arXiv:2603.01866v1 [math.GR] 2 Mar 2026

群中能量的期望值

MARCO BARBIERI、MARUŠA LEKŠE 和 ANDONI ZOZAYA

摘要。我们为作用能量的期望值给出明确的上界和下界，其中涉及从置换群及其作用域中分别均匀随机抽取的一对子集 (A Δ)。随后，我们将这些界推广到若干情形下的乘法能量。特别地，我们推导出形如 (A，A) 和 (A，A^{-1}) 的集合对的期望能量的精确渐近公式。最后，我们运用这些估计，推导出关于大增长子集存在性的概率结果，并比较集合 $|A^{*2}|$ 和 $|AA^{-1}|$ 的基数的典型行为。

目录

1. 引言 1 1.1. 动机 2 1.2. 一般界 2 1.3. 有限群 3 1.4. 无限群 3 1.5. 应用 4 1.6. 致谢 5 2. 预备 5 2.1. 记号 5 2.2. 能量的定义 6 2.3. 概率空间与抽样 7 3. 作用能量 8 4. 集合与自身的乘法能量 10 4.1. 有限群 13 4.2. 无限群 16 4.3. 可 amenable 群 18 4.4. 有限生成群 21 5. 集合与其逆元集的乘法能量 23 5.1. 有限群 25 5.2. 无限群 26 5.3. 可 amenable 群 26 5.4. 有限生成群 30 6. 大增长子集 32 6.1. 有限群 33 6.2. 无限群 33 7. 和集或差集支配 36 参考文献 38

1. 引言

集合 A 的和集 $A+A$ 或乘积集 A^{*2} 的基数与 $|A|$ 成线性关系，在加性组合学和群论中发挥着核心作用。这一性质与强代数

2020 数学学科分类。 主分类：20P05；次分类：05E16、11B13。关键词和短语。 作用能量、乘法能量、群中的增长。本文所呈现的研究始于 AZ 对 IMFM 的一次研究访问期间，由斯洛文尼亚研究与创新署资助，研究计划编号为 P1-0294。他衷心感谢所提供的支持与款待。MB 得到斯洛文尼亚研究与创新署计划 P1-0222 及资助项目 J1-50001 的支持，并且是意大利 INdAM 的 GNSAGA 研究组的成员。ML 得到斯洛文尼亚研究与创新署的支持，计划编号为 P1-0294。

结构密切相关，Freiman 型定理和近似群理论便是例证。检测并衡量这一现象的一种定量方法是能量，它记录了来自两个集合的元素对在乘积（或在置换表示的语境中，在像）中代数重合的数量。（能量的定义及其基本性质的讨论见第2.2节。）

本文所依据的一个指导性问题如下：在均匀随机抽取的子集中，结构化行为有多么罕见？我们并不聚焦于极值情形或显式构造的例子，而是通过计算适当能量量的期望值来研究随机子集的典型行为。这一概率观点使我们能够将结构性结果纳入定量框架，并评估某些加法组合现象在一般群中实际上有多么罕见。

1.1. **动机**。大能量会迫使出现许多代数重合，而小能量通常对应于扩张。因此，能量充当代数结构与增长之间的中介。这一关系由如下不等式加以形式化

$$|AB| \geq \frac{|A|^2|B|^2}{E(A,B)},$$

其中 A 与 B 是环境群 G 的子集，且 $E(A,B)$ 是它们的能量。（该不等式在稍更一般的设定下的证明可见定理 7。）在固定两个正整数 k 与 h，并适当地定义一种抽取 k-子集 A 与一个h-子集 B 的方式（它们现在是随机变量，在 G 的幂集中取值，见第 2.3 节）后，詹森不等式给出

$$\mathbb{E}[|\mathsf{AB}|] \geq \frac{k^2h^2}{\mathbb{E}[E(\mathsf{A},\mathsf{B})]}.$$

Th因此，关于能量期望值的信息可立即转化为乘积集大小的下界。 r
the 乘积集的大小。

设 A_k 是从整数区间 k中均匀随机抽取的一个 $[-n,n]$ 子集。按照[57, 第 2.1], 节，(A_k,A_k) 的预期加法能量可以用一个显式量给出上界，进而得到倍增期望值的下界

$$\liminf_n \mathbb{E}\big[\,|\mathsf{A}_k+\mathsf{A}_k|\,\big] \geq \frac{k^3}{2k+1}. \tag{A}$$

这个不等式表明，在整数的随机子集中，和集异常小的集合极为罕见。

本文旨在将这一理念推广到远超整数情形的范围。事实上，我们的目标是将方程（A）推广到更广泛的背景中，并以此为次要成果，研究能量如何依赖于环境群的代数性质。

1.2. 一般界。实现这一目标所采用的主要创新，是一种双重计数技巧，它将均匀随机抽取一个含 k 个元素的子集时能量期望值的计算，转化为计数包含四个指定元素的 k 子集的数量。更确切地说，我们为离散群 G 赋予一个有限滤子列 (F_n)，选取一个非递减函数 $k\colon \mathbb{N}\to\mathbb{N}$，并从 F_n 中均匀随机抽取 k 个子集 A_k。若 G 是置换群，我们还固定定义域的一个滤过 (Φ_n) 和一个非递减函数$h\colon \mathbb{N}\to\mathbb{N}$，并通过从 Φ_n 中抽样 h 个子集 Δ_h，以类似方式进行。（底层概率空间在第 2.3 节中定义。）

这一框架使我们能够确定一对 (A_k,Δ_h) 的作用能量上界和下界，其中 A_k 是置换群 G 的一个 k-子集，而 Δ_h 是点集的一个 h-子集。这些界仅取决于 k、h和作用域的大小，并且对离散群的任意作用都成立（见定理 A）。我们强调，如果 k 和 h 都是有界函数，而 G 及其定义域是无限的，那么期望能量将收敛至下界 $\lim_n kh$。这一数值与自由群的生成集作用于无限树上一组两两距离至少为 2 的顶点时的能量相同（见定理 2）。此外，在 $kh \ll |\Phi_n|$这一情形下，结合定理 A、定理 7 和詹森不等式，我们便可立即得到

$$\mathbb{E}[|\Delta_h\cdot\mathsf{A}_k|] \geq \frac{kh}{1+o(1)}.$$

请注意，这是渐近意义下的最优结果，因为 h个点组成的子集在 k 群元素作用下的像不会超过 kh。

由于定理 A 的界是紧的，且可由正则作用达到（下界由满足 k 有界的无限群达到，而上界由满足 k 等于其基数的有限群达到），下一步我们将集合 Δ_h 特化为 G的一个特定子集，并通过其（右）正则作用将其视为作用在自身上的置换群。

我们的第一个选择是 $\Delta_h = \mathsf{A}_k$ 本身，因为关于 $E(\mathsf{A}_k,\mathsf{A}_k)$ 的上界可转化为 A_k^{*2}基数的下界，这与公式（A）的思路一致。定理 B给出了 A_k 与其自身的乘法能量期望值的上界和下界。当 $k \ll \sqrt{|F_n|}$时，这些界在渐近意义下是紧的，如 ?? 10?? 11 所示。它们以滤过与中心化子的交集大小表示，因此取决于环境群的结构，揭示了非交换性如何影响典型的能量值。

我们的第二种选择是 $\Delta_h = \mathsf{A}_k^{-1}$，即由$\mathsf{A}_k$中元素的逆元组成的集合。定理J 给出了这一对$(\mathsf{A}_k,\mathsf{A}_k^{-1})$期望能量的精确上界和下界，并以群中对合的密度表示。这些界通常更紧，并且呈现出定理B中不会出现的抵消现象。因此，对基数$|\mathsf{A}_k\mathsf{A}_k^{-1}|$的约束通常低于对 $|\mathsf{A}_k^{*2}|$的约束。

请注意，将通常的公式应用于定理B和J 中得到的上界，并代入能量最坏情形上界所对应的参数，可得在 $k \ll \sqrt{|E_n|}$这一范围内，

$$\mathbb{E}[|\mathsf{A}_k^{*2}|] \geq \frac{k^2}{3+o(1)}, \quad \text{and} \quad \mathbb{E}[|\mathsf{A}_k\mathsf{A}_k^{-1}|] \geq \frac{k^2}{3+o(1)}\,.$$

1.3. **有限群**。在有限群情形下，可以利用特征标理论对定理B 和J 加以改进。

定理C 给出了这一对$(\mathsf{A}_k,\mathsf{A}_k)$的乘法能量的显式闭式公式，该公式用群的共轭类数量以及实型和四元数型不可约特征标的数量表示（这些概念将在第4.1节定义）。若 k 为固定整数，且考虑一列阶趋于无穷的群，则这已经能为许多群类给出精确的渐近结果，其中包括非阿贝尔单群。事实上，在这种情况下，公式（C）、定理7和詹森不等式推出

$$\mathbb{E}[|\mathsf{A}_k^{*2}|] \geq \frac{k^2}{1+o(1)}\,.$$

这种行为已是最佳可能，因为 $|\mathsf{A}_k^{*2}| \leq k^2$。（此外，我们可以利用等式 (C) 得到前一个不等式中 $o(1)$ 项的精确衰减。）

定理 K 将此公式特化为一对 $(\mathsf{A}_k,\mathsf{A}_k^{-1})$的乘法能量。所得表达式同样是显式的，并将期望能量的计算归结为决定对合数量的特征论数据（见定理 15）。此外，由于 $\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k^{-1})]$ 的渐近行为仅取决于所考察群中对合所占的比例，因此，对于两类迥然不同的群——奇数阶可解群和单群——我们得到相同的渐近扩张。此外，若对合所占比例的 上极限被某个实数 ι所界定，则可得

$$\mathbb{E}[|\mathsf{A}_k\mathsf{A}_k^{-1}|] \geq \frac{k^2}{2+\iota+o(1)}\,.$$

1.4. 无限群。在无限群的情形下，定理 B 和 J 的推广更为微妙。我们先考察这对 $(\mathsf{A}_k, \mathsf{A}_k)$。有限情形已经表明，渐近展开的首项应当涉及群的交换概率 $\mathrm{cp}_\mu(G)$ 和平方关联概率 $\mathrm{sq}_\mu(G)$。（这里，$\mathrm{cp}_\mu(G)$ 是两个随机元素彼此交换的概率，而 $\mathrm{sq}_\mu(G)$ 是两个随机元素具有相同平方的概率。）这两个不变量分别在方程 (D) 和 (E) 中定义。正如记号所示，它们原则上可能取决于测度的选择，或者等价地，取决于滤过级数（见第 4.2 节）。更确切地说，定理 D 表明，对于一个无限离散群 G、一个有限滤过级数 (F_n) 以及 $k \ll \sqrt{|F_n|}$，记 μ 为由该滤过诱导的测度，我们有

——

$$\mathbb{E}[E_n(\mathsf{A}_k,\mathsf{A}_k)] = \big(1+\mathrm{cp}_\mu(G)+\mathrm{sq}_\mu(G)\big)k^2 + o(k^2).$$

特别地，我们得到了方程 (A)，因为 $\mathrm{cp}^{\mu}(\mathbb{Z}) = 1$ 且 $\mathrm{sq}^{\mu}(\mathbb{Z}) = 0$，无论选择何种测度，该公式都成立。同一公式还给出了以下渐近界

$$k^2 \;\leq\; \liminf_n \mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k)] \;\leq\; \limsup_n \mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k)] \;\leq\; 3k^2 - 2k.$$

在第4节的其余部分，我们将探讨这些界何时能够达到。为此，我们考察两种情形：可 amenable 群和有限生成群。

第4.3 节讨论可 amenable 群。在这里，我们借鉴了关于可 amenable 群中交换概率的现有文献（例如参见 [56]）。因此，我们的主要任务是处理平方关联概率。对于剩余有限可 amen 群 G，我们证明，$\mathrm{sq}^{\mu}(G)$ 只有在 G 几乎阿贝尔时才可能为正，并且$\mathrm{sq}^{\mu}(G)$ 不依赖于 μ。所得结论以及能量极限行为的相应推论，汇总于定理E中。

在第4.4节中，我们假设 G 是一个有限生成群，并具有生成集 S。自然的穷竭方式是取单位元周围的词度量球$\mathbf{B}_S(n)$。在这一情形下，正如 [2], 中所引入的，交换概率是否取决于 S的选择，仍是一个悬而未决的问题。我们预计，除非 G 几乎阿贝尔，否则平方关联概率应当趋于零。由于次指数增长群是可 amenable 的，且这些球构成 Følner序列，因此我们只需考虑指数增长的情形。在定理I中，我们猜想，对于指数增长群，

$$\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k)] = k^2 + o(k^2).$$

我们验证定理 I 对于几何群论中若干重要群族的正确性：词双曲群（定理 23）、直角阿廷群（定理 24），以及形如 $H \operatorname{wr} \mathbb{Z}$ 的广义灯笼群（定理 25）。

在第 5.2 节中，我们考察这一对 $(\mathsf{A}_k, \mathsf{A}_k^{-1})$。有限情形表明，控制 $\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k^{-1})]$ 渐近行为的不变量是对合密度 $\iota^{\mu}(G)$，也就是随机选取的元素的阶为 2 的概率，见方程（H）。遗憾的是，我们无法在完全一般的情形下证明这一点。不过，在定理 L 中，我们提出问题：在 $k \ll \sqrt{|F_n|}$的范围内，

$$\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k^{-1})] = (2 + \iota_{\mu}(G))\, k^2 + o(k^2)\,.$$

我们再次将关于无限群的讨论分为两部分。首先讨论可和情形（见第 5.3 节）。我们证明了先前猜想的剩余有限可 amenable 群的渐近公式，并确立了对合概率的基本性质。具体而言，$\iota^{\mu}(G)$ 与 Følner序列无关（见定理 29），而且 $\iota^{\mu}(G) \neq 0$ 当且仅当 G 几乎阿贝尔（见定理 28）。这些结果及其对期望能量的相应推论，汇总于定理 M。

与此同时，对于有限生成群中的词度量和球过滤，相关情形同样是具有指数增长的群（见第 5.4节）。在这种情况下，定理O 询问是否

$$\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k^{-1})] = 2k^2 + o(k^2)\,.$$

我们在几何群论中的若干自然群族中证明了这一点，尤其是词双曲群（见定理 33）以及某些广义灯笼群（见定理 34）。

1.5. 应用。 上述能量估计可与联系能量和增长的等式结合起来，从而获得关于存在大增长子集的概率性结果。

作为第一个应用，在定理 G中，我们给出 Neumann 关于小平方性质的一个替代证明（假设条件更严格，即群 G是剩余有限且可 amenable）。更确切地说，我们证明，若对于每个有限子集 $A \subseteq G$ 都有$|A^{*2}| < |A|^2$，那么 G 是有限-阿贝尔-有限群。

我们证明了有限群中存在加法基的一个近似版本，且其 G 基数尽可能小。（加法基的定义及其基数的已知结果见第5.4节。）具体而言，定理P 指出，对于每个无界函数 $h\colon\ \mathbb{N} \to \mathbb{N}$以及每个常数 $\epsilon > 0$，只要有限群 G 足够大，就存在一个子集 A 使得

$$|A| \leq |G|^{\frac{1}{2}} h(|G|), \quad \text{and} \quad |A^{*2}| \geq (1-\epsilon)|G|\,.$$

据我们所知，这是不依赖有限单群分类的此类最强结果。相比之下，若允许使用该分类，则 h 可以取为常数函数，且 $\epsilon = 0$。

同样，在不依赖分类的背景下，若底层群没有小的非平凡线性表示（也就是说，它是拟随机的），定理P 可以加强为一个直径型结果：具体而言， $G = A^{*6}$ （见定理Q）。

类似地，稀疏基提供了自然数的子集实例：这些集合的密度为零，但其和集的密度却为正。（定义见第6.2节。）在定理S中，我们分别证明了有限群正向极限中的类似现象。更确切地说，存在一个集合 A，对于某个合适的左不变测度， $\mu(A) = 0$ 但$\mu(A^{*2}) = 1$。

另一方面，我们还探讨了一个受加性组合问题启发的问题：具有 $|AA^{-1}|$ $|A^{*2}|$ 的集合，还是具有 $|A^{*2}| \geq |AA^{-1}|$ 的集合更常见。（已知结果简述见第7节。）在 $1 \ll k \ll \sqrt{|F_n|}$区域中，定理U 表明，以正概率，两个比值 $|AA^{-1}|/|A^{*2}|$ 和 $|A^{*2}|/|AA^{-1}|$都被某个绝对常数所界定。我们的抽样模型与以往研究和差占优所用的模型截然不同。此前大多数研究依赖伯努利抽样模型，即每个元素都被独立选取。因此，随机集合的基数通常与 $|F_n|$相当，占优现象则源于微妙的边缘效应。相比之下，我们均匀抽取的 k-子集满足 $k \ll \sqrt{|F_n|}$，因而我们的结果处于真正的稀疏区域。此外，我们的结果表明，这两个基数不可能频繁地相差太大，而标准结果通常只将这些量与阈值1进行比较。

我们认为，证明中仅限于一阶矩估计，使我们无法处理更精细的最优性问题，从而促使我们研究定理 W 中所表述的高阶矩。

1.6. **致谢**。 我们感谢 Primož Potočnik 帮助发展了定理 K 的原始证明，这最终促成了目前的工作。我们也感谢 Urban Jezernik 的许多宝贵讨论，以及他对本论文早期草稿的有益意见。

2. Setup

2.1. 记号。 我们在此汇集本文所需的大部分标准记号。

集合与渐近。 对每个集合 X，我们用 $\mathcal{P}(X)$ 表示其幂集；并且，对每个正整数 k，我们用 $\mathcal{P}_k(X)$ 表示 X 中基数为 k 的子集族。我们将 x^{ℓ} 记为*Pochhammer* 符号，即 $x^{\underline{\ell}} = x(x-1)\dots(x-\ell+1)$。

对于整数值映射 $f\colon \mathbb{R} \to \mathbb{Z}_{>0}$，当求值点 n 可由上下文明确时，我们用简写 $\binom{N}{f}$ 表示 $\binom{N}{f(n)}$。

我们将反复比较定义在正整数上、取正值且最终单调不减的实值函数的极限行为。为此，我们使用标准的巴赫曼–朗道记号：给定两个这样的函数 f， g，我们记作

$$f \in o(g), \quad \text{if } \lim_k \frac{f(k)}{g(k)} = 0,$$
$$f \in O(g), \quad \text{if } \lim_k \frac{f(k)}{g(k)} \in (0, +\infty],$$
$$f \in \Theta(g), \quad \text{if } \lim_k \frac{f(k)}{g(k)} \in (0, +\infty)\,.$$

此外，我们也将使用维诺格拉多夫记号 $f \ll g$，意为 $f \in O(g)$。

群论。 对于任意群 G 及其任意元素 $x \in G$，我们记作

$$\mathbf{C}_G(x) = \{g \in G \mid gx = xg\}$$

关于 x 在 G中的中心化子。如果 G 是一个有限生成群，且其有限生成集为 S，我们用$\mathbf{B}_S(n)$表示相应凯莱图中以单位元为中心、半径为 n 的球，其中采用与之对应的词度量。

给定群 G的两个子集 A 和 B，我们记

$$AB = \{ab \mid a \in A, b \in B\}.$$

此外，若 $A = B$，我们不写 AA，而更倾向于使用符号 A^{*2}。因此，对于这种类型的 A 与自身进行 k 次乘积，我们记作 A^{*k}。最后，我们记作

$$\varinjlim G_n$$

分别表示正向极限。在我们的设定中，群 G_n 是有限的。

概率。 在概率论表述中，我们用 $\mathbb{P}[A]$ 表示事件 A发生的概率，用$\mathbb{E}$[X]表示随机变量X的期望。

2.2. **能量的定义**。 我们首先遵循 Murphy 未发表的手稿来定义作用能量 [45]。（手稿中的思想也见于 [6]。）

定义 1。 设 G 是一个离散群，设 $A \subseteq G$，令 Ω 为一个离散的 G-集，并令 $\Delta \subseteq \Omega$。我们将这一对 (A, Δ) 的作用能量 定义为

$$E(A, \Delta) = \#\left\{(a, b, \gamma, \delta) \in A^2 \times \Delta^2 \mid \gamma \cdot a = \delta \cdot b\right\}.$$

若 $\Omega = G$，且该作用对应于 G的右正则置换表示，则 (A, Δ) 的作用能量与 (A, Δ) 的乘法能量一致，正如陶哲轩在 [54]中所介绍的。此外，若 G 是阿贝尔的，我们便得到通常的 (A, Δ)加法能量（例如参见 [55]）。

