arXiv:2512.18302v1 [math.GR] 20 Dec 2025

有限群元素采样：使用累加器的乘积替换算法的效率。

MICHAŁ MARCINKOWSKI 和 PIOTR MIZERKA

摘要。设 G 是由 k 个元素生成的有限群。广为人知的乘积替换算法为采样 G 的生成集提供了一种有效方法。我们研究了该算法的一种改进形式，旨在输出 G 的单个元素。我们证明，经过 $O(k^2 \log |G|)$ 步后，输出的分布在 G 上接近均匀分布，这改进了迄今为止已知的最佳结果。证明通过谱隙估计展开，并使用了计算机辅助计算。

1. 引言

设 G 是一个有限群。我们关注一种高效算法，该算法能够从G 中以近似均匀分布进行采样。这类算法在计算群论中发挥着核心作用，因为许多其他算法都需要访问随机群元素 [5, 21]。人们经常需要处理规模大得惊人的有限群，例如，魔方群的阶约为 10^{19}。因此，无法简单地列出所有群元素并随机选择一个，因为生成这样的列表将需要难以承受的时间和内存。所以，我们需要有关 G 的额外信息，以便用于采样过程。假设我们同时给定 G 和一个生成元组 S （在此语境下，使用元组而非生成集更为方便），并不是一个苛刻的假设。随后，我们可以以各种方式将生成元相乘，从而生成 G作为输出。

为此，我们需要假设存在一种高效的方法，能够对 G 中的元素进行求逆和相乘，并且能够在计算机上高效表示这些运算的结果。这类群称为“黑箱群”，因为在描述对其进行操作的具体算法时，我们不会关注这些运算的实现细节。置换群的子群以及有限环上的矩阵群，是黑箱群中最重要的例子。

从 G 中采样一个元素的最简单方法，是根据其生成元组 S，从单位元出发，在 $(G, S \cup S^{-1})$ 的凯莱图上进行惰性随机游走。根据标准理论，该随机游走的分布会收敛到均匀分布。然而，即使对于 $\mathbb{Z}_n$ 这样非常简单的群，要使分布接近均匀分布所需的步数也可能多到难以计算，尤其是在 n 很大的情况下。

存在一些算法，其效率远高于在凯莱图上的随机游走。设计此类采样器最重要的技术之一基于乘积替换算法。该算法最初于 [4] 提出，同样基于随机游走，但这次游走的不是凯莱图，而是所有生成k元组构成的图，其中 $k = |S|$。因此，该算法首先输出一个生成元组，然后

可以取该元组的第一个元素作为 G的输出元素。据报道，这种技术在实践中效果良好，并且通过了统计检验。然而，一般而言，这个随机元素的分布并不收敛于均匀分布，参见 [2] 或定理2.2。有关乘积替换算法及相关问题的综述，参见[25]。

为克服这一困难，人们提出了乘积替换算法的若干变体 [14]。特别是，在“rattle”版本中，极限分布显然是均匀分布，但其收敛速率仍然未知。

人们发现，原始乘积替换算法（该算法对生成 k-元组进行采样）的行为与特殊自同构群 SAut(F_k) [17] 的 Kazhdan 性质（T）有关。SAut(F_k) 是否具有性质 (T) 曾是一个长期悬而未决的问题；在突破性论文 [9, 11] 中，该问题针对 $k > 4$ 得到了肯定回答，而在 [22] 中，SAut(F_4) 尚未解决的情形也得以解决。更重要的是，这些工作为相应的谱隙给出了非常好的估计。由这些估计可以立即推出，原始乘积替换算法的混合速率为 $O(k^2 \log |G|)$ 阶。这意味着，经过 $O(k^2 \log |G|)$ 步后，该算法输出的生成元组服从一个接近均匀分布的分布。

长期以来，人们一直未能为从 G 中抽取元素的乘积替换算法找到良好的估计。在 [13], 中，研究“rattle”版本向获得此类估计迈出了重要一步。然而，该研究假设 k 的阶为$\log |G|$，而当 G 较大时，这一规模可能大得难以承受。

本文关注乘积替换算法的一个变体。该变体是对“rattle”的轻微修改，并且从群作用的角度来看更易于分析。我们称之为乘积替换累加器算法。它基于生成元组空间上的随机游走，并在此空间中额外加入一个元素——累加器。随机游走进行 t步后，返回累加器。我们的主要定理如下。

定理 (定理5.6)**：** 设 G 是一个有限群，并配备一个生成 k-元组，满足 $k > 5$，并令 U_G 表示 G上的均匀分布。令 ν_t 表示乘积替换累加器算法经过 t步后返回的随机元素的分布。则

$$\|\nu_t - U_G\|_{\mathrm{tv}} < \epsilon \text{ for } t \geq \frac{23k^2}{k-5}((k+1)\log|G| + \log(\epsilon^{-1})),$$

其中，$\|\cdot\|_{\mathrm{tv}}$ 是全变差距离，$\log$ 是自然对数。

这个结果应作如下解读：为了确保 $\|\nu_t - U_G\|_{\mathrm{tv}} < e^{-1}$，我们需要进行约 $\frac{23k^2}{k-5}(k \log |G| + 1)$ 步，其中 e 表示欧拉数。这是代价最高的部分。此后，每额外进行 $\frac{23k^2}{k-5}$ 步，就可以保证 ν_t 与均匀分布的距离缩小 e 倍。

我们想要强调，定理5.6以及 [9,第 5 节2], 最有趣之处之一在于，关于 t 的界仅取决于 $|G|$。它完全不依赖于 G更内在的结构。

定理 5.6 中的估计与 [9], 中对原始乘积替换算法混合时间的估计几乎相同，因此，从抽取一个生成元组转为抽取 G 中的一个元素，不会带来多少额外开销。我们想强调，乘积替换累加器算法非常简单：每一步只进行一次乘法，至多进行一次群元素求逆。算法不涉及其他计算，因此关键只在于需要执行多少步，以及 G中的群运算成本。此外，所需内存非常少：只需存储 $k+1$ 个 G元素。

乘积替换算法及其各种变体的收敛速度可能远快于迄今得到的估计。然而，通过对谱隙进行经典分析，无法获得更好的渐近界，见定理 5.5。

最后，我们简要比较乘积替换累加器算法与其他抽样方法。在以下渐近界中，我们假设 $k \leq \log |G|$。Schreier-Sims 算法 [12, 28], 除了其他应用外，还可用于从置换群 S_n 的子群 G 中抽取一个元素。该算法需要耗费大量时间进行预处理阶段；在已知实现中，这一阶段至少需要 $\Theta(n^2 \log^3 |G|)$ 时间。但完成该阶段后，便可在 $\Theta(\log |G|)$ 时间内从 G 中均匀抽样。该算法至少需要存储 $\Theta(n \log |G|)$ 个 G [28, 定理 4.2.4] 元素。因此，即使对于置换群的子群，如果只需抽取少量元素，我们的算法也可能是更好的选择。另一类非常有趣的算法基于随机子乘积技术 [1]。Cooperman 提出了一种高效版本，其正确性已在 [6] 中得到证明。该算法在预处理阶段需要 $\Theta(\log^2 |G|)$ 步，之后便可在 $\Theta(\log |G|)$ 时间内从近似均匀分布中抽样。该算法的缺点是预处理阶段可能失败（尽管失败概率很小），并且需要存储 $\Theta(\log |G|)$ 个 G 元素。在时间效率方面，当 $k^2 < \log |G|$ 且需要抽样的元素数量较少时，可以保证乘积替换累加器算法优于 Cooperman 算法。此外，渐近估计中忽略的隐藏常数在 Cooperman 算法中可能很大。

