$ 确保 $|D_j|$ 是 j的严格递增函数；由于每个 D_j 都包含在有限集合 $A^4 \cap G$中，这又确保我们的过程最终终止。

接下来我们考察 $|A^4 \cap H_j|$ 如何随 j变化。首先，如果 $\ell = 0$ ，那么 $A^4 \cap G \subset S$，特别是

$$(\beta \log_3 |A^2 \cap G|)^{1/R} \leq \beta \log_3 |A^2 \cap G| \leq \log_3 |A^4 \cap G| \leq \log_3(3K|S|).$$

这意味着 (4.1) 平凡成立，因此无需证明。以下我们假设$\ell > 0$，这意味着 $|D_\ell| > 0$。一方面，根据终止条件，我们有

$$\frac{|A^4 \cap H_0|}{|A^4 \cap H_\ell|} \geq \frac{|A^4 \cap G|}{|S_\ell|} \geq \frac{|A^2 \cap G|}{3^{|D_\ell|}|S_0|}. \tag{4.3}$$

另一方面，我们断言，若 $m = |D'| = |D_{j+1} \setminus D_j|$，则

$$\frac{|A^4 \cap H_j|}{|A^4 \cap H_{j+1}|} \leq \left(K^{10}|A^2 \cap H_j \cap G_i|\right)^m. \tag{4.4}$$

事实上，在 $A^2 \cap H_j$ 上定义映射 σ 如下:

$$\sigma(a) = (ah_1a^{-1}, \ldots, ah_ma^{-1}),$$

其中 h_1、.....、 h_m是 $D' = D_{j+1} \setminus D_j$中元素的一个枚举。回想一下， $D' \subset A^4 \cap H_j \cap G_i$。因此，由于 $G_i \trianglelefteq G$，对于每个 $a \in A^2 \cap H_j$和 $x \in D'$，都有 $axa^{-1} \in A^8 \cap H_j \cap G_i$。于是， σ的像包含于 $(A^8 \cap H_j \cap G_i) \times \cdots \times (A^8 \cap H_j \cap G_i)$ 中。现在，令 Y为σ的一个最大纤维。根据 σ的定义，$Y^{-1}Y$ 中的每个元素都与 D' 中的每个元素可交换，因此属于 $(A^2 \cap H_j)^2 \cap H_{j+1}$。由此可得

$$|A^4 \cap H_{j+1}| \geq |Y^{-1}Y| \geq |Y| \geq \frac{|A^2 \cap H_j|}{|A^8 \cap H_j \cap G_i|^m}.$$

两次应用引理 2.13，我们得到

$$\frac{|A^4 \cap H_j|}{|A^4 \cap H_{j+1}|} \leq \frac{K^3|A^2 \cap H_j|}{|A^4 \cap H_{j+1}|} \leq K^3|A^8 \cap H_j \cap G_i|^m \leq (K^{10}|A^2 \cap H_j \cap G_i|)^m,$$

从而得到（4.4）。现在，（4.2）意味着

$$\begin{aligned} \log_3 |A^2 \cap H_j \cap G_i| &\leq \frac{1}{\beta}(|D'| + \log_3(3K|S_j|))^R \\ &= \frac{1}{\beta}(|D_{j+1}| + \log_3(3K|S_0|))^R. \end{aligned}$$

将其与（4.3）和（4.4）结合，并令 $\kappa := \log_3 K$ 以简化记号 y,

$$\begin{aligned}
&\text{对数}_3|A^2\cap G| - |D_\ell| - \text{对数}_3|S_0| \le \text{对数}_3|A^4\cap H_0| - \text{对数}_3|A^4\cap H_\ell| \\
&\qquad \le \sum_{j=0}^{\ell-1} |D_{j+1}\setminus D_j|\big(10\kappa + \log_3|A^2\cap H_j\cap G_i|\big) \\
&\qquad \le 10\kappa|D_\ell| + \frac{1}{\beta}\sum_{j=0}^{\ell-1}|D_{j+1}\setminus D_j|\big(|D_{j+1}| + 1 + \kappa + \log_3|S_0|\big)^R \\
&\qquad \le 10\kappa|D_\ell| + \frac{1}{\beta}|D_\ell|\big(|D_\ell| + 1 + \kappa + \log_3|S_0|\big)^R.
\end{aligned}$$

令 $\beta' := \min(\beta,\ 1/10)$。由于 $|D_\ell|,\ R\ge 1$，我们有

$$\begin{aligned}
\log_3|A^2\cap G| &\le |D_\ell|(1 + 10\kappa + \log_3|S_0|) + \frac{1}{\beta}|D_\ell|\big(|D_\ell| + 1 + \kappa + \log_3|S_0|\big)^R \\
&\le \frac{1}{\beta'}\Big(|D_\ell|(1 + \kappa + \log_3|S_0|) + |D_\ell|\big(|D_\ell| + 1 + \kappa + \log_3|S_0|\big)^R\Big) \\
&\le \frac{1}{\beta'}\big(|D_\ell| + \log_3(3K|S_0|)\big)^{R+1}.
\end{aligned}$$

重新整理得到（4.1），正如所需。 □

接下来，我们证明引理 3.8。该引理使我们能够从一个（$R,\ \beta$）-可交换群类 $\mathscr{H}$转到一个更大的类 $\mathscr{G}$，在这个类中，每个近似群都与 $\mathscr{H}$中的某个群有较大的交集。该引理基本上由引理 2.15 推出。

引理 *3.8* 的证明。令 $\mathscr{H}$为一个（$R,\ \beta$）-可交换群类，并令 G' 为一个群，使得对于˜满足以下条件：如果 $A\subset G'$ 是一个 K-近似群，那么存在一个子群 $H\le G$ 满足 $H\in\mathscr{H}$且

$$\big|\tilde{A}^2\cap H\big| \ge \frac{1}{(2K)^C}|\tilde{A}^2|^{\varepsilon}. \tag{4.5}$$

我们必须证明，对于任意具有子商 $G/N\cong G'$ 的群 Γ 、 Γ 的任意 K-近似子群 A，以及满足 $S\supset A^4\cap N$ 的任意含单位元的子集 $S\subset C_\Gamma(G)$，集合 $A^4\cap G$ 含有一个满足 $\langle D\rangle_\pm\cap S=\{1\}$ 且满足

$$|D| \ge (\beta'\log_3|A^2\cap G|)^{1/R} - \log_3(3K|S|) \tag{4.6}$$

其中 $\beta' = \frac{\beta\varepsilon}{3C+12}$。首先，令 $\pi\colon G\to G/N\cong G'$ 为自然商映射。集合 $\tilde{A} := \pi(A^2\cap G)$ 是 G' 的一个 K^3-近似子群。因此，我们可以找到某个子群 $H\le G'$，使得 $H\in\mathscr{H}$，并且在将 K^3 替换 K 后满足 (4.5)。对 K^3- 近似子群 $A^2\cap G$ 和投影 $\pi\colon G\to G'$ 应用引理 2.15，得到

$$\begin{aligned}
\frac{K^{11}|A^2\cap\pi^{-1}(H)|}{|(A^2\cap G)^2|} &\ge \frac{|(A^2\cap G)^6\cap\pi^{-1}(H)|}{|(A^2\cap G)^2|} \\
&\ge \frac{|\pi((A^2\cap G)^2)\cap H|}{|\pi((A^2\cap G)^2)|} \\
&= \frac{|\tilde{A}^2\cap H|}{|\tilde{A}^2|} \ge \frac{1}{(2K^3)^C}|\tilde{A}^2|^{-(1-\varepsilon)} \ge \frac{|A^2\cap G|^{\varepsilon}}{(2K^3)^C|(A^2\cap G)^2|}
\end{aligned}$$

（其中第一个不等式用到了引理 2.13）。由此可得

$$|A^2\cap\pi^{-1}(H)| \ge \frac{1}{(2K)^{3C+11}}|A^2\cap G|^{\varepsilon}. \tag{4.7}$$

现在，$\pi^{-1}(H)/N \cong H \in \mathscr{H}$，因此我们可以将 $\mathscr{H}$ 的（$R,\ \beta$）可交换性应用于 Γ 的子商 $\pi^{-1}(H)/N$，其中近似群为 A，含单位元的集合 $S \subset C_\Gamma(G) \subset C_\Gamma(\pi^{-1}(H))$ 包含 $A^4 \cap N$，从而得到某个两两交换的解离集 $D \subset A^4 \cap \pi^{-1}(H) \subset A^4 \cap G$，它满足 $\langle D\rangle_\pm \cap S = \{1\}$，并且

$$|D| \geq (\beta \log_3 |A^2 \cap \pi^{-1}(H)|)^{1/R} - \log_3(3K|S|). \tag{4.8}$$

若 $|A^2 \cap G|^\varepsilon < (2K)^{3C+12}$，则（因为 $R > 1$）

$$\left(\frac{\beta\varepsilon}{3C+12}\log_3|A^2\cap G|\right)^{1/R} \leq \frac{\beta\varepsilon}{3C+12}\log_3|A^2\cap G| < \log_3(2K) < \log_3(3K|S|),$$

且 (4.6) 显然成立。否则，(4.7) 意味着 $|A^2 \cap \pi^{-1}(H)| \geq |A^2 \cap G|^{\varepsilon/(3C+12)}$，因此由 (4.8) 可得 (4.6)。□

最后，我们证明引理 3.9。该引理使我们能够将 (R,β)-可交换性提升为在 A^4 中存在一个（准多项式级别）大的阿贝尔近似群，其中 A 是任意近似群。我们不直接将 (R,β)-可交换性应用于给定的集合 A，而是先应用 Sanders 的一个结果（命题 2.16），找到一个集合 S_0，其规模与 A 相差不大，并且它的一个大型迭代乘积集包含于 A^4 中。随后，我们将 (R,β)-可交换性应用于 S_0^2，从而找到 S_0^8 的一个大型两两交换无关子集 D。由于 S_0 的一个大型迭代乘积集包含于 A^4 中，我们可以利用 D 的独立性，找到 A^4 的一个两两可交换子集，其大小相对于 $|D|$ 呈指数级增长。

引理 3.9 的证明。 设 $\mathscr{G}$ 是一个 (R,β)-可交换族，并设 $G \in \mathscr{G}$。设 $A \subset G$ 是满足 $|A^3| \leq K|A|$ 的有限对称子集。我们必须找到 G 的某个阿贝尔子群 H，使得

$$|A^4 \cap H| \geq \exp\left(c\frac{(\beta\log|A|)^{1/(2R)}}{\log 2K}\right) \tag{4.9}$$

其中某个绝对常数为 $c > 0$。

由 Ruzsa 三角不等式可得 $|A^4| \leq K^2|A|$。设 $t \geq 4$ 为稍后选取的一个参数。我们先将命题 2.16 应用于 A。对于某个绝对常数 $C \geq 1$，可以找到一个中心化集合 S_0，使得 $S_0^{2t} \subset A^4$，并且

$$|S_0| \geq \exp\bigl(-4Ct^2(\log 2K)^2\bigr)|A|.$$

令 $L := K^2\exp(4Ct^2(\log 2K)^2)$，于是 $L|S_0| \geq |A^4| \geq |S_0^{2t}|$。令 $B := S_0^2$。将 Ruzsa 覆盖引理应用于 S_0^2 和 S_0，可得某个子集 $Y \subset G$，满足 $|Y| \leq |S_0^5|/|S_0| \leq L$ 和 $B^2 \subset YB$。因此，集合 B 是一个满足 $B^t \subset A^4$ 的 L-近似群。

因此，我们可以将 $\mathscr{G}$ 的 (R,β)-可交换性应用于 L-近似群 $B \subset G$，其中 $\Gamma = G$、$N = \{1\}$ 和 $S = \{1\}$。由此可得，B^4 包含一个两两交换的解离集 D，满足

$$|D| \geq (\beta\log_3|B|)^{1/R} - \log_3(3L). \tag{4.10}$$

令 $\ell := \min(|D|, \lfloor t/4\rfloor)$，并设 D' 是 D 中大小为 ℓ 的任意子集，使得 $(\{1\}\cup D')^\ell \subset B^t \subset A^4$。令 $H := \langle D'\rangle$ 为由 D' 生成的 G 的阿贝尔子群。集合 $(\{1\}\cup D')^\ell$ 包含 D' 的每个子集的乘积；由于 D' 无关，因此该集合的大小至少为 2^ℓ。由此可得 $|A^4 \cap H| \geq 2^\ell$。

剩下的任务是选择 t 以使 ℓ 最大。我们选取

$$t = \left\lfloor \frac{(\beta\log_3|A|)^{1/(2R)}}{5C\log(2K)} \right\rfloor.$$

通过充分减小 c，我们可以将上述所选 t 小于 4 的情形纳入 (4.9)。因此，我们可以假设 $t \geq 4$。我们声称 $|D| \geq t/4$。这就完成了证明：如果

$|D| \geq t/4$，那么不等式 $|A^4 \cap H| \geq 2^\ell \geq$ 指数函数$(t/8)$ 的形式为 (4.9)。事实上，我们有 ve

$$\begin{aligned}|D| &\geq (\beta \log_3 |B|)^{1/R} - \log_3(3L) \\ &\geq (\beta \log_3(|A|/L))^{1/R} - \log_3(3L) \\ &\geq (\beta \log_3 |A|)^{1/R} - 2\log_3(3L) \\ &\geq 25C^2t^2(\log 2K)^2 - 2\log(3K^2) - 8Ct^2(\log 2K)^2 > 15C^2t^2(\log 2K)^2 > t. \end{aligned}$$ □

5. Non-solvable groups: strategy and outline

接下来的四节将用于证明定理 1.12；我们也会在此过程中证明命题 1.13。在这些章节中，$\mathbb{F}$ 始终是一个代数闭域（特征任意）。这一性质可以不失一般性地加到定理 1.12 对 $\mathbb{F}$ 的陈述中。

本节概述我们将用于证明定理 1.12 的策略，并将定理 1.12 的证明归结为寻找一般线性群[9] $\mathrm{GL}_d(\mathbb{F})$的一个博雷尔子群，其与 A^2的交很大。

我们使用的所有术语和定义均在第 6.1 节中给出。

5.1. 策略。我们从 $A \subset \mathrm{GL}_d(\mathbb{F})$出发，希望找到某个阿贝尔群 $H \leq \mathrm{GL}_d(\mathbb{F})$，使其交 $A^2 \cap H$ 很大。首先，我们找到这样一个包含于一般线性群 $\mathrm{GL}_d(\mathbb{F})$的博雷尔子群中的群 H，然后使用定理 1.2 的一个更具针对性的版本（见第 5.3 节）来推出定理 1.12。在这份概要的其余部分，我们的目标是找到一个使 $|A^2 \cap \mathcal{B}|$ 很大的博雷尔子群 $\mathcal{B}$。

我们将通过依次寻找越来越小的分块三角子群（相对于某个基）来实现这一点，这些子群与 A^2 有较大的交集。一旦所有分块的大小都缩减为 1，A^2 中的许多元素就会包含在相对于某个基的上三角矩阵群中，这样我们便大功告成。

我们论证的出发点是下面这个简单的不等式；在前两节中，我们曾隐含地使用过它的一些变体。

引理 5.1。对于任意群 G 的任意子集 A 以及任意元素 $a \in A$，有

$$|A^2 \cap C(a)| \cdot |A^3 \cap \mathrm{Conj}(a)| \geq |A|.$$

证明。考虑由 $\sigma(g) = gag^{-1}$ 定义的映射 $\sigma\colon A \to A^3$。一方面，σ 的像包含在 $A^3 \cap$Conj(a) 内。另一方面，对于 σ 的每个纤维 S，集合 $S^{-1}S$ 包含在 $A^2 \cap C(a)$ 内。因此

$$|A| = \sum_{b \in \mathrm{im}\,\sigma} |\sigma^{-1}(b)| \leq |\mathrm{im}\,\sigma| \max_{b \in \mathrm{im}\,\sigma} |\sigma^{-1}(b)| \leq |A^3 \cap \mathrm{Conj}(a)| \cdot |A^2 \cap C(a)|.$$ □

因此，我们首先选取某个 $a \in A$。根据引理 5.1，$|A^2 \cap C(a)|$ 或 $|A^3 \cap$Conj$(a)|$ 中至少有一个很大。我们先考察第一种情况。集合 $C(a)$ 非常理想：它是一般线性群 $\mathrm{GL}_d(\mathbb{F})$ 的一个子群，同时也恰好是 $\mathrm{Mat}_d(\mathbb{F})$ 的某个子空间中的可逆矩阵集合。如果 $a \in \mathrm{GL}_d(\mathbb{F})$ 是一个正则半单元素（也就是说，它具有 d 个互不相同的特征值），那么 $C(a)$ 就是一个对角子群，因此只要 $A^2 \cap C(a)$ 很大，我们便立即得证。实际上，我们未必总能选取正则半单的 a。不过，如果 a “不太不规则”，即 a 不具有维数过大的特征子空间，那么 $C(a)$ 就会包含在某个分块三角子群中，而该子群比 $\mathrm{GL}_d(\mathbb{F})$ 本身小得恰到好处（见引理 6.7）；通过转而考虑 $A^2 \cap C(a)$，我们便能取得足够的进展。我们将利用命题 1.13 找到这样的元素 a，否则就直接将问题化归到一个简单得多的群上。

现在我们考察 $|A^3 \cap$Conj$(a)|$ 较大的情形。集合 Conj(a) 不如 $C(a)$ 那么规整。不过，它包含在余维一仿射子空间 $\mathbf{X} := \{x \in \mathrm{Mat}_d(\mathbb{F}) : \mathrm{tr}\, x = \mathrm{tr}\, a\}$ 中。这个集合与子群截然不同——它的乘法结构很差。我们将能够

[9] 在一般线性群$_d$($\mathbb{F}$) 中，*Borel subgroups* 指的是在某个基下由上三角矩阵组成的子群 es.

利用这一点。首先，如果 $A^3 \cap \mathbf{X}$ 很大，那么双重计数论证可知，存在许多 $a \in A$，使得 $A^4 \cap (\mathbf{X} \cap a\mathbf{X})$ 也很大。除非 a 是单位矩阵的标量倍，否则 $\mathbf{X} \cap a\mathbf{X}$ 是 $\mathrm{Mat}_d(\mathbb{F})$ 中一个余维二 仿射子空间，因此我们可以用更小的 $\mathbf{X} \cap a\mathbf{X}$ 替换 $\mathbf{X}$，而不会造成太大损失。另一方面，如果对于许多 $a \in A$，a 都是单位矩阵的标量倍，那么我们就能立即将问题约化到一个（小得多的）子群。采用这种方法的一个更复杂版本（其基础是引理 8.1），我们便能将“A^3 中许多元素具有相同的迹”这一陈述提升为大致如下的陈述：“A^2 与一般线性群 $\mathrm{GL}_d(\mathbb{F})$ 中某个维数至多为 $\frac{1}{\sqrt{2}}d^2$ 的分块三角子群有很大的交集。”

将这一思路贯彻到底的主要难点在于：在迭代过程的第 t 步，我们得到的不会是 $\mathrm{GL}^{d(t)}(\mathbb{F})$ 的一个子集，使得 $d(t)$ 是 t 的递减函数；而是某个 $\mathrm{GL}_d(\mathbb{F})$ 分块三角子群的子集（其中 d 固定），其分块会随着 t 增大而缩小。为在证明中保留这些数据，我们采用了基于向量空间中旗 的记号；见第 6.1 节。

5.2. **与先前工作的联系**。 定理 1.12 的证明受到多位作者在有界秩情形下证明单群凯莱图直径界的 Babai 猜想时所用方法的启发 [Hel08, Hel11, BGT11, PS16]。这些结果中的两个核心工具是逃离子簇 和*Larsen–Pink* 不等式。

这些结果最自然的表述是在特殊线性群 $\mathrm{SL}_d(\mathbb{F})$ 中。二者都依赖于代数簇的复杂度 这一概念；我们省略其定义，只指出由线性多项式定义的代数簇具有较低的复杂度。设 $A \subset \mathrm{SL}_d(\mathbb{F})$ 是一个 K-近似群。关于中心化集合的 Larsen–Pink 不等式（见 [BGT11, 定理 4.1]）大致表明，以下两种情况必有其一：

(a) 对于 $\mathrm{SL}_d(\mathbb{F})$ 的每个低复杂度子簇 $\mathbf{V}$，我们有

$$|A^2 \cap \mathbf{V}| \leq K^{O_{d,\mathbf{V}}(1)} |A|^{\dim \mathbf{V} / \dim \mathrm{SL}_d(\mathbb{F})}, \tag{5.1}$$

否则

(b) A完全包含于 $\mathrm{SL}_d(\mathbb{F})$ 的某个低复杂度子簇中。

逃离子簇（见 [Hel08，引理 4.4], [BGT11，引理 3.11], 或 [PS16，引理 51]）使我们能够将条件 (b) 中的子簇提升为子群：如果 A^m 包含于某个低复杂度子簇$\mathbf{V}$ 中（对于某个就 $\mathbf{V}$ 的复杂度而言足够大的 m），那么实际上A 包含于 $\mathrm{SL}_d(\mathbb{F})$ 的某个低复杂度子群中。

由于两个原因，我们无法直接使用文献中已有的这些结果：首先，当环境群 $\mathrm{SL}_d(\mathbb{F})$ 被非单群取代时，Larsen–Pink 不等式并不能直接适用；其次，关于 d 的定量依赖通常比我们所能接受的更弱。然而，(5.1) 中关于 $|A|$ 的定量依赖远比我们所需的 强：对于所关注的 $\mathbf{V}|$，我们完全可以接受 $|A^2 \cap$的一个相对适中的上界，而 (5.1) 除了关于 K、d 以及 $\mathbf{V}$ 的复杂度的依赖外已经是紧的。

现在考虑如上一小节所述应用引理 5.1 的情形，目标是找到一个包含许多 A^2 中元素的大型分块三角子群。由此可知，对于某个 a，

$$|A^2 \cap C(a)| \cdot |A^3 \cap \mathrm{Conj}(a)| \geq |A|.$$

如果 (5.1) 成立，那么 $|A^2 \cap C(a)|$ 和 $|A^3 \cap \mathrm{Conj}(a)|$ 都会在乘法因子 $K^{O_{d(1)}}$ 的范围内有界。然而，即使是像 $|A^2 \cap C(a)| \geq |A^2|^{d^{-10}}$ 这样的弱界，对我们的目的来说也已足够。这使我们可以假设 $|A^3 \cap \mathrm{Conj}(a)|$ 极大。特别地，令$\mathbf{X}$ 为由方程 $\mathrm{tr}\, x = \mathrm{tr}\ a$ 所定义的 $\mathrm{Mat}_d(\mathbb{F})$ 中余维一子簇，则当$\mathbf{V} = \mathbf{X}$ 时，我们得到与 (5.1) 矛盾的结论。事实上，我们得到一个在定性上接近 Larsen–Pink 不等式中条件 (b) 的论断：A^3 中如此大比例的元素包含在$\mathbf{X}$中（相对于其复杂度而言），以至于“逃离子簇”方法应当能在此情形下给出一个包含 A^3 中很大一部分元素的子群。换言之，通过定量刻画我们的迭代究竟需要什么，我们完全无需一般性的受 Larsen–Pink 启发的论证。我们需要的是“逃离仿射子空间”的定量版本。这由引理 6.6 给出，

该引理在下一节陈述，其证明受到文献中上述逃离结果证明的启发。

在证明直径界时，逃离子簇还有一项应用，这对我们的工作同样不可或缺。对于某个 $m = O_d(1)$，我们需要找出 A^m 中的正则半单元素。这确实是一个“逃离子簇”问题：非正则且非半单元素构成 $\mathrm{Mat}_d(\mathbb{F})$ 的一个子簇 $\mathbf{Z}$（由特征多项式的判别式刻画）。然而，对我们而言，这里的情况在两方面都不理想。首先，$\mathbf{Z}$ 无法包含在 $\mathrm{Mat}_d(\mathbb{F})$ 的某个仿射子空间中，因此我们无法像处理 $\mathrm{Conj}(a)$ 那样处理它。其次，我们无法保证 A 生成 $\mathrm{GL}_d(\mathbb{F})$ 的一个大子群。因此，没有理由期待 A^m 对任何 m 都包含正则半单元素；我们只能希望在情况并非如此时，将问题约化到一个更小的环境群。命题 1.13 揭示了这种两难局面；尽管它远不足以保证正则半单元素的存在，但对我们的目的而言已经足够。命题 1.13 的证明与一般逃离结果的证明无关，而是关键依赖于眼前这个特定的子簇；其思路受到 Haramaty–Shpilka 和 Lampert 在加法群 $\mathrm{Mat}_d(\mathbb{F})$ 中所用论证的启发，而非乘法情形下的论证。第 7 节开头解释了这一联系及其处理方法。

5.3. **最后一步：从可解到阿贝尔。**为结束本节，我们给出一个论证，其思路与第 4 节中的证明类似，并构成定理 1.12 证明的结尾。当假设可解群包含在某个域 $\mathbb{F}$ 上、某个 d 的一般线性群 $\mathrm{GL}_d(\mathbb{F})$ 的博雷尔子群 $\mathcal{B}$ 中时，该结果是定理 1.2 的一个更强版本。我们的界可以依赖于 d，但不依赖于域 $\mathbb{F}$。

引理 5.2。设 A 是一般线性群 $\mathrm{GL}_d(\mathbb{F})$的一个博雷尔子群中的 K-近似子群。存在一个阿贝尔子群 H，它属于一般线性群 $\mathrm{GL}_d(\mathbb{F})$，使得

$$|A^2 \cap H| \geq K^{-33}|A^2|^{1/d^4}.$$

我们用来证明引理 5.2 的论证与证明定理 1.2 时所用的方法相呼应。利用一般线性群 $\mathrm{GL}_d(\mathbb{F})$ 的两个关键性质，我们能够得到关于 $|A^2 \cap H|$ 的多项式界，使其为 H 阿贝尔。其一是：若 $\mathcal{B} \leq \mathrm{GL}_d(\mathbb{F})$ 是博雷尔子群，那么交换子群$[\mathcal{B}, \mathcal{B}]$（由对角线上全为 1 的上三角矩阵构成）是幂零的。其二是以下“有限维”条件。若群 t-中心有界，则称其满足以下条件：假设 $h_1, \dots, h_m \in \mathrm{GL}_d(\mathbb{F})$ 满足，对于每个 $1 \leq k \leq m$，每个 h_k 都是 $C(h_1) \cap \cdots \cap C(h_{k-1})$ 中的非中心元素。那么 $m \leq t$。

引理 5.3. 群 一般线性群$_d(\mathbb{F})$ 是(d^2-1)-中心有界的。

证明。 定义中心有界性所需的 $h_1, \dots, h_m$这一性质，要求 $\{h_k\}$线性无关（作为 $\mathrm{Mat}_d(\mathbb{F})$ 中的元素）；由于它们线性无关且彼此交换，我们得出 $m < d^2$。事实上，如果 h_k是 $\{h_1, \dots, h_{k-1}\}$的线性组合，那么 h_k与一般线性群 $\mathrm{GL}_d(\mathbb{F})$ 中所有满足以下条件的元素交换：它们都与 $h_1, \dots, h_{k-1}$交换，因此 h_k属于 $C(h_1) \cap \cdots \cap C(h_{k-1})$ 的中心。□

我们可以利用这一性质证明以下两个引理，它们的证明非常相似。第一个引理将我们的问题沿导出列“向下推进一级”；在我们的情形中，这足以将问题从可解群缩减到幂零群（因为一般线性群 $\mathrm{GL}_d(\mathbb{F})$ 的博雷尔子群的交换子群是幂零的）。第二个引理利用中心有界性，将幂零群转化为阿贝尔群，其结构与引理 3.7 的证明相似。

引理 5.4。设 G是一个 t-中心有界群，且 A 是 G的一个 K-近似子群。那么存在某个阿贝尔子群 $H \leq G$，使得

$$|A^2 \cap H| \cdot \left(K^{10}|A^2 \cap [G,G]|\right)^t \geq |A^2|.$$

证明。迭代构造一列元素 $h_1, h_2, \ldots \in A^2$，使得对于每个 $k \geq 0$，每个h_{k+1}都是 H_k的非中心元素：$= C(h_1) \cap \cdots \cap C(h_k)$。当无法再作出这样的选择时，终止该序列 $h_1, \ldots, h_m$；此时，集合 $A^2 \cap H_m$ 包含于阿贝尔群 $Z(H_m)$中。

我们应用 y 引理 5.1 得到 $A' := A^2 \cap H_k$ 对每个 k。结合引理 2.13，我们得出

$$|A^4 \cap H_{k+1}| \geq |(A')^2 \cap C(h_{k+1})| \geq \frac{|A'|}{|(A')^3 \cap \mathrm{Conj}(h_{k+1})|}.$$

我们还有

$$|A^8 \cap [G,G]| \geq |(A')^4 \cap \mathrm{Conj}(h_{k+1})h_{k+1}^{-1}| \geq |(A')^3 \cap \mathrm{Conj}(h_{k+1})|.$$

结合上述两个不等式并应用引理 2.13，得到

$$\frac{|A^2 \cap H_k|}{|A^2 \cap H_{k+1}|} \leq K^{10}|A^2 \cap [G,G]|.$$

对所有 $0 \leq k < m$ 将上述不等式相乘，我们得到

$$\frac{|A^2|}{|A^2 \cap H_m|} \leq \left(K^{10}|A^2 \cap [G,G]|\right)^m \leq \left(K^{10}|A^2 \cap [G,G]|\right)^t.$$

结论由此得出。 □

引理 5.5. 设 G 是一个 t-中心有界幂零群。设 A 是 G 的一个 K-近似子群。那么存在某个阿贝尔子群 $H \leq G$，满足

$$|A^2 \cap H| \geq \frac{1}{K^{10}}|A^2|^{1/(t+1)}.$$

证明。设

$$G = G_0 \rhd G_1 \rhd \cdots G_s = \{1\}$$

为 G 的下中心列（因此对每个 $i \geq 0$ 都有 $G_{i+1} = [G_i, G]$；由于 G 是幂零群，该列经过有限步后终止于平凡子群）。迭代选择一列元素 h_1，h_2，$\ldots \in A^2$，使得对每个 $k \geq 0$，每个 h_{k+1} 都是H_k 的非中心元素：$= C(h_1) \cap \cdots \cap C(h_k)$。只要这样的元素存在，我们就要求从 G_i 中选取 h_{k+1}，且使 i 尽可能大，从而

$$A^2 \cap H_k \cap G_{i+1} \subset A^2 \cap Z(H_k). \tag{5.2}$$

当不再存在这样的元素时，终止该序列的构造，并令 m为其长度。此时，我们有 $A^2 \cap H_m \subset A^2 \cap Z(H_m)$。

我们断言，对于每个 $1 \leq k \leq m$,

$$\frac{|A^2 \cap H_k|}{|A^2 \cap H_{k+1}|} \leq K^{10}|A^2 \cap Z(H_k)|. \tag{5.3}$$

为证明这一点，令 $A' := A^2 \cap H_k$，并取满足 $h_{k+1} \in G_i \setminus G_{i+1}$的 i。将引理 5.1 应用于 A' 和 h_{k+1}，得到

$$|(A')^2 \cap C(h_{k+1})| \cdot |(A')^3 \cap \mathrm{Conj}_{H_k}(h_{k+1})| \geq |A'|.$$