注意，如果 A 或 Δ 是无限集，则该对的能量自动为无限。因此，根据定理 1 的表述，作用能量只能为有限集提供信息。

设 A 和 Δ 为有限集。由于

$$\left\{(a, a, \gamma, \gamma) \in A^2 \times \Delta^2\right\} \subseteq \left\{(a, b, \gamma, \delta) \in A^2 \times \Delta^2 \mid \gamma \cdot a = \delta \cdot b\right\},$$

可推出 $E(A, \Delta) \geq |A||\Delta|$。此外，上述包含关系中的等式当且仅当 $\Delta \cdot A$ 中的每个元素都能以唯一方式表示为乘积 $\gamma \cdot a$，其中 $\gamma \in \Delta$和 $a \in A$。我们可以给出两个关于这一现象的具体例子。

例 2. 设 F_r 为秩为 r的自由群，并设 S 为 F_r的 r 个典范生成元的集合。我们将 F_r 在自身上的右正则作用解释为其在凯莱有向图 Cay(F_r, S) 上的作用，并选取 Δ 为两两距离至少为 2 的顶点的一个 h-子集。则

$$E(S, \Delta) = \#\left\{(x, y, v, w) \in S^2 \times \Delta^2 \mid xv = yw\right\} = kh,$$

因为字的等式 $xv = yw$ 成立当且仅当 $x = y$ 与 $v = w$。

例 3. 阿贝尔群的子集 A 称为*Sidon* 集，如果和集$A + A$的每个元素都有唯一表示为 $a + c$，其中 $a, c \in A$。在此设定下，方程 $a + c = b + d$成立当且仅当 $a = b$ 与 $c = d$。因此，

$$E(A, A) = \#\left\{(a, b, c, d) \in A^4 \mid a + c = b + d\right\} = k^2.$$

反之，注意到一旦三元组 $(a, b, \gamma) \in A^2 \times \Delta$ 被固定，则

$$\delta = \gamma \cdot ab^{-1} \in \Omega$$

可被唯一确定。因此，我们得到上界

$$E(A, \Delta) \leq |A|^2|\Delta|.$$

注 4. 请注意，这个界

$$E(A, \Delta) \leq |A||\Delta|^2$$

一般情况下并不成立，只有当 G 在 Ω 上的作用是半正则时才成立，也就是说，每个点的稳定子都是平凡的。（在此语境下，也常称这种作用是自由的。）特别地，它适用于乘法能量和加法能量。事实上，若固定三元组 $(b, \gamma, \delta) \in A \times \Delta^2$并选择 $g \in G$ 使得 $\gamma \cdot g = \delta$，那么

$$\gamma \cdot ab^{-1} = \delta, \quad \text{thus} \quad a \in G_\gamma gb.$$

因此，

$$E(A, \Delta) \leq |A||\Delta|^2 \max_{\gamma \in \Delta} |G_\gamma|.$$

这一考量为作用能量这一概念提供了一个自然的归一化常数 $|A|^2|\Delta|$，因此，只要 G和 Ω 带有有限滤过，该概念便适用于无限集。

我们关注可 *amenable* 群（关于背景和进一步参考资料，请参阅 [14, 第 4]章），即那些具有Følner序列（F_n）的群——也就是说，具有一列有限非空子集组成的滤过级数，使得对所有 $g \in G$,

$$\lim_n \frac{|gF_n \triangle F_n|}{|F_n|} = 0.$$

对于这样的 Følner序列，我们可以关联一个有限可加概率测度 $\mu\colon \mathcal{P}(G) \to [0,1]$, 定义为

$$\mu(S) = \lim_\omega \frac{|S \cap F_n|}{|F_n|}, \tag{B}$$

其中 ω 是 $\mathbb{N}$上的一个固定的非主超滤子。Følner性质意味着 μ 是左不变的，即，$\mu(gS) = \mu(S)$，对于每个 $g \in G$ 以及每个 $S \subseteq G$。（进一步讨论请参阅第4.2节。）

定义5。设 G 是一个可数可容许群，设 $A \subseteq G$，令 Ω 为一个可数的 G-集，并令 $\Delta \subseteq \Omega$。对于给定的两个 Følner序列（F_n）$\subseteq G$ 和（Φ_n）$\subseteq\Omega$，以及 $\mathbb{N}$上的非主超滤子 ω，我们将这对序列（A, Δ）的归一化作用能量定义为

$$\eta(A,\Delta) = \lim_\omega \frac{\#\left\{(a,b,\gamma,\delta) \in (A\cap F_n)^2 \times (\Delta \cap \Phi_n)^2 \mid \gamma\cdot a = \delta \cdot b\right\}}{|F_n|^2|\Phi_n|} \in [0,1]\,.$$

如果 G 或 Ω 是无限的，而 A 或 Δ 是有限的，那么归一化作用能量总是 0。相反，对于作用于有限域上的有限群，我们得到原能量的重归一化，即，

$$\eta(A,\Delta) = \frac{E(A,\Delta)}{|G|^2|\Omega|}\,.$$

注6。我们使用超滤子纯粹是为了确保极限值的存在。然而，在我们的计算中，期望能量通常与这一选择无关，事实上，它会按通常意义收敛。对于真极限，我们将记作 $\lim_n$；每当使用该记号时，均默认收敛成立。

重复我们用于作用能量的相同推理，可以证明归一化作用能量有如下界：

$$\eta(A,\Delta) \le \mu(A)^2\mu(\Delta)\,.$$

请注意，因此只有当 A 和 Δ的测度都为正时，归一化作用能量才有意义。

2.3. **概率空间与抽样**。我们所有的群和域都是离散的，并且都配备了两条递增的滤过级数或穷竭序列，$(F_n)_{n\in\mathbb{N}} \subseteq G$ 和 $(\Phi_n)_{n\in\mathbb{N}} \subseteq\Omega$，即

$$\bigcup_{n\in\mathbb{N}} F_n = G, \quad \bigcup_{n\in\mathbb{N}} \Phi_n = \Omega\,.$$

此外，如果滤过级数是递增的，则我们称

$$|F_n| < |F_{n+1}|, \quad |\Phi_n| < |\Phi_{n+1}|\,,$$

并且如果它们是嵌套的，则称

$$F_n \subseteq F_{n+1}, \quad \Phi_n \subseteq \Phi_{n+1}\,.$$

我们如下定义能量的滤过版本

$$E_n(A,\Delta) = E(A\cap F_n, \Delta \cap \Phi_n)\,.$$

注意到

$$\lim_\omega E_n(A,\Delta) = E(A,\Delta)\,,$$

并且，如果 G 是可 amenable 的，且两个滤过级数都是 Følner序列，那么

$$\lim_\omega \eta_n(A,\Delta) = \lim_\omega \frac{E_n(A,\Delta)}{|F_n|^2|\Phi_n|} = \eta(A,\Delta)\,.$$

现在，我们需要设定本文所考虑的概率空间。设 X 为一个离散集，$(X_n)_{n\in\mathbb{N}} \subseteq X$ 为 X的一个滤过，且 $k : \mathbb{N} \to \mathbb{N}$ 为一个非递减函数。这里需要强调的是，为了简化记号，当从上下文可以清楚地知道函数所取的整数n 时，我们将写作 k ，而非 $k(n)$。均匀随机抽取的 X_n -子集，A_k，等同于一个随机变量，其取值为 X_n 的所有 k-子集，并服从均匀概率。

讨论序列 (A_k) 在某种意义上是否收敛到$\mathcal{P}(X)$上的某个随机变量，超出了本研究的范围。在大多数情况下，对于所研究的量 $\mathbb{E}[E_n(\mathsf{A}_k,\mathsf{A}_k)]$ ，我们仍然能够求出其在 n 趋于无穷时的渐近展开。

3. 作用能量

我们现在给出作用能量期望值的上界和下界。

定理 A. 设 G 是一个离散群，Ω 是一个离散的 G-集，k、h ： $\mathbb{N} \to \mathbb{N}$ 是两个非递减函数，设 $_k$ 是从 F_n 中均匀随机抽取的一个 k-子集，且 Δ_h 是从 Φ_n 中均匀随机抽取的一个 h-子集。那么

$$kh \leq \mathbb{E}[E_n(\mathsf{A}_k, \Delta_h)] \leq kh\left(1 + \frac{(k-1)(h-1)}{2(|\Phi_n|-1)}\right).$$

特别地，对于从 G 中均匀随机抽取的每个A_k、 k-子集，以及对于从Ω 中均匀随机抽取的每个 Δ_h、h-子集，我们有以下推论。

(a) 如果 k 和 h 有界（并且，滥用一下记号，分别用 k 和 h 表示它们的极限），且 Ω 是有限的，

$$kh \leq \lim_n \mathbb{E}[E_n(\mathsf{A}_k, \Delta_h)] \leq kh\left(1 + \frac{(k-1)(h-1)}{2(|\Omega|-1)}\right).$$

(b) 如果 k 和 h 有界，且 Ω 是无限的，

$$\lim_n \mathbb{E}[E_n(\mathsf{A}_k, \Delta_h)] = kh\,.$$

(c) 如果 k、$h = \Theta(|F_n|)$，且 G 是可 *amenable* 的，那么

$$0 < \lim_\omega \mathbb{E}[\eta_n(\mathsf{A}_k, \Delta_h)] \leq \frac{1}{2},$$

否则，

$$\lim_\omega \mathbb{E}[\eta_n(\mathsf{A}_k, \Delta_h)] = 0\,.$$

证明。 考虑集合

$$\mathcal{S} = \left\{(a,b,\gamma,\delta,A,\Delta) \in F_n^2 \times \Phi_n^2 \times \mathcal{P}_k(F_n) \times \mathcal{P}_h(\Phi_n) \mid (a,b) \in A^2,\, (\gamma,\delta) \in \Delta^2,\, \gamma\cdot a = \delta \cdot b\right\}.$$

一方面，

$$\mathbb{E}[E_n(\mathsf{A}_k, \Delta_h)] = \binom{|F_n|}{k}^{-1}\binom{|\Phi_n|}{h}^{-1}|\mathcal{S}|\,. \tag{3.1}$$

另一方面，

$$|\mathcal{S}| = \sum_{a,b\in F_n,\gamma\in\Phi_n} \#\left\{(A,\Delta) \in \mathcal{P}_k(F_n)\times\mathcal{P}_h(\Phi_n) \mid (a,b)\in A^2, (\gamma,\gamma\cdot ab^{-1}) \in \Delta^2\right\}.$$

我们的目标是计算前一个等式的右侧。为此，我们将$\mathcal{S}$ 分成两个不相交集合：$\mathcal{S}_0$ 和$\mathcal{S}_1$, 前者包含满足 a 和 b 相等的元组，后者则包含二者不相等的元组。若 $a = b$，则 $\gamma\cdot ab^{-1} = \gamma$。特别地，

$$\begin{aligned}
|\mathcal{S}_0| &= \sum_{a\in F_n,\gamma\in\Phi_n} \#\left\{(A,\Delta) \in \mathcal{P}_k(F_n)\times\mathcal{P}_h(\Phi_n) \mid a\in A, \gamma\in\Delta\right\} \\
&= |F_n||\Phi_n|\binom{|F_n|-1}{k-1}\binom{|\Phi_n|-1}{h-1} \\
&= k\,h\binom{|F_n|}{k}\binom{|\Phi_n|}{h}.
\end{aligned}$$

现在假设 a 和 b 是不同的元素。我们无法保证 $\gamma\cdot ab^{-1}$ 是 Φ_n的元素。因此，我们得到

$$\begin{aligned}|\mathcal{S}_1| &= \sum_{a\neq b\in F_n,\gamma\in\Phi_n} \#\left\{(A,\Delta)\in\mathcal{P}_k(F_n)\times\mathcal{P}_h(\Phi_n)\mid (a,b)\in A^2,(\gamma,\gamma\cdot ab^{-1})\in\Delta^2\right\}\\ &= \sum_{a\neq b\in F_n,\gamma\in\Phi_n} \mathbf{1}_{\Phi_n}(\gamma\cdot ab^{-1})\binom{|F_n|-2}{k-2}\binom{|\Phi_n|-2}{h-2}.\end{aligned}$$

This 最后一个求和可能为零（见定理 2）；因此，我们只能给出 $|\mathcal{S}_1|\geq 0$。尽管如此

上界为

$$\begin{aligned}|\mathcal{S}_1| &= \sum_{a\neq b\in F_n,\gamma\in\Phi_n} \mathbf{1}_{\Phi_n}(\gamma\cdot ab^{-1})\binom{|F_n|-2}{k-2}\binom{|\Phi_n|-2}{h-2}\\ &\leq \binom{|F_n|}{2}\binom{|F_n|-2}{k-2}|\Phi_n|\binom{|\Phi_n|-2}{h-2}\\ &= \frac{k(k-1)h(h-1)}{2(|\Phi_n|-1)}\binom{|F_n|}{k}\binom{|\Phi_n|}{h}.\end{aligned}$$

注意，当 Ω 为有限集，且 n 足够大，使得 $\Omega=\Phi_n$时，等式成立。将其代入方程（3.1），即可证明第 (a) 项。

一般而言，将下界和上界代入方程（3.1），可得

$$kh\leq\mathbb{E}[E_n(\mathsf{A}_k,\Delta_h)]\leq kh\left(1+\frac{(k-1)(h-1)}{2(|\Phi_n|-1)}\right).$$

定理A 的其余陈述由此得出。 ■

注意，定理A (b) 表明，如果 k 和 h 有界，且 Ω 是无穷的，那么一对一般点 (A,Δ) 的预期行为是：对于 $\Delta\cdot A$中的每一点，都存在唯一一种方式将其表示为 $\gamma\cdot a$，这与定理 2相类似。这是合理的，因为随着点之间的距离变大，它们的像之间的重合趋于消失，而该作用开始类似于自由群在无穷正则树上的作用。

对于下一个例子，我们需要回顾以下引理，它是将 [54, 式(9)]推广到作用能量的结果。

引理7。 设 A 是离散群 G 的子集，并设 Δ 是一个 G-集 Ω 的子集。则，

$$E(A,\Delta)\geq\frac{|A|^2|\Delta|^2}{|\Delta\cdot A|}.$$

证明。 对于每个 $\omega\in\Omega$，我们定义，

$$r(\omega)=\#\left\{(a,\gamma)\in A\times\Delta\mid\omega=\gamma\cdot a\right\}.$$

注意，

$$\sum_{\omega\in\Delta\cdot A} r(\omega)=|A||\Delta|,\quad\text{and}\quad\sum_{\omega\in\Delta\cdot A} r(\omega)^2=E(A,\Delta).$$

由柯西-施瓦茨不等式，

$$|A|^2|\Delta|^2=\left(\sum_{\omega\in\Delta\cdot A} r(\omega)\right)^2\leq\left(\sum_{\omega\in\Delta\cdot A}1\right)\left(\sum_{\omega\in\Delta\cdot A} r(\omega)^2\right)=|\Delta\cdot A|E(A,\Delta).$$

两边除以 $|\Delta\cdot A|$即得结果。 ■

例 8. 近似群是具有较大乘法能量的集合的例子。（有关这一主题的引言，参见[57] 。）设 G 是一个离散群，且 A 是一个 κ-近似子群。于是，由定理7，

$$\frac{1}{\kappa}\leq\frac{|A|}{|A^{*2}|}\leq\frac{E(A,A)}{|A|^3}=\eta(A,A).$$

特别地，若 A 是一个子群，则 $\eta(A,A)=1$。

鉴于定理8，我们可以将定理A (c) 理解为：随机采样的 k-子集通常会产生某个对象，其归一化能量低于一个2-近似群的归一化能量。但其中可能有很大比例的2-近似群和真正子群。例如，若 G 是一个配备了Følner序列的局部有限群(F_n) ，该序列由有限群组成，并且 $k \geq |F_n|/2$，则对每一个 k-子集 $A_k \subseteq F_n$，

$$|A_k^{*2}| \leq |F_n| \leq 2k\,.$$

（此类群的一个例子是有限支撑对称群 $\mathrm{FSym}(\mathbb{Z})$，即整数上仅由具有有限支撑的置换构成的置换群。）另一方面，正如直觉所示，这种行为相当罕见。例如，对于固定的 k， k-子集（取自 C_2^n）的期望大小趋于 2^k ，当 n 趋于无穷时。由于定理 A(c) 在其当前的一般性下必须顾及前述现象，因此无法改进。

4. 集合与自身的乘法能量

现在我们将注意力限制于群通过右乘的正则作用，并进一步假设 $A = \Delta$。一方面，这仿照了方程（A）。另一方面，若没有这一额外假设，我们目前无法将定理 A作进一步改进。在此情形下，我们得到乘法能量期望值的如下上界和下界。

定理 B. 设 G 是一个离散群，设$(F_n)_{n\in\mathbb{N}} \subseteq G$ 是 G的一个对称有限滤过序列，设 $k\colon \mathbb{N} \to \mathbb{N}$ 是一个非递减函数，并设A_k 是从 F_n 中均匀随机抽取的一个 k-子集。那么

$$\begin{aligned}\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k)] \leq \frac{k^{\underline{4}}}{|F_n|-3} + \frac{k^{\underline{3}}}{(|F_n|-1)^{\underline{2}}}\,(4|F_n|-2) + \\ + k^{\underline{2}}\left(2 + \frac{\max_{x\in F_n\setminus\{1\}} |\mathbf{C}_G(x)\cap F_n| - 1}{|F_n|-1}\right) + k\,,\end{aligned}$$

and

$$\begin{aligned}\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k)] \geq \frac{k^{\underline{4}}}{(|F_n|-1)^{\underline{3}}}\left(|F_n|^2 - 5|F_n| + 2\right) + \\ + \frac{k^{\underline{3}}}{(|F_n|-1)^{\underline{2}}}\left(|F_n| - \max_{x\in F_n\setminus\{1\}} |\mathbf{C}_G(x)\cap F_n|\right) + k^2\,.\end{aligned}$$

在证明之前，我们先提取一个稍后会用到的结果。

引理9. 设$(F_n)_{n\in\mathbb{N}}$ 是群 G中的一个对称滤过序列。那么，

$$\sum_{y\in F_n^{*2}} |F_n \cap yF_n| = |F_n|^2\,.$$

证明. 注意到

$$F_n \cap yF_n = \{x \in F_n \mid x \in yF_n\} = \{(x,z) \in F_n^2 \mid xz^{-1} = y\}.$$

利用 F_n 是对称的这一假设，我们定义映射

$$\Psi\colon F_n^2 \to F_n^{*2}, \quad (x,z) \mapsto xz^{-1}\,.$$

Ψ的纤维，

$$\Psi^{-1}(y) = \left\{(x,z) \in F_n^2 \mid xz^{-1} = y\right\}\,,$$

划分 F_n^2。因此，

$$\sum_{y\in F_n^{*2}} |F_n \cap yF_n| = \sum_{y\in F_n^{*2}} \left|\Psi^{-1}(y)\right| = |F_n|^2\,.$$

■

定理 B 的证明。 我们使用与定理 A 的证明中相同的双重计数论证。我们得到

$$\mathbb{E}\left[E(\mathsf{A}_k, \mathsf{A}_k)\right] = \binom{|F_n|}{k}^{-1} \sum_{(a,b,c)\in F_n^3} \#\left\{A \in \mathcal{P}_k(F_n) \middle| (a\,,\, b,\, c,\, c^{-1}ab) \in A^4\right\}\,. \tag{4.1}$$

因此，我们的方法是确定等式（4.1）右侧的和。为此，我们将 F_n^3 的三元组集合划分为九个不相交集合，使得计算包含来自指定集合的三元组的 k-子集 A 的数量变得容易。具体地说，我们定义

$$\begin{aligned}
Q_1^{(1)} &= \{(a,b,c) \in F_n^3 \mid \#\{a,b,c\} = 3,\ ab = ca\}\,,\\
Q_1^{(2)} &= \{(a,b,c) \in F_n^3 \mid \#\{a,b,c\} = 3,\ ab = c^2\}\,,\\
Q_1^{(3)} &= \{(a,b,c) \in F_n^3 \mid \#\{a,b,c\} = 3,\ ab \neq ca,\ ab \neq c^2\}\,,\\
Q_2 &= \{(a,b,a) \in F_n^3 \mid a \neq b\}\,,\\
Q_3^{(1)} &= \{(a,b,b) \in F_n^3 \mid a \neq b,\ ab = ba\}\,,\\
Q_3^{(2)} &= \{(a,b,b) \in F_n^3 \mid a \neq b,\ ab \neq ba\}\,,\\
Q_4^{(1)} &= \{(a,a,c) \in F_n^3 \mid a \neq c,\ a^2 = c^2\}\,,\\
Q_4^{(2)} &= \{(a,a,c) \in F_n^3 \mid a^2 \neq c^2\}\,,\\
Q_5 &= \{(a,a,a) \in F_n^3\}\,.
\end{aligned}$$