概要。第 2 节回顾最初的乘积替换算法。第 3 节定义 $\Sigma'_k(G)$，即带有累加器的 G 的生成 k 元组所构成的图。随后定义群 A_k ，使得对于任意 G，图 $\Sigma'_k(G)$ 都是 A_k 的 Schreier 图。第 4 节定义乘积替换累加器算法，并证明累加器的分布收敛于 G 上的均匀分布。第 5 节证明主要结果。在该节中，我们结合计算机辅助计算与人工计算，证明 $\Delta_k^2 - 0.35(K-5)\Delta_k$ 是群环 $\mathbb{R}[\mathsf{A}_k]$ 中的平方和。定理 5.6 由此立即得出。为求完整，相关细节见第 5.3 节。第 6 节证明 A_k 是一个半直积，并指出 A_k 的性质 (T) 可由 [11, 命题 10] 直接推出。然而，这会使谱隙的界显著变弱

。最后，在第 7 节中，我们概述所用的计算机方法。

致谢。我们感谢 Marek Kaluba 在实现用于计算机计算的代码方面给予的帮助。我们还要感谢亚当·密茨凯维奇大学为数学与计算机科学学院的集群基础设施提供访问权限。

2. 乘积替换算法

设 $\mathrm{F}_k = \langle x_1, \dots, x_k \rangle$ 是秩为 k 的自由群。记 $\mathrm{Aut}(\mathrm{F}_k)$ 为 F_k 的自同构群。注意，自同构由其在生成元$x_1, \dots, x_k$上的像确定。对于 $\psi \in \mathrm{Aut}(\mathrm{F}_k)$ 和 $(g_1, \dots, g_s) \in \mathrm{F}_k^s$，我们将分别使用记号 $\psi(g_1, \dots, g_s) = (\psi(g_1) \dots, \psi(g_s)$。群 $\mathrm{Aut}(\mathrm{F}_k)$ 是有限生成的，并包含一个指数为 2 的子群，记作 $\mathrm{SAut}(\mathrm{F}_k)$，它由以下 Nielsen自同构生成：

$$R_{ij}^{\pm}(x_1, \dots, x_k) = (x_1, \dots, x_i x_j^{\pm}, \dots, x_k)$$
$$L_{ij}^{\pm}(x_1, \dots, x_k) = (x_1, \dots, x_j^{\pm} x_i, \dots, x_k).$$

也就是说，将第 i 个生成元与第 j 个生成元或其逆元相乘，乘在左侧或右侧。

设 G 为有限群，且 $k \in \mathbb{N}$。记 $\mathrm{Epi}(\mathrm{F}_k, G)$ 为从 F_k 到 G 的所有满同态的集合。在 $\mathrm{Epi}(\mathrm{F}_k, G)$ 上，我们通过前复合定义了一个左 $\mathrm{SAut}(\mathrm{F}_k)$- 作用：

$$\psi.e(x) = e(\psi^{-1}(x))$$

对 $\psi \in \mathrm{SAut}(\mathrm{F}_k)$、$e \in \mathrm{Epi}(\mathrm{F}_k, G)$ 和 $x \in \mathrm{F}_k$。令 $\Gamma_k(G)$ $\Gamma_k(G)$ 为对应于此作用及生成集的 Schreier 图

$$N_k = \{R_{ij}^{\pm}, L_{ij}^{\pm} \colon 1 \le i, j \le k\}.$$

$\Gamma_k(G)$ 的顶点是 $\mathrm{Epi}(\mathrm{F}_k, G)$ 的元素，并且当 $e_2 = s.e_1$ 时，对 $s \in N_k$ 存在一条有向标记边 $e_1 \xrightarrow{s} e_2$。$\Gamma_k(G)$ 的顶点之间可以有重边，也可以有自环。该图是正则图，其出度和入度均等于 $4k(k-1)$。

上面对 $\Gamma_k(G)$ 的描述很方便，因为它具有特殊自同构群 $\mathrm{SAut}(\mathrm{F}_k)$ 的明确作用。现在我们给出另一种描述，从乘积替换算法的角度来看，这种描述更加自然。

注意，每个满同态 $e \in \Gamma_k(G)$ 都由它在生成元 $e(x_i)$ 上的取值确定，并且 $(e(x_1) \dots, e(x_k))$ 是 G 的一个生成集。赋值 $e \mapsto (e(x_1) \dots, e(x_k))$ 在 $\Gamma_k(G)$ 的顶点与 G 的生成 k-元组之间建立了一一对应。因此

$$\mathrm{Epi}(\mathrm{F}_k, G) = \{(g_1, \dots, g_k) \colon \langle g_1, \dots, g_k \rangle = G\}.$$

这些元素 g_i 称为生成元。若两个生成 k-元组可以通过将第 j 个生成元或其逆元从左侧或右侧乘到第 i个生成元上而相互转换，则称它们是连通的。例如

$$(g_1, \ldots, g_k) \xrightarrow{L_{ij}} (g_1, \ldots, g_j^{-1} g_i, \ldots, g_k).$$

图 $\Gamma_k(G)$ 不一定是连通的。下文中我们始终固定一个初始生成 k-元组 S_0 （或等价地，一个初始满同态 e_0），并考虑 $\Gamma'_k(G)$，包含 S_0 的 $\Gamma_k(G)$ 的连通分支（为简便起见，我们在记号中省略 S_0 ）。$\Gamma'_k(G)$ 的顶点集合是 S_0 在 $\mathrm{SAut}(\mathrm{F}_k)$ 作用下的轨道。乘积替换算法 定义为从 S_0 出发，在 $\Gamma'_k(G)$ 上进行的惰性随机游走。与所有惰性随机游走一样，它收敛于均匀分布。

注 2.1。 本文倾向于使用惰性随机游走，因为我们在定理 5.6 中使用的估计仅适用于惰性随机游走。不过请注意，$\mathrm{SAut}(F_k)$ 具有长度为 2 的关系，即 $L_{ij}L_{ij}^{-1}$，以及长度为 5 的关系，即 $[L_{kj}^{-1}, L_{ji}] = L_{ki}$。由此可知$\Gamma'_k(G)$ 从任意顶点出发都有长度为 2 和 5 的自环。因此 $\Gamma'_k(G)$ 是非周期的，所以在 $\Gamma'_k(G)$上的简单随机游走也收敛于均匀分布。

例 2.2. 令 $e\colon \mathrm{F}_k \to \mathbb{Z}_n^k$, $n \in \mathbb{N}$ 为模 n 的阿贝尔化，或等价地为$S_0 = (v_1, \ldots, v_k)$，其中 $v_i \in \mathbb{Z}_n^k$ 是单位向量。那么， $\Gamma'_k(\mathbb{Z}_n^k)$ 的顶点是 $\mathbb{Z}_n^k$ 的正基，或等价地，是 $\mathrm{SL}_k(\mathbb{Z}_n)$ 的元素。此类基的成员（称为基向量）恰好是满足 $\gcd(x_1, \ldots, x_k, n) = 1$ 的向量 $x = (x_1, \ldots, x_k)$。 $\Gamma'_k(\mathbb{Z}_n^k)$ 上的（惰性）随机游走会收敛到 $\Gamma'_k(\mathbb{Z}_n^k)$ 顶点上的均匀分布。然而，如果我们输出随机游走所给生成元组的第一个坐标，那么这类元素的分布不会收敛到 $\mathbb{Z}_n^k$ 上的均匀分布。可以证明，它会收敛到 $\mathbb{Z}_n^k$ 的基向量上的均匀分布。

例 2.3. 这是上述例子的推广。设 $e\colon \mathrm{F}_k \to G$ 是一个满同态，且 $\ker(e)$ 在 $\mathrm{SAut}(\mathrm{F}_k)$ 下不变。令 $\Gamma'_k(G)$ 为 e 的连通分支。这样的满同态诱导出映射 $\bar{e}\colon \mathrm{SAut}(\mathrm{F}_k) \to \mathrm{Aut}(G)$，其定义如下：

$$\bar{e}(\psi)(e(x)) = e(\psi(x)).$$

此外，$\mathrm{Aut}(G)$ 在 $\mathrm{Epi}(\mathrm{F}_k, G)$ 上有一个自然的复合作用：若 $\psi \in \mathrm{Aut}(G)$ 且 $f \in \mathrm{Epi}(\mathrm{F}_k, G)$，则 $\psi.f = \psi \circ f$。在 $\Gamma'_k(G)$ 的顶点上，$\mathrm{SAut}(\mathrm{F}_k)$ 的作用经由 $\bar{e}$ 与 $\mathrm{SAut}(\mathrm{F}_k)$ 的反同态的逆复合，因子化为 $\mathrm{Aut}(G)$ 的作用。也就是说，我们有：

$$\psi.f = \bar{e}(\psi^{-1}).f \text{ for } \psi \in \mathrm{SAut}(\mathrm{F}_k) \text{ and } f \in \Gamma'_k(G).$$