现在，我们注意到 $\mathrm{Conj}^{H_k}(h_{k+1})h^{-1}_{k+1} \subset H_k \cap [G, G_i] = H_k \cap G_{i+1}$。由此得到 (5.3)：

$$|A^2 \cap H_k| \leq |A^4 \cap H_{k+1}| \cdot |A^8 \cap H_k \cap G_{i+1}| \leq K^{10}|A^2 \cap H_{k+1}| \cdot |A^2 \cap Z(H_k)|,$$

这里用到了引理 2.13 和 (5.2)。

最后，对每个 $0 \leq k < m$ 将式（5.3）相乘，并利用终止条件 $A^2 \cap H_m \subset A^2 \cap Z(H_m)$，得到

$$|A^2| \leq K^{10m} \prod_{k=0}^{m} |A^2 \cap Z(H_k)| \leq K^{10(m+1)} \left(\max_{\substack{H \leq G \\ H \text{ abelian}}} |A^2 \cap H| \right)^{m+1}.$$

结论由 G的 t-中心有界性得出。 □

引理 5.2 由引理 5.3 至 5.5 合并推出。

引理 *5.2* 的证明。设 $\mathcal{B}$ 是一般线性群 $\mathrm{GL}_d(\mathbb{F})$ 的一个博雷尔子群，且设 $A \subset \mathcal{B}$ 是 $\mathcal{B}$ 的一个 K-近似子群。由引理 5.3 可知，$\mathrm{GL}_d(\mathbb{F})$ 因而 $\mathcal{B}$ 是 (d^2-1)-中心有界的。由引理 5.4 可知，存在某个阿贝尔 $H_1 \leq \mathcal{B}$，使得

$$|A^2 \cap H_1| \cdot \big(K^{10}|A^2 \cap [\mathcal{B},\mathcal{B}]|\big)^{d^2-1} \geq |A^2|.$$

设 $A' := A^2 \cap [\mathcal{B},\mathcal{B}]$；由引理 2.13，$A'$ 是 $[\mathcal{B},\mathcal{B}]$ 的一个 K^3-近似子群。随后我们可将引理 5.5 应用于 A'，从而找到某个阿贝尔子群 $H_2 \leq [\mathcal{B},\mathcal{B}]$，使得

$$|A^2 \cap H_2| \geq \frac{1}{K^3}|(A')^2 \cap H_2| \geq \frac{1}{K^{33}}|A'|^{1/d^2}.$$

合并上述两个不等式可得

$$|A^2| \leq |A^2 \cap H_1| \cdot \Big(K^{10}\big(K^{33}|A^2 \cap H_2|\big)^{d^2}\Big)^{d^2-1} \leq \Big(K^{33} \max_{H \in \{H_1,H_2\}} |A^2 \cap H|\Big)^{d^4}.$$

结论得证。 □

6. Preliminary details of the proof of Theorem 1.12

本节首先介绍我们将在第 6 至 8 节中一直使用的一些记号，并证明一些相关的简单引理。然后，我们陈述引理 6.6；该引理将在第 8 节中证明，是一个“逃离仿射子空间”结果，使我们能够按照第 5.1 节中概述的方法处理 $|A^3 \cap \mathrm{Conj}(a)|$ 较大的情形。最后，我们假设命题 1.13 和引理 6.6 成立，从而推导出定理 1.12；在此过程中，我们反复选取第 5.1 节中所述的“不太不规则”的 $a \in A^2$。

6.1. 矩阵群与线性代数。 为了证明定理 1.12 和命题 1.13，我们需要一些关于矩阵群和代数的事实及记号。[10] 给定域 $\mathbb{F}$ 上的向量空间 V，我们用 $\mathrm{End}(V)$ 表示 V 的自同态（$\mathbb{F}$-）代数，用 $\mathrm{GL}(V)$ 表示 V 的自同构群。我们记 $\mathrm{Mat}_d(\mathbb{F}) := \mathrm{End}(\mathbb{F}^d)$，以及 $\mathrm{GL}_d(\mathbb{F}) := \mathrm{GL}(\mathbb{F}^d)$。下文中，对于矩阵群的一个元素 x，我们用 $\mathsf{m}(x)$ 表示 x 的任一特征子空间的最大维数。

定义 6.1（旗标与稳定子）。设 V 是一个有限维 $\mathbb{F}$-向量空间。其上的一个旗 $\mathcal{F}$ V是由子空间组成的嵌套序列 $\{0\} = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_m = V$。

- 正维向量空间 V 上的平凡旗是序列 $\{0\} \subsetneq V$。
- 若对每个 $1 \leq i \leq m$ 都有 $\dim V_i - \dim V_{i-1} = 1$，则旗 $\mathcal{F}$ 称为完备。
- 若定义 $\mathcal{F}$ 的序列中的每个子空间也出现在定义 $\mathcal{G}$ 的序列中，则旗 $\mathcal{G}$ 是 $\mathcal{F}$ 的细化。
- $\mathcal{F}$ 的稳定子是 $\mathrm{End}(V)$ 的一个分块上三角子代数，定义如下：

$$\{x \in \mathrm{End}(V) : xV_i \subset V_i \text{ for all } i\},$$

  我们将其记作 $\mathbf{P}_{\mathcal{F}}$。
- 我们将 $H_{\mathcal{F}} := \mathbf{P}_{\mathcal{F}} \cap \mathrm{GL}(V)$ 记作 $\mathcal{F}$ 的稳定子的可逆元素。
- 该抛物维数的 $\mathcal{F}$ 为

$$\mathrm{pdim}(\mathcal{F}) := \sum_{i=1}^{m} \big((\dim V_i - \dim V_{i-1})^2 - 1\big).$$

[10]我们的所有 代数都是某个域上的矩阵代数的（不一定含单位元的）子代数，并且矩阵乘法为 是乘积而非李括号。

- 每个$\mathbf{P}_{\mathcal{F}}$的元素都可下降为 V_i/V_{i-1}上的线性映射；由此得到一个映射 $\pi_i\colon \mathbf{P}_{\mathcal{F}} \to \mathrm{End}(V_i/V_{i-1})$。我们在$\mathbf{P}_{\mathcal{F}}$上定义向量值迹 为
$$\mathrm{vtr}_{\mathcal{F}}(x) := (\operatorname{tr}\pi_1(x), \operatorname{tr}\pi_2(x), \dots, \operatorname{tr}\pi_m(x)).$$
由于每个 π_i 都是一个 $\mathbb{F}$-代数同态，$\mathrm{vtr}_{\mathcal{F}}$ 是 $H_{\mathcal{F}}$上的类函数。
- 对于任意仿射子空间 $\mathbf{V} \subset \mathbf{P}_{\mathcal{F}}$，我们将-维数 $\mathcal{F}$定义为 $\mathbf{V}$
$$\dim_{\mathcal{F}} \mathbf{V} := \sum_{i=1}^{m} (\dim \pi_i(\operatorname{span}\mathbf{V}) - 1).$$
我们注意到 $\dim_{\mathcal{F}} \mathbf{P}_{\mathcal{F}} = \mathrm{pdim}(\mathcal{F})$。

我们常按以下方式细化旗：若在某个向量空间 V上有一面旗 $\mathcal{F} = (V_0, V_1, \dots, V_m)$，并且在某个商群 V_i/V_{i-1}上有一面旗 $\mathcal{F}_i = (W_0, \dots, W_k)$，则对$\mathcal{F}$进行 $\mathcal{F}_i$ 细化后得到的旗，是在 V_{i-1} 与 V_i之间插入 $V_{i-1} + \mathcal{F}_i$；即，
$$\begin{aligned}\{0\} = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{i-1} &= V_{i-1} + W_0 \\ &\subsetneq V_{i-1} + W_1 \subsetneq \cdots \subsetneq V_{i-1} + W_{k-1} \\ &\subsetneq V_{i-1} + W_k = V_i \subsetneq V_{i+1} \subsetneq \cdots \subsetneq V_k = V.\end{aligned}$$
若 $\mathcal{F}$是平凡旗，则 $H_{\mathcal{F}}$ =是 $\mathbb{F}$上的一般线性群 $\mathrm{GL}_d(\mathbb{F})$；而若 $\mathcal{F}$是完全旗，则 $H_{\mathcal{F}}$ 是 $\mathrm{GL}_d(\mathbb{F})$的一个博雷尔子群。我们的工作大多将在子群 $H_{\mathcal{F}}$ 中进行，其中的旗 $\mathcal{F}$ 起初是平凡旗，并在迭代过程中不断细化。读者不妨记住模型情形：$\mathcal{F}$是平凡旗 $\{0\} \subset \mathbb{F}^d$。

在 A^3 包含许多具有固定迹的元素时，下面的引理将对我们有所帮助。

引理 6.2. 设$\mathbf{V}$、$\mathbf{W} \subset \mathrm{Mat}_d(\mathbb{F})$ 为仿射子空间，并设 $t \in \mathbb{F}$。假设对于所有 $x \in \mathbf{V}$ 和 $y \in \mathbf{W}$，均有$\operatorname{tr}(xy) = t$。那么
$$\dim \operatorname{span}(\mathbf{V}) + \dim \operatorname{span}(\mathbf{W}) \leq d^2 + 1.$$

证明。对于所有 $x \in \mathbf{V}$ 和 $y \in \mathbf{W}$，条件 $\mathrm{tr}(xy) = t$ 意味着，对于每个$z \in \operatorname{span}\mathbf{V}$和 $w \in \mathbf{W} - \mathbf{W}$，均有 $\mathrm{tr}(zw) = 0$。$\operatorname{span}\mathbf{V}$和$\mathbf{W} - \mathbf{W}$都是 $\mathrm{Mat}_d(\mathbb{F})$ 的真正子空间，并且关于 Frobenius 内积彼此正交。由于 Frobenius 内积是非退化的，我们得出
$$\dim \operatorname{span}(\mathbf{V}) + \dim(\mathbf{W} - \mathbf{W}) \leq d^2.$$
结论现由以下事实得出：$\operatorname{span}\mathbf{W}$ 由$\mathbf{W} - \mathbf{W}$ 以及$\mathbf{W}$中的任意一个固定元素 w_0 张成，因此 $\dim(\mathbf{W} - \mathbf{W}) + 1 \geq \dim \operatorname{span}\mathbf{W}$。□

我们需要处理 $\mathrm{Mat}_d(\mathbb{F})$ 中仿射子空间的乘法结构。对于仿射子空间 $\mathbf{V}$，$\mathbf{W} \subset \mathrm{Mat}_d(\mathbb{F})$，定义
$$\begin{aligned}\mathrm{L}^*(\mathbf{W} \to \mathbf{V}) &:= \{x \in \mathrm{Mat}_d(\mathbb{F}) : x\mathbf{W} \subset \mathbf{V}\}; \\ \mathrm{R}^*(\mathbf{W} \to \mathbf{V}) &:= \{x \in \mathrm{Mat}_d(\mathbb{F}) : \mathbf{W}x \subset \mathbf{V}\}.\end{aligned}$$
对于非交换环 R，子集 $S \subset R$ 的双侧平移 是形如 aSb 的集合，其中可逆元为$a, b \in R^{\times}$。

我们将用到以下三个关于 L* 和 R* 的简单引理。

引理 6.3。若$\mathbf{V}$ 和$\mathbf{W}$ 是$\mathrm{Mat}_d(\mathbb{F})$的仿射子空间，那么$\mathrm{L}^*(\mathbf{W} \to \mathbf{V})$ 和$\mathrm{R}^*(\mathbf{W} \to \mathbf{V})$是$\mathrm{Mat}_d(\mathbb{F})$的仿射子空间。

证明。设 x_1，$x_2 \in \mathrm{Mat}_d(\mathbb{F})$ 满足 $x_1\mathbf{W}$ $x_2\mathbf{W} \subset \mathbf{V}$。那么，对于每个 $\lambda \in \mathbb{F}$ ，
$$(\lambda x_1 + (1-\lambda)x_2)\mathbf{W} \subset \lambda x_1\mathbf{W} + (1-\lambda)x_2\mathbf{W} \subset \lambda\mathbf{V} + (1-\lambda)\mathbf{V} \subset \mathbf{V}.$$
这意味着 L*($\mathbf{W} \to \mathbf{V}$) 是 $\mathrm{Mat}_d(\mathbb{F})$ 的仿射子空间；R* 的证明完全相同。 □

引理 6.4。 设 $\mathbf{V}$ 和$\mathbf{W}$ 是 $\mathrm{Mat}_d(\mathbb{F})$ 的仿射子空间。如果$\mathbf{W}$ 包含一个可逆元素，那么$\mathrm{L}^*(\mathbf{W} \to \mathbf{V})$ 包含于$\mathbf{V}$的某个右平移中。如果$\mathrm{L}^*(\mathbf{W} \to \mathbf{V})$ 包含一个可逆元素，那么$\mathbf{W}$ 包含于$\mathbf{V}$的某个左平移中。将L^*替换为R^*，并将“左”和“右”互换后，同样的两个性质仍然成立。

证明。 取 $a \in \mathbf{W}$ （分别地， $b \in \mathbf{L^*(W \to V)}$）为可逆的，则有 $\mathbf{L^*(W \to V)} \subset \mathbf{V}a^{-1}$ （分别地，$\mathbf{W} \subset b^{-1}\mathbf{V}$）。$\mathbf{R^*}$ 的证明相同。□

引理 6.5。 设 $\mathbf{V}$ 和 $\mathbf{W}$ 是$\mathrm{Mat}_d(\mathbb{F})$中的真仿射子空间，并假设$\mathbf{W}$ 包含一个可逆元素。那么

$$\dim \mathrm{L}^*(\mathbf{W} \to \mathbf{V}) \le \dim \mathbf{V}. \tag{6.1}$$

此外，假设 (6.1) 中等式成立，且$\mathbf{V}$ 包含一个可逆元素。那么存在$\mathrm{Mat}_d(\mathbb{F})$ 的一个子代数 $\mathbf{U}$，使得 ***(i)*** $(1+\mathbf{U}) \cap$ 一般线性群$_d(\mathbb{F})$ 是一般线性群$_d(\mathbb{F})$的一个子群，[11] ***(ii)*** $\mathbf{W}$ 包含于 $1+\mathbf{U}$ 的某个左平移中，且 ***(iii)*** $1+\mathbf{U}$ 包含于$\mathbf{V}$的某个左平移中。

证明。 为简化记号，记 $\mathbf{X} := \mathbf{L^*(W \to V)}$。设 $a \in \mathbf{W}$ 是某个可逆元素。由 $x \mapsto xa$ 给出的映射 $\mathbf{X} \to \mathbf{V}$ 是一个单射线性映射，由此可得 (6.1)。现在，假设等式成立。我们有

$$\mathbf{W} \subset \mathrm{R}^*(\mathbf{X} \to \mathbf{V}) = a^{-1}\,\mathrm{R}^*(\mathbf{X}a \to \mathbf{V}) = a^{-1}\,\mathrm{R}^*(\mathbf{V} \to \mathbf{V}),$$

其中，最后一个等式成立是因为 $\dim \mathbf{X} = \dim \mathbf{V}$。现在，令 $\mathbf{U} := \mathbf{R^*(V \to V)} - 1$。由引理 6.4, $1+\mathbf{U}$ 包含于$\mathbf{V}$的某个左平移中。由于 $\mathbf{R^*(V \to V)}$包含单位元，且由引理 6.3可知它是 $\mathrm{Mat}_d(\mathbb{F})$中的一个仿射子空间，故$\mathbf{U}$ 是 $\mathrm{Mat}_d(\mathbb{F})$的真正子空间。它在乘法下也封闭：若 $x, y \in \mathbf{U}$，则

$$x + y + xy = (1+x)(1+y) - 1 \in \mathrm{R}^*(\mathbf{V} \to \mathbf{V}) - 1 = \mathbf{U},$$

因此 $xy \in \mathbf{U}$。所以$\mathbf{U}$是 $\mathrm{Mat}_d(\mathbb{F})$的一个子代数，集合 $1+\mathbf{U}$包含于$\mathbf{V}$的某个左平移中，而$\mathbf{W}$ 包含于 $a^{-1}(1+\mathbf{U})$中，如所求。□

6.2. **定理 1.12 的部分证明**。 我们现在证明定理 1.12，但暂不证明命题 1.13及以下引理。

引理 6.6 (子空间到旗标引理)。 设 d 为一个正整数，并设 $\mathcal{F} = (V_0, V_1, \dots, V_m)$ 是 $\mathbb{F}^d$ 上的一个旗，其抛物维数为 D。设 A 为 K-近似子群，且 $H_{\mathcal{F}}$ 并令$\eta > 0$。假设对于某个 $\mathbf{t} \in \mathbb{F}^m$，有

$$\frac{|A^2 \cap \mathrm{vtr}_{\mathcal{F}}^{-1}(\mathbf{t})|}{|A^2|} \ge \eta.$$

那么存在 $\mathcal{F}$ 的某个细化 $\mathcal{G}$，其抛物维数至多为 $\frac{1}{\sqrt{2}}D$，并且满足

$$\frac{|A^2 \cap H_{\mathcal{G}}|}{|A^2|} \ge \Big(\frac{\eta}{2K}\Big)^{5d^6}.$$

这个引理将是第 8 节的主要结果之一，并将由一个更一般的“子空间到子群”引理推出。我们用它来处理引理 5.1 中出现的$|A^3 \cap \mathrm{Conj}(a)|$ 较大的情形。

为了证明定理 1.12，我们还需要下面这个引理，它说明了在 $|A^2 \cap C(a)|$ 较大的情形下，我们能获得多少提升。

引理 6.7. 对于每个 $a \in$ 一般线性群$_d(\mathbb{F})$，都存在某个旗 $\mathcal{F}$，其抛物维数至多为$d \cdot \mathsf{m}(a) - 1$，使得 $C(a) \subset H_{\mathcal{F}}$。

[11]事实上，这个条件可由 $\mathbf{U}$ 是 $\mathrm{Mat}_d(\mathbb{F})$ 的子代数这一事实推出。不过，由于它直接源自我们在此构造 $\mathbf{U}$ 的方式，我们更愿意直接将其写入引理的陈述中。

证明. 对于每个 λ，令 t_λ 表示 a 中具有特征值 λ的最大若尔当块的大小。对于每个$0 \le i \le t_\lambda$，令 $V_\lambda^i := \ker((a-\lambda)^i)$ 为 a 中具有特征值 λ且秩至多为 i的广义特征向量空间。对于任意 $v \in V_\lambda^i$ 以及任意 $b \in C(a)$,

$$(a-\lambda)^i bv = b(a-\lambda)^i v = 0,$$

所以 $bv \in V_\lambda^i$。因此 $C(a)$ 保持每个 V_λ^i 不变。

现在我们构造旗 $\mathcal{F}$。首先，任意将 a 的特征值排序为 λ_1、…、λ_m，并定义旗

$$\mathcal{F}' := \left(\{0\}, V_{\lambda_1}^{t_{\lambda_1}}, V_{\lambda_1}^{t_{\lambda_1}} + V_{\lambda_2}^{t_{\lambda_2}}, \dots, V_{\lambda_1}^{t_{\lambda_1}} + V_{\lambda_2}^{t_{\lambda_2}} + \cdots + V_{\lambda_{m-1}}^{t_{\lambda_{m-1}}}, \mathbb{F}^d\right)$$

使得 $\mathcal{F}'$ 中相邻子空间之间的商群自然地对应于广义特征子空间 $V_{\lambda_j}^{t_{\lambda_j}}$。接着，依次用以下旗细化 $\mathcal{F}'$

$$\mathcal{F}_j := \left(\{0\}, V_{\lambda_j}^1, V_{\lambda_j}^2, \dots, V_{\lambda_j}^{t_{\lambda_j}}\right)$$

对每个 $1 \le j \le m$，构造旗 $\mathcal{F}$。由于 $C(a)$ 保持每个 V_λ^i 不变，我们得出 $C(a) \subset H_{\mathcal{F}}$。此外，我们有

$$\operatorname{pdim} \mathcal{F} = \sum_{\lambda \text{ eig. of } a} \sum_{i=1}^{t_\lambda} \left(\dim(V_\lambda^i / V_\lambda^{i-1})^2 - 1\right) \le d\left(\max_{\lambda,i} \dim(V_\lambda^i / V_\lambda^{i-1})\right) - 1. \tag{6.2}$$

最后，由 $v \mapsto (a-\lambda)v$ 给出的映射 $V_\lambda^{i+1}/V_\lambda^i \to V_\lambda^i / V_\lambda^{i-1}$ 对每个 $i \ge 1$ 都是单射，因此当 $i = 1$ 时，维数 $\dim(V_\lambda^i / V_\lambda^{i-1})$ 取最大值。对于每个 λ，此维数至多为 $\mathrm{m}(a)$。因此，结论由 (6.2) 得出。□

最后，我们需要命题 1.13 的一个推论。

引理 6.8。设 $d \ge 8000$，且设 $A \subset$ 一般线性群$_d(\mathbb{F})$ 是一个 K-近似子群。设 $\delta \in (0,1]$ 是一个参数。那么以下情形之一成立：

- （不太不规则的元素）对于多于 $(1-\delta)|A^2|$ 个元素 $a \in A^2$，有 $\mathrm{m}(a) \le d(1 - \frac{1}{1200 \log\log d})$。
- （由良性子群控制）存在两个子空间 $V_1 \subset V_2 \subset \mathbb{F}^d$，满足 维数 $V_2 > \frac{9d}{10}$ 且 维数$V_1 < \frac{d}{10}$，使得至少 $(2K^8\delta^{-1})^{-3d^6}|A^2|$ 个 A^2 中的元素 a 满足以下性质：存在某个 $\lambda \in \mathbb{F}$，使得 $(a-\lambda)V_2 \subset V_1$。

证明。令 B为满足 $\mathrm{m}(a) \le d(1 - \frac{1}{1200 \text{双对数 } d})$ 的元素 $a \in A^2$ 所成的集合；集合 B 含单位元。若 $|B| \le \delta|A^2|$，则不太不规则的元素的结论成立。否则，Ruzsa 覆盖引理表明，B^4 可由至多 $|B^5|/|B| \le K^8\delta^{-1}$ 个 B^2 的平移覆盖，因此 B^2 是一个$K^8\delta^{-1}$-近似群。此外，B^2 中的每个元素都有一个余维数至多为 600^d 双对数 d 的特征子空间。因此，我们可以将命题 1.13 应用于 B^2，从而得到存在两个子空间$V_1 \subset V_2 \subset \mathbb{F}^d$，其维数满足 $\dim V_2 > \frac{9d}{10}$ 和 $\dim V_1 < \frac{d}{10}$，并且满足以下条件：若 $H \le \mathrm{GL}_d(\mathbb{F})$ 是由满足下述条件的元素 g 构成的子群：存在一个标量 $\lambda \in \mathbb{F}$，使得 $(g-\lambda)V_2 \subset V_1$，那么

$$|B^4 \cap H| \ge (2K^8\delta^{-1})^{-2d^6}|B^4|.$$

由引理 2.13 可得

$$|A^2 \cap H| \ge K^{-7}|A^8 \cap H| \ge K^{-7}|B^4 \cap H| \ge K^{-7}(2K^8\delta^{-1})^{-2d^6}|B^4| \ge K^{-7}(2K^8\delta^{-1})^{-2d^6}\delta|A^2|.$$

结论得证。□

现在我们开始证明定理 1.12。根据引理 5.2，只需找到一般线性群$_d(\mathbb{F})$的一个博雷尔子群，使其与 A^2有较大的交集。我们通过逐步考察子群 $H_{\mathcal{F}} \le$ 一般线性群$_d(\mathbb{F})$来进行迭代，并在每一步细化 $\mathcal{F}$。下面的技术引理描述了这一迭代过程。

引理 6.9。设 A 是一般线性群$_d(\mathbb{F})$的一个 K-近似子群，设 $\mathcal{F}$ 是 $\mathbb{F}^d$ 上的一面旗，其抛物维数为 $D>0$，并设 $\lambda,\varepsilon>0$ 满足

$$|A^2\cap H_{\mathcal{F}}|\geq\frac{1}{(2K)^{\lambda}}|A^2|^{\varepsilon}.$$

令 $\gamma=\min(1\,8000,1\,1200\log\log d)$ 若 $d>2$ 且 $\gamma=\frac{1}{4}$，否则。取满足条件的三元组 $(D',\lambda',\varepsilon')$

$$(D',\lambda',\varepsilon')\in\left\{\big(D-1,\lambda+85d^7,\varepsilon\big),\quad\left(\left\lfloor\frac{1}{\sqrt{2}}D\right\rfloor,\lambda+165d^6,\frac{\varepsilon}{2}\right),\quad\left(\lfloor(1-\gamma)D\rfloor,7,\frac{\varepsilon}{10d^6}\right)\right\}$$

存在 $\mathcal{F}$ 的一个细化 $\mathcal{G}$，满足 $\operatorname{pdim}\mathcal{G}\leq D'$ 且 $|A^2\cap H_{\mathcal{G}}|\geq\ {}^{1}\,(2K)_{\lambda'}\,|A^2|^{\varepsilon'}$。

在假设引理 *6.6* 和命题 *1.13* 成立的情况下，引理 *6.9* 的证明。记 $\mathcal{F}=(V_0,V_1,\dots,V_m)$，并令 π_i: $\mathbf{P}_{\mathcal{F}}\to\mathsf{End}(V_i/V_{i-1})$ 为自然环同态。记 $d_i:=\dim V_i-\dim V_{i-1}$，使得 $d_1+\cdots+d_m=d$。对于每个 i，记 Z_i 为 $\mathsf{GL}(V_i/V_{i-1})$ 的中心。最后，选取 $\delta:=(dK^{12})^{-1}$。

对于每个 $1\leq i\leq m$，集合 $B_i:=\pi_i(A^2\cap H_{\mathcal{F}})\subset\mathsf{GL}(V_i/V_{i-1})$ 是一个 K^3-近似群，由引理 2.13 得出。因此，对于每个 i，以下情况之一成立（在大型 d_i 情形下，我们应用引理 6.8）：
(1) $d_i=1$；(2) $1<d_i<8000$，且 (a) $|B_i^2\cap Z_i|\geq\delta|B_i^2|$，或者 (b) 对于严格多于 $(1-\delta)|B_i^2|$ 个元素 $b\in B_i^2$，有 $\mathsf{m}(b)\leq d_i-1$；或者 (3) $d_i\geq8000$，并且

(a) 存在某个关于 V_i/V_{i-1} 的旗 $\mathcal{F}_i$，满足[12] $\operatorname{pdim}\mathcal{F}_i\leq\frac{1}{50}(d_i^2-1)$，并且

$$|B_i^2\cap H_{\mathcal{F}_i}|\geq(2K^{24}\delta^{-1})^{-2d_i^6}|B_i^2|,$$

or

(b) 对于 strictly more than $(1-\delta)|B_i^2|$ elements $b\in B_i^2$, we have $\mathsf{m}(b)\leq d_i\Big(1-\frac{1}{1200\log\log d_i}\Big)$.