注意，元素 $c^{-1}ab$ 与 $Q_1^{(3)}$ 、 $Q_3^{(2)}$ 和 $Q_4^{(2)}$ 的三元组中出现的元素不同，而与其他情况下三元组中的某个元素相同。现在我们需要确定划分中每个集合的基数。首先，我们观察到

$$|Q_2| = |F_n|(|F_n| - 1), \quad \text{and} \quad |Q_5| = |F_n|\,.$$

现在我们着重给出三元组 $|Q_1^{(1)}|$、 $|Q_1^{(2)}|$ 和 $|Q_1^{(3)}|$ 的上界和下界。我们先推导 $Q_1^{(1)}$ 的基数上界。由于 F_n 是对称的，对于每个 $y \in F_n$，我们定义一个单射

$$\psi_y \colon F_n \to F_n \times F_n y \times y F_n, \quad x \mapsto (x, x^{-1}y, yx^{-1})\,.$$

我们断言

$$\left(\bigcup_{y \in F_n^{*2}} \{\psi_y(x) \mid x \in F_n \setminus \mathbf{C}_G(y)\} \right) \cap F_n^3 = Q_1^{(1)}\,. \tag{4.2}$$

一方面，如果 $y \in F_n^{*2}$ 和 $(x,\ x^{-1}y,\ yx^{-1}) \in F_n^3$，那么

$$xx^{-1}y = y = yx^{-1}x\,.$$

条件 $x \notin \mathbf{C}_G(y)$ 意味着 x、 $x^{-1}y$ 和 yx^{-1} 两两不同，因此 $(x, x^{-1}y, yx^{-1}) \in Q_1^{(1)}$。另一方面，对于每个 $(a,b,c) \in Q_1^{(1)}$，令 $x = a \in F_n$ 和 $y = ab \in F_n^{*2}$。那么， $b = x^{-1}y$ 和

$$c = aba^{-1} = xx^{-1}yx^{-1} = yx^{-1}\,.$$

若 $(ab)^a = ab$，则 $c = b^a = b$，这与 (a,b,c) 的选取相矛盾。因此，对于 $y \in F_n^{*2}$， $(a,b,c) = \psi_y(x)$，且 $x \in F_n \setminus \mathbf{C}_G(y)$。这就证明了该断言。

注意，对于 $x \in F_n \setminus \mathbf{C}_G(y)$， $\psi_y(x) \in F_n^3$ 当且仅当 $x \in (F_n \cap F_n y \cap y F_n) \setminus \mathbf{C}_G(y)$，这意味着

$$|\psi_y(F_n \setminus \mathbf{C}_G(y)) \cap F_n^3| = \left|(F_n \cap yF_n \cap y^{-1}F_n) \setminus \mathbf{C}_G(y)\right| \leq |F_n \cap yF_n|\,.$$

因此，根据定理 9，

$$|Q_1^{(1)}| \leq \sum_{y \in F_n^{*2}} |F_n \cap yF_n| = |F_n|^2\,.$$

注意，若 G 是阿贝尔的，则 $Q_1^{(1)}$ 为空。特别是，无法推出比 $|Q_1^{(1)}| \geq 0$更好的下界。

现在我们将注意力转向 $|Q_1^{(2)}|$。注意，在定理 2的情形下， $|Q_1^{(2)}| = 0$。因此，我们只着重给出一个上界。我们定义

$$r_n(x) = \#\{(a,b) \in F_n^2 \mid ab = x\}, \quad \text{and} \quad S = \{c^2 \mid c \in F_n\}\,.$$

注意，通过双重计数，

$$E(F_n, F_n) = \sum_{x \in G} r_n(x)^2\,.$$

利用柯西-施瓦茨不等式和能量上界，我们计算得到

$$\begin{aligned}|Q_1^{(2)}| &\leq \sum_{c\in F_n} r_n(c^2)\\ &= \sum_{x\in G} r_n(x)\mathbf{1}_S(x)\\ &\leq \left(\sum_{x\in G} r_n(x)^2\right)^{1/2}\left(\sum_{x\in G}\mathbf{1}_S(x)^2\right)^{1/2}\\ &= E(F_n,F_n)^{1/2}|S|^{1/2}\\ &\leq |F_n|^{3/2}|F_n|^{1/2}\\ &= |F_n|^2\,.\end{aligned}$$

注意到

$$|Q_1^{(1)}|+|Q_1^{(2)}|+|Q_1^{(3)}| = |F_n|(|F_n|-1)(|F_n|-2)\,.$$

因此，

$$|F_n|\left(|F_n|^2-5|F_n|+2\right) \leq |Q_1^{(3)}| \leq |F_n|(|F_n|-1)(|F_n|-2)\,.$$

我们转而考察这一对 $Q_3^{(1)}$ 和 $Q_3^{(2)}$。与另一种情形相比，分析要简单得多。注意到

$$|Q_3^{(1)}|+|Q_3^{(2)}| = |F_n|(|F_n|-1), \quad \text{and} \quad |Q_3^{(1)}| = \sum_{x\in F_n}(|\mathbf{C}_G(x)\cap F_n|-1)\,.$$

由此可得

$$0 \leq |Q_3^{(1)}| \leq |F_n|\left(\max_{x\in F_n\setminus\{1\}}|\mathbf{C}_G(x)\cap F_n|-1\right),$$

从而

$$|F_n|\left(|F_n|-\max_{x\in F_n\setminus\{1\}}|\mathbf{C}_G(x)\cap F_n|\right) \leq |Q_3^{(2)}| \leq |F_n|(|F_n|-1)\,,$$

最后，为了证明定理 $Q_4^{(1)}$ 和 $Q_4^{(2)}$ B，我们不必显式计算其基数，只需给出显然的界。因此，由于

$$|Q_4^{(1)}|+|Q_4^{(2)}| = |F_n|(|F_n|-1)\,,$$

我们得到，对于 $i\in\{1,2\}$，

$$0 \leq |Q_4^{(i)}| \leq |F_n|(|F_n|-1)\,.$$

为了计算 $E(\mathsf{A}_k,\mathsf{A}_k)$ 的期望值，我们需要确定有多少个子集 A 包含三元组 $(a,b,c)\in Q_i$，具体取决于定义 Q_i 的条件。我们对划分集合性质的初步考察表明，

(i) 对于 $Q_1^{(3)}$，$\#\{a,b,c,d\}=4$；(ii) 对于 $Q_1^{(1)}$，$Q_1^{(2)}$，$Q_3^{(2)}$ 和 $Q_4^{(2)}$，$\#\{a,b,c,d\}=3$；(iii) 对于 Q_2，$Q_3^{(1)}$ 和 $Q_4^{(1)}$，$\#\{a,b,c,d\}=2$；(iv) 最后，对于 Q_5，$\{a,b,c,d\}=\{a\}$；

因此，将结果代入方程（4.1），可得

$$\begin{aligned}\mathbb{E}\left[E(\mathsf{A}_k,\mathsf{A}_k)\right] =& \binom{|F_n|}{k}^{-1}\left[\binom{|F_n|-4}{k-4}|Q_1^{(3)}|+\binom{|F_n|-3}{k-3}(|Q_1^{(1)}|+|Q_1^{(2)}|+|Q_3^{(2)}|+\right.\\ &\left.+|Q_4^{(2)}|)+\binom{|F_n|-2}{k-2}(|Q_2|+|Q_3^{(1)}|+|Q_4^{(1)}|)+\binom{|F_n|-1}{k-1}|Q_5|\right]\,.\end{aligned}$$

将我们计算出的各子集的上界代入后，即可得到最终公式。 ∎

我们强调，作为定理 B 的推论，若 $k\ll\sqrt{|F_n|}$，则有

$$k^2 \leq \mathbb{E}[E_n(\mathsf{A}_k,\mathsf{A}_k)]-O\left(\frac{k^4}{|F_n|}\right)\leq 3k^2\,,$$

并且，如果 $k\ll\sqrt[3]{|F_n|}$，

$$k^2 \leq \mathbb{E}[E_n(\mathsf{A}_k,\mathsf{A}_k)]-O\left(\frac{k^4}{|F_n|}\right)\leq 3k^2-2k\,.$$

若不对模型增加额外假设，这些渐近界就无法进一步改进。以下示例对此进行了展示，其中我们始终假设 $k \ll \sqrt[3]{|F_n|}$ 。

例10。 设 G 是二元域上的无限可数维向量空间，即， $G = C_2^{\aleph_0}$，并设 F_n 是由基数递增的有限子集构成的滤过级数。沿用定理B证明中的记号，由于 G 是初等阿贝尔群，

$$|Q_4^{(2)}| = 0, \quad \text{and} \quad |Q_4^{(1)}| = |F_n|(|F_n| - 1)\,,$$

并且，由于每个元素的阶为 2，

$$|Q_1^{(1)}| = |Q_1^{(2)}| = 0 \quad \text{and} \quad |Q_1^{(3)}| = |F_n|(|F_n| - 1)(|F_n| - 2)\,.$$

因此，上界和下界渐近等价。准确地说，

$$\lim_n \frac{\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k)]}{3k^2 - 2k} = 1\,.$$

例11。 海森堡群

$$H(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{Z} \right\}\,.$$

是一个可 amenable 群，并且对于一般的 Følner 滤过，满足

$$\lim_n \frac{\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k)]}{k^2} = 1\,.$$

这将在第4.2节中使用定理E予以证明。

4.1. **有限群**。 颇有趣的是，在撰写证明时，我们发现，只要知道滤过级数中的每个集合包含多少个平方根，就能加强这一结果。若群是有限群，这最终就相当于计算群中平方根的数量。这个问题可以借助特征标理论来处理（通过广为人知的定理14，其本质上仿照了 [33, 引理 4。4]）。回想一下，对于 χ 的不可约特征标 G，*Schur-Frobenius*指标 χ 定义为

$$\mathbf{s}(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2)\,.$$

算子 s 的取值范围相当有限，仅由集合 $\{-1, 0, 1\}$ 构成（见 [33, 定理 4.5]）。此外，我们可以根据 $\mathsf{s}(\chi)$ 的取值将不可约特征标分为三类。具体而言，若 $\mathsf{s}(\chi) = 1$，则称 χ 为实型；若 $\mathsf{s}(\chi) = 0$，则称 χ 为复型；若 $\mathsf{s}(\chi) = -1$，则称χ 为四元数型。对于有限群 G，我们用 $\kappa(G)$ 表示 G 的不可约特征标数量（或者等价地， G 的共轭类数量，见 [33, 推论 2.5]），并定义 $\varepsilon(G)$为实型和四元数型（但非复型）不可约特征标的数量。显然， $\varepsilon(G) \le \kappa(G)$；又由于一旦知道 G 的特征标表，Schur-Frobenius指标便可明确计算，因此 $\varepsilon(G)$ 也同样如此（见定理15的证明）。

第 4.1 节的主要结果如下。我们将在若干辅助引理之后证明它。

推论 C. 设 G 为一个有限群，设 $k \in \mathbb{N}$ 为满足 $k \le |G|$的正整数，并设A_k 为从 G中均匀随机抽取的一个 k-子集。则，

$$\begin{aligned} \mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k)] = {} & \frac{k^{\underline{4}}}{(|G|-1)^{\underline{3}}} \left(|G|^2 - 5|G| + \varepsilon(G) + \kappa(G) + 3\right) \\ & + \frac{2\,k^{\underline{3}}}{(|G|-1)^{\underline{2}}} \left(2|G| - \varepsilon(G) - \kappa(G) - 1\right) \\ & + \frac{k^{\underline{2}}}{|G|-1} \left(\varepsilon(G) + \kappa(G) - 1\right) + k^2\,. \end{aligned}$$

以下两个引理是众所周知的：我们在此加以证明，因为我们无法在文献中轻易找到易于查阅的证明。

引理 12。 设 G是一个有限群。那么，

$$\sum_{y \in G} |\mathbf{C}_G(y)| = \kappa(G)|G|\,.$$

证明。 设 $C \in \mathrm{Cl}(G)$ 是一个包含元素 $y \in C$ 的共轭类。根据轨道稳定子引理，

$$|C||\mathbf{C}_G(y)| = |G|\,.$$

因此，先对每个共轭类求和，再对 $\kappa(G)$ 个共轭类求和，

$$\sum_{y\in G}|\mathbf{C}_G(y)| = \sum_{C\in\mathrm{Cl}(G)}|C||\mathbf{C}_G(y)| = \sum_{C\in\mathrm{Cl}(G)}|G| = \kappa(G)|G|\,.$$

■

注 13。 注意，定理12给出

$$\frac{\kappa(G)}{|G|} = \frac{|\{(x,y)\in G^2 :\ xy = yx\}|}{|G|^2} = \mathrm{cp}(G)\,,$$

其中 cp称为有限群的交换概率 。Gustafson 在研究非阿贝尔群中交换对的最大数量时引入了这一概念 [29]，此后它在文献中受到广泛关注（例如，参见 [12, 23, 28, 43, 49]）。

对于有限群 G 的元素 $g \in G$，我们用 $r(g)$ 表示其平方根的数量，即

$$r(g) = \#\left\{x \in G \mid x^2 = g\right\}\,.$$

引理 14。 设 G 是一个有限群，$g \in G$ 是一个元素。则，

$$r(g) = \sum_{\chi\in\mathrm{Irr}(G)}\mathbf{s}(\chi)\chi(g)\,.$$

证明。 由于映射 $r\colon\ G \to \mathbb{N}$ 是类函数，

$$r(g) = \sum_{\chi\in\mathrm{Irr}(G)}\langle r,\chi\rangle\chi(g)\,.$$

因此，剩下要确定的是内积 $\langle r,\chi\rangle$。尽管如此，请注意

$$r(g) = \sum_{x\in G}\mathbf{1}_g(x^2)\,.$$

由此可得

$$\langle r,\chi\rangle = \frac{1}{|G|}\sum_{y\in G}r(y)\chi(y) = \frac{1}{|G|}\sum_{y\in G}\sum_{x\in G}\mathbf{1}_y(x^2)\chi(y) = \frac{1}{|G|}\sum_{x\in G}\chi(x^2) = \mathbf{s}(\chi)\,.$$

将上述结果代回 $r(g)$ 的第一个公式，证明即告完成。 ■

在深入定理的证明之前，我们再提取另一个特征标理论等式 C.

引理15。 设 G为一个有限群。则，

$$\sum_{g\in G}r(g)^2 = \varepsilon(G)|G|\,.$$

证明。 根据定理14，我们计算得

$$\sum_{g\in G}r(g)^2 = \sum_{g\in G}\left(\sum_{\chi\in\mathrm{Irr}(G)}\mathbf{s}(\chi)\chi(g)\right)^2 = \sum_{\chi,\psi\in\mathrm{Irr}(G)}\left(\mathbf{s}(\chi)\mathbf{s}(\psi)\sum_{g\in G}\chi(g)\psi(g)\right)\,.$$

利用特征标正交性，并注意到若 χ 赋予一个复表示，则 $\mathbf{s}(\chi)^2 = 0$；否则 $\mathbf{s}(\chi)^2 = 1$，可得

$$\sum_{g\in G}r(g)^2 = |G|\sum_{\chi\in\mathrm{Irr}(G)}\mathbf{s}(\chi)^2 = \varepsilon(G)|G|\,,$$

即得所需结果。 ■

注记16。 与定理13的思路相同，我们可以将比值 $\varepsilon(G)/|G|$ 解释为两个群元素具有相同平方的概率。（我们将这个量称为平方关联概率。）事实上，按它们共同的平方$(x,y) \in G^2$ 对满足 $x^2 = y^2$ 的元素配对进行计数，可得 g:

$$\left|\{(x,y)\in G^2 \mid x^2 = y^2\}\right| = \sum_{g\in G}\left|\{x \mid x^2 = g\}\right|^2 = \sum_{g\in G}r(g)^2\,,$$

并且，根据定理 15，我们得出

$$\left|\{(x,y)\in G^2 \mid x^2=y^2\}\right| = |G|\varepsilon(G)\,.$$

因此，

$$\frac{\varepsilon(G)}{|G|} = \frac{\left|\{(x,y)\in G^2 \mid x^2=y^2\}\right|}{|G|^2}\,.$$

定理 C 的证明。 的有限性 G 意味着我们可以假设，当 n 足够大时，$F_n = G$。在这一范围内，我们需要得到划分中所有集合基数的显式表达式。

我们从这一对 $Q_4^{(1)}$ 和 $Q_4^{(2)}$ 开始。一个基本的计数论证（见定理 16）结合定理 15给出：

$$|Q_4^{(1)}| = \sum_{g\in G} r(g)^2 = \varepsilon(G)|G|\,.$$

由于 $|Q_4^{(1)}| + |Q_4^{(2)}| = |G|(|G|-1)$，因此

$$|Q_4^{(2)}| = |G|(|G|-1-\varepsilon(G))\,.$$

由 $|Q_4^{(1)}|$ 的计算，我们可以立即推出 $Q_1^{(2)}$ 中三元组的数量。事实上，注意到满足 $ab=c^2$ 为 $|G|(|G|-1)$ 的三元组 $(a,\ b,\ c)\in G^3$（其中 $a\neq c$）的数量为，因为只要选定 a 和 c，b 就唯一确定。注意，$b\neq c$；虽然不排除 $b=a$ 的可能性，但在这种情况下，$(a,\ b,\ c)\in Q_4^{(1)}$。因此，

$$|Q_1^{(2)}| = |G|(|G|-1) - |Q_4^{(1)}| = |G|(|G|-1-\varepsilon(G))\,.$$

现在我们使用 $|Q_1^{(1)}|$ 公式（4.2来处理。由于对于每个群元素 $y\in G$，$G = yG = Gy$，定理 12 推出

$$\begin{aligned}
|Q_1^{(1)}| &= \sum_{y\in G} |(G\cap Gy\cap yG)\setminus \mathbf{C}_G(y)| \\
&= \sum_{y\in G} |G\setminus \mathbf{C}_G(y)| \\
&= |G|^2 - \sum_{y\in G} |\mathbf{C}_G(y)| \\
&= |G|(|G|-\kappa(G))\,.
\end{aligned}$$

由此可得

$$|Q_1^{(3)}| = |G|(|G|^2-5|G|+3+\varepsilon(G)+\kappa(G))\,.$$

最后，再次利用定理12，

$$|Q_3^{(1)}| = \sum_{y\in G}|\mathbf{C}_G(y)| - |G| = |G|(\kappa(G)-1),\quad \text{and}\quad |Q_3^{(2)}| = |G|(|G|-\kappa(G))\,.$$

As 划分中的每个集合都有明确计算出的基数，重复这一计算 s
fro从定理B 的证明可得结论。 ■

如前所述，若已知一个群的特征标表，我们可以利用定理C来计算 $\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)]$。

例 17. 令 $G=\mathrm{GL}_2(q)$。对于 q 为偶数的情形，$\varepsilon(G)=q+1$ 和 $\kappa(G)=q^2-1$。（注意，利用上述公式直接计算即可得到 $\varepsilon(G)$。）由此可得

$$\begin{aligned}
\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)] = {} & \frac{\left(3+q+q^2-5(q-1)^2q(1+q)+(q-1)^4q^2(1+q)^2\right)k^{\underline{4}}}{((q-1)^2q(1+q)-1)^{\underline{3}}} \\
& + \frac{2\left(-1-q-q^2+2(q-1)^2q(1+q)\right)k^{\underline{3}}}{((q-1)^2q(1+q)-1)^{\underline{2}}} \\
& + \frac{(-1+q+q^2)\,k^{\underline{2}}}{(q-1)^2q(1+q)-1} + k^2\,.
\end{aligned}$$

对于 q 为奇数的情形，同理可得 $\varepsilon(G) = q+3$ 和 $\kappa(G) = q^2-1$。因此，

$$\begin{aligned}\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)] = &\frac{\left(3+q+q^2-5(q-1)^2q(1+q)+(q-1)^4q^2(1+q)^2\right)k^{\underline{4}}}{((q-1)^2q(1+q)-1)^{\underline{3}}}\\ &+\frac{2\left(-1-q-q^2+2(q-1)^2q(1+q)\right)k^{\underline{3}}}{((q-1)^2q(1+q)-1)^{\underline{2}}}\\ &+\frac{(-1+q+q^2)\,k^{\underline{2}}}{(q-1)^2q(1+q)-1}+k^2\,.\end{aligned}$$

对于较大的有限群，我们还可以有力地控制 $\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)]$ 的渐近行为。事实上，设 (G_n) 是一个有限群序列（其阶逐渐增大），k 为正整数，且 (A_k) 是从 G_n 中均匀随机抽取的 k-子集序列。公式在 (G_n) 上的渐近行为（该公式见定理 C）可以完全由 $\varepsilon(G_n)+\kappa(G_n)$ 的渐近行为来理解。确实，

$$\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)] = \left(1+\frac{\varepsilon(G_n)+\kappa(G_n)}{|G_n|-1}\right)k^2-\frac{\varepsilon(G_n)+\kappa(G_n)}{|G_n|-1}k+O\left(\frac{1}{|G_n|}\right)$$