这意味着， $\Gamma'_k(G)$ 的顶点都位于 e 在 $\bar{e}(\mathrm{SAut}(\mathrm{F}_k))$ 作用下的轨道中。这个作用显然是忠实的。因此，边上的标签反向后（L_{ij} 变为 L_{ij}^{-1}，依此类推）的 $\Gamma'_k(G)$，同构于带有生成元组 $\bar{e}(N_k)$ 的 $\bar{e}(\mathrm{SAut}(\mathrm{F}_k))$ 的凯莱图。我们将 G 的基元素定义为在 $\Gamma'_k(G)$ 中某个生成 k-元组里出现的任意元素（注意，基元素的概念可能取决于 e）。利用 $\bar{e}(\mathrm{SAut}(\mathrm{F}_k))$ 的传递性，可以证明，由 $\Gamma'_k(G)$ 上的随机游走给出的元组的第一个元素，其分布收敛于基元素上的均匀分布。

3. 随机变化的凯莱图上的随机游走

设 $\mathbb{Z}*\mathrm{F}_k$ 是秩为 $k+1$ 的自由群，其中 $\mathbb{Z}=\langle x_0\rangle$，且 $\mathrm{F}_k=\langle x_1,\ldots,x_k\rangle$。考虑 $\mathrm{E}_k(G)$ 这一 $\mathrm{Epi}(\mathbb{Z}*\mathrm{F}_k,G)$ 的子集，它由那些在子群 F_k 上已经是满射的满同态组成。也就是说，对于每个 $e\in\mathrm{E}_k(G)$，元素 $e(x_0)$ 可以任意取值，而元素 $e(x_1)\ldots,e(x_k)$ 生成 G。因此，$\mathrm{E}_k(G)$ 具有积集 $G\times\mathrm{Epi}(\mathrm{F}_k,G)$ 的结构。我们还可以将 $\mathrm{E}_k(G)$ 理解为如下元组的集合：

$$\mathrm{E}_k(G)=\{(g_0|g_1,\ldots,g_k)\colon g_0\in G,\langle g_1,\ldots,g_k\rangle=G\}.$$

我们用（$g_0|g_1$，……，g_k）代替（g_0，g_1，……，g_k），以突出最后一个元素k 和第一个元素的不同作用。此类元组的第一个元素 g_0 称为累加器。最后的 k 个元素称为生成元。

设A_k A_k 为$\mathrm{SAut}(\mathbb{Z}*\mathrm{F}_k)$的子群，由以下两类自同构生成。

C-生成元： $L_{0i}^{\pm}$ 和 $R_{0i}^{\pm}$ 对于 $i=1$，……，k。

N-生成元： $L_{ij}^{\pm}$ 和 $R_{ij}^{\pm}$ 对于 i，$j\in 1$，……，k。

我们有 $4k$ C 个生成元和 $4k(k-1)$ 个 N-生成元。总而言之，A_k 由 $4k^2$ 个元素生成。

引理 3.1. 群A_k 作用于$\mathrm{E}_k(G)$上。

证明。 若 $(g_0|g_1,\ldots,g_k)\in\mathrm{E}_k(G)$，则将某个 $g_i^{\pm}$（其中 $i=1,\ldots,k$）乘到 g_0上，可得到 $\mathrm{E}_k(G)$ 中的一个元素。因此， $L_{0i}^{\pm}$ 和 $R_{0i}^{\pm}$ 对 $i=1,\ldots,k$ 作用于 $\mathrm{E}_k(G)$。也可以对最后 k 个元素进行尼尔森变换。因此， $L_{ij}^{\pm}$ 和 $R_{ij}^{\pm}$ 对 $i,j\in 1,\ldots,k$ 作用于 $\mathrm{E}_k(G)$。□

令$\Sigma_k(G)$ 为由 A_k 在 $\mathrm{E}_k(G)$ 上的作用以及 A_k 的生成集所定义的 Schreier 图，该生成集由 C-生成元和 N-生成元组成。由 C-生成元标记的边称为 C-边。对 N-生成元和 N-边也采用相同的约定。

图 $\Sigma_k(G)$ 自带一种自然的子图结构，反映积分解 $G\times\mathrm{Epi}(\mathrm{F}_k,G)$，以及 C-边与 N-边之间的区别。下面更精确地描述这一分解。令投影为：

$$\pi_C\colon\ \mathrm{E}_k(G)\to G$$
$$\pi_N\colon\ \mathrm{E}_k(G)\to\mathrm{Epi}(\mathrm{F}_k,G)$$

由……给出

$$\pi_C(g_0|g_1,\ldots,g_k)=g_0$$
$$\pi_N(g_0|g_1,\ldots,g_k)=(g_1,\ldots,g_k)$$

注意， π_N 按如下方式诱导出图映射 π_N： $\Sigma_k(G)\to\Gamma_k(G)$： N边被映射到 $\Gamma_k(G)$的边上，并保留其标签；而每条 C边$e_1\xrightarrow{s}e_2$ 都被压缩为顶点 $\pi_N(e_1)=\pi_N(e_2)\in\Gamma_k(G)$。

设 $S=(g_1、\ldots\ldots、\ g_k)\ \in \Gamma_k(G)$是 G的一个生成 k元组。有向左右凯莱图 $Cay(S,\ G,\ S)$定义如下:

(1) $Cay(S,\ G,\ S)$ 的顶点是 G 的元素。

(2) There is a labeled edge $v_1 \xrightarrow{L_i^{\pm}} v_2$ if $v_2 = g_i^{\pm} v_1$ and $v_1 \xrightarrow{R_i^{\pm}} v_2$ if $v_2 = v_1 g_i^{\pm}$ for $1 \le i \le k$.

注意，此处的 S 不是生成集，而是一个生成 k-元组。特别地，生成元 g_i 可以重复，也可以等于 G 的单位元。因此，$Cay(S,\ G,\ S)$ 的顶点之间可以有重边，也可以有自环。这就是我们用 S 中的指标而不是生成元来标记边的原因。此外，我们使用的标记方式对应于 $\Sigma_k(G)$ 中的 C-标记。

引理 3.2。 设 $S \in \Gamma_k(G)$。考虑顶点子集

$$\pi_N^{-1}(S) = \{(g|S) \colon g \in G\} \subset \Sigma_k(G).$$

$\Sigma_k(G)$ 中由 C-边在 $\pi_N^{-1}(S)$ 上张成的子图同构于 $Cay(S, G, S)$。标记在如下意义下得到保留：标记为 C-生成元 $R_{0i}^{\pm}$ 或 $L_{0i}^{\pm}$ 的边，分别对应于 $Cay(S, G, S)$ 中标记为 $R_i^{\mp}$ 或 $L_i^{\mp}$ 的边。

引理 3.3。 设 $g \in G$。考虑顶点子集

$$\pi_C^{-1}(g) = \{(g|S) \colon S \in \Gamma_k(G)\} \subset \Sigma_k(G).$$

Σ_k（G）由 π_C^{-1}（g）中的 N-边所张成的子图同构于 Γ_k（G），且标签保持不变。

因此，将 $\Sigma_k(G)$ 限制在 C-边上，得到一族 $Cay(S,\ G,\ S)$，其指标由 $\Gamma_k(G)$ 的顶点给出。如果将 $\Sigma_k(G)$ 限制在 N-边上，那么对于每个 $g \in G$，我们都会看到 $\pi_C^{-1}(g)$ 上由 N-边所张成的同一个图 $\Gamma_k(G)$。