若某个 i: 满足 (2a) 或 (3a)，则无论哪种情况，我们都有某个 $1\leq i\leq m$ 以及一个关于V_i/V_{i-1} 的旗 $\mathcal{F}_i$（在 (2a) 的情形下，这是一个完全旗），满足 $\operatorname{pdim}\mathcal{F}_i\leq d_i^2-2$，并且

$$\frac{|B_i^2\cap H_{\mathcal{F}_i}|}{|B_i^2|}\geq\frac{\delta^{2d^6}}{(2K)^{48d^6}}.$$

将引理 2.15 应用于 K^3-近似子群 $A^2\cap H_{\mathcal{F}}$ 和投影映射 π_i，可得，事实上，

$$\frac{\delta^{2d^6}}{(2K)^{48d^6}}\leq\frac{|(A^2\cap H_{\mathcal{F}})^6\cap\pi_i^{-1}(H_{\mathcal{F}_i})|}{|(A^2\cap H_{\mathcal{F}})^2|}\leq\frac{|A^{12}\cap\pi_i^{-1}(H_{\mathcal{F}_i})|}{|A^2\cap H_{\mathcal{F}}|}.$$

令 $\mathcal{G}$ 为将 $\mathcal{F}$ 用 $\mathcal{F}_i$ 加细后得到的旗，使得 $H_{\mathcal{G}}=\pi_i^{-1}(H_{\mathcal{F}_i})$。利用引理 2.13，我们得到

$$\frac{\delta^{2d^6}}{(2K)^{48d^6}}\leq K^{11}\frac{|A^2\cap H_{\mathcal{G}}|}{|A^2\cap H_{\mathcal{F}}|}.$$

利用我们对 δ 的选择以及不等式 $2^d>d$，可得

$$|A^2\cap H_{\mathcal{G}}|\geq\frac{\delta^{2d^6}}{(2K)^{48d^6+11}}|A^2\cap H_{\mathcal{F}}|\geq\frac{1}{(2K)^{72d^6+2d^7+11}}|A^2\cap H_{\mathcal{F}}|\geq\frac{1}{(2K)^{85d^7+\lambda}}|A|^{\varepsilon}.$$

由此得到关于 $D'=D-1$、$\lambda'=\lambda+85d^7$ 和 $\varepsilon'=\varepsilon$ 的结果。

[12]按照引理 6.8 中的记号，这个旗是将旗 $\{0\}\subsetneq V_1\subsetneq V_2\subsetneq\mathbb{F}^{d_i}$ 用 V_2/V_1 上的任意完全旗加细后得到的。界 $\operatorname{pdim}\mathcal{F}_i\leq\frac{1}{50}(d_i^2-1)$ 由 $\dim V_1<\frac{d_i}{10}<\frac{9d_i}{10}<\dim V_2$ 这一事实可得。

如果对每个 i，(1)、(2b) 或 (3b) 成立： 对每个 i，定义

$$e_i := \begin{cases} 1 & \text{if } d_i = 1 \\ d_i - 1 & \text{if } d_i < 8000 \\ d_i - \frac{d_i}{1200 \log\log d_i} & \text{if } d_i \geq 8000, \end{cases}$$

并令 $S_i := \{b \in \text{一般线性群}(V_i/V_{i-1}) : \mathrm{m}(b) > e_i\}$。对于每个 i，我们都有 $|B_i^2 \cap S_i|/|B_i^2| < \delta$。将引理 2.15 应用于 K^3-近似子群 $A^2 \cap H_{\mathcal{F}}$ 和投影映射 π_i，可得

$$\frac{|(A^2 \cap H_{\mathcal{F}})^2 \cap \pi^{-1}(S_i)|}{|(A^2 \cap H_{\mathcal{F}})^2|} \leq K^{12} \frac{|B_i^2 \cap S_i|}{|B_i^2|} < K^{12}\delta = \frac{1}{d}.$$

由于 $m \leq d$，由并集界可知，存在某个 $a_0 \in (A^2 \cap H_{\mathcal{F}})^2$，使得对于任意 $1 \leq i \leq m$，都有 $\pi(a_0) \notin S_i$，即对于每个 i，$\mathrm{m}(\pi(a_0)) \leq e_i$。令 $B := (A^2 \cap H_{\mathcal{F}})^2$。由于 $A^2 \cap H_{\mathcal{F}}$ 是一个K^3-近似群，B 是一个 K^6-近似群。

现在应用引理 5.1，可得

$$|B^2 \cap C(a_0)| \cdot |B^3 \cap \mathrm{Conj}(a_0)| \geq |B|.$$

令 $\eta := |A|^{-\varepsilon/(10d^6)}$ 为一个参数。以下两种情况之一成立：

(i) $|B^3 \cap$猜想$(a_0)| \geq \eta |B|$

或 (ii) $|B^2 \cap C(a_0)| \geq 1/\eta$。

若情形 (i) 成立： 令 $\mathbf{t} := \mathrm{vtr}_{\mathcal{F}}(a_0)$，使得 $\mathrm{Conj}(a_0) \subset \mathrm{vtr}_{\mathcal{F}}^{-1}(\mathbf{t})$。令 $\tilde{B} := B^2$ 为一个 K^{12}-近似群。我们有

$$\frac{|\tilde{B}^2 \cap \mathrm{vtr}_{\mathcal{F}}^{-1}(\mathbf{t})|}{|\tilde{B}^2|} \geq \frac{|B^3 \cap \mathrm{Conj}(a_0)|}{|B^4|} \geq \frac{\eta}{K^{18}}.$$

因此，我们可以对 $H_{\mathcal{F}}$ 的 K^{12}-近似子群 $\tilde{B}$ 应用引理 6.6，找到 $\mathcal{F}$ 的某个细化 $\mathcal{G}$，其抛物维数至多为 $\frac{1}{\sqrt{2}}D$，且满足

$$\frac{|\tilde{B}^2 \cap H_{\mathcal{G}}|}{|\tilde{B}^2|} \geq \left(\frac{\eta}{2K^{30}}\right)^{5d^6}.$$

利用引理 2.13 将此不等式展开为关于 A 的陈述，得到

$$\left(\frac{\eta}{2K^{30}}\right)^{5d^6} \leq \frac{|\tilde{B}^2 \cap H_{\mathcal{G}}|}{|\tilde{B}^2|} \leq \frac{|A^{16} \cap H_{\mathcal{G}}|}{|A^2 \cap H_{\mathcal{F}}|} \leq \frac{K^{15}|A^2 \cap H_{\mathcal{G}}|}{|A^2 \cap H_{\mathcal{F}}|}.$$

我们得出

$$|A^2 \cap H_{\mathcal{G}}| \geq \frac{\eta^{5d^6}}{(2K)^{150d^6+15}} |A^2 \cap H_{\mathcal{F}}| \geq \frac{1}{(2K)^{165d^6+\lambda}} |A|^{\varepsilon/2}.$$

这就得到了结果，其中 $D' = \frac{1}{\sqrt{2}}D$，$\lambda' = \lambda + 165d^6$ 和 $\varepsilon' = \varepsilon/2$。

若情形 (ii) 成立： 对每个 i，由引理 6.7，$\pi_i(C_{H_{\mathcal{F}}}(a_0)) = C_{\mathrm{GL}(V_i/V_{i-1})}(\pi_i(a_0))$ 包含于某个旗 $\mathcal{F}_i$ 对应的 $H_{\mathcal{F}_i}$ 中，其抛物维数至多为 $d_i e_i - 1$。我们选择 $\gamma = 1/4$；若 $d \leq 2$，则取 $\gamma = \min(\frac{1}{8000}, \frac{1}{1200 \log\log d})$，否则取其他值；这足以保证，只要 $d_i > 1$，就有 $e_i \leq (1-\gamma)d_i$。因此，对于每个 i（包括满足 $d_i = 1$ 的那些 i），都有 $d_i e_i - 1 \leq (1-\gamma)(d_i^2 - 1)$。由此，对所有 $\mathcal{F}_i$ 进行细化 $\mathcal{G}$ $\mathcal{F}$ 所得的结果满足

$$\mathrm{pdim}\, \mathcal{G} = \sum_{i=1}^{m} \mathrm{pdim}\, \mathcal{F}_i \leq (1-\gamma)\, \mathrm{pdim}\, \mathcal{F}$$

以及 $H_{\mathcal{G}} = \bigcap_{i=1}^{m} \pi_i^{-1}(H_{\mathcal{F}_i})$。这意味着 $C(a_0) \subset H_{\mathcal{G}}$。利用引理 2.13，我们得出

$$|A^2 \cap H_{\mathcal{G}}| \geq |A^2 \cap C(a_0)| \geq K^{-7}|A^8 \cap C(a_0)| \geq K^{-7}|B^2 \cap C(a_0)| \geq \frac{1/\eta}{K^7} = K^{-7}|A|^{\varepsilon/(10d^6)}.$$

由此可得结果，其中 $D' = (1-\gamma)D$、 $\lambda' = 7$ 和 $\varepsilon' = \varepsilon/(10d^6)$。 □

最后，我们可以使用引理 6.9 中描述的迭代来证明定理 1.12。

在引理 *6.6* 和命题 *1.13* 的假设下证明定理 *1.12*。若 $d = 1$，则结果可由取 $H =$ 一般线性群$_1(\mathbb{F})$ 得出，因此以下假设 $d > 1$。我们从一个 K-近似群$A \subset$ 一般线性群$_d(\mathbb{F})$ 开始。将 $\mathcal{F}_0 := (\{0\}, \mathbb{F}^d)$ 初始化为平凡旗。同时将 $D_0 := d^2 - 1$ 、 $\lambda_0 := 0$ 和 $\varepsilon_0 := 1$ 初始化。由 $(\mathcal{F}_i, D_i, \lambda_i, \varepsilon_i)$，我们将找到 $(\mathcal{F}_{i+1}, D_{i+1}, \lambda_{i+1}, \varepsilon_{i+1})$，并保持以下性质：$\operatorname{pdim} \mathcal{F}_i \le D_i$ 且

$$|A^2 \cap H_{\mathcal{F}_i}| \ge \frac{1}{(2K)^{\lambda_i}} |A^2|^{\varepsilon_i}. \tag{6.3}$$

$(\mathcal{F}_{i+1}, D_{i+1}, \lambda_{i+1}, \varepsilon_{i+1})$ 的构造是通过将引理 6.9 应用于 $(\mathcal{F}_i, D_i, \lambda_i, \varepsilon_i)$ 得到的。序列 $\{D_i\}$ 在 i 中严格递减，因此对某个 $\ell < d^2$，有 $D_\ell = 0$；当这种情况首次出现时，我们便终止该过程。条件 $D_\ell = 0$ 意味着 $\mathcal{F}_\ell$ 是一个完全旗，因此 $H_{\mathcal{F}_\ell}$ 是博雷尔子群。根据引理 2.13， $A^2 \cap H_{\mathcal{F}_\ell}$ 是一般线性群$_d(\mathbb{F})$ 的一个 K^3-近似子群。因此，我们可以使用引理 5.2 找到一般线性群$_d(\mathbb{F})$ 的某个阿贝尔子群 H，并且由 (6.3)，

$$|A^2 \cap H| \ge K^{-3} |(A^2 \cap H_{\mathcal{F}_\ell})^2 \cap H| \ge K^{-102} |A^2 \cap H_{\mathcal{F}_\ell}|^{1/d^4} \ge \frac{1}{(2K)^{\lambda_\ell + 102}} |A^2|^{d^{-4}\varepsilon_\ell}.$$

因此，剩下的就是对 λ_ℓ 给出上界，并对 ε_ℓ 给出下界。

为了给 λ_ℓ 限定上界，我们注意到，对于每个 i，都有 $\lambda_{i+1} - \lambda_i \le 165d^7$。因此， $\lambda_\ell = \lambda_\ell - \lambda_0 \le 165d^9$。为了给 ε_ℓ 限定上界，我们注意到，只要 $D_{i+1} = D_i - 1$，就有 $\varepsilon_{i+1} = \varepsilon_i$。因此，只要 $\varepsilon_{i+1} < \varepsilon_i$，我们就有 $D_{i+1}/D_i \le 1 - \gamma$，其中，如果 $d > 2$，则 ~~$\gamma = \min(\frac{1}{8000}, \frac{1}{200 \log\log d})$~~，否则为 $\gamma = 1/4$。此外，在每个这样的步骤中， ε_i至多只能减少一个 $10d^6$ 的因子。由于 $D_{\ell-1} \ge 1$，我们得出

$$\varepsilon_\ell \ge \frac{\varepsilon_{\ell-1}}{10d^6 \varepsilon_0} \ge \left(\frac{1}{10d^6}\right)^{1+\log_{1-\gamma}(d^2)} \ge \exp\left(-\frac{80 \log^2 d}{\gamma}\right).$$

这足以得到该结果。 □

7. Not-too-irregular elements in matrix groups

本节旨在证明命题 1.13 的以下弱版本。我们用 $\operatorname{rk} m$ 表示矩阵 m 的秩。[13]

引理 7.1。 设 $d, s \ge 6$，且 $A \subset$ 一般线性群$_d(\mathbb{F})$ 是一个 K-近似子群。假设 A^2 中的每个元素 a 都满足 $\operatorname{rk}(a-1) \le s$。那么存在 $\mathbb{F}^d$ 的子空间 U 和 W，满足维数 U，维数 $W \le 30s$ 对数的对数 s，使得至少有 $(2K)^{-60s}|A^2|$ 个元素 $a \in A^2$ 满足 $(a-1)W^\perp \subset U$。

我们将在下一节把这一结论提升为命题 1.13。

我们对引理 7.1 的证明大致遵循 Haramaty 和 Shpilka [HS10]在加法情形下提出的迭代过程。文献中与我们的方法最相近的类似命题，是 Lampert 的以下引理；它与 [HS10, 引理 3.5]相当相关。

引理 7.2 （ [Lam25, 引理 2。3]的弱版本。 设 $\mathbf{X} \subset \operatorname{Mat}_d(\mathbb{F})$ 是一个子空间，并假设对每个 $x \in \mathbf{X}$，都有 $\operatorname{rk} x \le r$。那么存在 $\mathbb{F}^d$ 的子空间 U和 W，满足 维数 U，维数 $W \le 2r$，使得 $\mathbf{X}W^\perp \subset U$。

引理 7.1 中的情形与引理 7.2 中的情形类似。主要区别在于，我们的集合 A 具有丰富的乘法结构，而不是拥有一个具有丰富加法结构的低秩算子集合。这使我们的论证复杂得多，并最终导致了引理 7.1 中的 $\log\log s$项。

[13]在本节中，我们为每个向量空间赋予内积结构，以便可以方便地讨论正交补。这仅仅是为了记号上的便利；我们的结果均不实质依赖于所选的内积结构。

我们先介绍线性代数中的以下简单事实，它本质上是对 [HS10 引理 3.5] 的证明中一项计算的“无坐标”版本。

引理 7.3。设 x、y：$U \to W$ 为线性算子。我们有

$$\dim(\operatorname{im} x + \operatorname{im} y) + \dim\big((\ker x)^\perp + (\ker y)^\perp\big) \le \operatorname{rk} x + \operatorname{rk} y + \operatorname{rk}(x+y).$$

证明。映射 x 经过一个维数为 $\operatorname{rk} x$ 的向量空间进行分解。因此，我们可以找到一个维数为 $\operatorname{rk} x$ 的向量空间 V_x、一个满射 m_x：$U \twoheadrightarrow V_x$，以及一个单射 n_x：$V_x \hookrightarrow W$，使得 $x = n_x m_x$。类似地定义 V_y、m_y 和 n_y。令 $V := V_x \oplus V_y$，并考虑由 $mu = (m_x u,\ m_y u)$ 和 $n(v_x,\ v_y) = n_x v_x + n_y v_y$ 定义的映射 m：$U \to V$ 和 n：$V \to W$。我们有 $nm = x + y$。因此，我们可以写成

$$\begin{aligned}
\dim\ker(x+y) &= \dim\ker(nm) \\
&\le \dim\ker n + \dim\ker m \\
&= \dim V - \dim\operatorname{im} n + \dim(\ker m_x \cap \ker m_y) \\
&= \dim V_x + \dim V_y - \dim(\operatorname{im} n_x + \operatorname{im} n_y) + \dim(\ker x \cap \ker y) \\
&= \operatorname{rk} x + \operatorname{rk} y - \dim(\operatorname{im} x + \operatorname{im} y) + \dim U - \dim\big((\ker x \cap \ker y)^\perp\big).
\end{aligned}$$

上式左侧为 $\dim U - \operatorname{rk}(x+y)$。因此，利用以下事实：对于 U 的子空间 U_1 和 U_2，有 $(U_1 \cap U_2)^\perp = U_1^\perp + U_2^\perp$，并重新整理可得结论。□

推论 7.4。设 x, y：$U \to W$ 为线性算子。设 ι 为 $y \hookrightarrow U$ 的包含映射，π 为 $U \twoheadrightarrow U/\operatorname{im} y$ 的投影。则

$$2\operatorname{rk}(\pi x \iota) \le \operatorname{rk}(\pi x) + \operatorname{rk}(x\iota) \le \operatorname{rk}(x+y) + \operatorname{rk} x - \operatorname{rk} y.$$

证明。注意到 $\operatorname{rk} y = \dim\operatorname{im} y = \dim(\ker y)^\perp$。我们计算

$$\operatorname{rk}(\pi x) = \dim(\operatorname{im}\pi x) = \dim(\operatorname{im} x / \operatorname{im} y) = \dim(\operatorname{im} x + \operatorname{im} y) - \dim(\operatorname{im} y);$$

$$\operatorname{rk}(x\iota) = \dim(\ker y) - \dim((\ker x) \cap (\ker y)) = \dim\big((\ker x)^\perp + (\ker y)^\perp\big) - \dim(\ker y)^\perp.$$

结合引理 7.3 即得结论。□

现在我们概述引理 7.2 的证明，这将有助于理解我们的方法。设 $\mathbf{X} \subset \operatorname{End}(V)$ 是一个子空间。通过对 k 使用归纳法，可以证明如下结论：存在维数至少为 $d - 2r(1 - 2^{-k})$ 的向量空间 U_k 和 W_k，一个单射 ι_k：$U_k \hookrightarrow V$，以及一个满射 π_k：$V \twoheadrightarrow W_k$，使得对每个 $x \in \mathbf{X}$，都有 $\operatorname{rk} \pi_k x \iota_k \le 2^{-k} r$。取 $k = \lceil \log_2 r \rceil$ 后即可得到引理 7.2。基例 $k = 0$ 恰为引理 7.2 的假设；归纳步骤则通过应用推论 7.4 得出：选取 $y \in \mathbf{X}$ 使 $\operatorname{rk} \pi_k y \iota_k$ 最大，并定义

$$U_{k+1} := (\ker \pi_k y \iota_k)^\perp, \quad W_{k+1} := W_k / \operatorname{im}(\pi_k y \iota_k),$$

并分别令 ι_{k+1} 和 π_{k+1} 为自然复合映射 $U_{k+1} \hookrightarrow U_k \hookrightarrow V$ 和 $V \twoheadrightarrow W_k \twoheadrightarrow W_{k+1}$。由于 $\operatorname{rk} \pi_k y \iota_k \le 2^{-k} r$，空间 U_{k+1} 和 W_{k+1} 的余维数至多为 $2r(1 - 2^{-(k+1)})$。最后，推论 7.4 加上我们对 y 的选择，足以得出关于 $\pi_{k+1} x \iota_{k+1}$ 的必要秩界。

我们对引理 7.1 的证明采用了类似的策略，其中的迭代步骤围绕推论 7.4 展开。

引理 7.5。设 U、V 和 W 为向量空间，设 K、r、s、ε、$\eta > 0$，设 A 为 $\mathrm{GL}(V)$ 的 K-近似子群，并设 ι：$U \hookrightarrow V$ 和 π：$V \twoheadrightarrow W$ 分别为单射和满射线性映射。假设 $S \subset A^2$ 满足以下性质：

(i) $|S| \ge \varepsilon |A^2|$，*(ii)* 对于每个 $a \in S$，都有 $\operatorname{rk}(\pi(a-1)) \le s$，且 *(iii)* 对于每个 $a \in S$，都有 $\operatorname{rk}(\pi(a-1)\iota) \le r$。

那么，存在向量空间 U'和 W'、映射 $\iota'\colon U'\hookrightarrow V$和 $\pi'\colon V\twoheadrightarrow W'$、子集 $S'\subset A^2$，以及三元组 $(\rho,\ell,m)\in\{(1-\eta,r,1),(3\eta,2s,2)\}$，使得
(1) ι' 是单射，且 π' 是满射；*(2)* 维数 $U-$维数 U'和维数 $W-$维数 W'均至多为 ℓ；*(3)* $|S'|\geq\frac{\varepsilon^m}{4K}|A^2|$；*(4)* 对每个 $a\in S'$，都有$\operatorname{rk}(\pi'(a-1)\iota')\leq\rho r$。

证明。 我们先定义以下集合。

$$\begin{aligned}S_0&:=\big\{a\in S:\operatorname{rk}(\pi(a-1)\iota)\leq r(1-\eta)\big\};\quad S_1:=S\setminus S_0.\\T&:=\big\{(b,c)\in S_1\times S_1:bc^{-1}\in A^2\big\}.\\T_0&:=\big\{(b,c)\in T:\operatorname{rk}(\pi(b-c)\iota)\leq r(2-3\eta)\big\};\\T_1&:=\big\{(b,c)\in T:\operatorname{rk}(\pi(b-c)\iota)>r(2-3\eta)\big\}.\end{aligned}$$

若 $|S_0|\geq\frac{1}{4}|S|$**：** 我们可以取$(\rho,\ \ell,\ m)=(1-\eta,\ r,\ 1)$。选取 $S'=S_0$；我们只需取$(\pi',\ \iota',\ U',\ W')=(\pi,\ \iota,\ U,\ W)$。

若 $|S_0|<\frac{1}{4}|S|$**：** 我们有 $|S_1|>\frac{3}{4}|S|$。利用柯西–施瓦茨不等式，可以给 T的大小一个下界。设 X 满足 $|X|\leq K$ 和 $A^2\subset AX$，并令 $f\colon A^2\to X$ 定义为对每个 $a\in A^2$都有$a\in Af(a)$。我们有

$$\begin{aligned}|T|&\geq\#\{(b,c)\in S_1\times S_1:f(b)=f(c)\}\\&=\sum_{x\in X}|f^{-1}(x)\cap S_1|^2\\&\geq\frac{1}{K}\left(\sum_{x\in X}|f^{-1}(x)\cap S_1|\right)^2=\frac{|S_1|^2}{K}\geq\frac{3}{4K}|S||S_1|.\end{aligned}$$

因此，我们得到

$$\max\big(|T_0|,|T_1|\big)\geq\frac{3}{8K}|S||S_1|.\tag{7.1}$$

若 $|T_0|\geq|T_1|$**：** 取$(\rho,\ \ell,\ m)=(1-\eta,\ r,\ 1)$。根据（7.1），存在某个 $c\in S_1$使得$S':=\{bc^{-1}:\ (b,c)\in T_0\}\subset A^2$的大小至少为 $\frac{3}{8K}|S|\geq\frac{\varepsilon}{3K}|A^2|$。记 $y:=\pi(c-1)\iota$。令 ι_c为包含映射 $\ker y\hookrightarrow U$，令 π_c为投影 $W\twoheadrightarrow W/\operatorname{im}y$，并定义

$$U':=\ker y,\ W':=W/\operatorname{im}y,\ \iota':=c\iota\iota_c,\ \pi':=\pi_c\pi.$$

由于 $c\in S_1$，我们有 $r(1-\eta)\leq\operatorname{rk}y\leq r$。这意味着 $\dim U-\dim U'\leq r$且 $\dim W-\dim W'\leq r$。因此，只需证明

$$\operatorname{rk}(\pi'(a-1)\iota')\leq r(1-\eta)$$

对每个 $a\in S'$均成立。事实上，令 $b=ac$，使得 $(b,\ c)\in T_0$。记 $x:=\pi(a-1)c\iota=\pi(b-c)\iota$，并将推论 7.4 应用于 x和 y，得到

$$2\operatorname{rk}(\pi'(a-1)\iota')=2\operatorname{rk}(\pi_cx\iota_c)\leq\operatorname{rk}(x+y)+\operatorname{rk}x-\operatorname{rk}y.\tag{7.2}$$

由于 $(b,c)\in T_0$，我们有 $\operatorname{rk}x=\operatorname{rk}(\pi(b-c)\iota)\leq r(2-3\eta)$；又由于 $x+y=\pi(b-1)\iota$ with $b\in S$，我们有 $\operatorname{rk}(x+y)\leq r$。由 (7.2) 得

$$2\operatorname{rk}(\pi'(a-1)\iota')\leq r(2-3\eta)+r-r(1-\eta)=2r(1-\eta),$$

这就足够了。

若 $|T_1|>|T_0|$**：** 我们取 $(\rho,\ell,m)=(3\eta,2s,2)$。由于 $|T_1|=\max(|T_0|,|T_1|)\geq\frac{3}{8K}|S||S_1|$，存在某个 $a\in SS^{-1}\cap A^2$，使得至少

$$\frac{\frac{3}{8K}|S||S_1|}{|A^2|}\geq\frac{9}{32K}\frac{|S|^2}{|A^2|}>\frac{\varepsilon^2}{4K}|A^2|$$

对 (b, ab) 属于 T_1。令 $S' := \{b \in S \colon (b, ab) \in T_1\}$。记 $z := \pi(a-1)$。令 π_a 为$W \to W/\operatorname{im} z$ 的投影，并令

$$U' := U,\ W' := W/\operatorname{im} z,\ \iota' := \iota,\ \pi' := \pi_a \pi.$$

由于 $a \in SS^{-1}$ 可以写成某个 $b, c \in S$ 的 bc^{-1}，性质 (ii) 表明

$$\operatorname{rk} z = \operatorname{rk} \pi(b-c)c^{-1} = \operatorname{rk} \pi(b-c) \le \operatorname{rk} \pi(b-1) + \operatorname{rk} \pi(c-1) \le 2s,$$

因此 $\dim W - \dim W' \le 2s$。所以，剩下要证明的是，对于每个 $b \in S'$，都有 $\operatorname{rk}(\pi'(b-1)\iota') \le 3\eta r$。令 $x := \pi(b-1)\iota$，并令 $y := \pi(a-1)b\iota$。将推论 7.4 应用于 x 和 y，得到

$$\dim((\operatorname{im} x)/(\operatorname{im} y)) \le \operatorname{rk}(x+y) + \operatorname{rk} x - \operatorname{rk} y. \tag{7.3}$$

由于 $b \in S$，我们有 $\operatorname{rk} x \le r$。由于 $(b, ab) \in T_1$，我们有 $\operatorname{rk} y = \operatorname{rk} \pi(ab-b)\iota > (2-3\eta)r$。此外，$(b, ab) \in T_1$ 意味着 $ab \in S$，所以我们有 $\operatorname{rk}(x+y) = \operatorname{rk} \pi(ab-1)\iota \le r$。最后，由于 $y = zb\iota$，我们有 $\operatorname{im} y \subset \operatorname{im} z$，因此

$$\dim(\operatorname{im} x/\operatorname{im} y) \ge \dim(\operatorname{im} x/\operatorname{im} z) = \operatorname{rk}(\pi_a x) = \operatorname{rk}(\pi_a \pi(b-1)\iota) = \operatorname{rk}(\pi'(b-1)\iota').$$

将此与 (7.3) 结合可得

$$\operatorname{rk}(\pi'(b-1)\iota') \le \operatorname{rk}(x+y) + \operatorname{rk} x - \operatorname{rk} y \le r + r - (2-3\eta)r = 3\eta r$$

对每个 $b \in S'$，均如此。 □

现在，我们已经具备证明引理 7.1 所需的大部分内容。剩下的工作是准确描述如何迭代引理 7.5。为此，我们需要以下技术引理，它描述了一种渐近最优的迭代过程。

引理 7.6. 设 V 是一个向量空间，A 是 $GL(V)$ 的一个 K-近似子群。假设对每个元素 $a \in A^2$，都有 $\operatorname{rk}(a-1) \le s$。对每个正整数 k，以下结论成立。对于 $\alpha_k := 2^{1-2^{k/2}}$，存在维数至少为 $(\dim V) - 4ks$ 的空间 U_k 和 W_k、一个单射$\iota_k \colon U_k \hookrightarrow V$，以及一个满射 $\pi_k \colon V \twoheadrightarrow W_k$，使得对于$A^2$中的至少 $(4K)^{-30/\alpha_k^{1/2}}|A^2|$ 个元素 a，有 $\operatorname{rk}(\pi_k(a-1)\iota_k) \le \alpha_k s$。

证明。令 $\alpha_k := 2^{1-2^{k/2}}$，定义序列 $\{t_k\}$，使得 $t_0 = 0$ 且 $t_{k+1} = 2t_k + \frac{6\alpha_k}{\alpha_{k+1}} - 5$。可以手动验证，对每个 $k \ge 0$，都有 $t_k \le 30\alpha_k^{-1/2}$。（当 k 较大时，有 $t_k \sim \alpha_k^{-0.292\ldots} = \alpha^{-(1-2^{-1/2})\ k}$。）因此，只需证明将 $(4K)^{-30/\alpha_k^{1/2}}$ 替换为 $(4K)^{-t_k}$ 后的引理结论。我们对 k 使用归纳法来证明。对于 $k = 0$，我们可以令 $U_k = W_k = V$ 和 ι_k 以及 π_k 为单位元映射。

现在，假设我们有 $(U_k, W_k, \iota_k, \pi_k)$，并希望构造 $(U_{k+1}, W_{k+1}, \iota_{k+1}, \pi_{k+1})$。为此，我们反复应用引理 7.5。初始化

$$\left(U^{(0)}, W^{(0)}, \iota^{(0)}, \pi^{(0)}, r^{(0)}, t^{(0)}\right) = (U_k, W_k, \iota_k, \pi_k, \alpha_k s, t_k).$$

给定 $(U^{(i)},\ W_{(i)}\iota^{(i)},\ \pi^{(i)},\ r^{(i)},\ t^{(i)})$，我们应用引理 7.5，其中 $\varepsilon = (4K)^{-t^{(i)}}$ 和 $\eta = \frac{\alpha_{k+1} s}{3r^{(i)}}$。展开所得结果，我们得到某个状态

$$\left(U^{(i+1)}, W^{(i+1)}, \iota^{(i+1)}, \pi^{(i+1)}, r^{(i+1)}, t^{(i+1)}\right)$$

其中至少有 $(4K)^{-t^{(i+1)}}|A^2|$ 个元素 a 满足 A^2

$$\operatorname{rk}\left(\pi^{(i+1)}(a-1)\iota^{(i+1)}\right) \le r^{(i+1)},$$

并且我们的参数之间满足以下关系之一：

(a)
- $t^{(i+1)} = t^{(i)} + 1$,
- $r^{(i+1)} = (1-\eta)r^{(i)} = r^{(i)} - \frac{1}{3}\alpha_{k+1} s$, and
- $\dim U^{(i)} - \dim U^{(i+1)}, \dim W^{(i)} - \dim W^{(i+1)} \le r^{(i)}$; or

(b)
- $t_{(i+1)} = 2t_{(i)} + 1$,
- $r_{(i+1)} = 3\eta r_{(i)} = \alpha_{k+1}s$，以及
- 维数 $U_{(i)}$ − 维数 $U_{(i+1)}$，维数 $W_{(i)}$ − 维数 $W_{(i+1)} \leq 2s$。

（此外，所有此类元素都满足 $\mathrm{rk}(\pi^{(i+1)}(a-1)) \leq \mathrm{rk}(a-1) \leq s$。）当 $r^{(j)} \leq \alpha_{k+1}s$ 时，我们在 $(U^{(j)}, W_{(j)}\iota^{(j)}, \pi^{(j)}, r^{(j)}, t^{(j)})$ 处终止该过程，并令

$$(U_{k+1}, W_{k+1}, \iota_{k+1}, \pi_{k+1}, t_{k+1}) = (U^{(j)}, W^{(j)}, \iota^{(j)}, \pi^{(j)}, t^{(j)}).$$

注意，在任何落入情形 (b) 的步骤之后，不等式 $r^{(j)} \leq \alpha_{k+1}s$ 都会自动成立。因此，由于对每个 $0 \leq i \leq j$ 都有 $r^{(i)} \leq r^{(0)} - \frac{i}{3}\alpha_{k+1}s$，我们必有

$$j + 2 \leq \frac{3\alpha_k}{\alpha_{k+1}}. \tag{7.4}$$

因此，在该过程终止之前，我们至多执行 $\frac{3\alpha_k}{\alpha_{k+1}} - 1$ 次情形步骤，随后至多执行一次情形 (b) (a) 步骤。由此可得

$$\dim U_k - \dim U_{k+1}, \dim W_k - \dim W_{k+1} \leq jr^{(0)} + 2s \leq \left(2 + \frac{3\alpha_k^2}{\alpha_{k+1}}\right)s \leq 4s$$

并利用（7.4），

$$t^{(j)} \leq 2t^{(j-1)} + 1 = 2(t^{(0)} + j - 1) + 1 \leq 2t_k + \frac{6\alpha_k}{\alpha_{k+1}} - 5 = t_{k+1}.$$

令 $t_{k+1} = t^{(j)}$，则至少有 $(4K)^{-t_{k+1}}|A^2|$ 个 a 来自 A^2，且满足

$$\mathrm{rk}(\pi_{k+1}(a-1)\iota_{k+1}) \leq r^{(j)} \leq \alpha_{k+1}s,$$

正如所需。 □

注 7.7. 引理 7.6 中描述的迭代过程在不同参数之间存在一定的权衡。例如，对于任意固定的 $\varepsilon > 0$，可以将 $(4K)^{-30/\alpha^{-1/2}}$ 项替换为 $(4K)^{-30/\alpha^{-\varepsilon}}$，代价是将维数递减从 $4ks$ 提高到某个较大的$C = C(\varepsilon)$对应的 Cks。（这可以通过将双指数衰减率 $\alpha_k \sim 2^{-2^{k/2}}$ 替换为$\alpha_k \sim 2^{-\beta^k}$ 来实现，其中某个 $\beta \in (1, \sqrt{2})$。）然而，无论愿意在 $4K$ 的指数上承受多大的损失，使用我们的方法都无法得到渐近地小于 $s\log\log(1/\alpha)$ 的密度递减。