例如，若序列 (G_n) 由非阿贝尔单群构成，则 $\kappa(G_n)$ 关于 $|G_n|$ 次线性增长。因此，由于 $\varepsilon(G) \le \kappa(G)$，

$$\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)] = k^2+\Theta\left(\frac{\varepsilon(G_n)+\kappa(G_n)}{|G_n|}\right). \tag{C}$$

Me另一方面，若群 G_n 是奇数阶阿贝尔群，则 $\kappa(G_n) = |G_n|$ 且 $\varepsilon(G_n) = 0$，于是我们得到

$$\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)] = 2k^2-k+\Theta\left(\frac{1}{|G_n|}\right).$$

注 18. 我们可以刻画满足 $\lim_n \mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)] = k^2$ 的有限群序列：回顾比值 $\kappa(G_n)/|G_n|$ 作为交换概率的解释即可，如定理 13 所述。Neumann 在 [46, 定理 1] 中证明，对于某个正的常数 $\alpha > 0$，$\mathrm{cp}(G_n) > \alpha$ 当且仅当 G_n 是 (α-有界)-阿贝尔-(α-有界)群。（这里，α-有界表示有限且其阶至多为某个函数 f 的值 $f(\alpha)$，该函数仅依赖于 α。）因此，由于 $\varepsilon(G_n) \le \kappa(G_n)$，量 $\kappa(G_n)+\varepsilon(G_n)$ 关于 $|G_n|$ 线性增长，当且仅当每个 G_n 都是有限-阿贝尔-有限群，其中有限部分一致有界。

4.2. 无限群。我们在 ?? 13?? 16 中已经观察到，对于有限群，量$\mathbb{E}[E(\mathsf{A}_k,\ \mathsf{A}_k)]$ 关键取决于比值 $\kappa(G)/|G|$ 和 $\varepsilon(G)/|G|$，它们分别表示一对元素 $x,\ y \in G$ 均匀随机抽取后满足方程 $xy = yx$ 和$x^2 = y^2$的概率。将均匀计数测度替换为 μ 上的有限可加概率测度后，这一概率解释可以原样推广到无限群。μ 本节的主要目标是为无限群发展相应的概念。

设 $w \in F_k$ 是关于 k 个变量的一个字。对于固定的群 G，我们将由代入定义的相关字映射记为

$$w\colon G^k \longrightarrow G$$

相应的字映射。相对于有限可加测度 μ，G 的 w-概率为

$$\mathbb{P}_\mu(w;G) = \mu^{\otimes k}\Big(\big\{(g_1,\dots,g_k)\in G^k \;\big|\; w(g_1,\dots,g_k)=1\big\}\Big).$$

例如，交换概率，即换位子字$w = \gamma_2 = [x,y]$的 w-概率，明确地说，

$$\mathrm{cp}_\mu(G) = (\mu\otimes\mu)\Big(\big\{(x,y)\in G^2 \;\big|\; xy=yx\big\}\Big) = \int_G \mu\big(\mathbf{C}_G(x)\big)\,d\mu(x)\,, \tag{D}$$

已得到广泛研究（关于可和情形，见 [56]；关于有限生成群的词度量中由球导出的滤过，见 [2]）。

任意穷竭都会给出一个有限可加测度。事实上，设 $(F_n)_{n\in\mathbb{N}}$ 是一个递增的有限子集序列，其并集为 G。每个 F_n 都定义了有限支撑的概率测度

$$\mu_n(X) = \frac{|X\cap F_n|}{|F_n|},\quad X\subseteq G,$$

或者，等价地， $\ell^\infty(G)$ 上的平均泛函

$$f \mapsto \frac{1}{|F_n|}\sum_{g\in F_n} f(g).$$

根据巴拿赫–阿劳格鲁定理， $\ell^\infty(G)^*$ 的单位球在弱-$*$ 拓扑下是紧的，因此上述序列存在一个弱-$*$ 收敛子列。任何这样的子列极限都定义了 $\ell^\infty(G)$上的均值m，即

$$m(f) = \lim_{k\to\infty} \frac{1}{|F_{n_k}|}\sum_{g\in F_{n_k}} f(g), \quad f \in \ell^\infty(G)\,.$$

因此，由下式给出的 G上的相应有限可加概率测度 μ 为

$$\mu(X) = m(\mathbf{1}_X) = \lim_{k\to\infty} \mu_{n_k}(X), \quad X \subseteq G.$$

引理19. 设 G 是一个群，且$(F_n)_{n\in\mathbb{N}}$ 是 G中的一个滤过级数。那么，对于任意非主超滤子 ω *in* $\mathbb{N}$,

$$\lim_{\omega} \frac{1}{|F_n|^2}\sum_{x\in F_n} |\mathbf{C}_G(x)\cap F_n| = \mathrm{cp}_\mu(G)\,.$$

证明。 我们将交换指示函数定义为

$$\mathbf{c}(x,y) = \begin{cases} 1 & \text{if } xy = yx\,,\\ 0 & \text{otherwise}\,. \end{cases}$$

于是，

$$\frac{1}{|F_n|^2}\sum_{x\in F_n} |\mathbf{C}_G(x)\cap F_n| = \frac{1}{|F_n|^2}\sum_{x,\,y\in F_n} \mathbf{c}(x,y)\,.$$

根据引理前的讨论，取超极限后，

$$\begin{aligned}\lim_{\omega} \frac{1}{|F_n|^2}\sum_{x\in F_n} |\mathbf{C}_G(x)\cap F_n| &= \int_{G\times G} \mathbf{c}(x,y)\,d(\mu\otimes\mu)(x,y)\\ &= \int_G \mu\left(\mathbf{C}_G(x)\right)\,d\mu(x)\\ &= \mathrm{cp}_\mu(G)\,.\end{aligned}$$

这就是所需的等式。 ∎

根据定理 16，在定理 C中，对 k^2的系数的唯一其他可能贡献，由两个独立的 μ-随机元素取自 G 且平方相同的概率控制。我们将这个量定义为平方关联概率，并令

$$\mathrm{sq}_\mu(G) = \mathbb{P}_\mu(w;G), \quad \text{where } w(x,y) = x^2y^{-2}\,. \tag{E}$$

推论D。 设 G 是一个无限群，设 (F_n) 是 G中的一个对称滤子序列，设$k:\mathbb{N}\to\mathbb{N}$ 是一个非递减函数，且 $k \ll \sqrt{|F_n|}$，并设 A_k 是 F_n的一个随机 $\overline{k}$-子集。那么

$$\mathbb{E}[\mathsf{A}_k,\mathsf{A}_k] = (1+\mathrm{cp}_\mu(G)+\mathrm{sq}_\mu(G))k^2 + o(k^2)\,.$$

此外，若 $k \ll \sqrt[3]{|F_n|}$,

$$\mathbb{E}[\mathsf{A}_k,\mathsf{A}_k] = (1+\mathrm{cp}_\mu(G)+\mathrm{sq}_\mu(G))k^2 - (\mathrm{cp}_\mu(G)+\mathrm{sq}_\mu(G))k + o(k)\,.$$

证明。 定理 19 蕴含比值 $|Q_3^{(1)}|/|F_n|^2$ 收敛至 $\mathrm{cp}^\mu(G)$。与此同时，按定义， $|Q_4^{(1)}|/|F_n|^2$ 的超极限为 $\mathrm{sq}^\mu(G)$。由此，依照定理 B证明中的相同计算，结论立即成立。

∎

4.3. **可 amenable 群**。 现在我们聚焦于 G 可 amenable，且 (F_n) 是一个真正的 Følner序列这一情形。根据定义，穷竭均值及其对应的有限可加测度都是左不变的。在这种情况下，交换概率已有充分的理解： $\mathrm{cp}_\mu(G)$ 的值与具体采用哪个 Følner序列以及沿哪个子列取弱$*$ 极限无关。此外，当且仅当 G 是有限-阿贝尔-有限群（见 [56, 定理 1.14 和命题 1.15]）时，该不变量为正；或者，若 G 是有限生成的，则其几乎阿贝尔。

回到定理 11，注意海森堡群是有限生成且可 amenable 的，但并非几乎阿贝尔，因此 $\mathrm{cp}(G) = 0$，且与 μ的具体选取无关。此外，平方映射 $x \mapsto x^2$ 是单射，因此

$$|Q_4^{(1)}| = 0 \quad \text{and} \quad |Q_4^{(2)}| = |F_n|(|F_n| - 1)$$

对每个有限滤子列都成立。将这些值代入定理 D 即可得到所需的极限。

我们现在的目标是证明平方关联概率的相应结果。首先给出下面这个一般引理，它对每个字 w都成立。（下面的证明受到[2, 命题 23]的启发。）

引理 20。 设 G 是一个带有左不变测度 μ的可 *amenable* 群，且 $N \trianglelefteq G$ 是一个有限指数正规子群。那么，

$$\mathbb{P}(w;\, G/N) \geq \mathbb{P}_\mu(w;\, G).$$

证明。 为简化记号，设 $p(G) = \mathbb{P}_\mu(w;\, G)$，且 $p(G/N) = \mathbb{P}(w;\, G/N)$。令 W为 G^k 中满足 w的元组所组成的集合，即，

$$W = \{(g_1, \dots, g_k) \in G^k \mid w(g_1, \dots, g_k) = 1\},$$

并令（F_n）为 Følner序列， ω 为 $\mathbb{N}$ 上实现 μ的非主超滤子。反设 p（G/N） $< p$（G）。因此，存在 $\epsilon > 0$ 和 $R \in \omega$，使得对所有$n \in R$,

$$p(G/N) + \epsilon < \frac{|W \cap F_n^k|}{|F_n|^k}.$$

此外，由于 μ是左不变的， μ（gN） $= 1/|G$：对每个 $g \in G$， $N|$。特别地，固定 $g \in G$后，对每个 $\delta > 0$，都存在 $S_g \in \omega$，使得对所有 $n \in S_g$,

$$\frac{|gN \cap F_n|}{|F_n|} \leq \frac{1}{|G : N|} + \delta. \tag{4.3}$$

为 N 在 G中的陪集选取一个左横截集 T。由于陪集的代表元只有有限个，交集

$$S = R \cap \bigcap_{t \in T} S_t$$

非空，且属于 ω。假设 δ 足够小，使得

$$\frac{\epsilon}{p(G/N)(2^k - 1)|G : N|} > \delta, \quad \text{and} \quad \frac{1}{|G : N|} > \delta.$$

我们计算

$$\begin{aligned}
p(G/N) + \epsilon &\leq \frac{|W \cap F_n^k|}{|F_n|^k} \\
&\leq \frac{1}{|F_n|^k} \sum_{\substack{\mathbf{h} \in (G/N)^k \\ w(\mathbf{h}) = 1}} \#\{\mathbf{g} \in F_n^k \mid \mathbf{g} \equiv \mathbf{h} \mod N^k\} \\
&\leq \frac{1}{|F_n|^k} \sum_{\substack{\mathbf{h} \in (G/N)^k \\ w(\mathbf{h}) = 1}} \prod_{i=1}^{k} |h_i N \cap F_n| \\
&\leq \frac{1}{|F_n|^k} \max_{t \in T} |tN \cap F_n|^k \sum_{\substack{\mathbf{h} \in (G/N)^k \\ w(\mathbf{h}) = 1}} 1 \\
&= \frac{1}{|F_n|^k} \max_{t \in T} |tN \cap F_n|^k \cdot \#\{\mathbf{h} \in (G/N)^k \mid w(\mathbf{h}) = 1\}.
\end{aligned}$$

回顾

$$p(G/N) = \frac{\#\{\mathbf{h} \in (G/N)^k \mid w(\mathbf{h}) = 1\}}{|G:N|^k},$$

我们还利用公式（4.3），得到

$$\begin{aligned} p(G/N) + \epsilon &\le \frac{1}{|F_n|^k} \max_{t\in T} |tN \cap F_n|^k \cdot p(G/N)|G:N|^k \\ &\le p(G/N)\,(1 + |G:N|\delta)^k\,. \end{aligned}$$

根据初等估计，对于每个 $x \in (0,1)$，$(1+x)^k \le 1 + (2^k - 1)x$ 我们得出

$$p(G/N) + \epsilon \le p(G/N)(1 + (2^k - 1)|G:N|\delta)\,.$$

这与我们对 δ 的选择矛盾，从而完成证明。 ∎

现在我们刻画平方关联概率 $\mathrm{sq}^\mu(G)$ 为正的可 amenable 群。为此，我们还需要假设 G 是剩余有限的。

引理 21. 设 G 是一个剩余有限的可 *amenable* 群，且 μ 是定义在 G 上的左不变有限可加概率测度。假设 $\mathrm{sq}^\mu(G) > 0$。那么， G 几乎阿贝尔。

证明。 假设 $\mathrm{sq}^\mu(G) = \alpha > 0$。根据定理 20， $\mathrm{sq}(G/N) \ge \alpha$ 对G的每个有限商群都成立。因此，由 ?? 13?? 16,

$$\alpha \le \mathrm{sq}(G/N) = \frac{\varepsilon(G/N)}{|G/N|} \le \frac{\kappa(G/N)}{|G/N|} = \mathrm{cp}(G/N)\,,$$

因此， G/N中至少有 $\alpha|G/N|$ 个可交换对。回想一下， G嵌入在有限群完备化中

$$\hat{G} = \varprojlim_{N \trianglelefteq_{\mathrm{fin}} G} G/N\,.$$

ˆ因此，在带有哈尔测度 μ_H 的 G 中，我们有

$$\mu_H \otimes \mu_H \left(\left\{ (x,y) \in \hat{G}^2 \mid xy = yx \right\} \right) \ge \alpha\,.$$

因此，根据 [32, 定理 1。1], ˆG 几乎阿贝尔。若记 ˆ $A \trianglelefteq$ ˆG 为有限指数阿贝尔ˆ ˆ子群 G，则 $A = A \cap G$ 是 G的有限指数阿贝尔子群，证毕。 ∎

接下来我们证明，当 G 几乎阿贝尔时，$\mathrm{sq}(G) = \mathrm{sq}^\mu(G)$ 与 μ 的选取无关。在开始证明之前，我们回顾一下， G 上的任意左不变测度 μ 都会在有限指数子群 $H \le G$ 上诱导出一个左不变测度 μ_H，其定义为

$$\mu_H(X) = \frac{\mu(X)}{\mu(H)} = |G:H|\,\mu(X), \quad X \subseteq H.$$

因此，对每一个有界的 $f \in \ell^\infty(G)$，我们有

$$\int_G f(g)\,d\mu(g) = \frac{1}{|G:H|} \sum_{t\in T} \int_H f(s(t)\,a)\,d\mu_H(a), \tag{4.4}$$

其中 T 是 H 在 G中的左横截，且 $s\colon T \to G$ 是一个截面映射。

引理 22. 设 G是一个几乎阿贝尔群。则 $\mathrm{sq}^\mu(G)$ 不依赖于 G上的左不变测度 μ 。

证明。设

$$S = \{(x,y) \in G^2 \mid x^2 = y^2\}\,,$$

并设 $\mathbf{1}_S$ 为其特征函数。则，

$$\mathrm{sq}_\mu(G) = \int_{G\times G} \mathbf{1}_S(x,y)\,d(\mu\otimes\mu)(x,y).$$

令 $A \trianglelefteq G$ 为有限指数正规阿贝尔子群，并将商群 G/A记为 Q。固定一个截面 $s\colon Q \to G$，使得 $s(1) = 1$。利用 s给出的 Q 在 A 上的共轭作用，对于每个$q \in Q$，我们定义自同构 $f_q \in \mathrm{Aut}(A)$，其定义为 $f_q(a) = a^{s(q)}a$。我们将对角 2-余循环记为 δ_q，即， $\delta_q = s(q^2)^{-1}s(q)^2 \in A$，因此对于任意 $q \in Q$ 和 $a \in A$，

$$(s(q)a)^2 = s(q^2)\delta_q f_q(a).$$

因此，我们注意到 $(s(q)a)^2 = (s(r)b)^2$ 当且仅当

$$q^2 = r^2 \text{ in } Q \quad \text{and} \quad \delta_q f_q(a) = \delta_r f_r(b) \text{ in } A.$$

现在，对每个 q， $r \in Q$ 定义群同态

$$F_{q,r} \colon A \times A \to A, \quad (a,b) \mapsto f_q(a) f_r(b)^{-1}.$$

假设 $q^2 = r^2$，平方相等的数对由 $\delta_q \delta_r^{-1}$经由 $F_{q,r}$的纤维给出。具体而言，考虑

$$\mathcal{S}(Q) = \{(q,r) \in Q^2 \mid q^2 = r^2 \text{ and } s(q)A \cap s(r)A \neq \varnothing\};$$

那么，只要 $(q, r) \in \mathcal{S}(Q)$，就存在 $(\tilde{a}, \tilde{b}) \in A^2$ 使得 $F_{q,r}(\tilde{a}, \tilde{b}) = \delta_q \delta_r^{-1}$。因此，应用方程（4.4），

$$\begin{aligned}
\mathrm{sq}_\mu(G) &= \frac{1}{|G:A|^2} \sum_{(q,r)\in\mathcal{S}(Q)} (\mu_A \otimes \mu_A)\big(\{(a,b) \in A^2 \mid F_{q,r}(a,b) = \delta_q\delta_r^{-1}\}\big) \\
&= \frac{1}{|G:A|^2} \sum_{(q,r)\in\mathcal{S}(Q)} (\mu_A \otimes \mu_A)\big((\tilde{a},\tilde{b})\ \ker(F_{q,r})\big) \\
&= \frac{1}{|G:A|^2} \sum_{(q,r)\in\mathcal{S}(Q)} (\mu_A \otimes \mu_A)\big(\ker(F_{q,r})\big) \\
&= \frac{1}{|G:A|^2} \sum_{(q,r)\in\mathcal{S}(Q)} \frac{1}{|A^2 : \ker(F_{q,r})|}\,.
\end{aligned}$$

由于最后一个表达式与测度 μ 无关，证明完成。 ■

综合以上结果，我们得到定理 B 和定理 D的如下特例。

推论 E。 设 G 是一个有限生成无限可 *amenable* 群，设 $(F_n) \subseteq G$ 是 G的对称 *Følner*序列，设 $k\colon \mathbb{N} \to \mathbb{N}$ 是一个非递减函数，并设 A_k 是从 F_n中均匀随机抽取的一个 k-子集。

(a) 假设对于某个常数 $\alpha \in [0,1]$，有 $k = \alpha|F_n| + o(|F_n|)$。那么，

$$\alpha^4 \leq \mathbb{E}[\eta_n(\mathsf{A}_k, \mathsf{A}_k)] \leq \alpha^4 + \alpha^3\,.$$

(b) 假设 G 是几乎阿贝尔的，且 $k \ll \sqrt{|F_n|}$。那么，

$$\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k)] = k^2\,(1 + \mathrm{cp}(G) + \mathrm{sq}(G)) + o(k^2)\,.$$

(c) 假设 G 不是几乎阿贝尔的，且 $k \ll \sqrt{|F_n|}$。那么，

$$k^2 \leq \mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k)] \leq 2k^2 + o(k^2)\,.$$

此外，当 G 还是剩余有限的时，

$$\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k)] = k^2 + o(k^2)\,.$$

证明。 条目 (a) 可由定理 B直接计算得到。

为证明条目（b）和（c），我们注意到，定理 19 蕴含比值 $|Q_3^{(1)}|/|F_n|^2$ 收敛于 $\mathsf{cp}(G)$，并且根据定理 1，$\mathsf{cp}(G) = 0$，当 G 不是几乎阿贝尔时。此外，按定义，$|Q_4^{(1)}|/|F_n|^2$ 的超极限为 $\mathsf{sq}_\mu(G)$。根据定理 21，当 G 是剩余有限时，$\mathsf{sq}(G) = \mathsf{sq}_\mu(G)$ 与 μ 无关；而当 G 进一步不是几乎阿贝尔时，$\mathsf{sq}(G) = 0$。从这里开始，计算与定理 B 的证明完全相同。 ■

请注意，在定理 21 中使用“剩余有限性”似乎只是一个技术细节，而非结构性要求。因此，我们提出以下问题，以加强定理 E （c）。

问题 F。 我们能否在定理中去掉剩余有限这一假设21和定理E (c)?