回忆一下，$\Gamma'_k(G)$ 是 $\Gamma_k(G)$ 中包含给定生成 k-元组 S_0 的连通分支。令

$\Sigma'_k(G)$ 是 $(1|S_0)$ 的连通分支。我们有 $\pi_N(\Sigma'_k(G)) = \Gamma'_k(G)$。

从 $(1|S_0)$ 出发在 $\Sigma'_k(G)$ 上进行的随机游走可以描述如下。我们设想，在任何时刻，我们都处于 G 的某个元素中，而在 G 上看到的是一个左—右凯莱图的结构。我们从单位元 $e \in G$ 出发，所看到的图是 $Cay(S_0,\ G,\ S_0)$。选择一条 C-边时，随机游走沿着 $Cay(S_0,\ G,\ S_0)$ 中的一条边前进。选择一条 N-边会使凯莱图的结构变成另一个 $Cay(S,\ G,\ S)$。接着，我们会在 $Cay(S,\ G,\ S)$ 中行走一段时间，直到再次改变凯莱图。因此，在 $\Sigma'_k(G)$ 中行走可以理解为在一个随机变化的凯莱图上进行随机游走。

注 3.4. 令 LA_k LA_k 按 A_k的方式定义，但对于 C-生成元，我们只采用左 Nielsen 自同构 $L_{0i}^{\pm}$。在 $\Sigma_k(G)$中描述 LA_k 时，我们将使用标准凯莱图代替左右凯莱图。我们在第 5 节证明的所有定理对 $_k$ LA均成立，且常数相同。由于生成元具有对称性，我们更倾向于使用 A_k。

4. 乘积替换累加器算法

设 Γ 为一张图。在 Γ 上的惰性随机游走是指以 $\frac{1}{2}$ 的概率停留在原处，并以 $\frac{1}{2}$ 的概率移动到一个均匀随机选取的邻居。设 G 为一个有限群，且 S_0 是给定的一个生成 k元组，属于 G。我们考虑以下算法，它是文献 [14] 中“rattle”算法的一个小幅修改。

乘积替换累加器算法 (G, S_0)**：**

(1) 从 $(1|S_0) \in \Sigma_k'(G)$ 开始。(2) 在 $\Sigma_k'(G)$上进行 t 步惰性随机游走。
(3) 返回累加器（所得元组的第一个元素）。

设 μ_t 为在 $\Sigma_k'(G)$上进行 t 步惰性随机游走所得的分布，并设 $\nu_t = \pi_C^*(\mu_t)$为累加器在 G 上的分布。请注意，虽然（2）中的惰性随机游走定义了一个马尔可夫链，但累加器所对应的随机变量序列不再是马尔可夫链。

在继续之前，我们先回顾一些经典定义。设 X 为一个有限集，设 U_X为 X上的均匀概率分布，即对于每个 $x \in X$， $U_X(x) = \frac{1}{|X|}$。
对于 X 上的两个概率分布 μ 和 ν，我们定义全变差距离：

$$\|\mu - \nu\|_{\mathrm{tv}} = \frac{1}{2} \sum_{x \in X} |\mu(x) - \nu(x)|.$$

设 $A\colon X \to Y$ 是有限集之间的映射。我们用 $A^*(\mu)$ 表示 μ 的推前，即 $A^*(\mu)(y) = \mu(A^{-1}(y))$。

引理 4.1. A^* 是一个压缩映射，也就是说

$$\|A^*(\mu) - A^*(\nu)\|_{\mathrm{tv}} \le \|\mu - \nu\|_{\mathrm{tv}},$$

其中 μ 和 ν 是 X上的分布。

引理 4.2. 分布 ν_t 收敛到 G 上的均匀分布，并且

$$\|\nu_t - U_G\|_{\mathrm{tv}} \le \|\mu_t - U_{\Sigma_k'(G)}\|_{\mathrm{tv}}.$$

证明. </style}我们有 $|\pi_C^{-1}(g)| = |\Gamma_k'(G)|$。因此它与 $g \in G$ 无关。于是

$$\pi_C^*(U_{\Sigma_k'(G)})(g) = U_{\Sigma_k'(G)}(\pi_C^{-1}(g)) = \frac{|\Gamma_k'(G)|}{|\Sigma_k'(G)|} = \frac{1}{|G|}$$

因此 $\pi_C^*(U_{\Sigma_k'(G)}) = U_G$。现在我们应用定理 4.1 以及这一事实： μ_t 收敛到 $\Sigma_k'(G)$上的均匀分布。 □

5. 主要结果的证明

设 R 是一个环，$*\colon R \to R$ 是一个映射。我们称 $\xi \in R$ 为平方和，并记作 $\xi \geq 0$，如果对于某个 $\xi_i \in R$，有 $\xi = \Sigma_i \xi_i^* \xi_i$。本文中，我们令 $R = \mathbb{R}[G]$ 为群 G 的群环，其中 $*$ 是 $\xi \geq 0$ $g^* = g^{-1}$ 的线性延拓，或者令 $R = \mathbf{L}(\mathbb{C}^V)$ 为 $\mathbb{C}^V$ 上线性自同态构成的环，其中 $*$ 表示厄米转置。

为证明主要结果，我们采用 [9]中提出的策略。首先，我们仔细选取一个元素 $\xi \in \mathbb{R}[\mathrm{A}_5]$，并通过计算机计算证明 $\xi \geq 0$。接着，利用人工计算以及 $\xi \geq 0$这一事实，我们证明对于 $k > 5$，有 $\Delta_k^2 - 0.35(k-5)\Delta_k \geq 0$ 并且$\Delta_5^2 - 1.41\Delta_5 \geq 0$，其中 Δ_k 是A_k的群拉普拉斯算子。由此可轻易推出定理5.6。

5.1. 平方拉普拉斯算子的分解。设 $k \in \mathbb{N}$。对于每一对指标$i \neq j$，我们定义部分拉普拉斯算子 $\Delta_{ij} \in \mathbb{R}[\mathbf{A}_k]$ 为：

$$\Delta_{ij} = (1 - L_{ij})(1 - L_{ij})^* + (1 - R_{ij})(1 - R_{ij})^*.$$

我们还定义 $\Delta_{ii} = 0$。与 C-生成元和 N-生成元相关的拉普拉斯算子为：

$$\Delta_k^C = \sum_{1 \leq s \leq k} \Delta_{0s} \qquad \Delta_k^N = \sum_{1 \leq i,j \leq k} \Delta_{ij}.$$

$\mathbf{A}_k$ 的完整非归一化群拉普拉斯算子为：Δ_k

$$\Delta_k = \Delta_k^C + \Delta_k^N.$$

现在我们着重研究拉普拉斯算子的平方。我们有

$$\Delta_k^2 = (\Delta_k^C)^2 + \{\Delta_k^C, \Delta_k^N\} + (\Delta_k^N)^2,$$

其中

$$\{\Delta_k^C, \Delta_k^N\} = \Delta_k^C \Delta_k^N + \Delta_k^N \Delta_k^C.$$

我们将进一步分解上述各项。在下面的求和中，指标始终从 1 取到 k。

分解 $(\Delta_k^C)^2$：

我们有

$$(\Delta_k^C)^2 = \mathrm{Sq}_k^C + \mathrm{Adj}_k^C,$$

其中

$$\begin{aligned} \mathrm{Sq}_k^C &= \sum_s \Delta_{0s}^2 \\ \mathrm{Adj}_k^C &= \sum_{s \neq t} \Delta_{0s} \Delta_{0t}. \end{aligned}$$

$\{\Delta_k^C, \Delta_k^N\}$的分解：

我们有

$$\{\Delta_k^C, \Delta_k^N\} = \mathrm{Adj}_k^{CN} + \mathrm{Opp}_k^{CN},$$

其中

$$\begin{aligned}\mathrm{Adj}_k^{CN} &= \sum_{i,j} \{\Delta_{0i} + \Delta_{0j}, \Delta_{ij}\} \\ \mathrm{Opp}_k^{CN} &= \sum_{|\{s,i,j\}|=3} \{\Delta_{0s}, \Delta_{ij}\}.\end{aligned}$$