现在我们可以证明引理 7.1。

引理 *7.1* 的证明。令集合 $V := \mathbb{F}^d$。选取 $k = \lfloor 2\log_2\log_2(2s)\rfloor + 1$，使得 $\alpha := 2^{1-2^{k/2}}$ 位于区间 $[2^{1-\sqrt{2}}s^{-\sqrt{2}}, s^{-1})$ 内。将引理 7.6 应用于 $A \subset$ 一般线性群(V)。我们得到维数至少为 $(\dim V) - 4ks$ 的向量空间 U_k 和 W_k，一个单射 $\iota_k\colon U_k \hookrightarrow V$，以及一个满射 $\pi_k\colon V \twoheadrightarrow W_k$，使得对于 A^2 中至少有 $(4K)^{-30/\alpha^{1/2}}|A^2|$ 个元素 a，有 $\mathrm{rk}(\pi_k(a-1)\iota_k) \leq \alpha s$。令 S 为所有此类 $a \in A^2$ 组成的集合。由于 $\alpha s < 1$，对于所有 $a \in S$，我们有 $\pi_k(a-1)\iota_k = 0$。我们还得到

$$|S| \geq (4K)^{-30\alpha^{-1/2}}|A^2| \geq (2K)^{-60s}|A^2|,$$

其中后一个不等式成立，因为 $s \geq 6$。令 $U := \mathrm{im}\,\iota_k$ 和 $W := (\ker\pi_k)^\perp$ 的维数至多

$$4ks \leq 8s\log_2\log_2(2s) + 4s \leq 30s\log\log s,$$

其中，后一个不等式成立是因为 $s \geq 6$。由于对所有 $a \in S$ 都有 $\pi_k(a-1)\iota_k = 0$，因此对所有这样的 a，都有 $(a-1)W^\perp \subset U$。证明至此完成。□

8. The subspace-to-subgroup lemma

本节的主要目标是证明引理 6.6，以及一个类似命题，从而使我们能够由引理 7.1 推出命题 1.13。这样便完成了定理 1.12 和命题 1.13 的证明。

本节中我们先引入一些记号，并在后文沿用。我们将以下称为“情形（$\star$）”。设 d 是一个正整数，且 $\mathcal{F} = (V_0, V_1, V_2, \dots, V_m)$ 是 $\mathbb{F}^d$ 上的一个旗，其抛物维数为 D。设 A 是 $H_{\mathcal{F}}$ 的一个 K-近似子群，并设 $\mathbf{V} \subset \mathbf{P}_{\mathcal{F}}$ 是一个与 A^2 相交的真仿射子空间。设 $\eta := |A^2 \cap \mathbf{V}|/|A^2|$。记 π_i 为环同态 $\mathbf{P}_{\mathcal{F}} \to \mathrm{End}(V_i/V_{i-1})$。

本节的核心是以下单步操作，我们将反复迭代它。

引理 8.1。在情形($\star$)中，设 k 是任意一个正整数。存在某个正整数 $j \leq k$ 以及 $\mathbf{P}_{\mathcal{F}}$ 的某个仿射子空间 $\mathbf{W}$，满足 维数$\mathbf{V}$ $-$ 维数$\mathbf{W}$ $\geq j-1$ 且

$$\left(\frac{|A^2 \cap \mathbf{W}|}{|A^2|}\right)\left(\frac{|A^2 \cap \mathrm{L}^*(\mathbf{W} \to \mathbf{V})|}{|A^2|}\right)^{k-j} \geq \left(\frac{\eta}{2K}\right)^k.$$

在这个引理的结论中，我们有 $\dim \mathbf{V} - \dim \mathbf{W} \geq j-1$，而不是 $\dim_{\mathcal{F}} \mathbf{V} - \dim_{\mathcal{F}} \mathbf{W} \geq j-1$。这只是因为 $\dim$ 比 $\dim_{\mathcal{F}}$ 稍容易控制（而在 $\mathcal{F}$ 为平凡旗的模型情形下，两者几乎相同）。在我们的迭代过程中，这个条件只是为了确保迭代终止，而终止的精确定量性质并不那么重要。

证明。我们首先证明

$$\sum_{a_1,\dots,a_k \in A^2} \left| A^2 \cap \bigcap_{i=1}^k a_i^{-1}\mathbf{V} \right| \geq \left(\frac{\eta}{K}\right)^k |A^2|^{k+1}. \tag{8.1}$$

事实上，我们首先注意到，对于每个 $x \in A^2$，都有 $|A^2 x \cap A^2| \geq |A|$：如果对某个 $a \in A$ 有 $x \in Aa$，那么 $Aa \subset A^2 x \cap A^2$，因为 A 是含单位元的。这使我们能够计算

$$\begin{aligned}
\sum_{a_1,\dots,a_k \in A^2} \left| A^2 \cap \bigcap_{i=1}^k a_i^{-1}\mathbf{V} \right| &= \sum_{b \in A^2} \sum_{a_1,\dots,a_k \in A^2} \prod_{i=1}^k 1_{a_i^{-1}\mathbf{V}}(b) \\
&= \sum_{b \in A^2} \left(\sum_{a \in A^2} 1_{a^{-1}\mathbf{V}}(b) \right)^k \\
&= \sum_{b \in A^2} |A^2 b \cap \mathbf{V}|^k \\
&\geq |A^2| \left(\frac{1}{|A^2|} \sum_{b \in A^2} |A^2 b \cap \mathbf{V}| \right)^k \\
&\geq |A^2| \left(\frac{1}{|A^2|} \sum_{b \in A^2} \sum_{x \in A^2 \cap \mathbf{V}} 1_{A^2 b}(x) \right)^k \\
&= |A^2| \left(\frac{1}{|A^2|} \sum_{x \in A^2 \cap \mathbf{V}} |A^2 x \cap A^2| \right)^k \\
&\geq |A^2| \left(\frac{1}{|A^2|} \sum_{x \in A^2 \cap \mathbf{V}} |A| \right)^k = \frac{|A^2 \cap \mathbf{V}|^k |A|^k}{|A^2|^{k-1}} \geq \left(\frac{\eta}{K}\right)^k |A^2|^{k+1}.
\end{aligned}$$

现在我们将（8.1）中的求和拆开。对于 A^2中的每个元素元组$\mathbf{a}=(a_1,\dots,a_k)$，令 $S_{\mathbf{a}}\subset\{1,\dots,k\}$ 为一个满足以下条件的最小规模集合

$$\bigcap_{i=1}^{k} a_i^{-1}\mathbf{V}=\bigcap_{i\in S_{\mathbf{a}}} a_i^{-1}\mathbf{V}.$$

根据（8.1），存在某个集合 $S_0\subset\{1,\dots,k\}$，使得

$$\sum_{\mathbf{a}:S_{\mathbf{a}}=S_0}\left|A^2\cap\bigcap_{i=1}^{k}a_i^{-1}\mathbf{V}\right|\geq\left(\frac{\eta}{2K}\right)^k|A^2|^{k+1}.$$

不妨设 $S_0=\{1,\dots,j\}$，其中某个非负整数 $j\in\{0,1,\dots,k\}$。于是我们可以写成

$$\sum_{a_1,\dots,a_j\in A^2}\left|A^2\cap\bigcap_{i=1}^{j}a_i^{-1}\mathbf{V}\right|\cdot\left|\left\{a\in A^2:a^{-1}\mathbf{V}\supset\bigcap_{i=1}^{j}a_i^{-1}\mathbf{V}\right\}\right|^{k-j}\geq\left(\frac{\eta}{2K}\right)^k|A^2|^{k+1}.$$

这意味着，对于某个仿射子空间 $\mathbf{W}:=a_1^{-1}\mathbf{V}\cap\cdots\cap a_j^{-1}\mathbf{V}$，它属于 $\mathbf{P}_{\mathcal{F}}$，

$$\left(\frac{|A^2\cap\mathbf{W}|}{|A^2|}\right)\left(\frac{\left|\{a\in A^2:a\mathbf{W}\subset\mathbf{V}\}\right|}{|A^2|}\right)^{k-j}\geq\left(\frac{\eta}{2K}\right)^k.$$

如果 $j=0$，那么 $\mathbf{W}=\mathbf{P}_{\mathcal{F}}$，因此没有任何 $a\in A^2$ 能够满足 $a\mathbf{W}\subset\mathbf{V}$（因为 $\mathbf{V}$ 是 $\mathbf{P}_{\mathcal{F}}$ 的真仿射子空间）。我们由此得出 $j>0$。此外，根据我们对 $S_0=\{1,\dots,j\}$ 的选择，对于 $1\leq i\leq j$，交集 $\mathbf{W}^{(i)}:=a_1^{-1}\mathbf{V}\cap\cdots\cap a_i^{-1}\mathbf{V}$ 必须各不相同——如果 $\mathbf{W}^{(i-1)}=\mathbf{W}^{(i)}$，那么可以从定义 $\mathbf{W}$ 的交集中移除项 a_i^{-1}，这与 $S_{\mathbf{a}}$ 的定义矛盾。因此，由于 $\dim\mathbf{W}^{(1)}=\dim\mathbf{V}$，且链中的所有包含映射

$$\mathbf{W}^{(1)}\supset\mathbf{W}^{(2)}\supset\cdots\supset\mathbf{W}^{(j)}=\mathbf{W}$$

是适当的，因此我们有 $\dim\mathbf{V}-\dim\mathbf{W}\geq j-1$，如所需。 □

引理 8.1 的第一个应用是在 $\mathbf{V}=\mathrm{vtr}^{-1}(\mathbf{t})$ 的情形下，将 $\mathbf{V}$ 约化为一个 $\mathcal{F}$-维子空间。

引理 8.2。 在情形 $(\star)$下工作，并设对于某个 $\mathbf{t}\in\mathbb{F}^m$，有 $\mathbf{V}\subset\mathrm{vtr}^{-1}(\mathbf{t})$。则存在某个仿射子空间 $\mathbf{V}'\subset\mathbf{P}_{\mathcal{F}}$，其 $\mathcal{F}$-维数至多为 $D/2$，包含于 $\mathbf{V}$ 的某个双侧平移中，并且满足

$$\frac{|A^2\cap\mathbf{V}'|}{|A^2|}\geq\left(\frac{\eta}{2K}\right)^{d^2}.$$

证明。 将引理 8.1 应用于 A 和 $\mathbf{V}$，其中 $k=d^2$。我们得到某个正整数 $j\leq d^2$ 以及 $\mathrm{Mat}_d(\mathbb{F})$ 中的某个仿射子空间 $\mathbf{W}$，其维数至多为 $\dim\mathbf{V}-(j-1)$，并满足

$$\left(\frac{|A^2\cap\mathbf{W}|}{|A^2|}\right)\left(\frac{|A^2\cap\mathrm{L}^*(\mathbf{W}\to\mathbf{V})|}{|A^2|}\right)^{d^2-j}\geq\left(\frac{\eta}{2K}\right)^{d^2}.\tag{8.2}$$

写成$\mathbf{X}:=\mathrm{L}^*(\mathbf{W}\to\mathbf{V})$。根据引理 6.4，我们首先注意到，$\mathbf{W}$ 和$\mathbf{X}$ 都包含于$\mathbf{V}$ 的某个双侧平移中。现在，若 $j=d^2$，则 $\dim\mathbf{W}=0$，于是由 (8.2) 结合$\mathbf{V}'=\mathbf{W}$即可得出结论。否则，(8.2) 导出较弱的结论

$$\min\left(\frac{|A^2\cap\mathbf{W}|}{|A^2|},\frac{|A^2\cap\mathbf{X}|}{|A^2|}\right)\geq\left(\frac{\eta}{2K}\right)^{d^2}.\tag{8.3}$$

现在，由于对于每个 $x \in \mathbf{X}$ 和 $y \in \mathbf{W}$，$\mathrm{vtr}(xy) = \mathbf{t}$，因此对每个$1 \le i \le m$都有 $\mathrm{tr}(\pi_i(x)\pi_i(y)) = t_i$。由引理 6.2，我们于是有 $\dim\mathrm{span}\ \pi_i(\mathbf{X}) + \dim\mathrm{span}\ \pi_i(\mathbf{W}) \le d_i^2 + 1$。这表明

$$\begin{aligned}\dim_{\mathcal{F}} \mathbf{W} + \dim_{\mathcal{F}} \mathbf{X} &= \sum_{i=1}^{m} (\dim(\operatorname{span} \pi_i(\mathbf{W})) + \dim(\operatorname{span} \pi_i(\mathbf{X})) - 2) \\ &\le \sum_{i=1}^{m} (d_i^2 - 1) = D.\end{aligned}$$

因此，$\{\mathbf{W}、\mathbf{X}\}$ 中有一个的 $\mathcal{F}$维数至多为 $D/2$。取$\mathbf{V}'$ 为 $\{\mathbf{W}、\mathbf{X}\}$ 中 $\mathcal{F}$维数较小的那个，由（8.3）可得结论。□

其次，我们迭代引理 8.1，得到 A^2 与一个集合有较大的交，而该集合比一般的仿射子空间更具结构性。

引理 8.3。在情形$(\star)$中，存在某个子代数$\mathbf{U} \subset \mathbf{P}_{\mathcal{F}}$，使得 $1+\mathbf{U}$ 包含于$\mathbf{V}$ 的某个双侧平移中，并且

$$\frac{|A^2 \cap (1+\mathbf{U})|}{|A^2|} \ge \frac{\eta^{d^4}}{(2K)^{d^6+3}}.$$

证明。令$\mathbf{V}_0 := \mathbf{V}$ 且 $k_0 := d^4$。对于每个 $i \ge 0$，给定$\mathbf{V}_i$ 和 k_i，使用引理 8.1 找到某个正整数 $j =: j_i \le k_i$ 以及 $\mathrm{Mat}_d(\mathbb{F})$ 中的某个仿射子空间$\mathbf{W}_i$，满足 $\dim\mathbf{V}_i - \dim\mathbf{W}_i \ge j_i - 1$ 并且

$$\left(\frac{|A^2 \cap \mathbf{W}_i|}{|A^2|}\right)\left(\frac{|A^2 \cap \mathrm{L}^*(\mathbf{W}_i \to \mathbf{V}_i)|}{|A^2|}\right)^{k_i - j_i} \ge \left(\frac{\eta}{2K}\right)^{k_i}. \tag{8.4}$$

定义 $k_{i+1} := k_i - j_i$ 以及$\mathbf{V}^{i+1} := \mathrm{L}^*(\mathbf{W}_i \to \mathbf{V}_i)$。若 $\dim\mathbf{V}_{i+1} = \dim \mathbf{V}_i$，则终止该过程，并令 ℓ 为此情况出现时的指数，因此 $\dim \mathbf{V}_\ell = \dim\mathbf{V}^{\ell+1}$。我们注意到以下性质：

(1) 根据引理 6.5，对每个 i，都有 $\dim \mathbf{V}_{i+1} \le \dim\mathbf{V}_i$。这意味着对每个 $i \le \ell$，都有 $\dim \mathbf{V}_i \le \dim \mathbf{V}_0 - i$。特别地，$\ell \le \dim\mathbf{V}_0 < d^2$。(2) 由于 $\dim \mathbf{V}_i - \dim \mathbf{W}_i \ge j_i - 1$，对每个 i，必有 $j_i \le \dim \mathbf{V}_i + 1 \le \dim\mathbf{V}_0 + 1$。结合 (1) 和所选的 $k_0 = d^4$，这保证 k_i 在整个迭代过程中始终为正。(3) 根据引理 6.4，每个 $\mathbf{V}^{i+1}$ 都包含在 $\mathbf{V}_i$的某个右平移中。因此，$\mathbf{V}_\ell$ 包含在$\mathbf{V}$的某个右平移中。(4) 再次根据引理 6.5，由于

$$\dim \mathbf{V}_{\ell+1} = \dim \mathrm{L}^*(\mathbf{W}_\ell \to \mathbf{V}_\ell) = \dim \mathbf{V}_\ell$$

且 $\mathbf{W}_\ell$ 和 $\mathbf{V}_\ell$ 都含有可逆元素，存在某个由 $\mathrm{Mat}_d(\mathbb{F})$ 构成的子代数$\mathbf{U}$，以及某个 $b \in$一般线性群$_d(\mathbb{F})$，使得 (i) $(1+\mathbf{U}) \cap$一般线性群$_d(\mathbb{F})$ 是一般线性群$_d(\mathbb{F})$ 的子群，(ii) $\mathbf{W}_\ell \subset b(1+\mathbf{U})$，且 (iii) $1+\mathbf{U}$ 包含在$\mathbf{V}_\ell$的某个左平移中。

令 $H := (1+\mathbf{U}) \cap \mathrm{GL}_d(\mathbb{F})$，根据 (4)，它是 $\mathrm{GL}_d(\mathbb{F})$ 的一个子群。结合 (3) 和 (4) 可知，$1+\mathbf{U}$ 包含于 $\mathbf{V}$ 的某个双侧平移中。令 $\eta_i := |A^2 \cap \mathbf{V}_i|/|A^2|$。由 (8.4)，我们有

$$\eta_{i+1}^{k_{i+1}} \ge \left(\frac{\eta_i}{2K}\right)^{k_i}$$

对于每个 i。这意味着，利用 (8.4)，

$$\frac{|A^2 \cap \mathbf{W}_\ell|}{|A^2|} \ge \left(\frac{\eta_\ell}{2K}\right)^{k_\ell} \ge \eta_0^{k_0} \prod_{i=0}^{\ell} \left(\frac{1}{2K}\right)^{k_i} \ge \left(\frac{\eta_0}{(2K)^{\ell+1}}\right)^{k_0} \ge \left(\frac{\eta}{(2K)^{d^2}}\right)^{d^4}.$$

特别地， $|A^2\cap bH|$ 非空。设 $a_0\in A^2\cap bH$ 是任意一个元素。由于 $a_0^{-1}(A^2)\subset A^4$，利用引理 2.13 可得

$$K^3|A^2\cap H|\geq |A^4\cap H|\geq |a_0^{-1}A^2\cap a_0^{-1}bH|=|A^2\cap bH|\geq |A^2\cap \mathbf{W}_\ell|.$$

我们得出结论

$$\frac{|A^2\cap(1+\mathbf{U})|}{|A^2|}=\frac{|A^2\cap H|}{|A^2|}\geq\frac{|A^2\cap\mathbf{W}_\ell|}{K^3|A^2|}\geq\frac{\eta^{d^4}}{(2K)^{d^6+3}}.$$

□

证明引理 6.6 所需的最后一步，是从子代数 $\mathbf{U}$ 转到某个$\mathbf{P}_\mathcal{G}$，使得 $\mathcal{G}$ 是 $\mathcal{F}$的一个细化。为此，我们使用 Burnside 定理 [Bur05], , 该定理指出，代数闭域上矩阵代数的每个真子代数都有某个非平凡不变子空间。（我们需要在正特征下应用 Burnside 定理；相关的一个不错的参考文献是 [LR04]。）

引理 8.4。设 $\rho\in(0,\ 1)$。对每个满足$\mathbf{U}\subset\mathbf{P}_\mathcal{F}$且满足维数$_\mathcal{F}\mathbf{U}\leq\rho\,\mathrm{pdim}(\mathcal{F})$的子代数，都存在一个细化 $\mathcal{G}$，它满足张成$\mathbf{U}\subset\mathbf{P}_\mathcal{G}$且$\mathrm{pdim}(\mathcal{G})\leq\rho^{1/2}\,\mathrm{pdim}(\mathcal{F})$。

证明。记 $\mathrm{U}=\overline{\text{为 U 的张成空间。对每个 }1\leq i\leq m\text{，令 }\mathcal{F}_i=(U_i,0,\dots,U_{i,m_i})\text{ 为一个由 }\pi_i}$ (U) 稳定的极大旗。对每个 $1\leq j\leq m_i$，我们有一个映射$\phi_{i,j}$ ，它从 π_i(U)映到 End($U_{i,j}/U_{i,j-1}$)。$\phi_{i,j}$ 的像是 End($U_{i,j}/U_{i,j-1}$) 的一个含单位元的子代数。因此，Burnside 定理意味着 im$\phi_{i,j}$ 要么是整个 End($U_{i,j}/U_{i,j-1}$)，要么拥有某个不变子空间。然而，这种不变子空间的存在与旗 $\mathcal{F}_i$ 的极大性矛盾。因此，我们得出结论：

$$\dim\pi_i(\overline{\mathrm{U}})\geq\max_{1\leq j\leq m_i}\dim(U_{i,j}/U_{i,j-1})^2.$$

记 $d_{i,j}:=$ 维$U_{i,j}/U_{i,j-1}$，并令 $\Delta_i:=$ 维 π_i(U)，使得 $d_{i,j}\leq\sqrt{\Delta_i}\leq d_i$ 对每个$\overline{1\leq j\leq m_i\text{ 都成立。我们有}}$

$$\begin{aligned}\sum_{j=1}^{m_i}(d_{i,j}^2-1)&\leq\sum_{j=1}^{m_i}\left(d_{i,j}\sqrt{\Delta_i}-\frac{d_{i,j}}{\sqrt{\Delta_i}}\right)\\&=d_i\cdot\frac{\Delta_i-1}{\sqrt{\Delta_i}}\\&=\left((\Delta_i-1)d_i^2\left(1-\frac{1}{\Delta_i}\right)\right)^{1/2}\\&\leq\left((\Delta_i-1)d_i^2\left(1-\frac{1}{d_i^2}\right)\right)^{1/2}=\sqrt{d_i^2-1}\cdot\sqrt{\Delta_i-1}.\end{aligned}\tag{8.5}$$

令 $\mathcal{G}$ 为 $\mathcal{F}$ 的细化，该细化通过在每个 V_i/V_{i-1} 中插入 $\mathcal{F}_i$ 中的项而得到，因此$\mathbf{U}\subset\mathbf{P}_\mathcal{G}$ 根据 $\mathcal{F}_i$ 的$\overline{\text{定义成立。利用 (8.5) 和柯西–施瓦茨不等式，我们可以对其作如下界定}}$

$$\begin{aligned}\mathrm{pdim}\,\mathcal{G}&=\sum_{i=1}^{m}\sum_{j=1}^{m_i}(d_{i,j}^2-1)\\&\leq\sum_{i=1}^{m}\sqrt{d_i^2-1}\sqrt{(\dim\pi_i(\overline{\mathrm{U}}))-1}\\&\leq\left(\sum_{i=1}^{m}(d_i^2-1)\right)^{1/2}\left(\sum_{i=1}^{m}\big(\dim\pi_i(\overline{\mathrm{U}})-1\big)\right)^{1/2}\\&=(\mathrm{pdim}\,\mathcal{F})^{1/2}(\dim_\mathcal{F}\mathbf{U})^{1/2}\leq\rho^{1/2}\,\mathrm{pdim}\,\mathcal{F}.\end{aligned}$$

□

现在我们已经具备证明引理 6.6 所需的一切。

引理 *6.6* 的证明。 回顾引理 6.6 的陈述：我们处于 (⋆) 的情形，其中 $\mathbf{V} = \mathrm{vtr}_{\mathcal{F}}^{-1}(\mathbf{t})$，某个 $\mathbf{t} \in \mathbb{F}^m$。根据引理 8.2，我们可以找到一个仿射子空间 $\mathbf{V}' \subset \mathbf{P}_{\mathcal{F}}$，其 $\mathcal{F}$-维数至多为 $D/2$，并满足

$$\frac{|A^2 \cap \mathbf{V}'|}{|A^2|} \geq \left(\frac{\eta}{2K}\right)^{d^2}.$$

现在我们再次处于 (⋆) 的情形，其中 η 被 $(\eta/(2K))^{d^2}$ 取代，而$\mathbf{V}$ 被较小的$\mathbf{V}'$取代。因此，我们可以应用引理 8.3，找到某个子代数$\mathbf{U} \subset \mathbf{P}_{\mathcal{F}}$，使得 $1+\mathbf{U}$ 包含在$\mathbf{V}'$ 的某个双侧平移中，并且满足

$$\frac{|A^2 \cap (1+\mathbf{U})|}{|A^2|} \geq \frac{1}{(2K)^{d^6+3}} \left(\frac{\eta}{(2K)^{d^2}}\right)^{d^4} = \frac{\eta^{d^6}}{(2K)^{2d^6+3}}.$$

由于 $1+\mathbf{U}$ 包含在$\mathbf{V}'$的某个双侧平移中，我们有 $\dim_{\mathcal{F}} \mathbf{U} \leq \dim_{\mathcal{F}} \mathbf{V}' \leq D/2$。由引理 8.4，我们可以找到 $\mathcal{F}$的某个细化 $\mathcal{G}$，使得 $\mathrm{span}\,\mathbf{U} \subset \mathbf{P}_{\mathcal{G}}$ 且 $\mathrm{pdim}(\mathcal{G}) \leq \frac{1}{\sqrt{2}} D$。由于$\mathbf{U} \subset \mathbf{P}_{\mathcal{G}}$，我们还有 $1+\mathbf{U} \subset \mathbf{P}_{\mathcal{G}}$。特别地，$\mathbf{U}$ 的每个可逆元素都包含在 $1+$ $H_{\mathcal{G}}$ 中。我们得出

$$\frac{|A^2 \cap H_{\mathcal{G}}|}{|A^2|} \geq \frac{|A^2 \cap (1+\mathbf{U})|}{|A^2|} \geq \left(\frac{\eta}{2K}\right)^{5d^6},$$

如所需。 □

最后，我们必须推出命题 1.13。唯一缺少的要素是下面这个引理，它对 $\mathbb{F}^d$ 的子代数施加限制：这些子代数将某个向量空间中的每个元素映射到另一个固定的向量空间中。

引理 8.5. 设 U 和 W 是 $\mathbb{F}^d$的子空间，并设$\mathbf{X}$ 是$\mathrm{Mat}_d(\mathbb{F})$的子代数，满足$\mathbf{X}W^{\perp} \subset U$。那么存在满足 $V_1 \subseteq U$和 $W^{\perp} \subseteq V_2$的子空间 $V_1 \subset V_2 \subset \mathbb{F}^d$，使得$\mathbf{X}V_2 \subset V_1$。

证明. 令 $V_2 := \{v : \mathbf{X}v \subset U\}$，并令 $V_1 := U \cap V_2$。由$\mathbf{X}W^{\perp} \subset U$这一事实可知，$V_1 \subseteq U$和 $W^{\perp} \subseteq V_2$。此外，根据 V_2的定义，有$\mathbf{X}V_2 \subset U$。最后，由于$\mathbf{X}$ 在乘法下封闭，我们有

$$\mathbf{X}(\mathbf{X}V_2) \subset \mathbf{X}V_2 \subset U.$$

因此，每个 $v \in \mathbf{X}V_2$ 满足$\mathbf{X}v \subset U$，因此 $v \in V_2$。这意味着$\mathbf{X}V_2 \subset U \cap V_2 = V_1$，证毕。 □

命题 *1.13* 的证明。在下文中，我们记 $r := 600^{d^{\log\log d}}$以及 $s := 2r$。~~注意，~~ $r < d/12$。

设 $A \subset \mathrm{GL}_d(\mathbb{F})$ 是一个 K-近似子群，并假设我们不处于“非太不规则元素”的情形，即每个元素 $a \in A^2$ 都满足 $\mathrm{m}(a) \leq d - r$。我们的第一步是构造一个近似群 B，其结构控制着 A 的结构，并且满足引理 7.1 的前提条件。

我们首先注意到，对每个 $k \geq 1$，A^k 的每个元素都有一个余维数至多为 rk 的特征子空间。事实上，如果 $a_1, \ldots, a_k \in A$ 的特征子空间分别为 $V_1, \ldots, V_k$，那么 $V_1 \cap \cdots \cap V_k$ 是 $a_1 \cdots a_k$ 的一个特征子空间，其余维数至多为 $\mathrm{codim}\ V_1 + \cdots + \mathrm{codim}\ V_k$。特别地，由于 $r < d/12$，A^6 的每个元素都有一个余维数严格小于 $d/2$ 的特征子空间。对于 $a \in A^6$，令 λ_a 为与该（唯一）特征子空间对应的特征值。

定义映射 ϕ：$A^6 \to$ 一般线性群$_d(\mathbb{F})$，其定义为 $a \mapsto \lambda_a^{-1} a$。我们声称，若 $k\ell \leq 6$，则 $\phi|_{A^k}$ 是一个 Freimanℓ-同态。事实上，如果 a_1、……、a_ℓ、b_1、……、$b_\ell \in A^k$满足 $a_1 \cdots a_\ell = b_1 \cdots b_\ell$，那么

$$\lambda_{a_1} \cdots \lambda_{a_\ell} = \lambda_{a_1 \cdots a_\ell} = \lambda_{b_1 \cdots b_\ell} = \lambda_{b_1} \cdots \lambda_{b_\ell},$$

因此结论得证。将其应用于 $k = 3$ 和 $\ell = 2$，由 [Toi20, 引理 2.7.4] 可得$B := \phi(A)$是一个 K-近似群。此外，对于每个 $b \in B$，B 的 1-特征子空间的余维数至多为 r。这意味着 B^2 中任意元素的 1-特征子空间的余维数至多为 $s = 2r$。等价地，对于每个 $b \in B^2$，我们有 $\mathrm{rk}(b-1) \leq s$。

现在我们将引理 7.1 应用于 B，这是可行的，因为 $s \geq 6$ （因为 $d \geq 8000$）。我们得到 $\mathbb{F}^d$ 的子空间U 和 W，满足

$$\dim U, \dim W \leq 30s \log\log s < 30s \log\log d = \frac{d}{10}$$

其满足

$$|\{b \in B^2 : (b-1)W^\perp \subset U\}| \geq \frac{1}{(2K)^{60s}}|B^2|.$$

设$\mathbf{V} := \{x \in \mathrm{Mat}_d(\mathbb{F}) : (x-1)W^\perp \subset U\}$。这是 $\mathrm{Mat}_d(\mathbb{F})$ 的一个仿射子空间，并且由于 $\dim U, \dim W < d/10$，它真包含于 $\mathrm{Mat}_d(\mathbb{F})$ 中。因此，我们处于情形（$\star$），其中 $\mathcal{F}$为平凡旗（$\{0\}, \mathbb{F}^d$）、近似群 B，且 $\eta := |B^2 \cap \mathbf{V}|/|B^2| \geq (2K)^{-60s}$。于是，我们可以应用引理 8.3，找到某个子代数 $\mathbf{X} \subset \mathbf{P}_{\mathcal{F}}$，使得 $1+\mathbf{X}$包含于$\mathbf{V}$ 的某个双侧平移 $c_1\mathbf{V}c_2$中，并且满足

$$\frac{|B^2 \cap (1+\mathbf{X})|}{|B^2|} \geq \frac{\eta^{d^4}}{(2K)^{d^6+3}} \geq \frac{1}{(2K)^{d^6+3+60sd^4}} \geq \frac{1}{(2K)^{2d^6-5}}. \tag{8.6}$$

设$\mathbf{V}' := c_1(\mathbf{V}-1)c_2$，从而$\mathbf{V}'c_2^{-1}W^\perp \subset c_1U$；我们有$\mathbf{V}'$是 $\mathrm{Mat}_d(\mathbb{F})$ 的一个真正的子空间。由于 $1 \in 1+\mathbf{X} \subset c_1\mathbf{V}c_2$，我们有 $1 - c_1c_2 \in \mathbf{V}'$。这意味着

$$\mathbf{X} \subset \mathbf{V}' - (1-c_1c_2) = \mathbf{V}'.$$

因此，$\mathbf{X}(c_2^{-1}W^\perp) \subset c_1U$。对$\mathbf{X}$应用引理 8.5，可得存在子空间 $V_1 \subset V_2 \subset \mathbb{F}^d$ 满足

$$\dim V_1 \leq \dim(c_1U) = \dim U < \frac{d}{10},$$
$$\dim V_2 \geq \dim(c_2^{-1}W^\perp) = \dim W^\perp > \frac{9d}{10},$$