最后，我们记录一下上述渐近界的一个应用。若群 G 具有小平方性质，则对每个整数 $k \geq 2$以及每个 k-子集 $A \subseteq G$， A^{*2} 的大小都严格小于 k^2。这一概念由 Freiman 于 [26] 针对 $k = 2$提出，随后在 [7, 9, 25]中得到进一步发展。鉴于定理18，我们的方法为 Neumann 的一个结果提供了一种新颖的证明（参见 [31, 定理 1]），前提是该群在某种意义上可以由有限群逼近。

推论G。 设 G 是一个剩余有限可 *amen* 群。若 G 对某个整数 k 满足小平方性质，则 G 是有限-阿贝尔-有限群。

证明。 我们的证明是验证反命题的真实性。假设 G 是一个并非有限-阿贝尔-有限群的剩余有限可 amen 群。结合定理 21 和 [56, 定理 1。14], 我们得到，对于每个左不变测度 μ，$\mathrm{sq}^{\mu}(G) = \mathrm{cp}^{\mu}(G) = 0$。因此，对于随机的 k-子集 A_k，由定理 E，

$$\lim_n \mathbb{E}\left[E(\mathsf{A}_k, \mathsf{A}_k)\right] = k^2 .$$

因此，由詹森不等式和定理 7，

$$\lim_n \mathbb{E}\left[|\mathsf{A}_k^{*2}|\right] = k^2 .$$

因此，对于每个正整数 $k \geq 2$，存在 $N(k)$，使得对于 $n \geq N(k)$，

$$\mathbb{E}\left[|\mathsf{A}_k^{*2}|\right] \geq k^2 - \frac{1}{2} .$$

由于该随机变量仅取整数值，因此可知存在一个集合 A_k，使得 $|A_k^{*2}| = k^2$，从而 G 不具有小平方性质，证毕。 ■

类比于推论F，我们期望这一结果能推广到所有可 amenable 群这一类。鉴于 [56, 定理 1.14], 实现这一点的一种自然途径，是对下列问题给出肯定的回答。

问题H. 是否对每个可 amenable 群都成立：$\mathrm{sq}^{\mu}(G) \leq \mathrm{cp}^{\mu}(G)$?

4.4. **有限生成群。** 现在我们将注意力转向带有词度量的有限生成群。设 S 是 G 的一个有限生成集，并设 $(F_n)_{n\in\mathbb{N}} = (\mathbf{B}_S(n))_{n\in\mathbb{N}}$ 是由 S 诱导的词度量中围绕单位元的球所构成的滤过级数。由定理 D，在 $k \ll \sqrt{|F_n|}$这一范围内，

$$\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k)] = k^2\big(1 + \mathrm{cp}_{\mu}(G) + \mathrm{sq}_{\mu}(G)\big) + o(k^2) .$$

注意，先验地，平方关联概率与交换概率都可能依赖于生成集 S的选取，从而也依赖于有限穷竭测度 μ。交换概率这一概念在此设定下于 [2], 中被引入，尽管作者考虑的是使 上极限 得以达到的子列。由此得到的不变量 $\mathrm{cp}_S(G)$ （我们使用下标 S 以强调其对生成集而非测度的依赖性）是否与 S的选取无关，仍是一个未决问题。进一步有人猜想，$\mathrm{cp}_S(G)$ 非零当且仅当 G 是几乎阿贝尔的（见 [2, 猜想 1.6]）。

回想次指数增长的群是可 amenable 的，此时存在由球构成的对称 Følner 序列。因此，$\mathrm{cp}^{\mu}(G)$ 与 $\mathrm{sq}^{\mu}(G)$ 的值与 μ 的选取无关，这分别由 [56, 推论 118] 和定理 21 得出。此外，我们猜想，对每一个群 G，若其具有指数增长，则 $\mathrm{sq}_S(G)$ 与 $\mathrm{cp}_S(G)$ 均为零。因此，我们提出如下猜想。

猜想 I. 设 G 是一个指数增长的有限生成群。设 $k\colon \mathbb{N} \to \mathbb{N}$ 是满足 $k \ll \sqrt{|\mathbf{B}_S(n)|}$ 的非递减函数，并设 A_k 是在词球$\mathbf{B}_S(n)$中均匀随机抽取的 F_n 的一个 k-子集。则，

$$\lim_n \mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k)] = k^2 .$$

我们证明了这一猜想对于某些群类是正确的，而对于这些群类，交换概率已经是已知的。

例 23 （字双曲群）。 设 G 是一个非初等双曲群，并设 S是 G的有限生成集。无论生成集如何取， 交换概率$_S$（G） $=0$ （见 [2, 定理 1。7]）。

对于平方关联概率，设 Tor(G) 表示 G 的挠元集合，并回顾

$$\#\{(x,y)\in \mathbf{B}_S(N)^2 \mid x^2=y^2\}=\sum_{g\in G} r_n(g)^2=\sum_{g\in \mathrm{Tor}(G)} r(g)^2+\sum_{g\notin \mathrm{Tor}(G)} r_n(g)^2\,.$$

对于第一项，

$$\sum_{g\in \mathrm{Tor}(G)} r_n(g)^2\le |\,\mathrm{Tor}(G)|^2\,,$$

且 [19, 定理 1.1]给出

$$\limsup_n \frac{|\,\mathrm{Tor}(G)|}{|\mathbf{B}_S(n)|}=0\,.$$

对于第二项，回顾双曲群中无限阶元素的中心化子是有限-by-$\mathbb{Z}$ 或有限-by-(C_2*C_2)的（见 [10, 推论 III.Γ.3.10]），并且存在界 $C>0$，它控制 G 的有限子群的大小，且仅依赖于双曲常数（见 [10, 定理 III.Γ.3.2]）。固定一个无限阶元素 $x\in G$ ，并设 $N\trianglelefteq \mathbf{C}_G(x^2)$为有限正规子群，使得$\mathbf{C}_G(x^2)/N$ 同构于 $\mathbb{Z}$ 或 C_2*C_2。注意， $\mathbb{Z}$或 C_2*C_2 中的两个元素具有相同的平方根，当且仅当它们都是挠元。因此，若$x^2=y^2$对元素 $y\in G$成立，则 $x\equiv y \pmod N$，从而 $y=mx$ 对 $m\in N$成立。因此，$r_n(x^2)\le |N|\le C$。于是，

$$0\le \limsup_n \frac{1}{|\mathbf{B}_S(n)|^2}\sum_{g\notin \mathrm{Tor}(G)} r_n(g)^2\le \limsup_n \frac{|\mathbf{B}_S(n)|C^2}{|\mathbf{B}_S(n)|^2}=0\,.$$

因此，sq$_S$(G) $=0$。

例 24 （直角阿廷群）。 设 $G=G(\Gamma)$ 是定义在有限图 Γ 上的无限直角阿廷群，并配备典范生成集 $S=V(\Gamma)\cup V(\Gamma)^{-1}$。一方面， [58, 定理 6] 给出 cp$_S$($G$) $=0$。另一方面，直角阿廷群是双可序的（见 [22]）。因此，平方根唯一，即，若 $g^m=h^m$ 对某个 $m\ge 1$成立，则 $g=h$。因此，平方映射 $g\mapsto g^2$ 是单射，且 sq$_S$(G) $=0$ （对任意生成集均成立）。

例 25 （具有无限循环顶群的广义灯笼群）。 设 G 是限制 wreath 积 $H\,\mathrm{wr}\,\mathbb{Z}=H^{\mathbb{Z}}\rtimes\mathbb{Z}$，其中 H 是一个有限生成群。一方面，对于任意生成集，cp$_S$(G) $=0$ （见 [18, 定理 2] 和 [20, 定理 A]）。

另一方面，假设 $x=(h,\ t^n)$ 和 $y=(k,\ t^m)$ 的平方相同，但二者不同。我们计算得

$$x^2=(hh^{t^n},\,t^{2n})=(kk^{t^m},\,t^{2m})=y^2\,.$$

由于在 $\mathbb{Z}$, $n=m$ 中平方映射是单射。记 $h=(h_i)_{i\in\mathbb{Z}}$ 和 $k=(k_i)_{i\in\mathbb{Z}}$。前面的等式意味着

$$h_ih_{i-n}=k_ik_{i-n} \tag{4.5}$$

假设存在 $i_0\in\mathbb{Z}$ 使得 $h_{i_0}\neq k_{i_0}$，并令 i_0 在满足该性质的元素中取最小值。因此，除非 $n=0$， $h_{i_0-n}=k_{i_0-n}$。代入方程（4.5），得到矛盾$h_{i_0}=k_{i_0}$。因此， $n=0$，且 x，y 都属于基群 $H^{\mathbb{Z}}$。于是，将平方相同的配对集合拆分为两类：其中元素彼此不同的配对，以及元素不相同的配对，我们得到

$$\frac{\left|\{(x,y)\in \mathbf{B}_S(n)^2 \mid x^2=y^2\}\right|}{|\mathbf{B}_S(n)|^2}\le \frac{|\mathbf{B}_S(n)|+\left|\{(x,y)\in \mathbf{B}_S(n)^2 \mid x\neq y, x^2=y^2\}\right|}{|\mathbf{B}_S(n)|^2}\,.$$

结合前面的讨论与 [20, 定理 B], ，可得

$$\lim_n \frac{\left|\{(x,y)\in \mathbf{B}_S(n)^2 \mid x^2=y^2\}\right|}{|\mathbf{B}_S(n)|^2}\le \lim_n \frac{1}{|\mathbf{B}_S(n)|}+\frac{|H^{\mathbb{Z}}\cap \mathbf{B}_S(n)|^2}{|\mathbf{B}_S(n)|^2}=0\,.$$

因此，sq$_S$(G) $=0$。

5. 集合与其逆元集的乘法能量

另一个自然的替代对象是 Δ，而非 A 其本身，是其逆元集合，A^{-1}，因为此处会出现自然的抵消现象。在这种情况下，我们的掌控力更强：我们不必研究 F_n中的特定元素对或三元组的性质，只需计算滤过的每个集合中出现了多少个对合。这一点将在定理26中明确说明。我们的主要结果并不依赖这一事实，因为它只是对定理A的直接推广。

定理 J. 设 G 是一个离散群，设 $(F_n) \subseteq G$ 是 G 的一个对称滤子序列，设$k\colon \mathbb{N} \to \mathbb{N}$ 是一个非递减函数，并设 A_k 是从 F_n 中均匀随机抽取的一个 k-子集。那么，

$$\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k^{-1})] \leq \frac{k^{\underline{4}}}{|F_n|-3} + \frac{k^{\underline{3}}}{(|F_n|-1)^{\underline{2}}}\,(2|F_n|-1) + 3k^2 - 2k\,,$$

and

$$\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k^{-1})] \geq \frac{k^{\underline{4}}}{(|F_n|-1)^{\underline{3}}}\left(|F_n|^2 - 4|F_n| + 2\right) + 2k^2 - k\,.$$

证明。此证明与定理 B的证明基本相同。因此，我们只强调差异所在之处。首先，通常的双重计数告诉我们

$$\mathbb{E}\left[E(\mathsf{A}_k, \mathsf{A}_k^{-1})\right] = \binom{|F_n|}{k}^{-1} \sum_{(a,b,c)\in F_n^3} \#\left\{A \in \mathcal{P}_k(F_n) \middle| (a,b,c,ba^{-1}c) \in A^4\right\}\,.$$

我们之前使用的划分中包含一些空集。因此，我们只需使用以下七个集合：

$$\begin{aligned}
Q_1^{(1)} &= \{(a,b,c) \in F_n^3 \mid \#\{a,b,c\} = 3,\, ba^{-1}c = a\}\,,\\
Q_1^{(2)} &= \{(a,b,c) \in F_n^3 \mid \#\{a,b,c\} = 3,\, ba^{-1}c \neq a\}\,,\\
Q_2 &= \{(a,b,a) \in F_n^3 \mid a \neq b\}\,,\\
Q_3^{(1)} &= \{(a,b,b) \in F_n^3 \mid a \neq b,\, ba^{-1}b = a\}\,,\\
Q_3^{(2)} &= \{(a,b,b) \in F_n^3 \mid a \neq b,\, ba^{-1}b \neq a\}\,,\\
Q_4 &= \{(a,a,c) \in F_n^3 \mid a \neq c\}\,,\\
Q_5 &= \{(a,a,a) \in F_n^3\}\,.
\end{aligned}$$

再一次，很容易看出

$$|Q_2| = |Q_4| = |F_n|(|F_n|-1), \quad \text{and} \quad |Q_5| = |F_n|\,.$$

现在我们将对这两对对象分别进行讨论：$Q_1^{(1)}$ 和 $Q_1^{(2)}$，以及 $Q_3^{(1)}$ 和 $Q_3^{(2)}$。

我们先讨论前一对。记 I 为所有对合（包括单位元 ）in G。对于每个 $y \in F_n^{*2}\setminus I$，我们定义一个单射

$$\psi_y : F_n \to F_n \times yF_n \times y^{-1}F_n,\, x \mapsto (x, yx, y^{-1}x)\,.$$

我们断言

$$\left(\bigcup_{y\in F_n^{*2}\setminus I} \psi_y(F_n)\right) \cap F_n^3 = Q_1^{(1)}\,.$$

一方面，如果 $y \in F_n^{*2}\setminus I$ 且 $(x, yx, y^{-1}x) \in F_n^3$，那么

$$(yx)x^{-1}(y^{-1}x) = x\,.$$

由于 $y^2 \neq 1$，我们看到 x, yx 和 $y^{-1}x$ 两两不同，因此 $(x, yx, y^{-1}x) \in Q_1^{(1)}$。另一方面，对于每个 $(a,b,c) \in Q_1^{(1)}$，令 $x = a \in F_n$ 和 $y = ba^{-1} \in F_n^{*2}$。于是，$b = yx$ 并且

$$c = ab^{-1}a = xx^{-1}y^{-1}x = y^{-1}x\,.$$

若 $y^2 = 1$，则 $ba^{-1} = ab^{-1}$，从而 $c = b$，这与 (a,b,c) 的选择相矛盾。因此，对于 $y \in F_n^{*2}\setminus I$ 和 $x \in F_n$，有 $(a,b,c) = \psi_y(x)$。这证明了该断言。注意，$\psi_y(x) \in F_n^3$ 当且仅当 $x \in F_n \cap yF_n \cap y^{-1}F_n$，这意味着

$$|\psi_y(F_n) \cap F_n^3| = |F_n \cap yF_n \cap y^{-1}F_n| \leq |F_n \cap yF_n|\,.$$

因此，利用定理 9,

$$0 \leq |Q_1^{(1)}| \leq \sum_{y \in F_n^{*2} \setminus I} |F_n \cap yF_n| \leq |F_n|^2 .$$

由于 $|Q_1^{(1)}| + |Q_1^{(2)}| = |F_n|(|F_n| - 1)(|F_n| - 2)$，我们得到

$$|F_n| \left(|F_n|^2 - 4|F_n| + 2 \right) \leq |Q_1^{(2)}| \leq |F_n|(|F_n| - 1)(|F_n| - 2) .$$

对于这一对 $Q_3^{(1)}$ 和 $Q_3^{(2)}$，在当前证明中我们采用平凡界

$$0 \leq |Q_3^{(1)}| \leq |F_n|(|F_n| - 1) \quad \text{and} \quad 0 \leq |Q_3^{(2)}| \leq |F_n|(|F_n| - 1) .$$

最后，我们注意到

$$\text{(F)} \qquad \mathbb{E}\left[E(\mathsf{A}_k, \mathsf{A}_k^{-1})\right] = \binom{|F_n|}{k}^{-1} \left[\binom{|F_n| - 4}{k - 4} |Q_1^{(2)}| + \binom{|F_n| - 3}{k - 3} (|Q_1^{(1)}| + |Q_3^{(2)}|) + \right.$$
$$\left. + \binom{|F_n| - 2}{k - 2} (|Q_2| + |Q_3^{(1)}| + |Q_4|) + \binom{|F_n| - 1}{k - 1} |Q_5| \right] .$$

证明的其余部分只是计算。 ∎

我们从定理 E_n（A_k，A_k^{-1}）中得到的渐近界已经比定理 J 对 E_n（A_k，A_k）给出的界更精确。我们有，若 $k \ll \sqrt{|F_n|}$,

$$2k^2 \leq \mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k)] - O\left(\frac{k^4}{|F_n|}\right) \leq 3k^2 ,$$

并且，如果 $k \ll \sqrt[3]{|F_n|}$,

$$2k^2 - k \leq \mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k)] - O\left(\frac{k^4}{|F_n|}\right) \leq 3k^2 - 2k ,$$

至于定理 B，这些渐近界是紧的，因此若不对模型添加额外假设，就无法改进。对于任意穷竭，初等阿贝尔 2-群都能达到上界，因为 $Q_3^{(2)}$ 为空，因此 $|Q_3^{(1)}| = |F_n|(|F_n| - 1)$。另一方面，$Q_3^{(1)}$ 中的每个元素的阶都整除 2，因此当 G 无挠时，$Q_3^{(1)}$ 为空，并且下界可以达到。

至于定理 B 的推论，理解这对 $|Q_4^{(1)}|$ 和 $|Q_4^{(2)}|$已经完成了大部分关键工作；我们对定理 J 的改进将主要来自对$|Q_3^{(1)}|$ 和 $|Q_3^{(2)}|$的理解。在此，集合 I（包含 G的所有对合）与滤过级数各集合的交集基数将发挥核心作用。

注记26。对于每个 $x \in F_n$，我们定义单射

$$\phi_x : F_n x^{-1} \cap (I \setminus \{1\}) \to F_n^3, \quad y \mapsto (x, yx, yx) .$$

我们断言

$$\left(\bigcup_{x \in F_n} \phi_x(F_n x^{-1} \cap (I \setminus \{1\})) \right) \cap F_n^3 = Q_3^{(1)} .$$

一方面，若 $(a,\ b,\ b) \in Q_3^{(1)}$，则令 $x = a \in F_n$ 和 $y = ba^{-1} \in F_n a^{-1}$，使得 $(a,\ b,\ b) = \phi_x(y)$。由于

$$x = a = ba^{-1}b = yxx^{-1}yx = y^2x,$$

我们有 $y \in I$。此外，由于 $a \neq ya$，$y \neq 1$。另一方面，若 $x \in F_n$ 且 $y \in F_n x^{-1} \cap I \setminus \{1\}$，则

$$(yx)x^{-1}(yx) = y^2x = x .$$

由于 $y \neq 1$，我们看到 $x \neq yx$，因此 $\phi_x(y) \in Q_3^{(1)}$。我们注意到

$$|\phi_x(F_n x^{-1} \cap (I \setminus \{1\})) \cap F_n^3| = |F_n x^{-1} \cap (I \setminus \{1\})| .$$

因此，注意到 $|Q_3^{(1)}| + |Q_3^{(2)}| = |F_n|(|F_n| - 1)$，我们有

$$0 \leq |Q_3^{(1)}| \leq \sum_{x \in F_n} |F_n x^{-1} \cap (I \setminus \{1\})| ,$$

and

$$|F_n|(|F_n|-1)-\sum_{x\in F_n}|F_nx^{-1}\cap(I\setminus\{1\})|\le|Q_3^{(2)}|\le|F_n|(|F_n|-1)\,.$$

我们强调，我们在定理 J 的证明中没有纳入这一考量，因为它可能比平凡界 $|F_n|(|F_n|-1)$ 更差。事实上，

$$\sum_{x\in F_n}|F_nx^{-1}\cap(I\setminus\{1\})|\le|F_n||F_n^{*2}\cap(I\setminus\{1\})|\,.$$

尽管这个最后的界在第 5.2 节中会很有用，但在一般情况下，我们无法排除 $|F_n^{*2}\cap(I\setminus\{1\})|$ 在 $|F_n|$ 中超线性增长的可能性。（尽管如此， $|F_n^{*2}|$ 本身在 $|F_n|$ 中可能呈超线性增长。例如，在指数增长群的球过滤中就会出现这种情况。）

5.1. **有限群**。现在我们回过头来，重点讨论 G 为有限群的情形。我们用 $\iota(G)$ 表示 G 的对合数量（包括单位元）。众所周知，在有限群中，对合的数量可以表示为

$$\iota(G)=r(1)=\frac{1}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\left(\chi(1)\sum_{g\in G}\chi(g^2)\right),$$

(Thi这可直接由定理 14 得出，类似的证明见 [33, 推论 4。6]。）

推论 K。设 G 是有限群， $k\in\mathbb{N}$ 是正整数，并设 A_k 是从 G 中均匀随机抽取的一个 k-子集。假设 ι 是 G 的对合数量（包括单位元）。那么

$$\begin{aligned}\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k^{-1})]=&\frac{k^{\underline{4}}}{(|G|-1)^{\underline{3}}}(|G|^2-4|G|+2+\iota(G))+\frac{k^{\underline{3}}}{(|G|-1)^{\underline{2}}}2\left(|G|-\iota(G)\right)\\&+\frac{k^{\underline{2}}}{(|G|-1)}\left(\iota(G)-1\right)+2k^2-k\,.\end{aligned}$$