$(\Delta_k^N)^2$的分解：

我们有

$$(\Delta_k^N)^2 = \mathrm{Sq}_k^N + \mathrm{Adj}_k^N + \mathrm{Opp}_k^N,$$

其中

$$\begin{aligned}\mathrm{Sq}_k^N &= \frac{1}{2}\sum_{i,j} (\Delta_{ij} + \Delta_{ji})^2 \\ \mathrm{Adj}_k^N &= \sum_{|\{i,j,l\}|=3} \Delta_{ij}(\Delta_{il} + \Delta_{li} + \Delta_{jl} + \Delta_{lj}) \\ \mathrm{Opp}_k^N &= \sum_{|\{i,j,l,m\}|=4} \Delta_{ij}\Delta_{lm}.\end{aligned}$$

5.2. 归纳。 设 $k \le K \in \mathbb{N}$，并设 S_K 通过置换指标作用于 $\{x_1, \ldots, x_K\}$。该作用在 $\mathbf{F}_{K+1}$ 上诱导出一个由自同构给出的作用（生成元 x_0 保持不变），进而在 $\mathbf{A}_K$ 上诱导出由共轭作用 $\psi \to \sigma\psi\sigma^{-1}$ 给出的作用。因此，$\sigma.L_{ij} = L_{\sigma(i)\sigma(j)}$，且 $\sigma.R_{ij} = R_{\sigma(i)\sigma(j)}$。

设 $\xi \in \mathbb{R}[\mathbf{A}_k]$。我们将对称化 S：$\mathbb{R}[\mathbf{A}_k] \to \mathbb{R}[\mathbf{A}_K]$ 定义为：

$$S(\xi) = \sum_{\sigma \in S_K} \sigma.\xi.$$

现在，我们将 S 应用于第5.1节分解中出现的元素。对于 Δ_k，我们有：

$$\begin{aligned}S(\Delta_k^C) &= (K-1)!\, k\, \Delta_K^C \\ S(\Delta_k^N) &= (K-2)!\, (k-1)k\, \Delta_K^N.\end{aligned}$$

对于 $(\Delta_k^C)^2$，我们有：

$$S(\mathrm{Adj}_k^C) = (K-2)!\,(k-1)k\ \mathrm{Adj}_K^C\,.$$

对于 $\{\Delta_k^C, \Delta_k^N\}$，我们有：

$$\begin{aligned} S(\mathrm{Adj}_k^{CN}) &= (K-2)!\,(k-1)k\ \mathrm{Adj}_K^{CN} \\ S(\mathrm{Opp}_k^{CN}) &= (K-3)!\,(k-2)(k-1)k\ \mathrm{Opp}_K^{CN}\,. \end{aligned}$$

最后，对于 $(\Delta_k^N)^2$，我们有：

$$\begin{aligned} S(\mathrm{Sq}_k^N) &= (K-2)!\,(k-1)k\ \mathrm{Sq}_K^N \\ S(\mathrm{Adj}_k^N) &= (K-3)!\,(k-2)(k-1)k\ \mathrm{Adj}_K^N \\ S(\mathrm{Opp}_k^N) &= (K-4)!\,(k-3)(k-2)(k-1)k\ \mathrm{Opp}_K^N\,. \end{aligned}$$

引理 5.1。 以下不等式在 $\mathbb{R}[\mathrm{A}_5]$ 中成立，其中 $\lambda_5 = 1.41$:

$$\mathrm{Adj}_5^C + \mathrm{Adj}_5^{CN} + \mathrm{Opp}_5^{CN} + (\Delta_5^N)^2 \geq \lambda_5 \Delta_5.$$

证明。 注意， Δ_{ij} 包含于增广理想中，且 $\Delta_{ij} = \Delta_{ij}^*$。 因此 $\xi = \mathrm{Adj}_5^C + \mathrm{Adj}_5^{CN} + \mathrm{Opp}_5^{CN} + (\Delta_5^N)^2$ 也具有同样的性质。现在，我们可以按照第 7 节所述求出数值近似并验证该不等式。 □

定理 5.2。 假设 $K > 5$，并令 Δ_K 为 A_K 的非归一化拉普拉斯矩阵。我们有 $\Delta_K^2 - 0.35(K-5)\Delta_K \geq 0$。对于 $K = 5$，我们有 $\Delta_5^2 - 1.41\Delta_5 \geq 0$.

证明。 令 $k = 5$，且 $K \geq 5$。利用定理5.1，应用算子 S 并除以$(K-2)!(k-1)k$，我们得到：

$$\begin{aligned} & & \mathrm{Adj}_K^C & & \\ & + & \mathrm{Adj}_K^{CN} & + & \tfrac{k-2}{K-2}\ \mathrm{Opp}_K^{CN} \\ & + \mathrm{Sq}_K^N + \tfrac{k-2}{K-2}\ \mathrm{Adj}_K^N & & + & \tfrac{(k-3)(k-2)}{(K-3)(K-2)}\ \mathrm{Opp}_K^N \\ & & & \geq & \tfrac{\lambda_k(K-1)}{k-1}\ \Delta_K^C + \lambda_k \Delta_K^N. \end{aligned} \tag{5.1}$$

由于 $K-2 \geq k-2$，Opp_K^{CN}的系数不大于 1。注意，$\mathrm{Opp}_K^{CN} \geq 0$和 $\mathrm{Opp}_K^N \geq 0$ [9, 引理 36]。

根据 [9, 注释 5.8]，我们有 $\mathrm{Adj}_k^N + 3\mathrm{Opp}_k^N \geq 1.37\Delta_k^N$。使用算子 S 并除以 $(K-3)!(k-2)(k-1)k$，得到

$$\mathrm{Adj}_K^N + \frac{3(k-3)}{K-3}\,\mathrm{Opp}_K^N \geq \frac{1.37(K-2)}{k-2}\Delta_K^N. \tag{5.2}$$

令 $u = 1 - \frac{k-2}{K-2} \geq 0$。我们将不等式 5.2 乘以 u 并加到不等式 5.1上。注意，此时 Adj_K^N 的系数变为1 而 Opp_K^N 的系数为：

$$\gamma = \frac{3(k-3)u}{K-3} + \frac{(k-3)(k-2)}{(K-3)(K-2)},$$

通过直接计算可知，其不大于 1。因此我们得到：

$$\begin{array}{rrrrl} & & \mathrm{Adj}_K^C & & \\ + & & \mathrm{Adj}_K^{CN} & + & \frac{k-2}{K-2}\ \mathrm{Opp}_K^{CN} \\ + & \mathrm{Sq}_K^N + & \mathrm{Adj}_K^N & + & \gamma\ \mathrm{Opp}_K^N \\ & & \geq & \frac{\lambda_k(K-1)}{k-1} & \Delta_K^C + (\frac{1.37(K-2)u}{k-2} + \lambda_k)\Delta_K^N. \end{array}$$

接下来，我们将 Opp_K^{CN} 和 Opp_K^N 的系数增至 1，并加上 $\mathrm{Sq}_K^C \geq 0$。得到：

$$\begin{array}{rrrrl} (\Delta_K^C + \Delta_K^N)^2 = & \mathrm{Sq}_K^C + & \mathrm{Adj}_K^C & & \\ & + & \mathrm{Adj}_K^{CN} & + \mathrm{Opp}_K^{CN} & \\ & + \mathrm{Sq}_K^N + & \mathrm{Adj}_K^N & + \mathrm{Opp}_K^N & \\ & & & \geq \frac{\lambda_k(K-1)}{k-1}\Delta_K^C + (\frac{1.37(K-2)u}{k-2} + \lambda_k)\Delta_K^N. \end{array} \tag{5.3}$$