以及$\mathbf{X}V_2 \subset V_1$。

现在，令 $H \leq \mathrm{GL}_d(\mathbb{F})$ 为所有满足存在某个标量 λ 使得 $(a-\lambda)V_2 \subset V_1$ 的 $\mathrm{GL}_d(\mathbb{F})$ 的集合。这是 $\mathrm{GL}_d(\mathbb{F})$ 的一个子群，并包含 $1+\mathbf{X}$ 的每个可逆元素。根据引理 2.15，注意到 $\phi|_{A^2}$ 是一个 Freiman 三同态，且 $\phi(A^2) = B^2$，可得

$$\frac{|A^2 \cap H|}{|A^2|} \geq K^{-5}\frac{|A^6 \cap H|}{|A^2|} \geq K^{-5}\frac{|A^6 \cap \phi^{-1}(1+\mathbf{X})|}{|A^2|} \geq K^{-5}\frac{|B^2 \cap (1+\mathbf{X})|}{|B^2|},$$

wher第一步中我们用到了引理 2.13。将此与 (8.6) 结合，即得结果 lt. □

9. Application: Quasi-polynomial bounds in non-abelian Roth's theorem

本节中，我们证明定理 1.10，该定理涉及不含三项等差数列的集合的增长。我们的一些中间步骤也将有助于证明定理 1.6 和定理 1.9，这两个定理将在下一节证明。本节主要关注证明中涉及阿贝尔群与非阿贝尔群之间衔接的部分。我们将陈述阿贝尔情形下所需的所有结果（即引理 9.2 和 9.3），并在第 11 节中证明它们。

本节首先给出定理 1.2 和 1.3 的一个推论，这对我们的两项应用都有帮助。第一部分表明，若 A 符合定理 1.2 和 1.3 中的情形，则存在一个较大的两两交换集，其小倍增且包含于 A 的某个平移中。第二部分是一个类似的“双边”结果，有助于理解平均三项等差数列。

引理 9.1。设 G 是一个群，$d \geq 3$ 是一个整数。假设以下条件之一成立：*(a)* G 是可解的；或 *(b)*G 是有限的，且没有同构于 交错群$_d$的子商。

(1) 设 $A \subset G$ 满足 $|AA^{-1}| \leq K|A|$。那么存在某个阿贝尔子群 $H \leq G$、某个元素 $g \in G$以及某个集合 $A_0 \subset gA \cap H$，使得 $|A_0 A_0^{-1}| \leq (2K)^{O(1)}|A_0|$ 并且

$$|A_0| \geq \exp\left(\Omega\left(\frac{\log^{1/8}|A|}{\exp(O(\log^2 d \log\log d))\log 2K}\right)\right). \tag{9.1}$$

(2) 设 $A \subset G$ 满足 $|A^2| \leq K|A|$。那么存在某个阿贝尔子群 $H \leq G$、某个 $g \in G$，以及某个满足 $|B_0 B_0^{-1}| \leq (2K)^{O(1)}|B_0|$ 的中心化集合 $B_0 \subset H$，

$$\#\big\{(x,y) \in B_0 \times B_0 : xgy \in A\big\} \geq (2K)^{-O(1)}|B_0|^2,$$

and

$$|B_0| \geq \exp\left(\Omega\left(\frac{\log^{1/8}|A|}{\exp(O(\log^2 d \log\log d))\log 2K}\right)\right). \tag{9.2}$$

证明。我们先证明 (1)。由于 $|AA^{-1}| \leq K|A|$，引理 2.14 表明存在一个中心化集合 $B \subset A^{-1}A$，满足 $|B| \geq |A|/2K$，并且

$$|B^m| \leq |AB^m| \leq |AB^m A^{-1}| \leq 2^m K^{2m+1}|B|$$

对所有正整数 m 都成立。特别地，$|B^3| \leq (2K)^{O(1)}|B|$。由定理 1.2 和 1.3，存在某个满足以下条件的两两可交换子集 $T \subset B^4$

$$|T| \geq \exp\left(\Omega\left(\frac{\log^{1/8}|B|}{\exp(O(\log^2 d \log\log d))\log 2K}\right)\right). \tag{9.3}$$

令 $H \leq G$ 为由 G 中的 T 生成的阿贝尔子群；如有必要，可将 T 替换为更大的交换集，从而不妨设 $T = B^4 \cap H$。现在，

$$\sum_{g \in TT^{-1}A^{-1}} |gA \cap TT^{-1}| = \sum_{a \in A} \sum_{b \in TT^{-1}} 1_{TT^{-1}A^{-1}}(ba^{-1}) = |A| \cdot |TT^{-1}|.$$

因此，存在某个 $g \in TT^{-1}A^{-1}$，使得 $A_0 := gA \cap TT^{-1} \subset gA \cap H$ 满足

$$|A_0| \geq \frac{|A| \cdot |TT^{-1}|}{|TT^{-1}A^{-1}|} = \frac{|A| \cdot |TT^{-1}|}{|ATT^{-1}|} \geq \frac{|A| \cdot |TT^{-1}|}{|AB^8|} \geq (2K)^{-O(1)}|TT^{-1}|. \tag{9.4}$$

结合 (9.3) 和 (9.4)，可知 A_0 足够大，满足 (9.1)。我们只需给 $|A_0 A_0^{-1}|$ 一个上界。我们有 $|B^{10}| \leq 2^{10}K^{21}|B| \leq 2^{10}K^{21}|B^2|$。因此，由 Ruzsa 覆盖引理可知，$B^4$ 是一个 $(2K)^{O(1)}$-近似群。因此，根据引理 2.13 和 (9.4)，我们有

$$|A_0 A_0^{-1}| \leq |(TT^{-1})(TT^{-1})^{-1}| \leq |B^{16} \cap H| \leq (2K)^{O(1)}|T| \leq (2K)^{O(1)}|A_0|.$$

这就完成了 (1) 的证明。

（2）的证明相当类似，但我们用 [Toi20, 定理 2.5.6] 代替引理 2.14。根据更强的假设 $|A^2| \leq K|A|$，我们可以找到一个子集 $B \subset A$，满足 $|B| \geq |A|/K$，且对于所有 m 都有 $|B^m| \leq K^{m-1}|B|$。此外，集合 $B' := (B \cup B^{-1} \cup \{1\})^2$ 是一个 $(2K)^{O(1)}$-近似群，其大小至多为 $7K^2|A|$，且至多 K^2 个左平移或右平移即可覆盖 A。根据定理 1.2 和 1.3，存在某个两两可交换子集 $T \subset (B \cup B^{-1} \cup \{1\})^4 \subset (B')^2$，满足大小界（9.3）。和之前一样，令 $H \leq G$ 为由 G 中的 T 生成的阿贝尔子群。令 $B_0 := (B')^2 \cap H$。由于 $B_0 \supset T$，（9.3）足以推出 B_0 足够大，从而满足（9.2）。现在，引理 2.13 推出 B_0 是一个 $(2K)^{O(1)}$-近似群，因此有 $|B_0 B_0^{-1}| \leq (2K)^{O(1)}|B_0|$。最后，（利用 B_0 含单位元）可得

$$\sum_{g \in B_0 B B_0} \#\{(x,y) \in B_0 \times B_0 : xgy \in A\} \geq \sum_{g \in B_0 B B_0} \#\{(x,y) \in B_0 \times B_0 : xgy \in B\} = |B| \cdot |B_0|^2,$$

因此存在某个 $g \in G$，使得

$$\#\{(x,y) \in B_0 \times B_0 : xgy \in A\} \geq \frac{|B| \cdot |B_0|^2}{|B_0 B B_0|}$$
$$\geq \frac{|B| \cdot |B_0|^2}{|(B')^5|} \geq \frac{|B| \cdot |B_0|^2}{(2K)^{O(1)}|B'|} \geq (2K)^{-O(1)}|B_0|^2. \qquad \square$$

9.1. 三项等差数列。现在我们转而关注不含三项等差数列的集合。我们先陈述阿贝尔情形下的以下两个结果，并将在第 11 节中证明它们。其证明结合了 [San12] 的主要结果——（本质上）弗雷曼–鲁扎定理的准多项式界——以及 Kelley 和 Meka [KM23] 关于 Roth 定理的最新进展，还有 Jaber、Liu、Lovett、Ostuni 和 Sawhney [JLL+25] 关于角定理的最新进展。在接下来的两个陈述中，我们对阿贝尔群使用加法记号。本节其他部分则一律使用乘法记号，即使对于包含在阿贝尔群中的集合也是如此。

引理 9.2 (阿贝尔局部罗斯定理)。 存在一个绝对常数 $c > 0$，使得以下结论成立。设 G_0 是一个阿贝尔群。设 $A \subset G_0$ 是一个子集，且若 x、$x+y$、$x+2y \in A$，则 $y = 0$。[14] 那么

$$\frac{|A-A|}{|A|} \geq \exp\Big(c \log^{1/144}|A|\Big).$$

引理 9.3 （阿贝尔局部角定理）。 存在一个绝对常数 $c > 0$，使得以下结论成立。设 G_0 是一个阿贝尔群。设 $B \subset G_0$ 是任意子集，并假设 $A \subset B \times B$ 满足：若 $(x,\ y)$，$(x+d,\ y)$，$(x,\ y+d) \in A$，则 $d = 0$。那么

$$\frac{|B-B|^2}{|A|} \geq \exp\Big(c \log^{1/7200}|B|\Big).$$

现在我们利用引理9.1至9.3证明定理 1.10。引理 9.1 的第一部分与罗斯型引理9.2将用于证明平移版本，而引理 9.1 的第二部分与角型引理9.3将用于证明平均版本。

定理*1.10*的证明。 回顾一下我们的情形：给定一个群 G 和一个有限子集 $A \subset G$。群 G 要么 (a) 是可解的，要么 (b) 是有限群，且不含同构于 $(\mathbb{Z}/2\mathbb{Z})^d$ 的子群，其中 $d = \exp(c\sqrt{\log\log|A|}/\log\log\log|A|)$（而 $c > 0$ 是一个我们可以自行选择的常数）。集合 A 不含平移型（分别为平均型）三项等差数列，我们希望给 $|AA^{-1}|/|A|$ （分别为 $|A^2|/|A|$）一个下界。

根据引理2.8，(b) 中的条件意味着 G没有同构于$(\mathbb{Z}/2\mathbb{Z})^{2d^2}$的子商。特别地，由于交错群 $\mathrm{A}_{d'}$ 有一个同构于$(\mathbb{Z}/2\mathbb{Z})^{\lfloor d'/2 \rfloor - 1}$ 的子群，且 G 的子商的子群也是 G的子商，我们得出 G 没有同构于 A_{4d^2+3}的子商。将 c 选得足够小后，我们对 d的选择也足够小，可以应用引理 9.1。

现在我们专门讨论平移型三项等差数列。假设 A 不含非平凡的平移型三项等差数列，并令 $K := |AA^{-1}|/|A|$。根据引理 9.1(1)，我们找到一个阿贝尔子群 $H \leq G$、某个$g \in G$以及一个满足 $|A_0 A_0^{-1}| \leq (2K)^{O(1)}|A_0|$ 的集合 $A_0 \subset gA \cap H$，并且

$$|A_0| \geq \exp\left(\Omega\left(\frac{\log^{1/8}|A|}{\exp(O(\log^2(4d^2+3)\log\log(4d^2+3)))\log 2K}\right)\right) \geq \exp\left(\Omega\left(\frac{\log^{1/9}|A|}{\log 2K}\right)\right) \tag{9.5}$$

（其中，后一个不等式可通过充分小地选取 c 得到）。由于 A_0 包含在 A 的一个左平移中，A_0 不含非平凡平移型三项等差数列这一性质也适用于

[14] 正如定理 1.10 的表述中所指出的，如果 G_0 有 2-挠，我们允许 $2y = 0$。

A_0。莫 此外， $A_0 \subset H$ 是阿贝尔群的一个子集。因此，我们应用引理 9.2，得到

$$(2K)^{O(1)} \geq \frac{|A_0 A_0^{-1}|}{|A_0|} \geq \exp\Big(\Omega\Big(\log^{1/144}|A_0|\Big)\Big). \tag{9.6}$$

结合 (9.5) 和 (9.6) 得到

$$\log 2K \gtrsim \log^{1/144}|A_0| \gtrsim \frac{\log^{1/1296}|A|}{\log^{1/144} 2K} \implies \log 2K \gtrsim \log^{1/1305}|A|.$$

这就证明了 (1)。

现在我们处理平均三项等差数列。假设 A 不包含非平凡的平移型三项等差数列，并令 $K := |A^2|/|A|$。由引理 9.1(2)，我们可找到某个阿贝尔子群 $H \leq G$、某个 $g \in G$，以及某个含单位元的集合 $B_0 \subset H$，满足 $|B_0 B_0^{-1}| \leq (2K)^{O(1)}|B_0|$ 且

$$(2K)^{-O(1)}|B_0|^2 \leq \#\big\{(x,y) \in B_0 \times B_0 : xgy \in A\big\}; \tag{9.7}$$

$$|B_0| \geq \exp\left(\Omega\left(\frac{\log^{1/9}|A|}{\log 2K}\right)\right). \tag{9.8}$$

令 $S := \{(x,\ y) \in B_0 \times B_0 :\ xgy^{-1} \in A\}$。由于 B_0 是含单位元的，(9.7) 推出 $|S|/|B_0|^2 \geq (2K)^{-O(1)}$。另一方面， S不含角形：若 $(x,\ y)$，$(xd,\ y)$，$(x,\ yd) \in S$，则

$$(xgy^{-1})^2 = xgy^{-1}d^{-1}dxgy^{-1} = (xg(yd)^{-1})((xd)gy^{-1})$$

只要 $d \neq 1$，就能在 A 中得到一个非平凡的平均三项等差数列。因此，由于 $S \subset B_0 \times B_0$ 和 B_0 位于阿贝尔群 H 中，引理 9.3 蕴含

$$\exp\Big(\Omega\Big(\log^{1/7200}|B_0|\Big)\Big) \leq \frac{|B_0 B_0^{-1}|^2}{|S|} = \frac{|B_0|^2}{|S|}\left(\frac{|B_0 B_0^{-1}|}{|B_0|}\right)^2 \leq (2K)^{O(1)}.$$

将该界与 (9.8) 比较可得

$$\log^{7200} 2K \gtrsim \log|B_0| \gtrsim \frac{\log^{1/9}|A|}{\log 2K},$$

这足以得到该结果。 □

10. 应用：拉姆齐凯莱图

在本节中，我们使用定理 1.3 以及来自 [CFPY24] 的结果来证明定理 1.6 和定理 1.9。与上一节一样，我们将需要一些来自（阿贝尔）加性组合学的结果，其证明将推迟到第 11 节。

我们首先概述 [CFPY24] 中关于阿贝尔情形下拉姆齐凯莱图存在性的证明。该工作的一项主要内容是以下计数结果，其证明仅使用组合论论证。

定理 10.1 ([CFPY24，定理 1。2])。 对于 $C = 6000$，以下结论成立：若 G 是一个阶为 N 的有限群，且 $n < N$ 是一个正整数，则大小为 n 、满足$|AA^{-1}| \leq Kn$ 的子集 $A \subset G$ 的数量至多为 $N^{C(K+\log n)}(2^C K)^n$.[15]

定理 10.1 与拉姆齐性质的关系如下：集合 $A \subset G$ 是 Cay(G, S) 中的团（分别为独立集），当且仅当 $AA^{-1} \setminus \{1\} \subset S$ （分别为 $AA^{-1} \setminus \{1\} \subset G \setminus S$）。

考虑从群 G 中均匀随机选取一个对称子集 S，并构造凯莱图 $\Gamma := \text{Cay}(G,\ S)$。集合 A 在 Γ 中构成团或独立集的概率至多为 $2^{-(|AA^{-1}|-3)/2}$。令 $n := \lceil C_1 \log N \rceil$，其中 C_1是某个较大的常数。对所有

[15]文中未给出常数 C 的具体值 [CFPY24], ，但从他们的论证中很容易得出 6000 这一取值；为明确起见，我们在此列出该值。此外，在 [CFPY24，定理 1.2], 中， 2^C 写作 C，但在他们的结果中， K 上的常数乘数约为 2^{1000} ，因此我们将其界定为 2^C ，以使 C 的取值保持适中。

$A \subset G$ 的集合应用并集界，并利用定理 10.1，可知以高概率，图 Γ 中不存在满足 $|AA^{-1}| \geq C_2 n \log n$ 的、大小为 n 的团或独立集 A（其中 C_2 是依赖于 C_1的某个常数）。因此，我们只需关注满足 $|AA^{-1}| = O(|A|\log|A|)$的那些集合 A。另一方面，对于比如 $G = (\mathbb{Z}/5\mathbb{Z})^n$ 的情形，即使当 $K = 1$时，定理 10.1 也几乎是紧的；而当 K较小时，并集界会失效：随机凯莱图 Γ 的团数约为 $\log|G|\log\log|G|$，而不是 $\log|G|$。

在 [CFPY24] 中，处理这类问题的方法是非均匀地选取随机生成集 S。具体而言，对于 G 阿贝尔群，若 $\gcd(|G|,6) = 1$，Conlon、Fox、Pham 和 Yepremyan 构造了一种定义在 G 的子集 S 上的分布（见 [CFPY24，第 4.2] 节），它具有足够的独立性，使前一段中的论证得以进行；同时，它还确定性地具有“避开子群”的性质：若 $x \neq 1$，则 $\{x, x^2, x^4, x^8\} \cap S$ 和 $\{x, x^2, x^4, x^8\} \cap (G \setminus S)$ 均非空。这保证了在所得的随机凯莱图中，任何满足 AA^{-1} 含有模式$\{x, x^2, x^4, x^8\}$ 的非平凡实例的集合 A，都不可能是团或独立集。利用 Pl¨ünnecke 不等式的论证 [CFPY24，引理 4.5] 表明，这样的集合必须满足$|AA^{-1}| \geq |A|^{1+1/144}$，因此，结合定理 10.1 使用并集界，足以得到所需结论。

对于非阿贝尔群 G，也可以完成这一构造。然而，利用 Pl¨unnecke 不等式的论证不再适用。我们使用定理 1.3 来绕过这一问题。若 $A \subset G$ 满足 $|AA^{-1}|$ 很小，那么定理 1.3（见引理 9.1）可给出一个包含在 A 的某个平移中的大交换集。随后，我们便可以利用映射 $A \mapsto AA^{-1}$ 的平移不变性来证明以下结果。

引理 10.2。对于每个正整数 r，都存在某个 $\eta_r \geq$ 指数函数$(-O($对数$^2 r$ 对数对数 $r))$，使得以下结论成立。假设 2^r 和 3^r 均不整除 $|G|$。假设 $A \subset G$ 满足如下性质：若 $\gcd(\mathrm{ord}(x),6) = 1$ 且 x、x^2、x^4、$x^8 \in AA^{-1}$，则 $x = 1$。那么

$$|AA^{-1}| > |A| \exp\Big(\eta_r \log^{1/16}|A|\Big).$$

我们将在第 10.3 节证明引理 10.2。

10.1. 构造拉姆齐凯莱图。现在我们已经概述了这一方法，接下来陈述凯莱图的随机化构造。随后，我们利用定理 10.1（即 [CFPY24，定理 1.2]）和引理 10.2 证明定理 1.6。该构造与 [CFPY24] 中使用的构造非常相似。

构造 10.3。设 G 为一个群。按如下方式随机选取 S 自 G。首先，将 $G \setminus \{1\}$ 的元素按照关系 $g \sim g^{-1}$划分为等价类。接着，在这些等价类之间构造一个图 Π：对于每个阶为奇数的 $x \in G \setminus \{1\}$，将 $x \sim x^{-1}$ 与 $x^2 \sim x^{-2}$ 连接。图 Π由若干环、自环（对应于阶为 3 的 G元素）以及孤立顶点（对应于阶为偶数的 G元素）组成。在 Π中找到一个极大匹配Σ。分别独立地执行以下操作：

- 对于每个不与匹配 Σ 中任何边关联的顶点 $g \sim g^{-1}$，以概率 $1/2$ 将 $\{g, g^{-1}\}$ 放入 S。
- 对于匹配 Σ 中的每条边 $(g \sim g^{-1}, g^2 \sim g^{-2})$，均匀随机地将 $\{g, g^{-1}\}$ 或 $\{g^2, g^{-2}\}$ 中的一个放入S。

我们将此构造的关键性质表述为以下两个简单引理，它们与 [CFPY24, Claims4.3 and 4.4] 非常相似。

引理 10.4。 **</style}对于任意集合，由构造 10.3 生成的 Cay(**G, S**)** </style} 中的 是团或独立集的概率至多为 $)^{/2}$。

证明。集合 A 是 Γ 中的团或独立集，当且仅当 $AA^{-1} \setminus \{1\} \subset S$ 或 $AA^{-1} \setminus \{1\} \subset G \setminus S$。由于 S 和 $G \setminus S$ 具有相同的分布，只需证明$AA^{-1} \setminus \{1\} \subset S$ 的概率至多为 $2^{-(|AA^{-1}|-1)/2}$。

令 Σ 为构造 10.3 中构造的匹配。如果 AA^{-1} 包含 Σ 的任何边，那么$AA^{-1}\setminus\{1\}$ 永远不可能属于 S。否则，对于 $g\in AA^{-1}\setminus\{1\}$ 的等价类 $g\sim g^{-1}$，它们各自独立地以概率 $1/2$ 属于 S。结论得证。□

引理 10.5. 设 $A\subset G$，并假设存在某个 $x\in G\setminus\{1\}$ 满足 $\gcd(\mathrm{ord}(x),6)=1$ 且 $x,x^2,x^4,x^8\in AA^{-1}$。那么，确定地，A 在由构造 *10.3* 生成的任何凯莱图 $\Gamma=\mathrm{Cay}(G,S)$ 中既不是团，也不是独立集。

证明. 等价类 $\{x\sim x^{-1},x^2\sim x^{-2},x^4\sim x^{-4},x^8\sim x^{-8}\}$（并非一定彼此不同）按此顺序位于辅助图 Π 中的一个圈上，该辅助图由构造 10.3 构造而成。由于 $\gcd(\mathrm{ord}(x),6)\neq 1$，这个圈不是自环。现在，由于 Σ 是 Π中的一个极大匹配，它必定包含以下边中的至少一条

$$\big\{(x\sim x^{-1},x^2\sim x^{-2}),(x^2\sim x^{-2},x^4\sim x^{-4}),(x^4\sim x^{-4},x^8\sim x^{-8})\big\}.$$

这意味着，G 中的这四对元素不可能同时全都属于 S，也不可能同时全都属于 $G\setminus S$。因此，存在某些 b_1，$b_2\in AA^{-1}\setminus\{1\}$ 使得 $b_1\in S$ 且 $b_2\notin S$。由此可得，A 既不是 Γ中的团，也不是独立集。□

定理 1.6 现在可由以下一般性结果推出。

引理 10.6。设 $C_0>0$ 和 $c_0\in(0,1)$ 为常数。设 G 为有限群，且 $\mathcal{D}$ 为 G 的子集上的概率分布，使得若 $S\sim\mathcal{D}$ 和 $\Gamma=\mathrm{Cay}(G,S)$，则满足以下两个性质：

(i) 对任意集合 $A\subset G$，A 是 Γ 中的团或独立集的概率至多为$C_0\cdot 2^{-c_0|AA^{-1}|}$。*(ii)* 任意大小为 $n=\lceil 12000c_0^{-1}\log|G|\rceil$ 且满足 $|AA^{-1}|\le 20c_0^{-1}n\log n$的 $A\subset G$，确定地既不是 Γ中的团，也不是独立集。

假设相对于 C_0 和 c_0，N 足够大。那么，图 Γ 是 $12000c_0^{-1}$-*Ramsey Cayley* 图的概率至少为 $1-1/N$。

证明。这个引理 本质上是定理 10.1 的推论，所用论证见 [CFPY24, 定理 4.2] 的证明。为完整起见，我们在此给出证明。

令 $C:=6000$ 为定理 10.1 中给出的常数。记 $C_1:=2Cc_0^{-1}$。令 $N:=|G|$ 和 $n:=\lceil C_1\log N\rceil$。我们可以假设 $n\ge 2^{4C}$。根据条件 (ii)，在 Γ 中，任何大小为 n 且满足$|AA^{-1}|\le 20c_0^{-1}n\log n$ 的子集 $A\subset G$ 都既不是团，也不是独立集。

剩下要证明的是，大小为 n、且 $|AA^{-1}|$ 大于此阈值的集合 A 不太可能是团或独立集。固定某个 $m\in[20c_0^{-1}n\log n,n^2]$，并令 $K:=m/n$。考虑满足 $|A|=n$ 和 $|AA^{-1}|=m$ 的那些集合。根据定理 10.1，这样的集合至多有 $N^{C(K+\log n)}(CK)^n$ 个。由 (i) 可知，每个这样的集合在 Γ 中成为团或独立集的概率不超过 $C_0\cdot 2^{-c_0m}$。由并集界可知，Γ 中存在任何一个这样的集合成为团或独立集的概率至多为

$$\begin{aligned}C_0 2^{-c_0Kn}N^{C(K+\log n)}(2^CK)^n &\le C_0\left(2^{-c_0K}e^{C_1^{-1}C(K+\log n)}2^Cn\right)^n\\ &= C_0\exp\Big(n\Big(-c_0K\log 2+\frac{c_0}{2}(K+\log n)+C\log 2+\log n\Big)\Big)\\ &\le C_0\exp\left(n\left(\frac{5}{2}\log n-c_0K\left(\log 2-\frac{1}{2}\right)\right)\right)\le C_0\exp(-n\log n),\end{aligned}$$

因为 $K\ge 20c_0^{-1}\log n$。对 m 的所有可能取值应用并集界可知，以至少 $1-C_0n^{-(n-2)}$ 的概率，在 Γ 中不存在大小为 n 的团或独立集。证明至此完成。□

现在我们可以证明定理 1.6 了。

定理 *1.6* 的证明。设 r 是一个正整数，G 是一个阶既不是 2^r 的倍数，也不是 3^r 的群。我们必须证明，只要 $|G|$ 相对于 r 足够大，群 G 就有一个 24000-拉姆齐凯莱图。

我们将引理 10.6 应用于由构造 10.3 给出的、定义在 G 的子集上的概率分布，其中取 $C_0 = 2^{3/2}$ 和 $c_0 = 1/2$。令 S 从该分布中选取，并令 $\Gamma := \mathrm{Cay}(G, S)$。根据我们对 C_0 和 c_0 的选择，条件 (i) 表明，集合 A 在 Γ 中为团或独立集的概率至多为 $2^{(|AA^{-1}|-3)/2}$；这正是引理 10.4。

取 $n := \lceil 24000 \log |G| \rceil$。为验证引理 10.6 的条件 (ii)，我们必须证明，任何大小为 n、且有可能（即以非零概率）在 Γ 中成为团或独立集的集合 A，都必须满足 $|AA^{-1}| > 40n \log n$。这由引理 10.2、引理 10.5 及一些计算可得。事实上，根据引理 10.5，对于阶与 6 互素的 $x \neq 1$，任何这样的集合 A 都必须避开模式 $\{x, x^2, x^4, x^8\}$。接着，根据引理 10.2，任何这样的集合都必须满足

$$|AA^{-1}| \geq n \exp\Big(\eta_r \log^{1/16} n\Big), \tag{10.1}$$

对于某个 $\eta_r \geq \exp(-O(\log^2 r \log\log r))$。回想一下，我们的条件是：整除 N 的 2 和 3 的幂的最大乘积至多为 $\exp(\exp((\log\log\log N)^{1/3}))$。这意味着上界为 $r \leq 2\exp((\log\log\log N)^{1/3})$，因此（当 N 大于某个绝对常数时）

$$\log^2 r \log\log r \leq 2(\log\log\log N)^{3/4}.$$

因此，只要 N 足够大，我们就有 $\eta_r \geq \exp(-(\log\log\log N)^{3/4}) > \log^{-1/32} n$。由 (10.1)，进而有 $|AA^{-1}| \geq n \exp(\log^{1/32} n) > 40n \log n$。这证明了条件 (ii)，并完成了证明。□

10.2. **推广定理 1.6**。现在我们修改构造 10.3，以证明定理 1.9：在不含大型初等 2-子群或 3-子群，也不含（特定的）大型循环子群的群中寻找拉姆齐凯莱图。关于当这些子群中的任意一种出现时我们的方法为何失效，见第 12.2 节。

我们用来证明定理 1.9 的构造推广了构造 10.3。对于偶数阶群，这种构造并非特别有用，因为引理 10.5 中的“避子群”性质完全忽略了 2-挠和 3-挠。为此，我们必须用其他配对方式取代 $\{x, x^2\}$，以处理偶数阶元素。一种自然的推广是：对 x 和 x^q 进行配对，其中 q 是使其不整除 x的最小素数。这基本上就是我们所做的：

构造 10.7。设 G是一个群。按如下方式随机选取 S 的一个子集 G。首先，按照关系 $g \sim g^{-1}$将 $G \setminus \{1\}$ 中的元素划分为等价类。接着，在这些等价类之间构造一个图 Π：每个 $x \sim x^{-1}$ 都与 $x^q \sim x^{-q}$ 相连，其中 q 是使其不整除 x的最小素数。（选择 q 也是使其不整除 x^q的最小素数。）图 Π 是若干环和自环的并。求出 Π中的一个极大匹配 Σ。独立地执行以下操作：

- 对于每个未与匹配 Σ 中任何边关联的顶点 $g \sim g^{-1}$，以概率 $1/2$ 将 $\{g, g^{-1}\}$ 放入 S。
- 对于匹配 Σ 中的每条边 ($g \sim g^{-1}$，$g^q \sim g^{-q}$)，均匀随机地将 $\{g, g^{-1}\}$ 或 $\{g^q, g^{-q}\}$ 之一放入 S。

现在，我们必须证明构造 10.7 中引理 10.4 和 10.5 的类似命题。引理 10.4 在此情形下仍然原封不动地成立；引理 10.5 的类似命题则复杂得多。

引理 10.8。对于任意集合 $A \subset G$，以下性质成立。

(1) A 在由构造 *10.7* 生成的 $\Gamma := \mathrm{Cay}(G, S)$ 凯莱图中是团或独立集的概率至多为 $2^{-(|AA^{-1}|-3)/2}$。

(2) 假设存在 $x \in G$，其阶不能被 24 整除，并且若 q 是不能整除 x的阶的最小素数，则 $x, x^q, x^{q^2}, x^{q^3} \in AA^{-1}$。那么，确定地说， A 既不是由构造 *10.7* 生成的任何凯莱图 $\Gamma := \mathrm{Cay}(G, S)$ 中的团，也不是独立集。

在证明引理 10.8 之前，我们需要下面这个简单引理，它说明了引理 10.8(2) 中常数 24 的由来。

引理 10.9. 对于任意 $m \nmid 24$，不整除 m 的最小素数 q 满足 $m \nmid q^2 - 1$.