证明。 由于 G 是有限的，我们可以假设，对每个 n， $F_n=G$，因此 G^{*2} 只不过是 G。在此假设下，我们可以明确计算 $|Q_1^{(1)}|$、 $|Q_1^{(2)}|$、 $|Q_3^{(1)}|$ 和 $|Q_3^{(2)}|$。将这些值代入常用公式即可得到所需结论。

具体而言，在计算 $|Q_1^{(1)}|$ 的基数时，我们得到

$$\begin{aligned}|Q_1^{(1)}|&=\sum_{y\in G\setminus I}\left|\psi_y(G)\cap G^3\right|\\&=\sum_{y\in G\setminus I}\left|G\cap yG\cap y^{-1}G\right|\\&=\sum_{y\in G\setminus I}|G|\\&=|G||G\setminus I|\\&=|G|(|G|-|I|)\,.\end{aligned}$$

因此，回想起 $|Q_1^{(1)}|+|Q_1^{(2)}|=|G|(|G|-1)(|G|-2)$，

$$|Q_1^{(2)}|=|G|(|G|^2-4|G|+|I|+2)\,.$$

同样，由定理 26，

$$|Q_3^{(1)}|=\left|\bigcup_{x\in G}\phi_x\left(I\setminus\{1\}\right)\right|=|G|(|I|-1),\quad\text{and}\quad|Q_3^{(2)}|=|G|\left(|G|-|I|\right).$$ ■

例 27. 我们再次考虑 $G=\mathrm{GL}_2(q)$。先假设 q 是一个奇整数。于是$|G|=(q+1)q(q-1)^2,$，并且直接查阅 G 的特征标表可得， $\iota(G)=q^2+q+2$，

and

$$\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k^{-1})] = \frac{k(1+k)(2+k)(3+k)\big(4+q+q^2-4(q-1)^2q(1+q)+(q-1)^4q^2(1+q)^2\big)}{(q-1)^2q(1+q)\big((q-1)^2q(1+q)-1\big)\big(1+(q-1)^2q(1+q)\big)} + \frac{k(1+k)\big(1+q+q^2\big)}{(q-1)^2q(1+q)-1} + \frac{2k(1+k)(2+k)\big(q^4-q^3-2q^2-2\big)}{(q-1)^2q\big(q^5-2q^3-1\big)} + 2k^2-k\,.$$

若 q 是一个偶整数，则 $|G| = (q+1)q(q-1)^2$, $\iota(G) = q^2$, 并且

$$\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k^{-1})] = \frac{k(1+k)(2+k)(3+k)\big(2+q^2-4(-1+q)^2q(1+q)+(q-1)^4q^2(1+q)^2\big)}{(q-1)^2q(1+q)\big((q-1)^2q(1+q)-1\big)\big(1+(q-1)^2q(1+q)\big)} + \frac{k(1+k)\big(q^2-1\big)}{(q-1)^2q(1+q)-1} + \frac{2k(1+k)(2+k)\big(1-2q-q^2+q^3\big)}{(q-1)^2\big(q^5-2q^3-1\big)} + 2k^2-k\,.$$

因此，对于任意有限群序列 (G_n)，且当 k 有界时，我们有如下渐近表达式

$$\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k^{-1})] = \left(2+\frac{\iota(G_n)}{|G_n|}\right)k^2 - \left(1+\frac{\iota(G_n)}{|G_n|}\right)k + O\left(\frac{\iota(G_n)}{|G_n|}\right)\,. \tag{G}$$

注意，对于奇数阶群，$\iota(G_n)$ 为零；并且对于阶不断增大的有限单群序列 (G_n)，$\lim_n \iota(G_n) = 0$ 。

5.2. **无限群**。 与有限群的情形一样，根据定理 26，精确极限同样取决于群中对合所占的比例。如第 4.2节所述，若 G 是赋有有限可加测度的群，则其对合概率 相对于 G和 μ定义为

$$\iota_\mu(G) = \mathbb{P}(G;\beta_2) = \mu(\{x\in G \mid x^2=1\})\,, \tag{H}$$

其中 $\beta_2(x) = x^2$ 是 2-Burnside 词。

注意，根据定义，对于 2-变体词 $w(x,\ y) = (x^{-1}y)^2$，比值 $|Q_3^{(1)}|/|F_n|^2$ 收敛于 $\mathbb{P}_\mu(G;w)$。因此，直接计算可得

$$\mathbb{E}[\mathsf{A}_k,\mathsf{A}_k] = (2+\mathbb{P}_\mu(G;w))k^2 + o(k^2),$$

对于任意测度。尽管如此，鉴于我们在有限群中观察到的现象，我们猜想 $E_n(\mathsf{A}_k,\ \mathsf{A}_k^{-1})$ 的期望值由对合概率决定。

问题 L. 设 G 是一个无限群，(F_n) 是 G 中的一个对称滤子，$k\colon \mathbb{N}\to\mathbb{N}$ 是一个满足 $k \ll \sqrt{|F_n|}$ 的非递减函数，且 A_k 是 F_n 的一个随机 k-子集。是否有

$$\mathbb{E}[\mathsf{A}_k,\mathsf{A}_k^{-1}] = (2+\iota_\mu(G))k^2 + o(k^2)\,?$$

虽然我们没有在完全一般的情形下解决这个问题，但我们在若干情形下给出了肯定的回答。

5.3. **可 amenable 群**。 借助左不变测度，我们刻画了对合概率严格为正的剩余有限群。我们首先记录一个适用于我们框架的辅助引理。（以下证明沿用了 [39, 定理2]的思路。）

引理 28. 设 G 是一个带有左不变测度 μ 的剩余有限可 *amen* 群。那么，$\iota_\mu(G) > 0$ 当且仅当存在一个有限指数正规阿贝尔子群 $A \trianglelefteq G$，并且存在 $t\in G$，使得 tA 中的每个元素都是对合。

证明。反向蕴含显而易见，因为利用测度的左不变性，

$$\iota_\mu(G) \geq \mu(tA) = \mu(A) = \frac{1}{|G:A|} > 0\,.$$

对于正向推论，我们利用 G 嵌入有限群完备化这一事实

$$\hat{G} = \varprojlim_{N\trianglelefteq_{\mathrm{fin}}G} G/N\,.$$

根据引理 20， $\iota(G/N) \geq \alpha$ 对于 G的每个有限商群，因而根据 [41, 引理 1], 可得$\mathrm{cp}(G/N) > \alpha^2$, 因此至少存在 $\alpha^2|G/N|$个可交换对，属于 G/N。因此，在 $\hat{}G$上，关于哈尔测度 μ_H，我们有

$$\mu_H \otimes \mu_H(\{(x,y) \in G^2 \mid xy = yx\}) \geq \alpha^2 .$$

因此，由 [39, 定理 1], $\hat{}G$ 是几乎阿贝尔的。设$\hat{}$ $A \trianglelefteq \hat{}G$ 为 A的一个有限指数阿贝尔正规$\hat{}$ $\hat{}$子群，从而 $A = A \cap G$ 是 G的一个有限指数阿贝尔正规子群。设 I 为 G的所有对合的集合，由于 A 在 G 中具有有限指数，且 $\mu(I) = \iota_\mu(G) > 0$，故存在 $g \in G$使得 $\mu(I \cap gA) > 0$。现在，通过最终将 g 替换为一个元素 $gh \in I$，我们可以假定 g 本身是一个对合。因此，

$$ga \in I \cap gA \quad \text{if, and only if,} \quad gaga = a^g a = 1 .$$

因此，若我们定义子群

$$H_g = \{a \in A \mid a^g a = 1\} , \tag{5.1}$$

则 $I \cap gA = gH_g$。利用哈尔测度的左不变性，

$$\mu_H(H_g) = \mu_H(gH_g) = \mu_H(I \cap gA) > 0 .$$

Th因此， H_g 在 G中具有有限指数，且 gH_g 中的每个元素都是对合，如所欲证。 ∎

现在我们证明，对于剩余有限可 amen 群 G，实际上 $\iota_\mu(G)$ 与 μ 无关。因此，在此上下文中我们将省略下标。

Le引理 29。 设 G 是一个带有左不变测度 μ 的剩余有限可 *amen* 群。则 $\iota_\mu(G)$ 与测度 μ 无关。

证明。 根据定理 28，如果 G 不是几乎阿贝尔群，那么对于每个左不变测度 μ，$\iota_\mu(G) = 0$。因此，我们可以假设存在一个有限指数阿贝尔正规子群 $A \trianglelefteq G$。取 T 关于 A 在 G中的一个左横截，并考虑由下式给出的集合 I 的对合划分：

$$I = \bigcup_{g \in T} I \cap gA .$$

设 T_0 为满足以下条件的 $g \in T$ 的集合： $I \cap gA$ 非空。注意，对于每个 $g \in T_0$，我们可以假设 g 本身就是一个对合。此外，令 H_g 为方程（5.1）中定义的子群，从而 $I \cap gA = gH_g$。由此可得

$$\iota_\mu(G) = \mu(I) = \sum_{g \in T} \mu(I \cap gA) = \sum_{g \in T_0} \mu(gH_g) = \sum_{g \in T_0} \mu(H_g) = \sum_{g \in T_0} \frac{1}{|G : H_g|} \tag{5.2}$$

其中，无限指数的倒数为零。由于最后一个表达式与 μ 无关，证明完成。 ∎

引理 30. 设 G 是一个几乎阿贝尔群，设 (F_n) 是一个 *Følner* 滤过，设 $k\colon \mathbb{N} \to \mathbb{N}$ 是一个非递减函数，并设 A_k 是从 G 中均匀随机抽取的一个 k-子集。假设 $k \ll \sqrt[4]{|F_n|}$。则

$$\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k^{-1})] = (2 + \iota(G))\, k^2 - (1 + \iota(G))\, k + o(1) .$$

特别地，当 G 是阿贝尔群时，

$$\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k^{-1})] = \left(2 + \frac{1}{|G : I|}\right) k^2 - \left(1 + \frac{1}{|G : I|}\right) k + o(1) ,$$

其中， I 是由对合构成的子群。

证明。设 $A \trianglelefteq G$ 是 G 的一个有限指数阿贝尔正规子群，设 T 是 G 中 A 的一个左横截，并设 T_0 是满足以下条件的 $g \in T$ 的集合：对于由所有对合构成的集合 I， $gA \cap I$ 非空。根据方程 (F)，我们将证明比值 $|Q_3^{(1)}|/|F_n|^2$ 在 n 趋于无穷时趋于 $\iota(G)$。对于每个 $g \in T_0$，我们按照方程 (5.1) 定义 H_g，使得 $gH_g = I \cap gA$。根据 $Q_3^{(1)}$ 的定义，我们注意到，

$$\frac{|Q_3^{(1)}|}{|F_n|^2} = \frac{1}{|F_n|^2} \sum_{g \in T_0} \#\{(x,y) \in F_n^2 \mid xy^{-1} \in gH_g\} - \frac{1}{|F_n|}$$

令 ω 为一个非主超滤子，并令 μ 为由 ω 与原 Følner序列共同导出的左不变均值。我们固定 $g \in T$。注意， $xy^{-1} \in gH_g$ 当且仅当，

$x \in gH_g y = gyH_g$，其中后一个等式源于 H_g 是 A中的特征子群，因而是 G中的正规子群。因此，我们计算

$$\begin{aligned}\lim_{\omega} \frac{1}{|F_n|^2} \#\{(x,y) \in F_n^2 \mid xy^{-1} \in gH_g\} &= \mu^{\otimes 2}\Big(\{(x,y) \in G^2 \mid xy^{-1} \in gH_g\}\Big) \\ &= \int_G \mu(gyH_g)\, d\mu(y) \\ &= \int_G \mu(H_g)\, d\mu(y) \\ &= \frac{1}{|G:H_g|},\end{aligned}$$

（当 $|G : H_g|$ 为无限时，最终表达式理解为零。）此外，由于该值与非主超滤子无关，超极限实际上是一个普通极限。因此，根据方程（5.2），

$$\lim_n \frac{|Q_3^{(1)}|}{|F_n|^2} = \sum_{g \in T_0} \lim_n \frac{\big|\{(x,y) \in F_n^2 \mid xy^{-1} \in gH_g\}\big|}{|F_n|^2} = \sum_{g \in T_0} \frac{1}{|G:H_g|} = \iota(G)\,.$$

证明的其余部分由通常的计算构成。 ∎

当对合概率为零时，因此， G 不是几乎阿贝尔群，我们预计 $|Q_3^{(1)}|$ 与 $|Q_3^{(2)}|$ 这一对不会对极限行为产生影响。特别地，上述公式在 $\iota\mu(G) = 0$的情况下仍然成立。

引理 31。 设 G 是一个剩余有限可 *amen* 群，且 $(F_n) \subseteq G$ 是一个 *Følner* 滤过，设 $k\colon \mathbb{N} \to \mathbb{N}$ 是一个函数，并设 A_k 是从 G 中均匀随机抽取的一个 k-子集。假设 G 不是几乎阿贝尔群，并且 $k \ll \sqrt[4]{|F_n|}$。那么，

$$\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k^{-1})] = 2k^2 - k + o(1)\,.$$

证明。 我们用 μ_n 表示与 F_n相关联的离散概率测度。关于 $\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k^{-1})]$ 的下界可直接由定理 J得出。对于上界，我们将证明$|Q_3^{(1)}| = o(|F_n|^2)$。鉴于定理 26，为此只需证明

$$\lim_n \frac{1}{|F_n|} \sum_{x \in F_n} \frac{|F_n \cap xI|}{|F_n|} = 0\,, \tag{5.3}$$

其中 I 是所有对合的集合。鉴于定理 28， I 的上 Banach 密度为零，即，

$$\sup_{(F_n)\ \text{Følner}} \limsup_{n\to\infty} \frac{|I \cap F_n|}{|F_n|} = 0.$$

因此，由 [8, 命题 A.6], ，每个左不变均值 m 满足 $m(\mathbf{1}_I) = 0$。

我们考虑伴随测度 $\tilde{\mu}_n$，从而对每一个 $S \subseteq G$， $\tilde{\mu}_n(S) = \mu_n(S^{-1})$，以及卷积测度 $\nu_n = \mu_n * \tilde{\mu}_n$。（注意到，若 Følner序列是对称的，则$\tilde{\mu}_n = \mu_n$。）注意

$$\nu_n(I) = \frac{1}{|F_n|^2} \#\{(x,y) \in F_n \times F_n \mid x^{-1}y \in I\} = \frac{1}{|F_n|^2} \sum_{x \in F_n} |F_n \cap xI|\,.$$

因此，方程（5.3）的左边是 $\lim_n \nu_n(I)$。

我们旨在证明， ν_n 导出了一个左不变均值。具体而言，若定义离散均值族

$$m_n(f) = \sum_{g \in G} f(g)\nu_n(g), \quad \text{for every } f \in \ell^\infty(G)\,,$$

任意超极限都是左不变的。由巴拿赫–阿劳格鲁定理，所有均值的集合在 $\ell^\infty(G)^*$ 中关于弱-$*$ 拓扑是紧的（见 [14, 定理 4.2.1]）。考虑任意弱-$*$收敛子列 $(m_{n_k})_{k\in\mathbb{N}}$。我们断言相应的弱-$*$ 极限是左不变的。设

$$L_g\colon G \to G, \quad x \mapsto gx$$

是左乘，其作用元为 g，并回顾 G 通过 L_g的推前作用于 G上的有限可加测度集合。特别地，

$$g \cdot \mu_n(S) = \mu_n(g^{-1}S), \quad S \subseteq G\,.$$

此外，由于 (F_n) 是一个 Følner序列，

$$\lim_n \|g \cdot \mu_n - \mu_n\|_1 = 0,$$

在 $\ell^1(G)$-范数下（参见 [14, 定理 4.9 的证明。2]）。因此，由于离散概率测度的卷积是一个 ℓ^1-压缩映射，

$$\lim_n \|g \cdot \nu_n - \nu_n\|_1 = \lim_n \|(g \cdot \mu_n) * \tilde{\mu}_n - \mu_n * \tilde{\mu}_n\|_1 \leq \lim_n \|g \cdot \mu_n - \mu_n\|_1 = 0\,.$$

最后，G 在所有均值集合上的等价左作用由 $g \cdot m(f) = m(f \circ L_{g^{-1}})$ 给出，并且根据 m_n的定义，

$$|(g \cdot m_n - m_n)(f)| \leq \|f\|_\infty \sum_{h \in G} |(g \cdot \nu_n)(h) - \nu_n(h)| = \|f\|_\infty \|g \cdot \nu_n - \nu_n\|_1\,.$$

特别是，

$$\lim_n |(g \cdot m_n - m_n)(f)| = 0\,.$$

因此，任意弱-$*$ 聚点都是 $\ell^\infty(G)$ 上的左不变均值，从而证明了该断言。

我们用 m 表示任意收敛子列 (m_{n_k}) 的极限点。由于 m 是左不变均值

$$\lim_k m_{n_k}(\mathbf{1}_I) = m(\mathbf{1}_I) = 0\,.$$

因此，

$$0 = \lim_n m_n(\mathbf{1}_I) = \lim_n \nu_n(I),$$

正如我们所希望的那样。 ∎

本节的结论如下。

推论M。设 G 是一个可和无限群，设 $(F_n) \subseteq G$ 是 G 的一个对称 *Følner* 序列，设 $k\colon \mathbb{N} \to \mathbb{N}$ 是一个非递减函数，并设 A_k 是从 F_n 中均匀随机抽取的一个 k-子集。

(a) 假设对于某个常数 $\alpha \in [0,1]$，有 $k = \alpha|F_n| + o(|F_n|)$。那么，

$$\mathbb{E}[\eta_n(\mathsf{A}_k, \mathsf{A}_k)] \leq \alpha^4 + \alpha^3\,.$$

此外，如果 G 只包含有限多个对合，

$$\mathbb{E}[\eta_n(\mathsf{A}_k, \mathsf{A}_k)] = \alpha^4\,.$$

(b) 假设 G 是剩余有限且非几乎阿贝尔的。那么

$$\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k^{-1})] = 2k^2 - k.$$

(c) 假设 G 是几乎阿贝尔的。那么，对合概率与 *Følner*序列无关，并且，

$$\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k^{-1})] = (2 + \iota(G))k^2 - (1 - \iota(G))k.$$

证明。条目(a) 的证明可由定理J直接计算得出。另一方面，条目(c) 由定理30推出，而条目(b) 由定理31推出。 ∎

定理28 的证明中使用剩余有限性似乎只是技术上的处理，并无深层的数学理由。因此，与定理F类似，我们提出以下问题。

Qu问题 N。我们能否在定理28 和定理 M (b)中去掉剩余有限这一假设？ ?