由于 $(K-2)u = K-5$、$k=5$ 和 $\lambda_k = 1.41$，我们有

$$\frac{1.37(K-5)}{k-2} + \lambda_k > \frac{\lambda_k(K-5)}{k-1} = 0.35(K-5).$$

因此 $\Delta_K^2 \geq 0.35(K-5)\Delta_K$。

如果 $K=5$，我们有 $u=0$ 根据不等式 5.3 可得 $\Delta_K^2 \geq 1.41\Delta_K$。

□

Note 由定理 5.2 可知，A_k 对 $k \geq 5$ [24]具有性质 (T)。

注 5.3。要证明定理 5.2，只需有 $\mathrm{Adj}_5^C + \mathrm{Adj}_5^{CN} + \mathrm{Opp}_5^{CN} \geq \lambda_5\Delta_5$ 对于某个 $\lambda_5 > 0$。然而，计算机计算无法验证这个不等式。因此我们添加了额外的一项 $(\Delta_5^N)^2$。

5.3. 谱隙估计。设 G 是一个有限群，S_0 是 G 的一个生成 k-元组。设 $\Sigma_k'(G)$ 是 $\Sigma_k(G)$ 中 $(1|S_0)$ 的连通分支。回顾一下，$\Sigma_k'(G)$ 是一个 $4k^2$- 正则图。由

$\Delta_{\Sigma_k'(G)}$

$\Delta_{\Sigma_k'(G)}$ 我们将 $\Sigma_k'(G)$ 的非归一化拉普拉斯矩阵记为 $\Delta_{\Sigma_k'(G)} = 4k^2 I - A$，其中 A 是 $\Sigma_k'(G)$ 的邻接矩阵。A 的每个元素表示连接给定两个顶点的有向边数量。$\Sigma_k'(G)$ 的谱隙是归一化拉普拉斯矩阵 $\frac{1}{4k^2}\Delta_{\Sigma_k'(G)}$ 的谱隙。

推论 5.4。 设 $k > 5$。 $\Sigma'_k(G)$ 的谱隙至少为 $0.35(k-5)4k^2$。

证明。令 V 为 $\Sigma'_k(G)$ 的顶点集合。由于 A_k 作用于 V，因此我们有酉表示 $\rho_G\colon \mathrm{A}_k \to \mathrm{U}(\mathbb{C}^V)$。我们也用 ρ_G 表示其到环上的线性延拓
$*$-同态 $\rho_G\colon \mathbb{R}[\mathrm{A}_k] \to \mathrm{L}(\mathbb{C}^V)$，其中 $\mathrm{L}(\mathbb{C}^V)$ 表示 $\mathbb{C}^V$ 的线性自同态空间。我们有

$$\rho_G(\Delta_k) = \Delta_{\Sigma'_k(G)}.$$

注意，如果 $\xi \in \mathrm{L}(\mathbb{C}^V)$ 且 $\xi^2 - \lambda\xi \geq 0$，那么 ξ 的谱隙至少为 λ。由定理 5.2，我们有 $\Delta^2_{\Sigma'_k(G)} - 0.35(k-5)\Delta_{\Sigma'_k(G)} \geq 0$，因此 $\Sigma'_k(G)$ 的谱隙至少为 $0.35(k-5)4k^2$。□

注记 5.5。定理 5.2 中不等式 $\Delta_k^2 - \lambda_k\Delta_k \geq 0$ 里的 λ_k 的增长不可能快于线性。事实上，A_k 映射满射到 $\mathrm{SAut}(\mathrm{F}_k)$，见第 6 节；而 $\mathrm{SAut}(\mathrm{F}_k)$ 进一步映射到 $\mathrm{SL}_k(\mathbb{Z})$，后者在 $V = \mathbb{Z}_3^k \setminus \{0\}$ 上传递地作用。此作用诱导出一个表示$\rho_k\colon \mathrm{A}_k \to \mathrm{U}(\mathbb{C}^V)$。注意，对于 $v = \Sigma_{i=1}^k(\delta_{e_i} - \delta_{-e_i}) \in \mathbb{C}^V$，我们有：

$$\sup_s \|\rho_k(s)v - v\| = \sqrt{\frac{2}{k}}\|v\|,$$

其中 s 遍历 A_k 的生成元。令 $\Delta_{\rho_k} = \rho_k(\Delta_k)$ 并令 λ_{ρ_k} 为Δ_{ρ_k}的谱隙。由定理 5.4可得 $\lambda_k \leq \lambda_{\rho_k}$。由于 v在 $\mathbb{C}^V$中与常值函数正交，且常值函数是 Δ_{ρ_k} 特征值为0 的唯一特征向量，因此有：

$$\lambda_{\rho_k} \leq \frac{\|\langle\Delta_{\rho_k}v, v\rangle\|}{\|v\|^2} = \frac{1}{\|v\|^2}\sum_s \|\rho_k(s)v - v\|^2 \leq 4k^2\left(\sqrt{\frac{2}{k}}\right)^2 = 8k.$$

因此，定理 5.2 是渐近紧的。

定理 5.6。 设 G 是一个有限群， S_0 是 G 的一个生成 k-元组， $k > 5$。设 ν_t 为经过 t 步后，(G, S_0) 的乘积替换累加器的分布。我们有

$$\|\nu_t - U_G\|_{\mathrm{tv}} < \epsilon \text{ for } t \geq \frac{8k^2}{0.35(k-5)}((k+1)\log|G| + \log(\epsilon^{-1})).$$

证明。 令 μ_t 为经过 t 步后，在 $\Sigma'_k(G)$ 上的惰性随机游走的分布。定理 5.4 以及将收敛到均匀分布的速率与 $\Sigma'_k(G)$ [15, 第 12] 章的谱隙联系起来的标准界给出：

$$\|\mu_t - U_G\|_{\mathrm{tv}} < \epsilon \text{ for } t \geq \frac{8k^2}{0.35(k-5)}\log\left(\frac{|\Sigma'_k(G)|}{\epsilon}\right).$$

该定理由定理 4.2 和不等式 $|\Sigma'_k(G)| < |G|^{k+1}$得出。

□

注 5.7. 对 $k = 5$ 采用类似论证可得

$$\|\nu_t - U_G\|_{\mathrm{tv}} < \epsilon \text{ for } t \geq \frac{8k^2}{1.41}((k+1)\log|G| + \log(\epsilon^{-1})).$$

推论 5.8。 固定 $k \geq 5$。由(G, S_0)索引的 $4k^2$-正则图族 $\Sigma'_k(G)$是扩张子，其中 G 是任意有限群，S_0 是 G 的一个生成 k-元组。

注 5.9. 定理 5.1 对 LA_5 也同样成立，且常数相同，即 $\lambda_5 = 1.41$，并且算子定义适当。定理 5.2 和定理 5.6 也以相同的常数继续成立。证明完全相同。

6. Alternative proof of property (T)

在这一补充段落中，我们证明 A_k 是一个半直积，并讨论另一种论证，以说明 A_k 具有性质 (T)。然而，这种论证给出的估计远不如定理 5.6。

引理 6.1. 群 A_k 同构于 $\mathrm{F}_k^2 \rtimes$特殊自同构群(F_k)，其中特殊自同构群(F_k)在 $\mathrm{F}_k^2 = \mathrm{F}_k \times \mathrm{F}_k$ 上的作用是典范作用的直积。