证明。 q 的定义蕴含 $\prod_{q'<q} q' \mid m$，其中乘积仅对素数取值。初等的 Bonse不等式指出，若 $q > 7$，则 $\prod_{q'<q} q' > q^2$ ；由此可得，若 $q \geq 11$，则 $m > q^2$ 。否则， $m \mid q^2 - 1$ 蕴含 $m \mid 48$。结果很容易手工验证。□

引理 *10.8* 的证明。 首先，第 (1) 部分的证明与引理 10.4 的证明相同。若 AA^{-1} 包含 Σ 的任意边，则 $AA^{-1} \setminus \{1\}$ 既不能包含在 S 中，也不能包含在 $G \setminus S$ 中。否则， $AA^{-1} \setminus \{1\}$ 中某个特定元素属于 S 这一事件，与至多另一个元素（其逆元）属于其中的事件相互独立，结论由此得出。

对于第 (2) 部分，设 x 的阶为 $m \nmid 24$， q 是不整除 m 的最小素数，而A满足 x， x^q， x^{q^2}， $x^{q^3} \in AA^{-1}$。等价类 $T := \{x \sim x^{-1}, x^q \sim x^{-q}, x^{q^2} \sim x^{-q^2}, x^{q^3} \sim x^{-q^3}\}$ （它们不一定两两不同）按此顺序位于构造 10.7 中构造的辅助图 Π 的一个圈上。设 ℓ 为相应圈的长度。由于$m \nmid 24$，引理10.9推出 $m \nmid q^2 - 1$。因此 x 既不等于 x^q，也不等于 x^{-q}，且 $\ell > 1$。

若 $\ell \geq 4$，则 T 构成 Π中一个圈上连续的四个顶点，因此包含极大匹配 Σ中的某条边。若 $2 \leq \ell < 4$，则 T 构成一个完整的圈，因此包含Σ中的某条边。无论哪种情况， $x^{q^i} \sim x^{-q^i}$ 与 $x^{q^{i+1}} \sim x^{-q^{i+1}}$ 之间都存在一条边，其中某个 $0 \leq i < 3$ 属于 Σ；因此，若 x^{q^i}， $x^{q^{i+1}} \in AA^{-1}$，则 A 在 Σ中既不是团，也不是独立集。□

定理 1.9 现在将以与定理 1.6 大致相同的方式，由定理 10.1、引理 10.8 以及下面这个类似引理 10.2 的命题推出。

引理 10.10。 存在一个绝对常数 $c > 0$，使得以下结论成立。

设 G 为有限群。设 Q、 r和 n 为正整数，其中 n 充分大， $r \leq$指数函数$(c\sqrt{\text{对数 对数 } n/\text{对数 对数 对数 } n})$，且 $Q \leq$指数函数$(\text{对数}^{1/27} n)$。假设 G 没有阶为 $\mathrm{lcm}(1, \ldots, Q)$ 的循环子群，没有同构于 $(\mathbb{Z}/2\mathbb{Z})^r$ 的子群，也没有同构于 $(\mathbb{Z}/3\mathbb{Z})^r$ 的子群。

假设大小为 n 的 $A \subset G$ 满足以下性质：若 x 是 G 的任意元素，且其阶不整除24，并且 q 是一个不整除 x的阶的最小素数，则 $\{x, x^q, x^{q^2}, x^{q^3}\} \not\subset AA^{-1}$。那么

$$|AA^{-1}| \geq |A| \exp\Big(\log^{1/118} |A|\Big).$$

我们将在下一个小节中证明引理 10.10。

定理 *1.9* 的证明。 令 $N := |G|$，并令 $n := \lceil 24000 \log N \rceil$。我们可以假设 n 足够大。我们必须证明，只要 G 不包含与 $(\mathbb{Z}/2\mathbb{Z})^r$ 或 $(\mathbb{Z}/3\mathbb{Z})^r$ 或 $\mathbb{Z}/\mathrm{lcm}(1, \ldots, Q)\mathbb{Z}$ 同构的子群，其中 $r := \lfloor \exp((\log\log\log N)^{1/3}) \rfloor$ 且 $Q := \lfloor \exp((\log\log N)^{1/27}) \rfloor$，那么 G 就有一个 24000-拉姆齐凯莱图。

我们将引理 10.6 应用于由构造 10.7 给出的 G 的子集上的概率分布，其中取 $C_0 = 2^{3/2}$ 和 $c_0 = 1/2$ 。从该概率分布中选取 S，并令 $\Gamma := \mathrm{Cay}(G, S)$。引理 10.6 的条件 (i)，在我们选择 C_0 和 c_0 的情况下，恰好就是引理 10.8(1)。剩下需要验证引理 10.6 的条件 (ii)。

只需证明，对于充分大的 N，任何大小为 n的集合 A，若有可能（即概率非零）成为 Γ 中的团或独立集，就必须满足 $|AA^{-1}| \geq n$指数函数$(\log^{1/118} n)$。考虑这样一个集合 A。我们首先应用引理 10.8(2)，得出对于任意阶不整除 24 的 $x \in G$，若 q是不能整除 x的阶的最小素数，则 x， x^q， x^{q^2}， x^{q^3} 不可能全部属于 AA^{-1}。由于 $n \geq \log N$，定理 1.9 的陈述中给出的关于 G 的避子群条件

足以推出引理 10.10 的避子群条件。因此，我们可以将引理 10.10 应用于 $A \subset G$，从而得出结论。□

10.3. 避免 AA^{-1} 中的模式。 为完成定理 1.6 和定理 1.9 的证明，我们只需证明引理 10.2 和引理 10.10。我们将从阿贝尔情形下的以下两个命题推出这两个引理。第一个命题引自 [CFPY24], ，可由鸽巢原理和 Pl¨unnecke–Ruzsa 不等式推出；第二个命题将在第 11 节证明。

引理 10.11 ([CFPY24，引理 4。5]的特例)。 设 G_0 为阿贝尔群， $A \subset G_0$为其子集，且若 $x, 2x, 4x, 8x \in A - A$，则 $x = 0$。那么

$$|A - A| \geq |A|^{1+1/144}.$$

引理 10.12。 设 G_0 为有限阿贝尔群。设 Q、 r和 n为正整数，且 n充分大， $r \leq \log^{1/3} n$，且 $Q \leq \exp(\log^{1/3} n)$。假设 G_0 没有阶为$\mathrm{lcm}(1,\dots,Q)$的循环子群，没有与$(\mathbb{Z}/2\mathbb{Z})^r$同构的子群，也没有与$(\mathbb{Z}/3\mathbb{Z})^r$同构的子群。

设 A 是 G_0的子集，并假设 A 满足 $|A| = n$ 和 $|A - A| \leq Kn$。假设$K \leq$ 指数函数$(\log^{1/13} n)$。那么存在某个素数 q 和某个 $t \in G_0$，使得

(1) t 的阶不整除24，*(2)* 每个素数 $q' < q$ 都整除 t的阶，但 q 不整除 t的阶，且

(3) $t, qt, q^2t, q^3t \in A - A$。

引理 *10.2* 的证明。 回想一下，我们在某个所在有限群 G 中有一个集合 $A \subset G$，其阶既不是 2^r 的倍数，也不是 3^r的倍数。此外， A 满足如下性质：若 $\gcd(\mathrm{ord}(x),6) = 1$且 $x, x^2, x^4, x^8 \in AA^{-1}$，则 $x = 1$。我们试图给 $|AA^{-1}|$ 一个下界。令 $K := |AA^{-1}|/|A|$。

我们首先注意到，由于 2^r 不能整除 G的任何子商的阶，群 G没有同构于交错群 A_{2r+2}的子商。这使我们能够对 $A \subset G$应用引理 9.1(1)。我们可找到某个阿贝尔子群 $H \leq G$、某个元素 $g \in G$以及某个集合 $A_0 \subset gA \cap H$，使其满足$|A_0 A_0^{-1}| \leq (2K)^{O(1)}|A_0|$ 并且

$$|A_0| \geq \exp\left(\Omega\left(\frac{\log^{1/8}|A|}{\exp(O(\log^2 r \log\log r))\log 2K}\right)\right). \tag{10.2}$$

令 $H_1 \leq H$ 为 H 中阶与 2 和 3 互素的极大子群（由于 H 是阿贝尔群，这样的子群是唯一的）。由于 H 的阶既不是 2^r 的倍数，也不是 3^r的倍数，因此 H_1 在 H 中的指数至多为 $2^{r-1}3^{r-1}$。特别地，我们可以找到某个子集 $A_1 \subset A_0$，它包含于 H_1 的某个左平移中，并满足 $|A_1| \geq 6^{-r}|A_0|$。

我们假设 A 具有模式避免性质（即 AA^{-1} 避免了模式 x， x^2， x^4， x^8，并满足某些条件）。该性质在左平移和取子集的操作下保持不变，因此 A_1 也满足相同的模式避免性质。此外，由于 $A_1A_1^{-1}$属于 H_1的某个共轭子群， $A_1A_1^{-1}$的每个元素的阶都与 6 互素。由此可知， A_1 满足更强的性质，即 $A_1A_1^{-1}$避免模式 $\{x, x^2, x^4, x^8\}$ 的所有 实例，且 $x \neq 1$。由于 A_1 包含于一个阿贝尔群中，我们可以应用引理 10.11 证明

$$(2K)^{O(1)}|A_0| \geq |A_0A_0^{-1}| \geq |A_1A_1^{-1}| \geq |A_1|^{1+1/144} \geq (6^{-r}|A_0|)^{1+1/144}.$$

整理上式可得 $|A_0| \leq 2^{O(r)}(2K)^{O(1)}$。将此界与 (10.2) 比较，得到

$$r + \log 2K \gtrsim \log|A_0| \gtrsim \frac{\log^{1/8}|A|}{\exp(O(\log^2 r \log\log r))\log 2K}.$$

这足以推出该结论。 □

引理 *10.10* 的证明。 回忆 $n = |A|$。令 $K := |AA^{-1}|/|A|$，并反设 $K \leq \exp(\log^{1/118} n)$。

首先，我们应用引理 2.8：假设 G 没有同构于 $(\mathbb{Z}/2\mathbb{Z})^r$的子群，这意味着 G 没有同构于 $(\mathbb{Z}/2\mathbb{Z})^{2r^2}$的子商。特别地，由于交错群 交错群$_d$ 有一个同构于 $(\mathbb{Z}/2\mathbb{Z})^{\lfloor d/2\rfloor-1}$的子群，我们得出 G 没有同构于 交错群$_{4r^2+3}$的子商。我们将引理 9.1(1)应用于 $A\subset G$。我们找到某个阿贝尔子群 $H\leq G$、某个元素 $g\in G$以及某个集合 $A_0\subset gA\cap H$，它满足$|A_0A_0^{-1}|\leq(2K)^{O(1)}|A_0|$ 并且

$$|A_0|\geq\exp\left(\Omega\left(\frac{\log^{1/8}|A|}{\exp(O(\log^2 r\log\log r))\log 2K}\right)\right). \tag{10.3}$$

令 $n':=|A_0|$。回忆 $K\leq\exp(\log^{1/117}n)$。取足够小的 c，则 (10.3) 足以推出 $n'\geq\exp(\log^{1/9}n)$。

我们假设 A 具有的模式避免性质在左平移和取子集合下保持不变，因此 $A_0\subset H$ 也满足相同的模式避免性质。此外， H 是G的一个子群，因此它没有阶为 $\operatorname{lcm}(1,\dots,Q)$ 且满足 $Q\leq\exp(\log^{1/27}n)\leq\exp(\log^{1/3}n')$ 的循环子群，没有同构于 $(\mathbb{Z}/2\mathbb{Z})^r$ 的子群，也没有同构于 $(\mathbb{Z}/3\mathbb{Z})^r$ 的子群，其中

$$r\leq\exp\left(c\sqrt{\frac{\log\log n}{\log\log\log n}}\right)\leq\log^{1/27}n\leq\log^{1/3}n'.$$

由于 H 是阿贝尔的，我们因此可以将引理 10.12 应用于大小为 n' 的 $A_0\subset H$，从而得到 $|A_0A_0^{-1}|/|A_0|=(2K)^{O(1)}\geq\exp(\log^{1/13}n')\geq\exp(\log^{1/117}n)$，这与我们对 K的假设矛盾。□

11. 在阿贝尔群中工作

现在，在假设纯阿贝尔结果——引理 9.2、9.3 和 10.12——成立的情况下，我们已经证明了定理 1.9 和 1.10。接下来需要证明这三个引理，我们将在本节中完成。补充说明一点：本节的所有结果都应用于引理 9.1 中找到的阿贝尔集合。由于引理 9.1 对输入集合大小的依赖是准多项式的，因此在论证余下部分，我们始终可以接受参数上的准多项式损失。特别是，Sanders 的准多项式 Bogolyubov–Ruzsa 引理 [San12] 发挥着重要作用。

11.1. 寻找稠密模型。 阿贝尔群中小倍增集合的一项重要性质是，它们的加法结构可以由某个所在阿贝尔群中占据较大比例的集合来刻画。换言之，小倍增集合具有稠密模型。在 Ruzsa 的证明 [Ruz94] Freiman 定理的过程中，构造这样的稠密模型是重要的一步。我们需要这一环节的一个定量界良好的版本；为此，我们采用 [San12]的主要结果。为了介绍这一结果，我们首先需要定义陪集进程。关于陪集进程的相关内容，我们只作简要介绍；如需了解更多细节和背景，请参阅[TV06, 第 4 节。4]。

定义 11.1（真对称陪集级数）。设 G 是一个阿贝尔群。G 中的一个对称陪集级数 M 是形如 $H+P$ 的集合，其中 G 是 H 的子群，而 P 是一个对称广义等差级数

$$P=\{a_1g_1+a_2g_2+\cdots+a_rg_r:(a_1,\dots,a_r)\in[-N_1,N_1]\times\cdots\times[-N_r,N_r]\}$$

对于某些 g_1，……，$g_r\in G$ 以及 N_1，……，$N_r\in\mathbb{Z}_{>0}$。数 r 称为对称陪集级数 M 的秩。如果映射 $H\times[-N_1,N_1]\times\cdots\times[-N_r,N_r]\to M$ 定义为

$$(h,a_1,\dots,a_r)\mapsto h+a_1g_1+a_2g_2+\cdots+a_rg_r$$

是一个双射。

定理 11.2 ([San12，定理 1.1])**.** 设 A 是阿贝尔群的一个子集，并假设 $|A-A| \leq K|A|$。那么 $2A-2A$ 包含一个真对称陪集级数 M，其秩为 $O(\log^6 2K)$，大小为

$$|M| \geq \exp\Big(-\log^{6+o(1)} 2K\Big)|A|.$$

作为定理 11.2 的推论，简单应用鸽巢原理可知，对于某个真对称陪集级数的某个平移 S，其大小与 $|A|$相当，集合 A 在其中的密度$|A\cap S|/|S|$ 很大。我们需要找到结构稍微更精确的集合 S，但愿意大幅牺牲 S 的大小。

为此，我们将有限阿贝尔群中的一个区间 定义为形如 $g_1 + [m]g_2 = \{g_1 + g_2, g_1 + 2g_2, \dots, g_1 + mg_2\}$ 的集合，其中 g_1，$g_2 \in G$，且 m 是不小于 g_2 的阶的正整数。下面的引理本质上是定理 11.2 的推论。它指出，阿贝尔群中任何具有小倍增的集合，都包含某个（在某种程度上）较大且性质良好的集合的大部分；该集合要么是一个区间，要么是某个初等 p-群的平移（其中的素数 p 不受我们控制）。这个引理的具体形式对于证明引理 10.12 是必要的，而我们所付出的准多项式损失不会对引理 9.2 和 9.3 的证明产生实质影响（在这两个陈述中，使用弗雷曼同构而非下面的引理，可以改进准多项式行为中的指数。）

引理 11.3. 设 G_0 是一个阿贝尔群。设 $A \subset G_0$ 的大小为 n，并假设 $|A-A| \leq K|A|$满足 $K \leq$ 指数函数$(\log^{1/12} n)$。

存在一个集合 $I \subset G_0$，满足以下条件：

(1) I 要么是 *(a)* 一个初等 p-群，要么是 *(b)* G_0中的一个区间。*(2)* A 至多可由指数函数$(O(\log^6 2K)) \cdot \frac{|A|}{|I|}$ 个 I的平移覆盖。*(3)* $|I| \geq$ 指数函数$(\Omega(\log^{1/2} n))$。

特别地，可以找到一个集合 S，它是这样一个 I 的平移，并且满足 $|A \cap S|/|S| \geq$指数函数$(-O(\log^6 2K))$。

证明。 通过修改 (3) 中隐含的常数，我们可以假设 n 充分大。现在，根据定理 11.2，我们可以找到一个包含于 $2A - 2A$ 中的真陪集进程 $M = H + P$，其大小至少为 $\exp(-O(\log^7 2K))|A - A|$，秩 r 至多为 $O(\log^6 2K)$。令 $\varepsilon_0 := |H + P|/|A|$。利用 Pl¨unnecke–Ruzsa 不等式得到 $|3A - 2A| \leq K^5|A|$后，Ruzsa 覆盖引理允许我们用 $K^5\varepsilon_0^{-1}$个 $(H + P) - (H + P) = H + 2P$的平移覆盖 A。记

$$P = \sum_{j=1}^{r} [-N_j, N_j]g_j$$

对于正整数 $N_1 \geq N_2 \geq \cdots \geq N_r$和元素 $g_j \in G$。集合 $H + 2P$可以被区间 I_j的$|H+2P|/|I_j|$ 个平移覆盖：$= [-2N_j, 2N_j]g_j$，对任意 j均成立；或者，也可以被 H的任意子群 J 的 $|H+2P|/|J|$个平移覆盖。由于 A 可以被

$$K^5\varepsilon_0^{-1} = \frac{K^5|A|}{|H + P|} \leq \frac{K^5 2^r|A|}{|H + 2P|}$$

$H + 2P$的平移覆盖，因此如上所述，对任意 I_j 或 J，条件 (2) 均成立。我们只需找到一个满足以下要求的I_j 或 J： (1) 类型符合要求，且 (3) 足够大。

我们对 K 的上界意味着，当 n足够大时，有 $|H + P| \geq n^{1/2}$。因此，要么$|P| \geq n^{1/4}$，要么 $|H| \geq n^{1/4}$。在前一种情况下，利用 P的适当性可得：

$$|I_1| = 4N_1 + 1 \geq \left(\prod_{j=1}^{r}(2N_j + 1)\right)^{1/r} = |P|^{1/r} \geq n^{1/(4r)} \geq \exp\left(\Omega\left(\frac{\log n}{\log^6 2K}\right)\right) \geq \exp\Big(\Omega(\log^{1/2} n)\Big)$$

根据我们对 K的上界，本情形下结论得证。

对于后一种情形，我们考察 H的结构。根据有限生成阿贝尔群基本定理，我们可以写成

$$H \cong \prod_{i=1}^{d} \mathbb{Z}/M_i\mathbb{Z}$$

对于某个正整数 d和某个 $M_1 \mid M_2 \mid \cdots \mid M_d$。设 p是 M_1的任意一个素因子。注意， H 有分别与 $\mathbb{Z}/M_d\mathbb{Z}$ 和 $(\mathbb{Z}/p\mathbb{Z})^d$同构的子群。令 $L := \max(M_d,\ p^d)$，于是H 有一个阶为 L的循环子群或初等 p-子群 J。我们有

$$|H| \le (M_d)^d \le L^{\log_2 L},$$

因此 $\log^2 L = \Omega(\log|H|) = \Omega(\log n)$。结论得证。（注意，循环群按定义是一个区间。）□

11.2. **三项等差数列与角形。** 引理 11.3 为阿贝尔群中小倍增集合提供了足够的结构信息，使我们能够从阿贝尔群中无三项等差数列子集和无角形子集密度的更标准结果，推导出引理 9.2 和 9.3。我们在阿贝尔情形中使用的关于三项等差数列的结果如下。

定理 11.4 (对 [BS23，定理 21]的**略微推广**）。设 G 是一个奇数阶阿贝尔群 N，且假设 $A \subset G$ 是一个避开模式 $\{x, x+y, x+2y\}$的非平凡实例的集合。那么

$$|A| \le N \exp\Big(-\Omega\Big(\log^{1/12} N\Big)\Big).$$

据我们所知，在围绕 Kelley 和 Meka 最近对 Roth 定理的改进而形成的文献中，定理 11.4 的表述尚未以完全相同的形式出现。不过，[BS23，定理 21], 的证明虽然名义上专门针对 $G \cong \mathbb{Z}/N\mathbb{Z}$ 这一情形，但可原封不动地应用于我们更一般的情形。（在 [BS23], 中，直到“提取”出其定理 21 的表述为止，整个论证都使用 Bohr 集的语言，因此完全不依赖所在阿贝尔群的结构。）

我们使用的关于角形的输入是以下结果，即 [JLL$^+$25]的主要结果。

定理 11.5 ([JLL$^+$25，定理 1。1])。设 G 是一个阶为 N 的阿贝尔群，并假设 $A \subset G \times G$ 是一个不含模式 $\{(x,y),(x+d,y),(x,y+d)\}$ 的非平凡实例的集合。那么

$$|A| \le N^2 \exp\Big(-\Omega\Big(\log^{1/600} N\Big)\Big).$$

引理 *9.2* 的证明。给定一个不含非平凡三项等差数列的集合 $A \subset G_0$，我们希望给 $|A-A|/|A|$ 一个下界。令 $n := |A|$ 且 $K := |A-A|/|A|$，并假设 $K \le$ 指数函数$(\log^{1/12} n)$（否则结论已得）。首先应用引理 11.3，找到一个集合 $S \subset G_0$，它要么是初等 p-群的一个平移，要么是 G_0 中的一个区间，并且满足

$$\frac{|A \cap S|}{|S|} \ge \exp\big(-O\big(\log^6 2K\big)\big); \tag{11.1}$$

$$|S| \ge \exp\Big(\Omega\Big(\log^{1/2} n\Big)\Big). \tag{11.2}$$

我们声称

$$\frac{|A \cap S|}{|S|} \le \exp\Big(-\Omega\Big(\log^{1/12}|S|\Big)\Big). \tag{11.3}$$

我们先证明情形 (a)。设 $s \in G_0$ 和 H 是一个初等 p 群，满足 $S = s + H$，并设 $B := (A-s) \cap H$，使得 $|B| = |A \cap S|$。若 $p = 2$，则 (11.1) 和 (11.2) 足以推出A 中有两个元素位于某个初等 2 群的同一平移中。因此， A 中有两个不同的元素 x 和 z，其差 $y := z - x$ 的阶为 2，于是 A 包含以下各项

x、 $x+y=z$和 $x+2y=x$，从而得到一个矛盾。因此 $p\neq 2$，我们对 $B\subset H$ 应用定理 11.4，得到 (11.3)。

若处于情形 (b)，令 $m:=|S|$，并取 $g_1,g_2\in G$ 使得 $S=\{g_1+ig_2\colon 1\leq i\leq m\}$。令 $B\subset[m]\subset\mathbb{Z}/(2m+1)\mathbb{Z}$ 为满足 $g_1+ig_2\in A\cap S$的所有 $i\in[m]$ 组成的集合。由于 $A\cap S$ 不含三项等差数列，且 B 的环境群选得足够大，集合 B 也不含三项等差数列。因此，将定理 11.4 应用于 $B\subset\mathbb{Z}/(2m+1)\mathbb{Z}$，即可得到 (11.3)。

无论哪种情形，(11.3) 都成立。将其与 (11.1) 和 (11.2) 结合可得

$$\log^{1/12}|S|\lesssim\log^6 2K\implies\log 2K\gtrsim\log^{1/72}|S|\gtrsim\log^{1/144}|A|.$$

结论得证。 □

引理 *9.3* 的证明。给定集合 $B\subset G_0$ 和 $A\subset B\times B$，其中 A 不含非平凡角，我们要证明：B 要么具有大倍增，要么在 $B\times B$中是稀疏的。令$K:=|B-B|/|B|$ 且 $\varepsilon:=|A|/|B|^2$。不妨设 $K\leq\exp(\log^{1/12}|B|)$，否则平凡界 $|A|\leq|B|^2$ 足以推出结论。因此，我们可以对$B\subset G_0$ 应用引理 11.3，从而找到集合 $I\subset G_0$，它或者是 (a) 一个初等 p-群，或者是 (b) G_0中的一个区间，并且对某个大小至多为 $\exp(O(\log^6 2K))\cdot\frac{|B|}{|I|}$ 的集合 Z，有$B\subset Z+I$；此外，$|I|\geq\exp(\Omega(\log^{1/2}|B|))$。由于 $A\subset B\times B\subset(Z\times Z)+(I\times I)$，我们可以找到某个 z_1,z_2 使得

$$\frac{\big|A\cap((z_1+I)\times(z_2+I))\big|}{|I|^2}\geq\frac{|A|}{|I|^2|Z|^2}=\varepsilon\cdot\left(\frac{|B|}{|I||Z|}\right)^2\geq\varepsilon\cdot\exp\big(-O(\log^6 2K)\big).\tag{11.4}$$

令 $A':=(A-(z_1,\ z_2))\cap(I\times I)$，使得 A' 在 $I\times I$ 中相对稠密。由于 A' 包含于某个无角集的平移中，A' 也无角。若 I 是一个初等 p-群，则可直接应用定理 11.5 得出

$$|A'|\leq|I|^2\exp\Big(-\Omega\Big(\log^{1/600}|I|\Big)\Big)\tag{11.5}$$

若 I 是长度为 m 的区间，我们可以（如上文引理 9.2 的证明中那样）将 A' 嵌入为 $(\mathbb{Z}/(2m+1)\mathbb{Z})^2$ 的无角子集，并得到 (11.5)。无论哪种情况，将 (11.5) 与 (11.4) 结合，再利用关于 I 的大小假设，可得

$$\log^{1/1200}|B|\lesssim\log^{1/600}|I|\lesssim\log\left(\frac{|I|^2}{|A'|}\right)\lesssim\log^6 2K+\log\varepsilon^{-1}\lesssim\log^6(2K\varepsilon^{-1}).$$

由于 $\frac{|B-B|^2}{|A|}=K^2\varepsilon^{-1}$，我们得出结论。 □

11.3. 在 $A-A$ 中寻找模式。 与三项等差数列和角形不同，据我们所知，引理 10.12 所指定的这一略显特殊的模式此前未曾出现在文献中。幸运的是，我们需要处理的模式是 [CFPY24, Lemma 4.5], 中所研究模式的变体，而且大致可以通过应用鸽巢原理找到。（另见 [CRS07], ，其中使用了类似的论证，在差集中寻找长等差数列。）在整数中，可以通过预先选取相关的素数 q 直接做到这一点。

引理 11.6. 设 Q、 R 和 N 为正整数。设 $A\subset[N]$ 的大小至少为 εN。对每个素数 $q<Q$，指定一个非负整数 s_q，并假设并非所有 q^{s_q} 都大于 Q。

假设 $N>8\varepsilon^{-12}Q^{10}R$。那么存在某个素数 $q<Q$ 以及至少 R 个 $t\in\mathbb{Z}\setminus\{0\}$ 的取值，使得

(1) $q^{s_q}\mid t$ 当 $(q')^{s_{q'}}\nmid t$ 对任意 $q'<q$成立，

且 *(2)* $t,qt,q^2t,q^3t\in A-A$。

证明。设 $\Delta := 2Q^7\varepsilon^{-8}$，并设 q 为满足 $q^{s_q} \leq \Delta$的最小素数。（这样的素数必定存在，因为某个 q^{s_q} 不大于 Q。）考虑映射 $\phi\colon A\times A\times A\times A \to (A+qA)\times(A+qA)\times(A+qA)$，其定义为

$$(a_0,a_1,a_2,a_3)\mapsto (qa_0+a_1, qa_1+a_2, qa_2+a_3).$$

我们有

$$\frac{|A|^4}{|A+qA|^3} \geq \frac{(\varepsilon N)^4}{((q+1)N)^3} \geq \varepsilon^4 Q^{-3}N,$$

因此，存在某个 $(u_1,u_2,u_3) \in (A+qA)\times(A+qA)\times(A+qA)$，它可以写作$\phi(a_0,a_1,a_2,a_3)$，且至少对应 $\varepsilon^4Q^{-3}N$ 个四元组 (a_0,a_1,a_2,a_3)。这些四元组中任意两个的第一坐标都不同，因为对于每个这样的四元组，我们有 $a_1 = u_1 - qa_0$、$a_2 = u_2 - qa_1$ 和 $a_3 = u_3 - qa_2$。令 A_0 为这些四元组第一坐标组成的集合，则 $|A_0| \geq \varepsilon^4Q^{-3}N$。若 $a_0, a_0' \in A_0$，则存在 $a_1,a_2,a_3,a_1',a_2',a_3' \in A$，使得对于每个 $1\leq i\leq 3$,

$$q^i(a_0-a_0') = q^ia_0 - q^ia_0' = (u_i-a_i)-(u_i-a_i') = a_i'-a_i \in A-A.$$

因此，对于 a_0 的任意 $t := a_0-a_0'$，$a_0'\in A_0$ 都满足条件 (2)。

现在，对于任意整数 m，记 $f(m)$ 为 A_0 中模 m 等价的不同元素有序对的数量。我们有

$$\begin{aligned} f(q^{s_q}) &\geq q^{-s_q}|A_0|^2 - |A_0|; \\ f\left((q')^{s_{q'}}q^{s_q}\right) &\leq (q')^{-s_{q'}}q^{-s_q}N^2 \leq \Delta^{-1}q^{-s_q}N^2 \quad \text{for each} \quad q'<q, \end{aligned}$$

其中第一行用到了柯西–施瓦茨不等式，第二行用到了 $A_0\subset[N]$ 这一事实以及我们对 q 的选择。因此，我们有

$$\begin{aligned} \#\left\{(a_0,a_0')\in A_0 : \begin{array}{c} q^{s_q} \mid a_0-a_0', \\ a_0=a_0' \text{ or} \\ (q')^{s_{q'}} \nmid a_0-a_0' \text{ for all } q'<q \end{array}\right\} &\geq |A_0| + f(q^{s_q}) - \sum_{q'<q} f((q')^{s_{q'}}q^{s_q}) \\ &\geq q^{-s_q}\left(|A_0|^2 - \frac{Q}{\Delta}N^2\right) \\ &\geq \Delta^{-1}\left(\varepsilon^4Q^{-3}|A_0|N - \Delta^{-1}\varepsilon^{-4}Q^4|A_0|N\right) \\ &= \frac{1}{4}Q^{-10}\varepsilon^{12}|A_0|N. \end{aligned}$$

其中我们用 $q<Q$ 和 $q^{s_q}\leq\Delta$，以及下界 $|A_0|\geq\varepsilon^4Q^{-3}N$，进行了化简。由于 $N \geq 8\varepsilon^{-12}Q^{10}R \geq 4\varepsilon^{-12}Q^{10}(R+1)$，上面的集合大小至少为 $(R+1)|A_0|$。特别地，存在某个 $a_0\in A_0$，使得至少有 R 个值 $a_0'\in A_0$，对每个 $q'<q$，它们模 q^{s_q} 与 a_0 等价，但模 $(q')^{s_{q'}}$ 与 a_0 不等价。对每个这样的 a_0'，取 t 为 a_0-a_0'，结论便得证。□