5.4. **有限生成群**。我们再次将注意力转向赋有词度量和由球组成的滤过的有限生成群。首先要指出，我们已经改进了 [57, 第 2 节1]中的主要结果：定理 M 不仅适用于整数，而且适用于任意具有次指数增长的剩余有限群，只要其滤过由球给出（因为球构成 Følner 滤过）；并且 k 可以取为任意满足以下条件的递增函数： $k \ll \sqrt[4]{|\mathbf{B}_S(n)|}$。

我们实际上猜想，这个公式对每个有限生成群都成立。

猜想 O。设 G 是一个无限群， S 是 G的有限生成集。那么，

(i) $\iota_S(G)$ 为正，当且仅当 G 几乎阿贝尔。(ii) 对每个满足 $k \ll \sqrt[4]{|\mathbf{B}_S(n)|}$ 的函数 k: $\mathbb{N} \to \mathbb{N}$ ，以及在$\mathbf{B}_S(n)$中均匀随机抽取的 G 的每个 A_k, k-子集，我们有

$$\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k^{-1})] = 2k^2 - k\,.$$

在几何群论中出现的若干标准群类里，对合密度为零是相当常见的现象。例如，对于字双曲群（见 [19]）或形如 H 与 $\mathbb{Z}$ 的广义灯笼群（见 [20]），无论生成集如何，情况都是如此。我们证实了这些群的猜想第二部分。

此外，值得注意的是，凭借 [51], ，若不考虑词度量，而考虑随机游走所诱导的概率分布，那么在其他几个类别中，命中对合的概率会呈指数衰减。

第一个例子基本上是平凡的。

例 32. 假设 G 只有有限多个对合。令 A_k 为 G 的一个 k-子集，且从$\mathbf{B}_S(n)$ 中均匀随机抽取，其中任意生成集为 S。那么

$$\mathbb{E}[E_n(\mathsf{A}_k, \mathsf{A}_k^{-1}) = 2k^2 - k\,.$$

例 33 (字双曲群**).** 设 G 是具有有限生成集 S的非初等字双曲群。利用定理 26，我们将证明比值 $|Q_3^{(1)}|/|\mathbf{B}_S(n)|^2$ 当 n趋于无穷时收敛到零。我们指出如下恒等式:

$$\begin{aligned}
|Q_3^{(1)}| &= \sum_{x \in B_S(n)} |\mathbf{B}_S(n)x \cap I| \\
&= \sum_{y \in I \cap \mathbf{B}_S(2n)} \left|\{x \in \mathbf{B}_S(n) \mid yx^{-1} \in \mathbf{B}_S(n)\}\right| \\
&= \sum_{y \in I \cap \mathbf{B}_S(2n)} \left|\mathbf{B}_S(1,n) \cap \mathbf{B}_S(y,n)\right|,
\end{aligned}$$

其中 $\mathbf{B}(z,n)$ 表示 n 半径、以 z 为中心的球，它位于 G 的凯莱图中，该凯莱图相对于S而言。此外，令 $|y|_S$ 表示 y 相对于 S中生成元的字长。根据 [10,命题 III.H.14], ，在每个双曲群 G中，都存在一个常数 $C > 0$ 使得

$$\mathbf{B}_S(1,n) \cap \mathbf{B}_S(y,n) \subseteq \mathbf{B}_S\left(z,\ n - \frac{|y|_S}{2} + C\right),$$

对于1与 y之间一条测地线的中点 z 。因此，

$$|\mathbf{B}_S(n) \cap y\mathbf{B}_S(n)| \le |\mathbf{B}_S(n - \tfrac{|y|_S}{2} + C)|\,.$$

按对合 y的长度分组，我们有

$$|Q_3^{(1)}| \le \sum_{i=0}^{2n} |I \cap \mathbf{B}_S(i)| \cdot |\mathbf{B}_S(n - \tfrac{i}{2} + C)|\,.$$

由 [19, 定理 1.1],存在两个正常数 d 和 D，使得

$$|I \cap \mathbf{B}_S(i)| \le d|\mathbf{B}_S(\tfrac{i}{2} + D)|\,.$$

因此，

$$|Q_3^{(1)}| \le d\sum_{i=0}^{2n} |\mathbf{B}_S(\frac{i}{2} + D)| \cdot |\mathbf{B}_S(n - \tfrac{i}{2} + C)|.$$

最后， G 具有纯指数增长：更具体地说， [17, 定理7。2] 得出存在两个常数 λ， $c > 1$ 使得对每个整数 $n \geq 0$,

$$c^{-1}\lambda^n \leq \mathbf{B}_S(n) \leq c\lambda^n \,.$$

因此,

$$|\mathbf{B}_S(\tfrac{i}{2} + D)| \cdot |\mathbf{B}(n - \tfrac{i}{2} + C)| \leq c^2\lambda^{n+D+C} \,,$$

and，因此， $|Q_3^{(1)}| \leq Mn\lambda^n$，对于足够大的常数 $M \geq 0$。最后，由于 $|\mathbf{B}_S(n)| \geq c^{-1}\lambda^n$ 我们计算

$$\frac{|Q_3^{(1)}|}{|\mathbf{B}_S(n)|^2} \leq \frac{Mn\lambda^n}{c^{-2}\lambda^{2n}} = \Theta(n\lambda^{-n}) \,.$$

特别地，比值 $|Q_3^{(1)}|/|\mathbf{B}_S(n)|^2$ 当 n 趋于无穷大时收敛到零。由此足以像定理30中那样得出结论，从而证明定理O 在此情形下成立。

例 34 （广义灯笼群）。 设 $G = H \operatorname{wr} \mathbb{Z}$ 是一个广义灯笼群， $N = H^{\mathbb{Z}}$ 是其基子群。假设 G 关于 S 具有夹逼指数增长，即，存在某些常数 c， $C > 0$,

$$c\lambda^n \leq |\mathbf{B}_S(n)| \leq C\lambda^n \,,$$

其中

$$\lambda = \lim_n \sqrt[n]{|\mathbf{B}_S(n)|}$$

是关于 G 的指数增长率，相对于 S。例如，当 H是有限群且生成集 S 包含 $\mathbb{Z}$的循环生成元时，情况便是如此。（根据 [35]的增长级数即可看出。另请参阅 [11, 引理 3。7] 以获取一个初等证明。）由每个对合都包含在 N这一事实出发，我们试图推导出 $|Q_3^{(1)}|/|\mathbf{B}_S(n)|^2$ 当 n 趋于无穷大时收敛到零。

由 [20, 定理 B],

$$\lim_n \frac{|\mathbf{B}_S(n) \cap N|}{|\mathbf{B}_S(n)|} = 0 \,.$$

特别地，由其证明可知，衰减比为

$$\frac{|N \cap \mathbf{B}_S(n)|}{|\mathbf{B}_S(n)|} \in o\left(\frac{1}{\log(n)}\right)$$

ind与生成集无关。注意，对于每个 $g \in G$，都存在一个常数 $m > 0$ suc使得

$$\frac{|\mathbf{B}_S(n) \cap Ng|}{|\mathbf{B}_S(n)|} \leq \frac{|\mathbf{B}_S(n + |g|_S) \cap N|}{|\mathbf{B}_S(n + |g|_S)|} \frac{|\mathbf{B}_S(n + |g|_S)|}{|\mathbf{B}_S(n)|} \leq \frac{m\lambda^{|g|_S}}{\log(n + |g|_S)} \,.$$

(我们用记号 $|g|_S$ 表示相对于生成集 S的 g 的字长。）因此，由于 I 包含于基群 N中，我们计算得

$$\begin{aligned}
\lim_n \frac{|Q_3^{(1)}|}{|\mathbf{B}_S(n)|^2} &= \lim_n \frac{1}{|\mathbf{B}_S(n)|} \sum_{x \in \mathbf{B}_S(n)} \frac{|\mathbf{B}_S(n) \cap Ix|}{|\mathbf{B}_S(n)|} \\
&\leq \lim_n \frac{1}{|\mathbf{B}_S(n)|} \sum_{x \in \mathbf{B}_S(n)} \frac{|\mathbf{B}_S(n) \cap Nx|}{|\mathbf{B}_S(n)|} \\
&\leq \lim_n \frac{m}{\lambda^n} \sum_{i=0}^{n} \frac{\lambda^i}{\log(n+i)} \\
&= 0 \,.
\end{aligned}$$

再一次，这就完成了该情形下定理O 的证明。

6. 大增长子集

我们对迄今所得估计的一项应用，是结合概率方法运用定理 7，找出具有大增长的离散群子集。这一研究方向目前十分活跃，尤其是在有限单群领域，近期进展包括 [21, 36, 52]。对于可解局部紧群，相关问题已从遍历论和测度论视角进行研究，见 [3, 8]。类似问题也在连续情形中得到探讨：例如，近期的突破 [34, 40]为紧李群中的小子集建立了锐利的测度加倍结果。

首先，我们证明一个引理，本节的大多数证明都会用到它。

引理 35. 设 $h:\ \mathbb{N}\to\mathbb{N}$ 是一个无界函数。那么，存在一个收敛到 1 的序列 δ_n，以及一个正整数 $M(h)$，使得对于每个配备递增滤过列 (F_n) 的离散群 G，以及每个满足 $|F_n|\geq M(h)$ 的整数 n，都存在一个子集 $A_n\subseteq F_n$，使得

$$|A_n|\leq |F_n|^{\frac{1}{2}}h(|F_n|)\quad and\quad |A_n^{*2}|\geq \frac{|F_n|}{\delta_n}\,.$$

证明. 首先，注意我们可以假设 $h(n)\leq \sqrt[4]{n}$，因为若该引理对函数 $\hbar$ 成立，则对任何更大的函数，该结论也成立，且 δ_n 和 $M(h)$ 保持不变。

对某个 $\alpha>0$，我们定义序列

$$\delta_n=1+\frac{3+\alpha}{h(n)^2}\,,$$

以及函数

$$k(n)=h(n)\sqrt{n}\,.$$

我们固定一个任意的离散群 G 及其递增滤过列(F_n)，并考虑一个随机的 $k(|F_n|)$子集A_k，它属于 F_n。根据定理B，当 n趋于无穷时，

$$\frac{|F_n|}{k^4}\mathbb{E}\left[E(\mathsf{A}_k,\mathsf{A}_k)\right]\leq 1+\frac{3}{h^2}+o\left(|F_n|^{-1/2}\right)\,.$$

根据马尔可夫不等式，

$$\mathbb{P}\left[E(\mathsf{A}_k,\mathsf{A}_k)\geq\frac{\delta_n k^4}{|F_n|}\right]\leq\frac{|F_n|}{\delta_n k^4}\mathbb{E}\left[E(\mathsf{A}_k,\mathsf{A}_k)\right]\,.$$

取其补事件可得，

$$\mathbb{P}\left[E(\mathsf{A}_k,\mathsf{A}_k)\leq\frac{\delta_n k^4}{|F_n|}\right]\geq 1-\frac{|F_n|\,\mathbb{E}\left[E(\mathsf{A}_k,\mathsf{A}_k)\right]}{\delta_n k^4}\geq\frac{1+\frac{3}{h^2}+o\left(|F_n|^{-1/2}\right)}{1+\frac{3+\alpha}{h^2}}\,.$$

事实上，根据 δ_n的选取，存在一个正整数 N，使得若 $n\geq M$，则该事件具有正概率。特别地，存在一个 k子集 A_n，它属于 F_n，使得

$$E(A_n,A_n)\leq\frac{\delta_n k^4}{|F_n|}=\delta_n h^4|F_n|\,.$$

因此，定理7 蕴含

$$|A_n^{*2}|\geq\frac{|A_n|^4}{E(A_n,A_n)}\geq\frac{h^4|F_n|^2}{\delta_n h^4|F_n|}=\frac{|F_n|}{\delta_n}\,,$$

如所期望 ∎

注记 36. 注意到，同一证明可逐字适用，只要我们将第二个副本 A_k 替换为 A_k^{-1}，并加入如下附加假设：F_n 是对称的。事实上，第 6 节的全部结果都可以针对对 $(\mathsf{A}_k,\mathsf{A}_k^{-1})$重新证明。为简洁起见，并鉴于我们在审美上更倾向于处理对 $(\mathsf{A}_k,\mathsf{A}_k)$，我们略去细节。

6.1. **有限群。** 所谓加法基，是指群 G 的一个子集 $A \subseteq G$，其性质为 $G = A^{*2}$。已知每个有限群 G 都具有一个加法基 A，使得 $|A| = O(|G|^{1/2})$，参见 [37]。然而，该证明依赖于有限单群分类。此外，这一概念既在数学 [1, 4, 48] 之内得到应用，也在其外的计算机科学 [16, 24, 38] 中得到应用。

定理 P 大致表明，渐近而言，存在一个基数略大于 $O(|G|^{1/2})$ 的集合，它几乎是一个加法基。我们的证明的新颖之处在于，它不依赖于有限单群分类。

定理 P。 对于每个 $\epsilon > 0$，以及每个无界函数 $h\colon \mathbb{N} \to \mathbb{N}$，存在一个正整数 $N = N(h, \epsilon)$，使得每个满足 $|G| \geq N$ 的有限群 G 都包含一个子集 A，使得

$$|A| \leq |G|^{\frac{1}{2}} h(|G|), \quad \textit{and} \quad |A^{*2}| \geq (1-\epsilon)|G|\,.$$

证明。令 δ_n 和 $M(h)$ 分别为定理 35 中所述的序列和整数。由于 G 是一个有限群，我们可以取滤过级数 (F_n)，其中 $F_i = G$ 对所有 i均成立。若 $|G| > M(h)$，根据定理 35，存在一个子集 A，使得

$$|A| = |G|^{\frac{1}{2}} h(|G|), \quad \text{and} \quad |A^{*2}| \geq \frac{|G|}{\delta_n}\,.$$

由于 δ_n 收敛于 1，存在一个整数 $N(h,\epsilon) \geq M(h)$，使得对于每个 $n \geq N(h,\epsilon)$，都有 $(1-\epsilon) \leq 1/\delta_n$。证明完毕。 ■

我们可以利用这一结果，在有限步内生成整个群，前提是 G 的代数结构不会使集合 A 陷入某个真子群。例如，设 G 是一个阶为 p^e 的 p-群，且 M 是 G 的一个阶为 p^{e-1} 的极大子群。G 的一个 k-随机子集 A_k 以正概率包含于 M，即

$$\mathbb{P}[\mathsf{A}_k \subseteq M] = \frac{\binom{p^{e-1}}{k}}{\binom{p^e}{k}} = \frac{1}{p^k} + o(1)\,,$$

其中，最后一个渐近关系是在 e 趋于无穷时成立的。因此，当 $A \subseteq M$、A^{*2} 时，它们无法生成整个群。为排除这类障碍，我们对 G 施加一个较弱的表示论条件。具体而言，我们假设 G 是 ϵ-拟随机的，也就是说，G 的每个非平凡线性表示的维数都至少为 $|G|^{\epsilon}$。（这一概念由 [27] 引入。拟随机群的代数分类已在 [5] 中给出。）

推论 Q. 对于每个 $\epsilon > 0$，以及每个满足 $1 \ll h(n)$ 的函数 $h\colon \mathbb{N} \to \mathbb{N}$，都存在一个正整数 $N = N(h,\epsilon)$，使得每个满足 $|G| \geq N$ 的 ϵ-拟随机群 G 都包含一个子集 A，满足

$$|A| \leq |G|^{\frac{1}{2}} h(|G|), \quad \textit{and} \quad A^{*6} = G\,.$$

证明。通过令 N 最终递增，可观察到

$$(1-\epsilon)|G| \geq |G|^{\frac{3-\epsilon}{3}}\,.$$

We 现在可以对所有涉及的集合均取为 A^{*2}，应用 Gowers 技巧（见 [47, 推论 1]）。 ■

6.2. **无限群。** 我们先在无限循环群 $\mathbb{Z}$ 中给出一个明确的例子：一个零测集经过一次乘积运算后便会显著增长。这是加法数论中一个著名现象的简单实例，称为稀疏基。它们是自然数的子集 A，密度为零，但其 k 重和集仍包含所有足够大的整数，因此密度为 1。（经典参考文献见 [13, 53]。）

例 37。 令 A 为平方数集合，即

$$A = \{\pm m^2 \mid m \in \mathbb{Z}\} \subseteq \mathbb{Z}\,.$$

对每个正整数 n，定义 $A_n = A \cap [-n, n]$。一方面，$[-n, n]$ 中平方数的个数为 $|A_n| = 2\lfloor \sqrt{n} \rfloor + 1$，因此，

$$\mu(A) = \lim_n \frac{|A_n|}{2n+1} = 0\,.$$

另一方面，整数 m 是平方差，当且仅当 $m \not\equiv 2$ (模 4)。因此，

$$\mu(A+A) = \lim_n \frac{|A_n + A_n|}{2n+1} = \frac{3}{4}.$$

因此，尽管 A 是一个零测集，但其和集具有正测度。

我们相信，这种现象实际上是可 amenable 群的一个普遍特征。

问题R。设 G 是一个可 amenable 群。是否存在一个子集 $A \subseteq G$，使得 $\mu(A) = 0$且 $\mu(A^{*2}) > 0$?

在本小节中，对于带有指定测度的有限群的有向极限，我们肯定地回答了这个问题。这一现象凸显了可 amenable 群中群乘法下测度的次可加性失效。

首先，我们注意到，Følner序列的任意子列 (F_n) 仍然是一个Følner序列。为了使用非主超滤子 ω 在 $\mathbb{N}$上的作用，根据式 (B)，从 $F_n)$ 定义有限可加测度 μ，我们可以取一个子列，而不改变 μ的值，前提是相应地调整超滤子。

具体而言，令 $f\colon \mathbb{N} \to \mathbb{N}$ 为与子列（$F_{f(n)}$）对应的递增函数。考虑定义在 $\mathbb{N}$ 上的非主超滤子 $f^{-1}(\omega)$，其定义如下

$$f^{-1}(\omega) = \{S \subseteq \mathbb{N} \mid f(S) \in \omega\}.$$

那么，对于每个 $A \subseteq G$，我们都有

$$\mu(A) = \lim_{\omega} \frac{|A \cap F_n|}{|F_n|} = \lim_{f^{-1}(\omega)} \frac{|A \cap F_{f(n)}|}{|F_{f(n)}|}.$$

因此，在下文中，我们将自由地取 Følner序列的子列，并默认为超滤子替换为相应的拉回，从而使所得测度 μ 保持不变。

特别地，当 G 是一个带有 Følner序列（F_n）的无限顺从群时，我们可以假设该序列

$$\alpha_n = \frac{|F_{n-1}|}{|F_n|}$$

有理数收敛于零，并且 $\alpha_n < 1$ 对每个 n都成立。此外，我们可以利用这一点得到衰减比任意快的 Følner 序列。对于任意递减的实数序列 β_i，由于序列 $|F_n|$ 无界（见 [14, 练习 4。52]），存在一个递增的整数序列 (n_i) 使得

$$|F_{n_i}| \geq \frac{|F_{n_{i-1}}|}{\beta_i}.$$

因此，子列（F_{n_i}）的衰减比为 $O(\beta_i)$。

我们需要以下技术引理，以得到所有子集均两两不交的 Følner 序列。

引理 38. 设 G为无限顺从群，且 $(G_n)_{n\in\mathbb{N}}$ 是嵌套 *Følner* 序列。存在 G的 *Følner*序列 $(F_n)_{n\in\mathbb{N}}$，使得该序列中的集合两两不交。

证明. 如证明之前所说明的，通过取一个子列，我们可以假设该序列

$$\alpha_n = \frac{|G_{n-1}|}{|G_n|}$$

收敛于零，并且 $\alpha_n < 1$ 对每个 n 都成立。设 (F_n) 为如下定义的有限集序列：

$$F_n = G_n \setminus G_{n-1}.$$

注意，这些集合按构造两两不交。我们旨在证明 (F_n) 实际上是 Følner 的。事实上，对每个 $g \in G$，我们计算得:

$$\begin{aligned}\frac{|F_n g \triangle F_n|}{|F_n|} &= \frac{|(G_n \setminus G_{n-1})g \triangle (G_n \setminus G_{n-1})|}{|G_n \setminus G_{n-1}|} \\ &\leq \frac{|G_n \triangle G_n g| + 2|G_{n-1}|}{(1-\alpha_n)|G_n|} \\ &= \frac{|G_n \triangle G_n g|}{(1-\alpha_n)|G_n|} + \frac{2\alpha_n}{1-\alpha_n}\,.\end{aligned}$$

The 最后一项趋于零，因为 (G_n) 是 Følner序列，且 α_n 趋于零。 ∎

回想一下，有限群的无限直极限

$$G = \varinjlim G_n$$

恰好是可数无限局部有限群。此外，它们是可 amenable 的，因为 (G_n) 构成一个由有限子群组成的嵌套 Følner 序列。在下一个定理中，我们考虑与此 Følner序列对应的左不变测度 μ 。

定理 S. 设 G 是一个可数无限局部有限群。那么，存在一个子集 $A \subseteq G$，使得

$$\mu(A) = 0, \quad \textit{and} \quad \mu(A^{*2}) = 1\,.$$

证明。 设 (G_n) 是由 G 的子群构成的 Følner序列，定义 μ ，并取一个非主超滤子 ω ，属于 $\mathbb{N}$。再设 (F_n) 是由 G_n 按定理 38中所述方式得到的 Følner序列。不失一般性，如定理 38陈述之前所述，我们假设

$$\beta_n = |F_{n-1}|/|F_n| \ll 1/n$$

并且，对于所有正整数 n, $\beta_n < 1$。最后，设 $1 \ll h < \sqrt[4]{n}$ 为一个函数。

根据定理35，存在一个收敛于 δ_n 的数列1 以及一个正整数 M 使得，若 $|F_n| \geq M$，则存在一个子集 $A_n \subseteq F_n$ 满足

$$|A_n| \leq |F_n|^{\frac{1}{2}} h(|F_n|) \quad \text{and} \quad |A_n^{*2}| \geq \frac{|F_n|}{\delta_n}\,.$$

我们定义

$$A = \bigcup_{n=M}^{\infty} A_n\,.$$

另一方面,

$$\begin{aligned}\mu(A) &= \lim_{\omega} \frac{|A \cap G_n|}{|G_n|} \\ &= \lim_{\omega} \frac{\left|A \cap \left(\bigcup_{j=0}^{n} F_j\right)\right|}{\left|\bigcup_{j=0}^{n} F_j\right|} \\ &\leq \lim_{\omega} \frac{\sum_{j=M}^{n} |A_j|}{\sum_{j=0}^{n} |F_j|} \\ &\leq \lim_{\omega} \frac{\sum_{j=M}^{n} |F_j|^{\frac{1}{2}} h(|F_j|))}{\sum_{j=0}^{n} |F_j|} \\ &= 0\,.\end{aligned}$$