证明。 设 $\mathrm{F}_k < \mathbb{Z} * \mathrm{F}_k$，其中 $\mathrm{F}_k = \langle x_1, \ldots, x_k \rangle$。注意， N-生成元生成特殊自同构群(F_k)，因此特殊自同构群(F_k) $<\mathrm{A}_k$。此外，A_k 中的元素固定 F_k，故将其限制在这个子群上，得到收缩:

$$p\colon \mathrm{A}_k \twoheadrightarrow \mathrm{SAut}(\mathrm{F}_k).$$

因此，A_k 同构于 ker(p) $\rtimes$ SAut(F_k)，其中 SAut(F_k)通过共轭作用于 ker(p)。令 $\psi \in$ ker(p)，则 ψ 固定所有 x_1，……，x_k；由于它由 C-生成元和N-生成元生成，因此要得到 x_0，我们只能在右侧和左侧乘以来自 F_k 的元素。因此，存在唯一的元素 l_ψ 和 w_ψ，它们属于 F_k，使得:

$$\psi(x_0, x_1, \ldots, x_k) = (l_\psi x_0 r_\psi, x_1, \ldots, x_k).$$

映射 $j(\psi) = (l_\psi^{-1}, r_\psi)$ 是 ker(p) 与 F_k^2之间的一个同构。事实上，它是单射的；又由于我们拥有所有生成元 $L_{0i}^{\pm}$ 和 $R_{0i}^{\pm}$，因此可以得到 F_k^2 中的每个元素。此外，由于

$$\psi_1\psi_2(x_0) = \psi_1(l_{\psi_2} x_0 r_{\psi_2}) = l_{\psi_2} l_{\psi_1} x_0 r_{\psi_1} r_{\psi_2},$$

我们有 $j(\psi_1\psi_2) = (l_{\psi_1}^{-1} l_{\psi_2}^{-1}, r_{\psi_1} r_{\psi_2}) = j(\psi_1)j(\psi_2)$，因此 j 是一个同态。由此可得，A_k 同构于 $\mathrm{F}_k^2 \rtimes$SAut(F_k)。

现在，我们通过同构 j 将 ker(p) 与 F_k^2 识别后，计算 SAut(F_k) 在 ker(p) 上的共轭作用。设 $\phi \in$SAut(F_k) $<\mathrm{A}_k$ 和 $\psi \in$ker(p) 满足 $j(\psi) = (l^{-1}, r)$。注意， $\phi(x_0) = x_0$。我们有

$$\begin{aligned}\phi\psi\phi^{-1}(x_0) &= \phi\psi(x_0)\\ &= \phi(lx_0r)\\ &= \phi(l)x_0\phi(r).\end{aligned}$$

因此， $j(\phi\psi\phi^{-1}) = (\phi(l^{-1})\ \phi(r))$，而 SAut($F_k$) 在 F_k^2 上的作用是典范作用的直积。

□

以类似的方式可以证明LA_k 同构于$F_k \rtimes \mathrm{SAut}(F_k)$，其定义见定理3.4，其中$LA_k$。

如果只关注A_k 或LA_k的性质 (T)，可以直接使用 [11,命题 10]。然而，与定理5.6所得结果相比，这种方法给出的谱隙估计要差得多。下面计算这些估计。

假设 G是一个群，且 S 是 G的一个固定生成集。(G, S) 的 Kazhdan 常数是满足下述条件的最大数 $\kappa(G)$:

$$\max_{s\in S} \|\rho(s)v - v\| \geq \kappa(G)\|v\|,$$

对于 G 的每个不可约酉表示 ρ 以及每个 $v \in \mathcal{H}_\rho$。

假设 $k \geq 4$。由 [9, 备注 5.11] 对于 $k \geq 5$，以及 [22] 对于 $k = 4$可知，SAut(F_k) 具有性质 (T)，且 Kazhdan 常数 κ(SAut(F_k)) 的量级为 $\frac{1}{\sqrt{k}}$。根据 [11,命题 10],，我们有 κ (LA_k) 至少为 k^{-1}的量级。由于 $A_k = F_k \rtimes LA_k$，再次利用 [11, 命题 10], 可得， $\kappa(A_k)$ 至少为 $k^{-1.5}$的量级。现在，我们需要估计 $\Sigma'_k(G)$ 关于 A_k 的谱隙，以及 LA_k的类似图的谱隙。据我们所知，由 Kazhdan 常数对谱隙给出下界的最佳估计见于 [26]。为使用该结果，我们需要自同构群中一个作用于 A_k的生成元上的子群，该子群为 A_k的自同构群的子群。这样的最大子群是 $\Phi = \mathbb{Z}_2^{k+1} \rtimes S_k$，更多细节见第 7.1 节。

Φ 对 A_k 的生成元作用所产生的最小轨道含有 $4k$ 个元素，因此，来自 [26] 的常数 α 等于 $\alpha(A_k) = \frac{4k}{4k^2} = \frac{1}{k}$。对 LA_k进行类似分析，其中 $\Phi = \mathbb{Z}_2^k \rtimes S_k$，可得 $\alpha(LA_k) = \frac{1}{2k-1}$。因此，我们得到的 $\Sigma'_k(G)$ 谱隙下界至少为 $\alpha(A_k)\kappa(A_k)^2$, ，这给出了 k^{-4} 阶的下界（注意，[26] 中的 Kazhdan 常数是我们所定义的 Kazhdan 常数的平方）。对于 LA_k ，我们得到 k^{-3} 阶的下界。这些估计远不如定理 5.2 推出的结果，也不如定理 5.6 中使用的结果。本文策略的关键在于，我们不经由 Kazhdan 常数，而是直接根据计算机计算估计谱隙。

7. 将计算机计算转化为严格证明

本节将说明我们如何得到 $\lambda_5 = 1.41$ 定理5.1 中的估计，以及针对LA_5的类似结果。本文的说明主要基于 [10]中的描述。

设 G 是由不含二阶元素的有限对称集 S 生成的群，令 Δ 为 G 关于 S的拉普拉斯算子。Ozawa证明了 Δ 是增广理想 $I[G]$中的一个序单位，这意味着对每个 $*$-不变的 $\xi \in I[G]$ ，都存在 $R_\xi \geq 0$ 使得 $\xi + R_\xi \Delta \geq 0$。更准确地说， Δ 是 $I[G]$ 的序单位这一概念，其定义实际上要求对来自 $I[G]$的有限多个 ξ_i ，有 $\xi + R_\xi \Delta = \sum_i \xi_i^* \xi_i$。然而，由于 $\Sigma^2 I[G] = \Sigma^2 \mathbb{R}[G] \cap I[G]$，我们只需要求 $\xi_i \in \mathbb{R}[G]$。

设 $\xi = \xi^* \in I[G]$。假设我们想证明存在一个正的 λ ，使得$\xi - \lambda\Delta \geq 0$。我们首先对 $\lambda_0 > 0$ 进行数值估计，并求出 $\xi - \lambda_0\Delta$的平方和分解。显然，由于计算机受到有限性约束，我们无法在整个无限群中搜索解。解决办法是将注意力限制在某个有限子集 $E \subset G$ 上，并寻找其分解

$$\xi - \lambda_0 \Delta \approx \sum_i \xi_i^* \xi_i, \tag{7.1}$$

其中每个 ξ_i的支撑都包含于 $E = \{1, g_1, \ldots, g_m\}$。通常取 E为某个小半径的球。然后可以将方程 7.1 等价地写成

$$\xi - \lambda_0 \Delta \approx \mathbb{x}^* Q^T Q \mathbb{x}$$

对于某个 $m \times m$ 实矩阵 Q ，以及

$$\mathbb{x} = \begin{bmatrix} 1 - g_1 \\ \vdots \\ 1 - g_m \end{bmatrix},$$

其中 $*$ 此处表示群环 $*$ 运算与矩阵转置的复合。

设 $r = \xi - \lambda_0 \Delta - \mathbb{x}^* Q^T Q \mathbb{x}$。我们有

$$\xi - (\lambda_0 - R_r)\Delta = \mathbb{x}^* Q^T Q \mathbb{x} + (r + R_r \Delta).$$

后一个表达式已经是平方和，这就可以完成证明。然而，我们还必须注意以下几个方面：

(1) 首先，我们必须确保 $R_r < \lambda_0$ ，而到目前为止，我们尚未给出 R_r 的任何上界。幸运的是，我们可以利用 T. Netzer 和 A. Thom 的以下结果：