我们指出，当 $Q \lesssim \log\log n$ 时，引理 11.6 基本上可由 [CFPY24, 引理 4.5],推出；而当 $Q \lesssim \log^{1/3} n$ 时，这可由 Croot、Ruzsa 和 Schoen [CRS07] 的一个结果推出（这两种论证的风格相似）。沿着这两条思路进行的论证，都是通过寻找许多 t，利用鸽巢原理使得 $t,\ 2t,\ 3t,\ \ldots,\ Q^3t$ 全都属于 $A-A$。因此，无论条件 (2) 强制 q 取何值，条件 (3) 都必然得到满足。我们的论证通过精确确定条件 (2) 强制的 q 取值，比 [CRS07] 提高了一个指数因子。

利用整数情形下的引理 11.6，我们能够证明引理 10.12。

引理 *10.12* 的证明。由于 G_0 是阿贝尔群，它是其 p-部分的直积，而每个部分都含有一个循环子群 $\mathbb{Z}/p\mathbb{Z}$。由 G_0 不含阶为 $\operatorname{lcm}(1,\ldots,Q)$ 的循环子群这一事实，我们得出存在某个素数 $q_0\leq Q$，使得 G_0 的 q_0-部分没有阶大于 Q 的元素。

令 S 为引理 11.3 中由 $A \subset G_0$ 得到的 G_0 的子集，因此 S 是以下对象之一的平移：(a) G_0 的一个初等 p-子群；或 (b) G_0 的一个循环子群中的中心区间；此外

$$\frac{|A \cap S|}{|S|} \geq \exp\bigl(-O(\log^6 2K)\bigr) \tag{11.6}$$

$$|S| \geq \exp\Bigl(\Omega(\log^{1/2} n)\Bigr). \tag{11.7}$$

我们依次讨论这些情形。

首先考虑情形 (a)。设 $S = x + H$，其中 H 是某个素数 p 的 p-群。由 (11.7) 以及我们的假设（即 G_0 没有与 $(\mathbb{Z}/2\mathbb{Z})^r$ 或 $(\mathbb{Z}/3\mathbb{Z})^r$ 同构的子群），可得 $p \notin \{2,3\}$。令 $q = 2$，于是 H 的每个元素的阶都与 q 互素。现在我们基本上重复引理 11.6 的证明的一部分。令 $A' := A \cap S$，并令 $\phi\colon A' \times A' \times A' \times A' \to 3A' \times 3A' \times 3A'$ 定义如下：

$$\phi(a_0, a_1, a_2, a_3) = (2a_0 + a_1, 2a_1 + a_2, 2a_2 + a_3).$$

由于根据 (11.6)、(11.7) 以及我们的假设 $K \leq \exp(\log^{1/13} n)$，有 $|3A'| \leq |3S| = |S|$ 和 $|A'|^4 > |S|^3$，映射 ϕ 不是单射。由此可知，存在 $a_0, \ldots\ldots, a_3, a_0', \ldots\ldots, a_3' \in A'$，满足对每个 $1 \leq i \leq 3$ 都有 $2a_{i-1} + a_i = 2a_{i-1}' + a_i'$，且 $(a_0, a_1, a_2, a_3) \neq (a_0', a_1', a_2', a_3')$。令 $t := a_0 - a_0' \neq 0$，使得对每个 $1 \leq i \leq 3$，$2^i t = a_i' - a_i$ 都属于 $A - A$；因此 t 满足条件 (3)。由于 t 的阶是 $p \geq 5$ 的一个（非平凡）幂，条件 (1) 和 (2) 也都满足。情形 (a) 的证明至此完成。

现在我们讨论情形 (b)。令 $m := |S|$，并令 $g_1, g_2 \in G$ 满足 $S = \{g_1 + ig_2 \colon 1 \leq i \leq m\}$，其中 g_2 的阶至少为 m。记 $H := \langle g_2 \rangle$ 为由 H 生成的 G_0 的循环子群，并令 N表示 H的阶。令 π 为由 $1 \mapsto g_2$ 给出的投影映射 $\mathbb{Z} \to H$，并令 π_0 为其在 $[m]$上的限制，因此 π_0 是 $[m]$ 与 $S - g_1$之间的双射。令 $A' := \{\pi_0^{-1}(a - g_1) \colon a \in A\} \subset [m]$，并令 $\varepsilon := \frac{|A \cap S|}{|S|} = |A'|/m$。对于每个素数 $q < Q$，令 q^{s_q} 为整除 N的 q 的最大次幂。令$R := 49$。

现在，我们将引理 11.6 应用于 $A' \subset [m]$ 和 $(s_q)_q$，注意到 $q_0^{s_{q_0}} \leq Q$ 和

$$m = |S| \geq \exp\Bigl(\Omega(\log^{1/2} n)\Bigr) \geq 400 \exp\Bigl(\Omega(\log^6 2K) + 10 \log^{1/3} n\Bigr) \geq 8\varepsilon^{-12} Q^{10} R$$

由 (11.6) 可知，因此满足引理 11.6 的假设。我们得到存在某个 $q < Q$，以及至少 49 个元素 $t \in \mathbb{Z} \setminus \{0\}$，使得对于任意 $q' < q$，都有 t、qt、q^2t、$q^3t \in A' - A'$和 $q^{s_q} \mid t$，且 $(q')^{s_{q'}} \nmid t$。对于 $t \in \mathbb{Z}$，素数 q 整除 $\pi(t)$ 的阶，当且仅当 $q^{s_q} \nmid t$。由于 π在 $A' - A' \subset [-(m-1)\ m-1]$ 上的纤维大小至多为 2，因此至少有 25 个 H中的元素 u 满足u、qu、q^2u，且 $q^3u \in \pi(A') - \pi(A') = A - A$，并且 q不整除 u的阶，而每个素数 $q' < q$都整除 u的阶。因此，对于 u的这 25 个取值中的任意一个，结论中的条件 (2) 和 (3) 均成立。结果由以下事实得出：作为一个循环群，H中阶整除 24 的元素至多有 24 个。□

12. Conclusion and open problems

We c最后，我们提出一些猜想，并对我们方法的局限性作一些评论 .

12.1. 阿贝尔子结构。 或许，我们主要结果引出的最自然问题是：定理 1.3 中关于 G 的假设（即 G 不含与 A_d同构的子商）在多大程度上是必要的。虽然我们的证明关键性地利用了这一假设（在应用定理 1.12 时，用它来控制环境一般线性群的维数），但我们猜想这一假设实际上并非必要。

猜想 12.1. 存在一个绝对常数 $c > 0$，使得以下结论成立。若 G 是一个群，且 A 是满足 $|A^3| \leq K|A|$ 的有限对称集，则存在一个交换集

$T \subset A^4$ 满足

$$|T| \geq \exp\left(\Omega\left(\frac{\log^c |A|}{\log 2K}\right)\right).$$

猜想 12.1 将使我们能够移除定理 1.10 中关于环境群 G 的所有条件。它还将允许我们对定理 1.6 和定理 1.9 作定量强化，尽管我们的方法还不够强大（正如我们将在下一小节中详述的那样），无法完全移除定理 1.9 中任何一项“避开子群”的条件。

在 $K = 1$ 情形下，猜想 12.1 将给出定理 1.1 的一种弱形式。据我们所知，目前尚无定理 1.1 的证明（或其中任何超对数界）能够避免使用主列和有限单群分类。因此，猜想 12.1 的证明很可能需要在近似群与真正的群之间建立紧密的定量联系，将主列和有限单群分类推广到近似群，或者给出一种不依赖分类的定理 1.1 新证明。

我们提出两个关于猜想 12.1 较弱版本的注记，这些版本可以用现有工具证明。

注 12.2. 如果环境群 G已知是无挠的，那么 Sanders 的结果命题 2.16 足以证明猜想 12.1 的一个类似命题，其中 $|T| \geq c\log^{1/2}|A|/\log 2K$。事实上，对于 $t = c\log^{1/2}|A|/\log 2K$，命题 2.16 保证存在某个非平凡集合 S，满足 $S^t \subset A^4$。如果 G 是无挠的，那么对任意 $s \in S \setminus \{1\}$ 取 $T = \langle s\rangle \cap A^4$ 即可得到所需结果。

注 12.3. 如果愿意牺牲让 K 随 $|A|$增长的能力，就可以证明猜想 12.1 的一个类似命题。具体而言，Breuillard–Green–Tao 近似群结构定理 [BGT12，定理 1.6] 可以与我们的工作结合起来，证明猜想 12.1 在如下情形成立：对于某个（不可有效计算的）增长函数 $F(K)$，有 $|A| \geq F(K)$。

我们粗略概述一下论证。首先，与我们的证明一样，我们找到某个近似群B，其大小与 A 相当，且对于某个 $t \geq \log^{\Omega(1)}|A|$，有 $B^t \subset A^4$。接下来，[BGT12 定理 1.6]说明，环境群中存在子群 $H \trianglelefteq G_0 \leq G$，使得 $B^4 \supset H$，并且 G_0/H是幂零的，而 B 可由 $O_K(1)$ 个 G_0的左平移覆盖。若 $|A|$ 相对于 K足够大，则有 $|B^2 \cap G_0| \geq |A|^{1/2}$。若 $|H| = |B^4 \cap H| = |A^4 \cap H|$ 在$|A|$中至少具有准多项式大小，我们便可利用 Pyber 的结果得出结论。否则，我们应用引理 3.10(1)，并利用G_0/H 是幂零的（因而是可解的）这一事实，找到某个两两交换的独立集 $D \subset B^2 \cap G_0$，其大小为多对数级（相对于 $|A|$）。随后，我们便可根据引理 3.9 的证明中的论证得出结论。

我们也认为，可以改进定理 1.12，使其对环境群的维数仅呈多项式依赖，而非准多项式依赖。

猜想 12.4。 存在某些多项式有界函数 $M_1, M_2\colon\ \mathbb{Z}_{>0} \to \mathbb{R}$，使得以下结论成立。设 $\mathbb{F}$ 为任意一个域，设 $d \geq 1$，并设 $A \subset$一般线性群$_d(\mathbb{F})$ 是某个 $K \geq 1$的 K-近似群。那么存在某个阿贝尔子群 $H \leq$一般线性群$_d(\mathbb{F})$，使得

$$|A^2 \cap H| \geq \frac{1}{(2K)^{M_1(d)}}|A^2|^{1/M_2(d)}.$$

注 12.5。 猜想 12.4 中的函数 M_2 必须至少以多项式速度增长。特别地， $M_2(d)$ 不可能以比 $d^{1/3}$ 更慢的速度增长。利用 Ol’shanskii 在 [Ol’78] 所作的构造可以看出这一点：该构造给出了阶为 p^n 的群，且其阿贝尔子群的阶均不超过 $p^{c\sqrt{n}}$。我们简述如下论证：

令 $n = m+k$ 尽可能小，并满足 $k^2 > 2m$，其中 k。Ol’shanskii 在 $(\mathbb{Z}/p\mathbb{Z})$ 上均匀随机地选取斜对称双线性形式 α_1、……、α_k，并按如下方式构造一个阶为 p^n 的群 $G_{m,\,k}$：$G_{m,\,k}$ 的底层集合为 $(\mathbb{Z}/p\mathbb{Z})^k \times (\mathbb{Z}/p\mathbb{Z})^m$，群运算为

$$(w, v) \cdot (w', v') = \left(w + w' + (\alpha_i(v, v'))_{1 \leq i \leq k}, v + v'\right).$$

根据 [Ol’78，引理 2], 这样的群（以高概率）不含阶为 p^{2k} 的阿贝尔子群。

设 B_i 是一个满足 $\alpha(v,v') = v^{\intercal}B_i v'$ 的矩阵。群 $G_{m,k}$ 通过映射嵌入一般线性群 $\mathrm{GL}_d(\mathbb{F}_p)$，其中 $d := (m+2)k = \Theta(n^{3/2})$

$$(w,v) \mapsto \bigoplus_{i=1}^{k} \begin{pmatrix} 1 & v^{\intercal} & w_i \\ & I_m & B_i v \\ & & 1 \end{pmatrix}.$$

然而，对于 $\mathrm{GL}_d(\mathbb{F}_p)$ 的任意阿贝尔子群 H，我们有

$$|G_{m,k}^2 \cap H| \le p^{2k} \le p^{4\sqrt{n}} \le p^{O(d^{1/3})}.$$

注意 $|G_{m,\,k}| = p^n = p^{\Theta(d^{2/3})}$。取足够大的 p，我们得出：若猜想 12.4 对某个 M_1，M_2 成立，则必有 $M_2(d) \ge cd^{1/3}$。

我们的论证有几个方面使我们无法得到与猜想 12.4 一样强的界。其中之一是命题 1.13 中出现了 $\log\log d$ 因子；若能将这个因子替换为一个常数，我们就能相应地在 $M_2(d)$ 的指数中省去一个 $\log\log d$ 因子。（事实上，更强得多的定量结果或许成立；见注记 12.10。）更重要的问题在于，我们只处理了一次代数簇。（例如，代数簇 $\mathrm{Conj}(a)$ 的余维数总是至少为 d，但我们从不直接考虑这个代数簇，而总是用它所包含的仿射子空间 $\{x : \mathrm{tr}\, x = \mathrm{tr}\, a\}$ 来替代。）这样做的好处是避免了随 d 指数增长的定量损失，而这类损失会出现在 [BDH24] 中（作者在那里证明了线性群乘积定理的强定量界）。然而，这意味着我们无法充分利用“a相对不规则”的情形。若 a 是正则半单的，则 $\mathrm{Conj}(a)$ 的余维数恰为 d，因此将其替换为 $\{x : \mathrm{tr}\ x = \mathrm{tr}\, a\}$ 所造成的损失不大。然而，若 a 有一个维数约为 d 的特征子空间，则 $\mathrm{Conj}(a)$ 的余维数为 $\Omega(d^2)$，而 Larsen–Pink 不等式告诉我们（在没有额外结构的情况下），$|A^3 \cap \mathrm{Conj}(a)|$ 对某个常数 δ 而言不应远大于 $|A|^{1-\delta}$。我们无法利用小代数簇 $\mathrm{Conj}(a)$ 的结构，为我们的目的推导出这一结论足够强的定量版本。

12.2. **拉姆齐凯莱图**。围绕我们的结果定理 1.6 和定理 1.9（关于拉姆齐凯莱图的存在性）所提出的核心问题，当然是阿隆猜想（猜想 1.4）——即，对某个绝对常数 C，每个有限群都有一个 C-拉姆齐凯莱图。我们已经对所有不含有形如 $(\mathbb{Z}/2\mathbb{Z})^r$ 或 $(\mathbb{Z}/3\mathbb{Z})^r$ 或 $\mathbb{Z}/\mathrm{lcm}(1,\dots,Q)\mathbb{Z}$ 的大子群的群证明了这一猜想。下面我们简要定性地解释为何即使在阿贝尔情形下，我们的方法也无法处理这些子群。

初等阿贝尔群中固有的困难最早由 Green [Gre05] 注意到。对于 p 一个固定的素数以及 $G = (\mathbb{Z}/p\mathbb{Z})^n$，在 G 上均匀随机生成的凯莱图以高概率含有大小为 $\Theta(\log|G| \log\log|G|)$ 的团；此外，这样的团可以取为 G 的一个子群。（对于 $p = 2$，这就是 [Gre05，定理 9]。）Conlon、Fox、Pham 和 Yepremyan 在 [CFPY24] 中再次强调了这一困难；他们关于 G 的凯莱图的主要组合结果在 $G = (\mathbb{Z}/p\mathbb{Z})^n$ 情形下是紧的。对于 $p > 3$，[CFPY24] 中构造的非均匀随机凯莱图提供了一种确定性确保 $(\mathbb{Z}/p\mathbb{Z})^n$ 的非平凡子群都不可能成为团或独立集的方法。然而，对于 $p \in \{2,3\}$，目前没有明确的方法修改均匀随机图，以避免大子群作为团出现。我们略微更一般的构造 10.7 也无法克服这一障碍，因此遇到了同样的问题。对于群 $G = (\mathbb{Z}/2\mathbb{Z})^n$ 具有拉姆齐凯莱图，一个必要但可能并不充分的条件由 [CFPY24，猜想 5.1] 提出。

避开 $\mathbb{Z}/\mathrm{lcm}(1,\dots,L)\mathbb{Z}$ 或许更能体现我们方法的特殊性。要使类似构造 10.7 的构造适用于某个群 G，对于许多 $g \in G$，必须存在某个不整除 g 的小素数 q。群 $\mathbb{Z}/\mathrm{lcm}(1,\dots,L)\mathbb{Z}$ 不满足这一条件。更具体地说，在引理 11.6 中用到了 $\mathbb{Z}/\mathrm{lcm}(1,\dots,L)\mathbb{Z}$-避开假设，由此得到的条件（即某个 q^{s_q} 不太大）至关重要。引理 11.6

只有在已经将范围限制到阿贝尔子群的一个陪集后，才会应用该引理；这就是为什么我们必须令参数 L 关于 $\log N$ 为准多项式，而非多项式。

在某些特定情况下，可以通过选择略有不同的构造来解决这一问题。对于群 $G = (\mathbb{Z}/\operatorname{lcm}(1, \ldots, n)\mathbb{Z})^k$ 当有界时 k，可以使用与构造 10.3 相关的构造。对于任意 $x \in G$，至多有 2^k 个元素 $y \in G$ 满足 $2y = x$。这使得我们能够采用一种随机化构造，其中引理 10.5 的一个略弱版本成立，但代价是：对于许多 x，必须确定性地要求满足 $2y = x$ 的那些元素 y 要么全部位于 S 内部（若 $x \notin S$），要么位于 S 外部（若 $x \in S$）。我们可以将引理 10.6 应用于这一构造，但必须取 $c_0 = \Theta(2^{-k})$。因此，我们发现 G 具有一个 $O(2^k)$-Ramsey 凯莱图。

基于上述讨论，我们重点指出阿隆猜想的两个特例。第一个特例是环境群为阿贝尔群的情形；如果能够去掉 $\mathbb{Z}/\operatorname{lcm}(1, \ldots, Q)\mathbb{Z}$-规避条件，那么由定理 1.9 即可推出这一特例。

问题 12.6. 阿贝尔群族

$$G_n := \left(\mathbb{Z}/\operatorname{lcm}\left(1, \ldots, 2^{2^n}\right)\mathbb{Z}\right)^n$$

是否具有拉姆齐凯莱图?

第二个特例是对称群的情形。无论从哪方面看，对称群都是我们的方法面临的天然障碍：它们具有大的初等阿贝尔子群、大的循环子群和大的合成秩。我们预计，要证明对称群的阿隆猜想，需要全新的思路。

问题 12.7. 对称群族是否具有拉姆齐凯莱图?

12.3. **杂项**。本文正文中出现了两个中间结论，我们认为它们或许具有独立的研究价值，因此希望在本结论部分特别指出。

首先是命题 1.13。命题 1.13 的一个自然推广是去掉 $\log\log d$因子，具体如下。

猜想 12.8. 存在某个常数 $c > 0$ 使得以下结论成立。设 $\mathbb{F}$ 是一个代数闭域，且 $A \subset$一般线性群$_d(\mathbb{F})$ 是一个 K-近似群。假设每个元素$a \in A^2$ 都有一个维数为$(1-c)d$的特征子空间。那么存在两个子空间 $V_1 \subset V_2 \subset \mathbb{F}^d$，使得维数 $V_2 -$维数$V_1 > cd$，且至少有$(2K)^{-O(d^{O(1)})}|A^2|$ 个元素 a属于 A^2并满足以下性质：存在某个 $\lambda \in \mathbb{F}$ 使得$(a-\lambda)V_2 \subset V_1$。

如果将假设放宽为 A^2 的每个元素对于任意 $m < d/2$都有一个维数为 m 的特征子空间，则无法得到上述形式的结论。考虑对角嵌入即可看出这一点

$$\mathrm{GL}_2(\mathbb{F}_q) \hookrightarrow \bigoplus_{i=1}^{k} \mathrm{GL}_2(\mathbb{F}_q) \leq \mathrm{GL}_{2k}(\mathbb{F}_q).$$

我们还提出一个问题，该问题直接源于我们证明定理 1.12 的需要。虽然命题 1.13 对于近似群不包含不太不规则的元素的情形给出了一个（定性）分类，但我们并未使用其全部强度。我们从其结论中所需的全部内容只是：$(2K)^{-O(d^{O(1)})}|A^2|$ 个元素属于 $\mathrm{Mat}_d(\mathbb{F})$ 的某个真仿射子空间。

问题 12.9。给定 d，使下述命题成立的最小 m 是多少?

令 $\mathbb{F}$ 为一个代数闭域，并令 $A \subset \mathrm{GL}_d(\mathbb{F})$ 为一个 K-近似群。假设每个元素 $a \in A^2$ 都有一个维数至少为 m 的特征子空间。那么存在某个仿射子空间$\mathbf{U}$，它包含 $\mathrm{Mat}_d(\mathbb{F})$ 的至少 $(2K)^{-O(d^{O(1)})}|A^2|$ 个元素。

即使在真正的群这一情形下，这个问题也可能很有趣。（这里，Burnside 定理或多或少要求这样的仿射子空间包含在 $\mathbb{F}^d$ 上某个非平凡旗的稳定子中。）

注记 12.10. 对于某个常数 c 和无穷多个 d，问题 12.9 中这样的 m 必须大于 $d \cdot e^{-c\sqrt{\log d_{\text{双对数}}}d}$，即使对于 $K = 1$ 也是如此。我们略述证明。令 n 为一个奇正整数，并考虑与权 $(n-1,\ n-2,\ \ldots\ldots,\ 1,\ 0)$ 相关联的 GL_n 的不可约表示 ρ。这个表示的维数为 $d := 2^{\binom{n}{2}}$。令 q 为一个较大的素数幂，并令 $G \leq \mathrm{GL}_d(\mathbb{F}_q)$ 为 $\mathrm{GL}_n(\mathbb{F}_q)$ 在此表示下的像。利用舒尔多项式可以计算得出，若 $t_1,\ \ldots\ \ldots,\ t_n$ 是某个 $a \in \mathrm{GL}_n(\mathbb{F}_q)$ 的特征值，那么相应的 $\rho(a) \in G$ 具有特征值 $t_1^{e_1}t_2^{e_2}\cdots t_n^{e_n}$，其重数等于 $x_1^{e_1}\cdots x_n^{e_n}$ 在展开式中的系数

$$\prod_{1\leq i<j\leq n}(x_i + x_j).$$

m 是此展开式中 $x_1^{(n-1)/2}\cdots x_n^{(n-1)/2}$ 的系数。每个 $\rho(a)$ 都有一个重数为 m 的特征值。事实上，可以证明（利用矩阵秩的下半连续性），每个 $\rho(a)$ 实际上都有一个维数为 m 的特征子空间。数值 m 统计了具有 n 个顶点的正则竞赛图的数量；渐近式 $m = d \cdot e^{-\Theta(\sqrt{\log d_{\text{双重对数}}\ d})}$ 则可由 McKay[McK90 定理 3.1]推出。

剩下要证明的是，当 q 充分大时，G 中属于 $\mathrm{Mat}_d(\mathbb{F}_q)$ 的任意仿射子空间的元素所占比例趋于零。反设不然。那么，存在一个关于 $\rho(a)$ 各元素的仿射线性方程，对 a 中正比例的元素成立。这是关于 a 各元素的一个多项式方程 $f(a_{11},\ \ldots\ldots,\ a_{nn}) = 0$（从 GL_n 的表示的任意一种显式描述中均可看出）。方程 $f = 0$ 要么恒成立，要么在 $\mathbb{F}_q^{n\times n}$ 中定义出一个余维数为正的代数簇。在后一种情况下，施瓦茨–齐佩尔引理意味着，在 $\mathrm{Mat}_n(\mathbb{F}_q)$ 中满足 $f = 0$ 的元素所占比例至多为 C_n/q，其中常数 C_n 仅依赖于 n。在前一种情况下，G 整体包含在 $\mathrm{Mat}_d(\mathbb{F}_q)$ 的某个仿射子空间中。将 Burnside 定理应用于由 $\{b-1:\ b \in G\}$ 生成的子代数，可知 G 有某个不变子空间。当 q 足够大时，这与 ρ 的不可约性矛盾。

最后，我们提出一个纯群论问题，它自然源自引理 2.8 的陈述。据我们所知，尽管这个陈述十分简单，但文献中尚未出现过这个问题。

问题 12.11。对于哪些有限群对 (H_1, H_2)，下述陈述成立：每个有限群 G 只要有一个与 H_1 同构的商群，就有一个与 H_2 同构的子群?

如果问题 12.11 中的条件对 (H_1, H_2) 成立，就写作 $H_1 \implies H_2$。

可以通过考察阿贝尔群范畴来理解问题 12.11 的由来。有限阿贝尔群基本定理表明，这类群的每个商群都同构于该群的一个子群。换言之，如果问题 12.11 中的所有群（包括环境群 G）都要求是阿贝尔群，那么当且仅当 H_2 同构于 H_1 的一个子群时，群对 (H_1, H_2) 才满足所述性质。问题 12.11 探究的是有限阿贝尔群的这一性质在多大程度上无法推广到非阿贝尔群。由于问题 12.11 涉及 H_1 的任意有限扩张的子群结构，因此一般而言，这似乎是一个相当困难的问题。

事实上，我们认为，即使当 H_1 和 H_2 是阿贝尔的时，问题 12.11 仍然很有趣；实际上，我们对这个问题的了解几乎都局限于这一情形。以下列表列出了这些有限的已知结果。

- 对于任意正整数 m，均有 $\mathbb{Z}/m\mathbb{Z} \implies \mathbb{Z}/m\mathbb{Z}$。事实上，若 $G/N \cong \mathbb{Z}/m\mathbb{Z}$，则将 G/N 的任意生成元提升到 G 后，其阶是 m 的倍数，因此它的某个幂的阶恰为 m。
- 对于素数 p，若 $m' < \sqrt{m}/2$，则有 $(\mathbb{Z}/p\mathbb{Z})^m \implies (\mathbb{Z}/p\mathbb{Z})^{m'}$。这就是引理 2.8 的陈述。
- 另一方面，对于 p 素数，$(\mathbb{Z}/p\mathbb{Z})^m \not\Longrightarrow (\mathbb{Z}/p\mathbb{Z})^{m'}$ 对于 $m' > \sqrt{8m+9}$ 成立。这是 [Ol'78]的主要结果。沿用 Ol'shanskii 的方法，Halasi、Podoski、Pyber 和 Szab´o[HPPS24，定理 1.9] 证明了一个更强的结果，其中 p 可以替换为任意素数幂。

特别是，对于任何非阿贝尔群 H_2，我们都不知道有任何满足 $H_1 \implies H_2$ 的情形。我们认为，尽管这种可能性不大，但似乎确实不存在这样的例子。与此相反，我们提出以下猜想。

猜想 12.12. 对于每个正整数 n，都存在某个正整数 N，使得$\mathrm{S}_N \implies \mathrm{S}_n$。

事实上，猜想 12.12 等价于：对于每个 H_2，都存在某个满足 $H_1 \implies H_2$ 的 H_1。

Acknowledgements

我们感谢 Jacob Fox 提出这一研究方向，在整个研究过程中与我们进行了许多有益的交流，并提出了大量建议，极大地改进了最终成果。我们还感谢 Daniel Altman、Amichai Lampert 和 Jonathan Tidor 就第 7 节进行了有趣的讨论；感谢 Tristan Shin 向我们指出 [BS23, Theorem 21]；感谢 Benjamin Church、Spencer Dembner 和 Vaughan McDonald 提供代数几何支持（包括但不限于引理 A.6 的证明）。

作者获得美国国家科学基金会研究生研究奖学金计划的支持，资助编号 DGE-2146755。此外，本材料部分基于作者在加利福尼亚州伯克利的西蒙斯·劳弗数学科学研究所驻留期间（2025年春季）获得美国国家科学基金会资助编号 DMS-1928930 的支持所开展的工作。

References

[Alo95] N. Alon. 研究问题：问题 220（BCC6）。 *Discrete Math.*，138:405–411，1995。[Alo02] N. Alon. 图幂。载于 *Contemporary combinatorics*，第 10 卷， *Bolyai Soc. Math. Stud.*，第 11–28 页。J´anos Bolyai 数学学会，布达佩斯，2002。[AO95] Noga Alon 和 Alon 奥利茨基。重复通信与拉姆齐图。 *IEEE Trans. Inform. Theory*，41 5 1276( ): –1289，1995。[Aus16] Tim Austin. 拟随机群上的 Ajtai-Szemer´edi 定理。载于 *Recent trends in combinatorics*，第 159 卷， *IMA Vol. Math. Appl.*，第 453–484 页。Springer， [Cham], 2016。[BDH24] Jitendra Bajpai、Daniele Dona 和 Harald Andr´es Helfgott. 非扭曲经典群的增长估计与直径界，2024。arXiv:2110.02942。[BGH87] Joe Buhler、Ranee Gupta 和 Joe Harris. 斜对称形式的各向同性子空间及 p群的极大阿贝尔子群。 *J. Algebra*，108(1):269–279，1987。[BGT11] Emmanuel Breuillard、Ben Green 和 Terence Tao. 线性群的近似子群。 *Geom.* , ( ): –819，2011。[*Funct. Anal.* 21 4 774
BGT12] Emmanuel Breuillard、Ben Green 和 Terence Tao. 近似群的结构。 *Publ. Math.Inst. Hautes Études Sci.*，116:115–221，2012。[BMZ97] Vitaly Bergelson、Randall McCutcheon 和 Qing Zhang. 可 amen 群上的罗斯定理。 *Amer.* , ( ): – 。[Bou64] N. *J. Math.* 119 6 1173 1211, 1997
Bourbaki. *Éléments de mathématique. Fasc. XXX. Algèbre commutative. Chapitre* , 第 *6: Valuations* *Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics]* 1308 1964 卷第 No. 卷。Her

mann，巴黎，。[BS92] L´aszl´o Babai 和 ´Akos Seress. 关于置换群的直径。 *European J. Combin.*，13(4):231– 243，1992。[BS23] Thomas F. Bloom 和 Olof Sisask. 无三项等差数列集合的 Kelley-Meka 界。 *Essent. Number Theory*，2(1):15–44，2023。[Bur05] W. Burnside. 关于任意线性代换群的可约性条件。 *Proc. London Math.* , : – 。[CFPY24] David *Soc. (2)* 3 430 435, 1905
Conlon、Jacob Fox、Huy Tuan Pham 和 Liana Yepremyan. 随机凯莱图的团数及相关主题，2024。arXiv:2412.21194。[CRS07] Ernie Croot、Imre Ruzsa 和 Tomasz Schoen. 稀疏和集中的等差数列。载于 *Combinatorial number theory* 157 164 2007 ，第 – 页。de Gruyter，

柏林，。[Dum19] Adrian Dumitrescu. 不同距离与等差数列。 *Discrete Appl. Math.*，256:38–41，2019。[EMPS25] Sean Eberhard、Brendan Murphy、L ´ ´ ´ *Duke Math. J.* 174 3 403 448, 2025
aszlo Pyber 和 Endre Szabo. 线性群中的增长。, ( ): – 。