另一方面，由于每个 G_n 都是一个子群，$G_n = G_n^{*2}$。因此，对于每个 $j \leq n$,

$$F_j^{*2} \subseteq G_j^{*2} = G_j \subseteq G_n\,.$$

因此，我们计算

$$\begin{aligned}\mu(A^{*2}) &= \lim_{\omega} \frac{\left|A^{*2} \cap G_n\right|}{|G_n|} \\ &\geq \lim_{\omega} \frac{\left|A^{*2} \cap \left(\bigcup_{j=0}^{n} F_j^{*2}\right)\right|}{\left|\bigcup_{j=0}^{n} F_j\right|} \\ &\geq \lim_{\omega} \frac{|A_n^{*2}|}{\sum_{j=0}^{n} |F_j|} \\ &\geq \lim_{\omega} \frac{\delta_n^{-1}|F_n|}{|F_n|(1+n\beta_n)} \\ &= \lim_{\omega} \frac{1}{\delta_n(1+n\beta_n)} \\ &= 1\,.\end{aligned}$$

因此， A 具有所需的性质。 ∎

请注意，由前一个定理给出的集合 A 的连续乘积不可能一直被限制在某个真子群中；该真子群的测度至多为 $1/2$，因此 A 必须生成 G。接下来很自然会问，相对于子集 A， G 的宽度 是多少。

Qu问题 T. 要确保 $A^{*(2+k)} = G$，还需要多少额外步骤 k？（该值 e
of k 也完全可能是无限的。）

7. 和集或差集支配

设 A 是整数 $\mathbb{Z}$ 的一个子集。若 A 满足 $|A+A| > |A-A|$，则称其为和集占优；若满足 $|A+A| < |A-A|$，则称其为差集占优；若满足 $|A+A| = |A-A|$，则称其为平衡。例如， [50] 中给出了这些情况的示例。由于加法满足交换律而减法不满足，人们或许会认为绝大多数集合都是差集占优的。但事实并非如此：若我们通过以概率 $1/2$ 选取每个整数，从而从{1，2，.....，n} 中抽样得到子集 A，那么 A 以正概率为和集占优（见 [42, 59]）。证明中所涉及的分析依赖于这样一个事实：在区间的主体部分，和集与差集的表现大致相同，真正起决定作用的是 A 的边缘部分中元素的分布。因此，人们或许会认为，若将抽样范围改为有限群 G，平衡子集出现的频率会更高，因为区间边缘部分的概念在此不再适用。事实上， [44] 证明了平衡子集以高概率出现。

本节中，我们利用能量估计和定理7，探讨一个类似的问题——允许比值为一个固定常数。此外，请注意，我们的概率空间与上述研究中使用的概率空间大不相同。（我们还指出，近期一些 [15, 30] 比较差占优与和占优的研究，通过改变抽样策略，为每个点使用不同的伯努利随机变量来分析这一情形。）事实上，在我们的情形中，我们考虑的是一个真正稀疏的情形，其中 $k \ll \sqrt{|F_n|}$，而在先前的模型中，A_k 的期望基数与 $|F_n|$成线性关系。

定理 U。令 G 为一个无限离散群，令(F_n) 为G的一个对称滤子序列，令 $k\colon\ \mathbb{N} \to \mathbb{N}$ 为一个满足 $k \ll \sqrt{|F_n|}$的无界函数，并令 δ、 $\epsilon \in (0,\ 1/3)$、 $c \in (0,\ 1)$ 为三个常数。那么，存在一个整数 $N = N(k$、δ、 $c)$，使得对每个整数 $n \geq N$，

$$\mathbb{P}\left[\frac{|\mathsf{A}_k\mathsf{A}_k^{-1}|}{|\mathsf{A}_k^{*2}|} \leq \left(\frac{1}{3}-\delta\right)^{-1}\right] > c\delta\,,$$

and

$$\mathbb{P}\left[\frac{|\mathsf{A}_k^{*2}|}{|\mathsf{A}_k\mathsf{A}_k^{-1}|} \leq \left(\frac{1}{3}-\epsilon\right)^{-1}\right] > c\epsilon\,.$$

证明。 回顾一下，应用定理7并结合詹森不等式，我们得到

$$\mathbb{E}[|\mathsf{A}_k^{*2}|] \geq \frac{k^4}{\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k)]}, \quad \text{and} \quad \mathbb{E}[|\mathsf{A}_k\mathsf{A}_k^{-1}|] \geq \frac{k^4}{\mathbb{E}[E(\mathsf{A}_k, \mathsf{A}_k^{-1})]}\,.$$

鉴于定理 B 和 J，

$$\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)] \le 3k^2\,(1+o(1))\,, \quad \text{and} \quad \mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k^{-1})] \le 3k^2\,(1+o(1))\,. \tag{7.1}$$

由此可得

$$\mathbb{E}[|\mathsf{A}_k^{*2}|] \ge \frac{k^2}{3+o(1)}, \quad \text{and} \quad \mathbb{E}[|\mathsf{A}_k\mathsf{A}_k^{-1}|] \ge \frac{k^2}{3+o(1)}\,. \tag{7.2}$$

考虑这两个互补事件

$$X_\delta = \left\{|\mathsf{A}_k^{*2}| \ge \left(\frac{1}{3}-\delta\right)|\mathsf{A}_k\mathsf{A}_k^{-1}|\right\}, \quad \text{and} \quad Y_\delta = \left\{|\mathsf{A}_k^{*2}| < \left(\frac{1}{3}-\delta\right)|\mathsf{A}_k\mathsf{A}_k^{-1}|\right\}.$$

由于随机变量 $|\mathsf{A}_k^{*2}|$ 与 $|\mathsf{A}_k\mathsf{A}_k^{-1}|$ 均在区间 $[k,k^2]$内取值，我们有 e

$$\mathbb{E}\left[\left(|\mathsf{A}_k^{*2}| - \left(\frac{1}{3}-\delta\right)|\mathsf{A}_k\mathsf{A}_k^{-1}|\right)\mathbf{1}_{X_\delta}\right] \le \left(k^2 - \left(\frac{1}{3}-\delta\right)k\right)\mathbb{P}[X_\delta]\,,$$

$$\mathbb{E}\left[\left(|\mathsf{A}_k^{*2}| - \left(\frac{1}{3}-\delta\right)|\mathsf{A}_k\mathsf{A}_k^{-1}|\right)\mathbf{1}_{Y_\delta}\right] \le 0\,.$$

因此，

$$\mathbb{E}\left[|\mathsf{A}_k^{*2}| - \left(\frac{1}{3}-\delta\right)|\mathsf{A}_k\mathsf{A}_k^{-1}|\right] \le \left(k^2 - \left(\frac{1}{3}-\delta\right)k\right)\mathbb{P}[X_\delta]\,.$$

将此与方程（7.2）相结合，我们得到

$$\begin{aligned}\mathbb{P}[X_\delta] &\ge \frac{\mathbb{E}[|\mathsf{A}_k^{*2}|] - \left(\frac{1}{3}-\delta\right)\mathbb{E}[|\mathsf{A}_k\mathsf{A}_k^{-1}|]}{k^2 - \left(\frac{1}{3}-\delta\right)k} \\ &\ge \frac{k^2\left(\frac{1}{3+o(1)} - \frac{1}{3} + \delta\right)}{k^2(1-o(1))}\,.\end{aligned}$$

第一个陈述的证明至此完成。

为证明第二个陈述，我们对互补事件重复相同的推理

$$X_\epsilon = \left\{|\mathsf{A}_k\mathsf{A}_k^{-1}| \ge \left(\frac{1}{3}-\epsilon\right)|\mathsf{A}_k^{*2}|\right\}, \quad \text{and} \quad Y_\epsilon = \left\{|\mathsf{A}_k\mathsf{A}_k^{-1}| < \left(\frac{1}{3}-\epsilon\right)|\mathsf{A}_k^{*2}|\right\}. \qquad \blacksquare$$

定理 U 的证明很容易调整：只需了解群的额外信息，而不必使用定理B 和 J，而是针对相应的无限情形援引其中一个推论。

此外，对于有限群序列，也可以给出类似的结果。

定理 V. 设 (G_n) 是一个有限群序列，并定义

$$\varepsilon = \limsup_n \frac{\varepsilon(G_n)}{|G_n|}, \quad \kappa = \limsup_n \frac{\kappa(G_n)}{|G_n|}, \quad \iota = \limsup_n \frac{\iota(G_n)}{|G_n|}\,.$$

设 k 为正整数，并设 $\delta \in (0,(1+\varepsilon+\kappa)^{-1})$、$\epsilon \in (0,(2+\iota)^{-1})$、$c \in (0,1)$ 为三个常数。那么，存在整数 $N = N(k,\delta,\epsilon,c)$ 使得，对于每个整数 $n \ge N$，

$$\mathbb{P}\left[\frac{|\mathsf{A}_k\mathsf{A}_k^{-1}|}{|\mathsf{A}_k^{*2}|} \le \left(\frac{1}{1+\varepsilon+\kappa}-\delta\right)^{-1}\right] > c\delta\,,$$

and

$$\mathbb{P}\left[\frac{|\mathsf{A}_k^{*2}|}{|\mathsf{A}_k\mathsf{A}_k^{-1}|} \le \left(\frac{1}{2+\iota}-\epsilon\right)^{-1}\right] > c\epsilon\,.$$

证明。 利用推论 C和 K，我们可以将方程（7.1）特化为

$$\mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k)] \le (1+\varepsilon+\kappa)k^2\,(1+o(1))\,, \quad \text{and} \quad \mathbb{E}[E(\mathsf{A}_k,\mathsf{A}_k^{-1})] \le (2+\iota)k^2\,(1+o(1))\,.$$

证明的其余部分与定理 U的证明相同。 $\blacksquare$

例如，若 (G_n)被选为一列非阿贝尔单群，则定理 V 的陈述的第一部分变为：对每个 δ，$c \in (0,1)$，

$$\mathbb{P}\left[\frac{|\mathsf{A}_k\mathsf{A}_k^{-1}|}{|\mathsf{A}_k^{*2}|} \le (1-\delta)^{-1}\right] > c\delta\,.$$

另一方面，我们认为定理U 和 V 中得到的下界远非最优。事实上，我们的论证完全依赖于相关随机变量期望值的下界，而这类下界本质上无法反映涨落或边缘现象。因此，尽管我们可以证明， $|A_k^{*2}|$ 和 $|A_kA_k^{-1}|$ 通常都不会比另一个大出超过一个常数因子，但我们的方法无法处理常数任意接近 1。

问题 W. 关于随机变量$E(A_k, A_k)$ 和 $E(A_k,A_k^{-1})$的 $h \geq 2$ 阶矩，可以得出什么结论？尤其是，我们能否根据这些信息，对 $|A_kA_k^{-1}|$和 $|A_k^{*2}|$的矩进行估计？

参考文献

[1] N. Alon、B. Bukh 和 B. Sudakov。离散 Kakeya 型问题与小基。Israel J. Math., 174:285–301, 2007.[2] Y. Antolín、A. Martino 和 E. Ventura。无限群的交换度。Proc. Am. Math. Soc., 145(2):479–485, 2017. [3] T. Austin。有界且可积的轨道等价下熵的行为。Geom. Funct. Anal., 26(6):1483–1525, 2016. [4] M. Barbieri、M. Lekše、P. Potočnik 和 K. Rekvényi。将子集与其像分离。预印本，arXiv:2508.20731，2025。[5] M. Barbieri 和 L. Sabatini。拟随机群与拟单群。Discrete Anal., 24: Paper no. 21, 2025。[6] V. Beck 和 C. Lecouvey。群作用与表示的加性组合问题中的次模函数。North-West. Eur. J. Math., 11:75–101, 2025.[7] Y. G. Berkovich、G.A. Freiman 和 C. E. Praeger。有限群的小平方与小立方性质。Bulletin of the Australian Mathematical Society, 44(3):429–450, 1991. [8] M. Björklund 和 A. Fish。可 amenable 群的遍历作用的近似不变性。Discrete Anal., 6, 2019.[9] L. V. Brailovsky 和 G. A. Freiman。群中的二元子集。载于《第四届集体现象国际会议》（莫斯科，1981），Ann. New York Acad. Sci. 第373卷，第183–190页。New York Acad. Sci., New York, 1981.[10] M. R. Bridson 和 A. Haefliger。《非正曲率度量空间》，Grundlehren der mathematischen Wissenschaften 第319卷。Springer-Verlag, Berlin, 1999.[11] J. Brieussel 和 A. Gournay。凯莱图中球面的连通性。Algebra Discrete Math., 26 246, 2018 2 190( ): – .[12] T. Browning。有限群交换概率的极限点。Bull. Lond. Math. Soc., 55 1403, 2023 3 1392( ): – .[13] J. W S. Cassels。关于自然数列的基。Abh. Math. Semin. Univ. Hamb., 21:247–257, 1957. [14] T. Ceccherini-Silberstein 和 M. Coornaert。《元胞自动机与群》。Springer Monogr. Math. Cham: Springer, 第2版，2023. [15] H. V. Chu、D King、N. Luntzlara、T. C. Martinez、S. J. Miller、L. Shao、C. Sun 和 V. Xu。推广和集缺失和的分布。J. Number Theory, 239:402–444, 2022. [16] P. Clote 和 E. Kranakis。布尔函数、不变群与并行复杂性。载于《会议论文集：复杂性理论中的结构，第四届年度会议》，第55–66页，Los Alamitos, CA, USA, 1989。IEEE Computer Society.[17] M. Coornaert。Gromov 意义下双曲空间边界上的 Patterson–Sullivan 测度。Pacific J. Math., 159(2):241–270, 1993. [18] C. G. Cox。交换度与灯笼群。Int. J. Algebra Comput., 28 1173, 2018 7 1163( ): – .[19] P. Dani。双曲群中无限阶元素的普遍性。预印本。[20] I. de las Heras、B. Klopsch 和 A. Zozaya。以无限循环顶群为底群的缠绕积的交换度。Eur. J. Math., 10(2):Paper no 25, 2024. [21] D. Dona、A. Maróti 和 L. Pyber。有限单群中子集乘积的增长。Bull. Lond. Math. Soc., 56(8):2704–2710, 2024. [22] G. Duchamp 和 J. Y. Thibon。自由部分交换群的简单序。Int. J. Algebra Comput., 2(3):351–355, 1992. [23] S. Eberhard。有限群的交换概率。Bull. Lond. Math. Soc., 47(5):796–808, 2015. [24] S. Evra、S. Gadot、O. Klein 和 I. Komargodski。在线性时间内验证群。载于《2024 IEEE 第65届计算机科学基础年会（FOCS）》，第2131–2147页，2024. [25] G. Freiman、M. Herzog、P. Longobardi、M. Maj、A. Plagne 和 Y. V. Stanchescu。有序群中的小倍增：生成元与结构。Groups Geom. Dyn., 11(2):585–612, 2017. [26] G. A. Freiman。群中的二元与三元子集。Aequationes Math., 22(2-3):140–152, 1981. [27] W. T. Gowers。拟随机群。Comb. Probab. Comput., 17(3):363–387, 2008. [28] R. M. Guralnick 和 G. R. Robinson。关于有限群中的交换概率。J. Algebra, 300 528, 2006 509: – .[29] W. H. Gustafson。两个群元素可交换的概率是多少？Am. Math. Mon., 80(9):1031– 1034, 1973.

[30] A. Hemmady、A. Lott 和 S. J. Miller。几乎所有集合在 $\mathbb{Z}/n\mathbb{Z}$中都是差集占优的。Integers, 17:paper a54, 15, 2017.[31] M. Herzog、P. Longobardi 和 M. Maj。群论中的一个组合问题。Israel J. Math., 82:329–340, 1993.[32] K. H. Hofmann 和 F. G. Russo。在紧群中， x 与 y 可交换的概率。Math. Proc. Camb. Philos. Soc., 153(3):557–571, 2012. [33] I. M. Isaacs。《有限群特征标理论》， Pure Appl. Math. 第69卷。Academic Press, New York, NY, 1976. [34] Y. Jing、C.-M. Tran 和 R. Zhang。SO(3)中小集合的测度加倍。预印本， arXiv: 2304.09619，2023.[35] D. L. Johnson。缠绕积的有理增长。载于《巴斯圣安德鲁斯群论会议1989：第2卷》，London Mathematical Society Lecture Note Series 第160卷，第309–315页。Cambridge University Press, Cambridge, 1991.[36] P. Keevash 和 N. Lifshitz。对称群的尖锐超收缩性及其应用。预印本，arXiv.2307.15030，2023.[37] G. Kozma 和 A. Lev。有限群的基与分解数。Arch. Math. (Basel), 58 424, 1992 5 417( ): – .[38] D. Kleitman、L. Finkelstein 和 T. Leighton。应用有限单群分类定理，以尽量减少均匀置换架构中的引脚数量。载于《VLSI算法与架构》，第三届爱琴海计算机研讨会论文集（希腊科孚岛，1988），Lecture Notes Comput. Sci. 第319卷，第247–256页。Springer, New York, 1988. [39] L. Lévai 和 L. Pyber。具有许多可交换对或对合的拟有限群。Arch. Math., 75 7, 2000 1 1( ): – .[40] S. Machado。紧李群中小子集的最小倍增。预印本， arXiv:2401.14062，2024. [41] A. Mann。含有许多对合的有限群。Proc. Am. Math. Soc., 122(2):383–385, 1994. [42] G. Martin 和 K. O'Bryant。许多集合的和比差多。载于《加性组合学》，第287–305页。Providence, RI: American Mathematical Society (AMS), 2007. [43] J. Martínez。有限群中 π 297 6 2287 2301, -元2024素的交换概率。Math. Nachr., ( ): – .[44] S. J. Miller 和 K. Vissuet。有限群中大多数子集都是平衡的。载于《组合与加法数论：根据2011年和2012年在纽约举行的CANT会议报告选编》，第147–157页。New York, NY: Springer, 2014. [45] B. Murphy。群作用组合学。预印本， arXiv:1907.13569，2019。[46] P. M. Neumann。群论中的两个组合问题。Bull. Lond. Math. Soc., 21(5):456–458, 1989. [47] N. Nikolov 和 L. Pyber。拟随机群的乘积分解与约当型定理。J. Eur. Math. Soc. (JEMS), 13(4):1063–1077, 2011. [48] L. Rédei 和 A. A. Rényi。关于用差表示数字1、2、.....、 N。Mat. Sb., N. Ser., 24/66:385–389, 1949. [49] D. J. Rusin。有限群中两个元素可交换的概率是多少？Pacific J. Math., 82(1):237–247, 1979. [50] I. Z. Ruzsa。和与差的数量。Acta Math. Hung., 59(3-4):439–447, 1992. [51] A. Sisto。收缩元素与随机游走。J. Reine Angew. Math., 742:79–114, 2018. [52] S. V. Skresanov。李型有限单群中的扩张子与正规子集增长。Bull. Lond. Math. Soc., 57(11):3429–3440, 2025. [53] A. Stöhr。一个 h阶的基，它构成所有自然数的集合。Math. Z., 42:739–743, 1937. [54] T. Tao。非交换群的积集估计。Combinatorica, 28(5):547–594, 2008. [55] T. Tao 和 V. H. Vu。《加性组合学》，Cambridge Studies in Advanced Mathematics 第105卷。Cambridge University Press, 2006. [56] M. C. H. Tointon。无限群的交换概率。J. Lond. Math. Soc., II. Ser., 101 1297, 2020 11 1280( ): – .[57] M. C. H. Tointon。《近似群导论》，London Mathematical Society Student Texts 第94卷。Cambridge University Press, Cambridge, 2020.[58] M. Valiunas。图乘积的有理增长与交换度。J. Algebra, 522:309–331, 2019. [59] Y. Zhao。由缺失的和与差刻画的集合。J. Number Theory, 131(11):2107–2134, 2011.

数学与物理学院 ，卢布尔雅那大学 ，亚德兰斯卡街 21 号 ，1000 卢布尔雅那，斯洛文尼亚。

电子邮件地址： marco.barbieri@fmf.uni-lj.si

数学、物理与力学研究所，亚德兰斯卡街19号，邮编1000，卢布尔雅那，斯洛文尼亚。另兼任：卢布尔雅那大学数学与物理学院，亚德兰斯卡街21号，邮编1000，卢布尔雅那，斯洛文尼亚。

电子邮件地址： marusa.lekse@imfm.si

统计、计算机科学与数学系，纳瓦拉公立大学，阿罗萨迪亚校区，31006 潘普洛纳，西班牙。另兼任：INAMAT ^{2}, 阿罗萨迪亚校区，31006 潘普洛纳，西班牙E

$mail\ add$址： andoni.zozaya@unavarra.es