[Erd47] P. Erd¨os. 关于图论的一些评论。 *Bull. Amer. Math. Soc.*，53:292–294，1947。[ES35] P. Erd¨os 和 G. 塞凯赖什。几何学中的一个组合问题。 *Compositio Math.*，2:463–470，1935。[ES76] P. Erd
″ *Linear and Multilinear Algebra* 3 4 307 312, os 和 E. G.
1975 76
Straus. 有限群有多阿贝尔？，( ): – / 。[Fre73] G. A. Freiman.
Foundations of a structural theory of set addition 37 *Translations of* ，第 Vol 卷，。
Mathematical Monographs 1973
美国数学会，普罗维登斯，RI，。译自俄文。[Gre05] Ben Green. 计数和集较小的集合，以及随机凯莱图的团数。
Combina-
torica 25 3 307 ，( ): –326，
2005。[Gre08] Ben Green. 关于 Freiman 模型的注记，2008。未发表的注记，网址：
https://people.maths.ox.ac.uk/greenbj/papers/nonabelianmodels.pdf。[GT20a] Robert M. Guralnick 和 Pham Huu Tiep. 截面秩与上同调。 *J. Algebra*，558:434–452，2020。[GT20b] Robert M. Guralnick 和 Pham Huu Tiep. 截面秩与上同调 II，2020。arXiv:2005.05243。[Hel08] H. A. Helfgott. $SL_2(\mathbb{Z}/p\mathbb{Z})$中的增长与生成。 *Ann. of Math. (2)*，167(2):601–623，2008。[Hel11] H. A. Helfgott. $SL_3(\mathbb{Z}/p\mathbb{Z})$中的增长。 *J. Eur. Math. Soc. (JEMS)*，13(3):761–851，2011。[HH12] Norbert Hegyv
´ ˝ *Israel J.* ari 和
Math. 189 397 411, 2012
Francois Hennecart. 关于海森堡群中 Freiman 模型的注记。，: – 。[HHP03] N. Hegyv´ari、F. Hennecart 和 A. Plagne. 关于 Erd″os 两个受限加法猜想的证明及进一步结果。 *J. Reine Angew. Math.*，560:199–220，2003。[HMPQ19] Zolt´an Halasi、Attila Mar´oti、L´aszl´o Pyber 和 Youming Qiao. 有限李型单群的改进直径界。 *Bull. Lond. Math. Soc.*，51(4):645–657，2019。[HPPS24] Zolt´an Halasi、K´aroly Podoski、L´aszl´o Pyber 和 Endre Szab´o. 关于具有秩为 k的极大初等阿贝尔正规子群的 p群。 *J. Algebra*，647:744–757，2024。[HS10] Elad Haramaty 和 Amir Shpilka. 关于三次和四次多项式的结构。载于 *STOC'10—*
Proceedings of the 2010 ACM International Symposium on Theory of Computing 331 340 ，第 – 页。
ACM，纽约，2010。[HS14] Harald A. Helfgott 和 ´Akos Seress. 关于置换群的直径。 *Ann. of Math. (2)*，179 2 611 658，2014 ( ): – 。[Hup67] B. Huppert. *Endliche Gruppen. I*，第
134 *Die Grundlehren der mathematischen Wis-* 卷 Band 卷，。
senschaften 1967
施普林格出版社，柏林-纽约，。[JLL+25] Michael Jaber、Yang P. Liu、Shachar Lovett、Anthony Ostuni 和 Mehtaab Sawhney. 角定理的拟多项式界，2025。arXiv:2504.07006。[KM23] Zander Kelley 和 Raghu Meka.
3 *2023 IEEE 64th Annual Symposium* 进展的强界。
on Foundations of Computer Science—FOCS 2023 933 973
载于，第 – 页。IEEE Computer Soc.，洛斯阿拉米托斯，CA，2023。[Lam25] Amichai Lampert. 三线性形式的切片秩与解析秩。 *Discrete Anal.*，第 25 号论文，6，2025。[Lon20] Jason Long. 关于群中的 Brown-Erd″os-S´os 猜想的注记。 *Combin. Probab. Comput.*，29(4):633– 640，2020。[LR04] Victor Lomonosov 和 Peter Rosenthal. 关于矩阵代数 Burnside 定理的最简证明。*Linear Algebra Appl.*，383:45–47，2004。[Mal40] A. Malcev. 关于无限群的同构矩阵表示。 *Rec. Math. [Mat. Sbornik] N.S.*，8 50 405 422，1940 / : – 。[Man71] Avinoam Mann. 2-群的生成元。 *Israel J. Math.*，10:158–159，1971。[McK90] Brendan D. McKay. 正则竞赛图、欧拉有向图和欧拉定向图的渐近数量。 *Combinatorica*，10(4):367–377，1990。[Mer64] Ju. I. Merzljakov. 有限秩局部可解群。 *Algebra i Logika Sem.*，3(2):5–16，1964。[Mil98] G.A. Miller. 关于阶为 p^α的运算群的一个重要定理，其中 p 为任意素数。 *Messenger of Math.*，27:119–121，1898。[Mue] Peter Mueller. 限制 $GL_m(\mathbb{Z}/n\mathbb{Z})$子群的合成因子。MathOverflow。网址：https://mathoverflow.net/q/137875（版本：2013-07-29）。[NST20] Rajko Nenadov、Benny Sudakov 和 Mykhaylo Tyomkyn. 群中的 Brown-Erd″os-S´os 猜想的证明。 *Math. Proc. Cambridge Philos. Soc.*，169(2):323–333，2020。[Ol'78] A. Yu. Ol'shanskii. 关于有限 p群的阿贝尔子群的阶与生成元个数的问题。 *Mat. Zametki*，23(3):337–341，1978。[Pac03] J´anos Pach. 点集诱导的线段中点。 *Geombinatorics*，13(2):98–105，2003。[Pet24] F. Petrov. 群环中存在许多零因子所蕴含的组合结果。 *Funct. Anal. Appl.*，58 1 80( ): –89，2024。[PS16] L´aszl´o Pyber 和 Endre Szab´o. 有限李型单群中的增长。 *J. Amer. Math. Soc.*，29(1):95– 146，2016。[PW10] Attila P´or 和 David R. Wood. 关于可见性与阻挡集。 *J. Comput. Geom.*，1(1):29–40，2010。

[Pyb97] L. Pyber. 有限群有多阿贝尔？ 载于 *The mathematics of Paul Erdős I* 13 *Algorithms* , , volume of , pages – . *Combin.* 372 384 1997 Springer, 柏林, . [Ruz92] I. Z. Ruzsa. 算术级数与和的数量。 *Period. Math. Hungar.*, 25 111, 1992 1 105( ): – .[Ruz94] I. Z. Ruzsa. 广义算术级数与和集。 *Acta Math. Hungar.*, 65(4):379–388, 1994. [San12] Tom Sanders. 关于Bogolyubov-Ruzsa引理。 *Anal. PDE*, 5(3):627–655, 2012. [San17] Tom Sanders. 在有限群的某些子集中求解 $xz = y^2$ 。 *Q. J. Math.*, 68(1):243–273, 2017. [Sch02] Tomasz Schoen. 受限和集的基数。 *J. Number Theory*, 96(1):48–54, 2002. [Sch25] Tomasz Schoen. 关于无级数集的和集的注记。 *Ramanujan J.*, 68(1):Paper No. 23, 9, 2025. [Shk21] I. D. Shkredov. 加性组合学与数论中的非交换方法。 *Uspekhi Mat.* , (( )): –180, 2021. [Sol13] *Nauk* 76 6 462 119 J´ozsef Solymosi. 有限群中的Roth型定理。 *European J. Combin.*, 34(8):1454–1458, 2013. [Sol15] J´ozsef Solymosi. 有限群中的(7, 4)猜想。 *Combin. Probab. Comput.*, 24(4):680–686, 2015. [SW20] J´ ozsef Solymosi and *Discrete Appl. Math.* 276 155 Ching Wong. 有限阿贝尔群中的Brown-Erdos-Sos猜想。, : –160, 2020.[Sym21] Peter Symonds. 秩、余类与上同调。 *Int. Math. Res. Not. IMRN*, 2021(22):17399–17412, 2021. [Tao08] Terence Tao. 非交换群的乘积集估计。 *Combinatorica*, 28(5):547–594, 2008. [Toi20] Matthew C. H. Tointon. *Introduction to approximate groups* 94 *London Mathematical Society* , volume of . *Student Texts* 2020 Cambridge University Press, Cambridge, .[TV06] Terence Tao and Van Vu. *Additive combinatorics* 105 *Cambridge Studies in Advanced Mathe-* , volume of . *matics* 2006 Cambridge University Press, Cambridge, . [Wil09] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer- Verlag London, Ltd., London, 2009. [Won20] Ching Wong. 关于有限群中稠密子结构的存在性。 *Discrete Math.*, 343 112025, 4, 2020 10( ): .

Appendix A. Understanding subquotients: proofs of Lemmas 2.7 and 2.8

本节证明正文中需要用到的两个纯粹的群论事实：引理 2.7 和 2.8。

我们先给出一个定义及其几个简单性质。对于素数 p和有限群 G，记 $r_p(G)$（分别记 $s_p(G)$）为满足以下条件的最大整数 t： G 有一个子群（分别有一个子商）同构于 $(\mathbb{Z}/p\mathbb{Z})^t$。沿用 Guralnick 和 Tiep [GT20a], 的说法，我们称 $s_p(G)$ 为 G的节 p秩 。

群的节 p秩在本文之外也有应用。它是群上同调中的一个重要不变量，能够控制群上同调的维数和复杂度；例如参见 [GT20a、GT20b、Sym21]。引理 2.8 使得前述论文的结果可以仅用子群的存在性来表述；我们尚不清楚，在该情形下， $r_p(G)$ 是否也是一个自然的不变量。

A.1. 理解截面 p-秩。

我们先介绍截面p-秩的两个简单性质。

引理 A.1. 设 G是一个有限群， N是一个正规子群。那么 $s_p(G) \le s_p(N) + s_p(G/N)$。

证明。 设 H/K 是 G 的一个子商，且同构于 $(\mathbb{Z}/p\mathbb{Z})^s$，其中 $s := s_p(G)$。由于 $H \cap N \trianglelefteq H$和 $H/(H \cap N) \le G/N$，我们有 $s_p(N) + s_p(G/N) \ge s_p(H \cap N) + s_p(H/(H \cap N))$。因此，只需证明将 (G, N) 替换为 $(H, H \cap N)$ 后的结论；换言之，我们可以假设 $H = G$。

现在，包含映射 $N \trianglelefteq G$ 诱导出一个包含映射 $N/(K \cap N) \trianglelefteq G/K$。由于 G/K 是一个初等阿贝尔群， $N/(K \cap N)$ 和

$$(G/K)/(N/(K \cap N)) \cong (G/N)/(K/(K \cap N))$$

是初等阿贝尔群，其秩之和为 s。因此

$$s_p(G) = \operatorname{rk} G/K = \operatorname{rk}\big(N/(K \cap N)\big) + \operatorname{rk}\big((G/N)/(K/(K \cap N))\big) \le s_p(N) + s_p(G/N). \qquad \square$$

引理 A.2. 对于任意有限群 G，有 $r_p(G) = r_p(\mathrm{Syl}^p(G))$ ，且 $s_p(G) = s_p(\mathrm{Syl}^p(G))$。

证明。第一个等式源于这样一个事实：G 的每个 p-子群都包含在 G的某个 Sylow p-子群中。对于第二个，由于 Syl$_p$(G) $\leq G$，显然 s_p(Syl$_p$(G)) $\leq s_p$(G)。为证明反向不等式，设 $s = s_p$(G)，并设 G 的一个子商同构于 $(\mathbb{Z}/p\mathbb{Z})^s$，记为 H/K。令 K的一个 Sylow-p 子群为 S_K，并令 H 中包含 S_K的一个 Sylow-p 子群为 S_H，从而$S_K = S_H \cap K$。于是我们有

$$S_H/S_K = S_H/(S_H \cap K) \leq H/K.$$

此外，$|S_H|/|S_K|$ 是 $|H|/|K| = |H/K|$的 p-部分；由于 H/K 是一个 p-群，我们得出 $S_H/S_K = H/K$。因此 H/K 是Syl$_p$(H)的商群，从而 s_p(Syl$_p$(G)) $\geq s_p$(Syl$_p$(H)) $\geq s = s_p$(G)。□

Given引理 A.2，引理 2.8 显然可由 p-群中的下述结果得出 s.

引理 A.3 (Thompson–Mann；见 [Man71，定理 A 与 B])。对任意有限 p-群 G，我们有 s_p(G) $\leq 2r_p$(G)^2。

事实上，一个更强的结论成立：r_p(G)可替换为 G的一个阿贝尔正规子群的最大秩。当 p 为奇数时，这是Thompson的一个经典结果（见 [Hup67，定理 III.12.3]），他证明了：若一个 p-群 G 的每个阿贝尔正规子群至多可由 r 个元素生成，则 G 的每个子群至多可由 $r(r+1)/2 \leq r^2$个元素生成。对于 $p = 2$，这由Mann的一个结果 [Man71，定理 B], 得出，并且似乎也曾由Ol'shanskii [Ol'78], 基于 Merzljakov更早的结果 [Mer64，定理 1]发现。我们指出，Ol'shanskii还给出了满足 s_p(G) =Ω(r_p(G)^2) 的 p-群的一个构造。因此，引理 A.3（从而引理 2.8）在常数因子意义下是紧的。

A.2. **交错子商**。现在我们证明引理 2.7；先证明第 (1) 部分。首先需要下面这个简单的引理。

引理 A.4. 设 G 是一个有限群，S 是一个有限单群。若 G 将 S 作为子商包含在内，则 G 的某个合成因子将 S 作为子商包含在内。

证明。设 $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = \{1\}$ 是 G 的一个合成列。设 $H \leq G$ 和 $N \trianglelefteq H$ 满足 $S \cong H/N$。群 $(H \cap G_i)/(N \cap G_i)$ 构成 $H/N \cong S$ 的一个次正规列，而此列的每个连续商群都是 G 中相应合成因子的子商。由 S 是单群这一事实可得结论：S 的任何次正规列都包含 S 作为连续商群。□

现在，引理 2.7(1)由下述结果推出。

引理 A.5。设 $\mathbb{F}$ 是任意域，且 $G \leq$ 一般线性群$_r(\mathbb{F})$是一个有限群。若 G包含交错群交错群$_d$ 作为子商，则 $r \geq d/7 - 1$。

与引理 A.5 类似的陈述曾出现在 Pete L. Clark 在 MathOverflow 上提出、由 Peter Mueller 回答的一个问题中 [Mue]（对于任意 m，讨论的是 GL$_r$($\mathbb{Z}/m\mathbb{Z}$)，而非对于任意 $\mathbb{F}$讨论 GL$_r$($\mathbb{F}$)）。我们给出引理 A.5 的一个自包含证明，因为我们能够在定量上改进 Mueller 的论证。

我们的第一步是论证可以假设 $\mathbb{F}$ 是有限的。

引理 A.6。设 G 是一个有限群，它嵌入某个域 $\mathbb{F}$上的一般线性群$_r(\mathbb{F})$ 中。那么存在一个有限域 $\mathbb{F}_q$，使得 G 嵌入一般线性群$_r(\mathbb{F}_q)$中。

引理 A.6 可由 [Mal40 的定理 VI–VIII]结合推出。为方便读者，我们简述一个由 Spencer Dembner 和 Benjamin Church 提供、运用环论的证明。

证明。令 $x_{g,\,i,\,j}$ 为 $g \in G$ 和 $1 \leq i,\ j \leq r$ 的变量，并通过 $(m_g)_{ij} = x_{g,\,i,\,j}$定义矩阵 $(m_g)_{g \in G}$。令 A 为由 $\{x_{g,i,j}\}$ 生成、带有关系 $x_{1,\,i,\,j} = 1$（当 $i = j$ 时）以及在 $i \neq j$时取 0 的有限型 $\mathbb{Z}$-代数，并且对每个 g、$h \in G$满足 $m_g m_h = m_{gh}$。

已知对于某个域 $\mathbb{F}$，存在一个嵌入 $G \hookrightarrow \mathrm{GL}_r(\mathbb{F})$。该嵌入给出了一个环同态 $\varphi\colon A \to \mathbb{F}$。令 $I := \ker \varphi$ 以及 $B := A/I$。环 B 嵌入到 $\mathbb{F}$ 中，因而是一个整环。此外，由于对每个 $g \in G \setminus \{1\}$ 都有 $\varphi(m_g) \neq \varphi(m_1)$，所以对每个这样的 g，我们都可以找到某个 (i_g, j_g)，使得 $x_{g,i_g,j_g} - x_{1,i_g,j_g} \notin I$。考虑将 B 在所有 $x_{g,i_g,j_g} - x_{1,i_g,j_g}$ 处局部化所得的局部化环 B'，其中 $g \in G \setminus \{1\}$ 遍历所有取值。环 B' 具有某个极大理想 $\mathfrak{m}$；由于 B' 是有限型 $\mathbb{Z}$-代数，商群 $B'/\mathfrak{m}$ 是一个有限域（见 [Bou64, 推论 5.3.4.1]）。将 B 除以 $\mathfrak{m}$ 的原像 $\mathfrak{p}$ 所得的商群嵌入到 $B'/\mathfrak{m}$ 中，因而同构于某个有限域 $\mathbb{F}_q$。商映射 $\pi\colon B \to B/\mathfrak{p} \cong \mathbb{F}_q$ 使我们得到一个同态 $\varphi'\colon G \to \mathrm{GL}_r(\mathbb{F}_q)$ 的存在性。由于对于理想 $\mathfrak{m}$ of B' 有 $\mathfrak{p} = B \cap \mathfrak{m}$，我们有 $\pi(x_{g,i_g,j_g}) \neq \pi(x_{1,i_g,j_g})$，从而对每个 $g \in G$ 都有 $\varphi'(g) \neq \varphi'(1)$。因此，同态 φ' 是单射，所要求的结论得证。□

引理 *A.5* 的证明。由引理 A.6 可知，对于某个素数幂 $q = p^k$，有 $G \leq$ 一般线性群$_r(\mathbb{F}_q)$。取一个不同于 p 的素数 $\ell \in \{3, 5\}$；必要时扩张我们的域，便可假设 $\ell \mid q-1$。我们的假设 $G \leq$ 一般线性群$_r(\mathbb{F}_q)$ 含有一个交错群$_d$-子商，这意味着一般线性群$_r(\mathbb{F}_q)$ 含有一个特殊正交群$_{d-2}$ 子商。特别地，由于特殊正交群$_{d-2}$ 有一个与 $(\mathbb{Z}/\ell\mathbb{Z})^{\lfloor (d-2)/\ell \rfloor}$ 同构的子群，我们得出

$$s_\ell(\mathrm{GL}_r(\mathbb{F}_q)) \geq \left\lfloor \frac{d-2}{\ell} \right\rfloor. \tag{A.1}$$

对于整数 n，我们用 $\nu_\ell(n)$ 表示使 $\ell^\nu \mid t$ 成立的最大 ν。考虑一般线性群$_r(\mathbb{F}_q)$ 的子群 $H \cong (\mathbb{F}_q^\times)^r \rtimes$特殊正交群$_r$，它由置换矩阵和对角矩阵的乘积构成。一般线性群$_r(\mathbb{F}_q)$ 中 H 的指数为

$$\prod_{t=1}^{r} \frac{q^{r-t}(q^t-1)}{t(q-1)}.$$

由于 $\ell \mid q-1$，指数提升引理意味着 $\nu_\ell(q^t-1) = \nu_\ell(q-1) + \nu_\ell(t)$。我们得出，一般线性群$_r(\mathbb{F}_q)$ 中 H 的指数与 ℓ 互素。特别地，H 含有一般线性群$_r(\mathbb{F}_q)$ 的一个西洛-ℓ子群。由引理 A.2 和 (A.1) 可知

$$s_\ell(H) = s_\ell(\mathrm{GL}_r(\mathbb{F}_q)) \geq \left\lfloor \frac{d-2}{\ell} \right\rfloor. \tag{A.2}$$

现在，由于 H 有一个正规子群 $(\mathbb{F}_q^\times)^r \cong (\mathbb{Z}/(q-1)\mathbb{Z})^r$，其商群为 S_r，引理 A.1 推出

$$s_\ell(H) \leq s_\ell((\mathbb{Z}/(q-1)\mathbb{Z})^r) + s_\ell(\mathrm{S}_r) \leq r + \nu_\ell(r!) \leq \frac{\ell r}{\ell - 1}.$$

由 (A.2) 以及我们对 $\ell \in \{3, 5\}$ 的选择可得

$$d \leq \ell \cdot s_\ell(H) + \ell + 1 \leq \frac{\ell^2}{\ell - 1} r + \ell + 1 \leq 7r + 6.$$ □

为证明引理 2.7(2)，我们需要使用有限单群分类以及这些群的一些性质。对此，我们参考 Wilson 的著作 [Wil09]。

定理 A.7（有限单群分类，摘自 [Wil09，第 1.2] 节）。设 S 是一个有限单群。那么以下情况之一成立：

（*a*） S 是一个素数阶循环群。（*b*） S 是一个交错群。（*c*） S 是一个经典群，可以是线性群 射影特殊线性群$_n$（q）、酉群 射影特殊酉群$_n$（q）、辛群 射影辛群$_{2n}$（q）或正交群 射影正交群$^\pm_n$（q）。（*d*） S 是一个李型例外群。（*e*） S 是26 个散在单群之一。

我们主要需要经典群和例外群的性质。我们先考虑经典群。

引理 A.8。如果 S 是 {射影特殊线性群$_n$（q）、射影特殊酉群$_n$（q）、射影辛群$_n$（q）、射影正交群$^\pm_n$（q）} 中的一个经典群，那么

(*1*) S 可以嵌入一般线性群$_r(\mathbb{F}_{q^2})$ 中，其中 $r = n^2$；并

且 (*2*) S 包含一个与交错群$_d$ 同构的子群，其中 $d = \lfloor n/2 \rfloor$。

证明。为证明 (1)，我们首先注意到，S 是 PGL$_n(\mathbb{F}_{q^2})$ 的一个子群；PGL$_n(\mathbb{F}_{q^2})$ 是 GL$_n(\mathbb{F}_{q^2})$ 除以数量矩阵所得的商群：

- 群 PSL$_n(q)$ 是 SL$_n(q)$ $\leq$GL$_n(\mathbb{F}_q)$ 除以数量矩阵所得的商群。
- 群 PSU$_n(q)$ 定义为 SU$_n(q)$ 除以数量矩阵所得的商群；而 SU$_n(q)$ 定义为 GL$_n(\mathbb{F}_{q^2})$ 的一个子群 [Wil09，第 3 节6]。
- 设 $n = 2m$。群 PSp$_{2m}(q)$ 定义为 Sp$_{2m}(q)$ 除以数量矩阵所得的商群；而 Sp$_{2m}(q)$ 定义为 GL$_{2m}(\mathbb{F}_q)$ 的一个子群 [Wil09，第 3 节5]。因此，它是 PGL$_n(\mathbb{F}_{q^2})$ 的一个子群。• 无论 n 的奇偶性和 $\pm$的符号如何，群 P$\Omega_n^{\pm}(q)$ 均定义为 GO($\mathbb{F}_q$, f) 除以数量矩阵所得的商群，其中 GO($\mathbb{F}_q$, f) 对应某个非退化对称双线性型f，且其本身定义为 GL$_n(\mathbb{F}_q)$ 的一个子群 [Wil09，第 3.7 节和第 3.8] 节。

性质 (1) 现可通过伴随作用 g: $m \mapsto gmg^{-1}$ 将 PGL$_n(\mathbb{F}_{q^2})$ 嵌入 GL(Mat$_n(\mathbb{F}_{q^2})$) $\cong$ GL$_{n^2}(\mathbb{F}_{q^2})$ 得到。

现在证明 (2)。

- 通过置换矩阵将 S$_n$ $\hookrightarrow$GL$_n(\mathbb{F}_q)$ 嵌入，可得到 A$_n$ $\hookrightarrow$SL$_n(q)$ 的嵌入，进而诱导出 A$_n$ $\hookrightarrow$PSL$_n(q)$ 的嵌入。
- 选取一组基后，可以将 SU$_n(q)$ 表示为 SL$_n(\mathbb{F}_{q^2})$ 的子群，由满足 $\sigma(g)^\intercal g = I$ 的矩阵g 组成，其中 σ 是逐项映射 $x \mapsto x^q$。根据这一描述，每个偶置换矩阵都属于 SU$_n(q)$，因此我们得到 A$_n$ $\hookrightarrow$PSU$_n(q)$ 的嵌入。
- 设 $n = 2m$。选取一组基后，可以写成

$$\mathrm{Sp}_{2m}(q) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} : A,B,C,D \in \mathrm{Mat}_m(\mathbb{F}_q), \begin{array}{c} A^\intercal C = C^\intercal A, \\ B^\intercal D = D^\intercal B, \\ A^\intercal D - C^\intercal B = I \end{array} \right\}.$$

  因此，我们可以通过将 g 映射到 diag(g, $(g^{-1})^\intercal$)，将 SL$_m(q)$ 嵌入 Sp$_{2m}(q)$。这会导出 PSL$_m(q)$ $\hookrightarrow$ PSp$_{2m}(q)$ 的嵌入，进而将 A$_m$ =A$^{n/2}$ 嵌入 PSp$_n(q)$。
- 正交群的情形稍微复杂一些。根据 [Wil09，方程 3.34],，当 q 为奇数时，存在包含映射 GO$_{2m+1}(q)$ $\leq$ GO$^{\pm}_{2m+2}(q)$；当 q 为偶数时，存在包含映射 Sp$_{2m}(q)$ $\cong$ GO$_{2m+1}(q)$ $\leq$ GO$^{\pm}_{2m+2}(q)$ [Wil09，第 3.8 节.2]。结合前一个要点，这足以证明 q 为偶数时的 (2)。当 q 为奇数时，只需证明 A$_{2m+1}$ $\leq$P$\Omega_{2m+1}(q)$。为此，我们只需选取一个基，使 GO$_{2m+1}(q)$ 恰好由满足 $g^\intercal g = I$ 的那些矩阵g 组成。在这个基下，所有偶置换矩阵都属于 SO$_{2m+1}(q)$，因而投影到 P$\Omega_{2m+1}(q)$。□

引理 A.9。如果 S 是李型例外群，那么 S 可以嵌入到某个素数幂 q 对应的一般线性群$_{10^4}(\mathbb{F}_q)$ 中。

证明。我们依次讨论李型例外群的各个类别。

- 群 $G_2(q)$ 包含于特殊正交群 SO$_7(q)$ $\leq$一般线性群 GL$_7(\mathbb{F}_q)$ [Wil09，第 4.3 节。2]。
- 对于每个素数幂 q，群 $F_4(q)$ 都可以定义为一般线性群 GL$_{26}(\mathbb{F}_q)$ 的一个子群 [Wil09，第 4.8 节。4]。
- 群 $E_6(q)$ 定义为一般线性群 GL$_{27}(\mathbb{F}_q)$ 的一个子群除以其标量 [Wil09，第 4.10 节。按照引理 A.8 的证明中所用的伴随作用，$E_6(q)$ 可以实现为一般线性群 GL$_{729}(\mathbb{F}_q)$ 的一个子群。
- 群 ${}^2E_6(q)$ 定义为 $E_6(q^2)$ 的一个子群除以标量，因此包含于一般线性群 GL$_{729}(\mathbb{F}_q)$ [Wil09，第 4 节。11]。
- 群 ${}^3D_4(q)$ 可定义为 P$\Omega_8^+(q^3)$ 的一个子群 [Wil09，第 4.6 节。1], 因此，根据引理 A.8(2)，它是 GL$_{64}(\mathbb{F}_{q^6})$ 的一个子群。

• 群 $E_7(q)$ 可定义为 $\mathrm{GL}_{56}(\mathbb{F}_q)$ 的一个子群对其标量取商群[Wil09，第 4.12 节。3]按照引理 A.8 的证明中的做法，利用伴随作用， $E_7(q)$ 可实现为 $\mathrm{GL}_{56^2}(\mathbb{F}_q)$ 的一个子群。

• 群 $E_8(q)$ 被定义为一个 248 维李代数的自同构群[Wil09，第 4.12 节。1]。因此，它是一般线性群$_{248}(\mathbb{F}_q)$的一个子群。
• 群 ${}^2B_2(2^{2n+1}) = \mathrm{Sz}(2^{2n+1})$ 被定义为辛群$_4(2^{2n+1})$的一个子群 [Wil09，第 4.2 节。1], 它本身是一般线性群$_4(\mathbb{F}_{2^{2n+1}})$的一个子群。
• 群 ${}^2G_2(3^{2n+1})$ 被定义为交错群 $G_2(3^{2n+1})$的一个子群 [Wil09，第 4.5 节。1], 我们已经观察到它是一般线性群$_7(\mathbb{F}_{3^{2n+1}})$的一个子群。
• 群 ${}^2F_4(2^{2n+1})$ 被定义为 $F_4(2^{2n+1})$的一个子群 [Wil09，第 4.9 节。1], 我们已经观察到它是一般线性群$_{26}(\mathbb{F}_{2^{2n+1}})$的一个子群。
• 蒂茨群 ${}^2F_4(2)'$ 是 ${}^2F_4(2)$ 的指数为 2 的子群 [Wil09, 第 4.9 节。4], 因此也是 $\mathrm{GL}_{26}(\mathbb{F}_2)$ 的子群。□

现在我们可以证明引理 2.7(2)了。

引理 A.10. 存在一个绝对常数 C，使得若 S 是一个不含有 交错群$_d$ 作为子商的有限单群，则存在某个 $r \leq Cd^2$ 和某个有限域 $\mathbb{F}$，使得$S \leq$一般线性群$_r(\mathbb{F})$。

证明。令 C 大于 26 个散在单群中每个群的阶。我们使用定理 A.7 .
若 $S \cong \mathbb{Z}/p\mathbb{Z}$ 是一个素数阶循环群，则 S 可通过单位根的 p次根嵌入到 $\mathrm{GL}_1(\mathbb{C})$ 中 $\cong \mathbb{C}^\times$。

如果 S 是交错群，那么 $S \cong$A$_r$ 对于某个 $r < d$成立，因此 S 可通过置换矩阵嵌入一般线性群 $\mathrm{GL}_{d-1}(\mathbb{F}_2)$。

如果 S 是经典群，那么引理 A.8(2)意味着

$$S \in \{\mathrm{PSL}_n(q), \mathrm{PSU}_n(q), \mathrm{PSp}_n(q), \mathrm{P}\Omega_n^{\pm}(q)\}$$

对于某个 $n \leq 2d+1$ 和某个素数幂 q成立。现在，引理 A.8(1)意味着，对于某个 $r \leq n^2 \leq (2d+1)^2 \leq Cd^2$, S 可以嵌入一般线性群 $\mathrm{GL}_r(\mathbb{F}_{q^2})$。

如果 S 是李型例外群，那么引理 A.9意味着，对于某个素数幂 q， S 可嵌入 $\mathrm{GL}_{10^4}(\mathbb{F}_q) \leq \mathrm{GL}_{Cd^2}(\mathbb{F}_q)$。

如果 S 是散在群，那么 S 可通过右正则表示嵌入 $\mathrm{GL}_{|S|}(\mathbb{F}_2) \leq \mathrm{GL}_C(\mathbb{F}_2) \leq \mathrm{GL}_{Cd^2}(\mathbb{F}_2)$。□

Department of Mathematics, Stanford University
Email address: carlsch@stanford.edu