> **定理 7.1**。 [20, 引理 2。1] 对于任意 $\xi = \xi^* \in I[G]$，存在 $R_\xi \geq 0$ 使得$\xi + R_\xi \Delta \geq 0$ 并且：
>
> $$R_\xi \leq m^2 ||\xi||_1,$$
>
> 其中 $||\eta||_1 = \sum_g |\xi_g|$ 表示 $\eta = \sum_g \eta_g g$ 的 ℓ_1 范数，而 m 是 ξ 的支撑中 g 相对于 S 的词长范数的最大值。

（2）为确保获得数值近似值后计算的严谨性，需使用区间算术进行计算。其思路是，群环元素的系数不再是普通实数，而是一些较小的区间

从而保证实际系数落在相应区间内。所有算术运算都能保持这种严谨性。

上述所有步骤均已在 [7] 中实现，并且此前已应用于 [10, 11, 9, 8]。

7.1. **求数值近似**。 为得到 λ和 Q的数值近似，可以采用半正定规划。我们略去相关说明，因为 [11]中已对此作了详尽描述。如其中所述，可以利用表达式 $\Delta^2 - \lambda\Delta$ 关于由 Nielsen 换位生成的生成集的对称性。韦德伯恩分解 由此可以大幅降低问题的复杂度。这同样适用于我们的情形。为了应用这一方法，我们必须确认，对于我们的群 $G \in \{\mathsf{A}_k, \mathsf{LA}_k\}$，拉普拉斯算子 Δ 和有限支撑集 E 是Φ-不变的，其中 Φ表示一个特定的花环积。

(1) 在 $G = \mathsf{A}_k$的情形下， Φ 是 $\mathbb{Z}_2 \wr S_{k+1} \cong \mathbb{Z}_2^{k+1} \rtimes S_{k+1}$ 的子群，由形如 $((a_0, \ldots, a_k)\ \sigma)$ 的元素生成，其中 $\sigma \in S_{k+1}$固定 0，且 S_{k+1}表示集合 $\{0, \ldots, k\}$的置换群。 Φ 在 G 上的作用定义如下

$$((a_0, \ldots, a_k), \sigma)T_{i,j} = \begin{cases} (T_{\sigma(i),\sigma(j)})^{\pm a_{\sigma(j)}}, & x_{\sigma(i)} = 1 \\ (T'_{\sigma(i),\sigma(j)})^{\mp a_{\sigma(j)}}, & x_{\sigma(i)} = -1, \end{cases}$$

其中， T' 表示 R 对应 $T = L$ 的情形， L 表示 $T = R$对应的情形。元素（$(a_0, \ldots, a_k)\ \sigma$）的作用，恰好是通过自由群 $\mathsf{F}_{k+1} = \langle x_0, \ldots, x_k \rangle$ 上的自同构进行共轭，该自同构将 x_i 映射为$x_{\sigma\, i}^{a_{\sigma(i)}}()$。

(2) 对于 $G = \mathsf{LA}_k$, $\Phi = \mathbb{Z}_2 \wr S_k \cong \mathbb{Z}_2^k \rtimes S_k$的情形，其中 S_k 表示集合 $\{1, \ldots, k\}$上的置换群。我们按照上文针对 $i > 0$的情形所用的相同公式，定义 Φ 在$T_{i,j}$ 上的作用。对于 $i = 0$ ，我们也采用相同做法，但忽略符号 T的翻转。这一点很重要，因为如果直接继承直积的共轭作用，就会翻转 T；而由于缺少生成元 R_{0j}，我们不能这样做。

在上述两种情况下，我们取 E 为某个有限半径球。显然， E 是Φ-不变的。

上述数值近似可以在适中的时间内获得（在我们的情况下不超过 2 小时），使用的是一台配备 32 GB 随机存取存储器的典型台式计算机。

7.2. **结果复现**。 我们请读者参阅包含我们代码的 GitHub 仓库 [18] 或 Zenodo 资源 [19]。我们还提供了 λ 和 Q的预计算数值近似。可以直接使用这些结果完成认证过程——这样便可以跳过整个数值近似部分。证明仍然是严格的，因为对于这一目的而言， λ和 Q的近似实际上是如何获得的并不重要。

Julia [3] 代码的实现 [18] 大量使用（有时通过其他软件包间接使用）以下软件包：Groups.jl [11, 9], IntervalArithmetic.jl[27], JuMP.jl [16], SCS [23], StarAlgebras.jl [11, 9], SymbolicWedderburn.jl [11, 9], 和PropertyT.jl [7]。

参考文献

[1] L. Babai. 顶点传递图的局部扩张与有限群中的随机生成。载于第二十三届 ACM 年度计算理论研讨会论文集，STOC ’91，第 164–174 页，美国纽约州纽约市，1991。美国计算机协会。doi:10.1145/103418.103440。[2] L. Babai 和 I. Pak. 群生成元的强偏差：对“乘积替换算法”的阻碍。第 50 卷，第 215–231 页。2004。SODA 2000 专刊。doi:10.1016/S0196-6774(03)00091-9。[3] J. Bezanson、A. Edelman、S. Karpinski 和 V. B. Shah. Julia：一种数值计算的新方法。《SIAM 评论》，59(1):65–98，2017。网址：https://epubs.siam.org/doi/10.1137/141000671，doi:10. 1137/141000671。[4] F. Celler、C. R. Leedham-Green、S. H. Murray、A. C. Niemeyer 和 E. A. O’Brien. 生成有限群的随机元素。《通讯代数》，23(13):4931–4948，1995。doi:10.1080/00927879508825509。[5] G. Cooperman、L. Finkelstein 和 N. Sarawagi. 置换群的随机基变换算法。ISSAC ’90，第 161–168 页，美国纽约州纽约市，1990。美国计算机协会。doi:10.1145/96877.96918。[6] J. D. Dixon. 生成有限群中的随机元素。《电子组合学杂志》/仅电子版/, 15(1):研究论文 R94，13 页–研究论文 R94，13 页，2008。网址：http:// eudml.org/doc/130477。[7] M. Kaluba. PropertyT.jl：用于在群环中运用平方和方法认证 Kazhdan 性质 (T)。https://github.com/kalmarek/PropertyT.jl，2024。[8] M. Kaluba 和 D. Kielak. 整数环上的 Chevalley 群的 Kazhdan 常数。《伊比利亚美洲数学评论》，41(4):1253–1269，2025。doi:10.4171/rmi/1534。[9] M. Kaluba、D. Kielak 和 P. W. Nowak. 关于 Aut(F_n) 和 SL$_n(\mathbb{Z})$ 的性质 (T)。《数学年刊》(2)，193(2):539–562，2021。doi:10.4007/annals.2021.193.2.3。[10] M. Kaluba 和 P. W. Nowak. 谱隙数值估计的认证。《群、复杂性与密码学》，10(1):33–41，2018。doi:10.1515/gcc-2018-0004。[11] M. Kaluba、P. W. Nowak 和 N. Ozawa. Aut($\mathbb{F}_5$) 具有性质 (T)。《数学年刊》，375(3-4):1169–1191，2019。doi:10.1007/s00208-019-01874-9。[12] D. E. Knuth. 置换群的高效表示。《组合数学》，11(1):33–43，1991。doi:10.1007/ BF01375471。[13] C. R. Leedham-Green. 关于乘积替换算法的一种变体。《格拉斯哥数学杂志》，66(1):221–228，2024。doi:10.1017/s0017089523000435。[14] C. R. Leedham-Green 和 S. H. Murray. 乘积替换算法的变体。载于《计算与统计群论》（拉斯维加斯，内华达州/霍博肯，新泽西州，2001），《当代数学》第 298 卷，第 97–104 页。美国数学学会，罗得岛州普罗维登斯，2002。doi:10.1090/conm/298/05116。[15] D. A. Levin、Y. Peres 和 E. L. Wilmer. 马尔可夫链与混合时间。美国数学学会，罗得岛州普罗维登斯，2009。另有 James G. Propp 和 David B. Wilson 撰写的一章。doi:10.1090/ mbk/058。[16] M. Lubin、O. Dowson、J. D. Garcia、J. Huchette、B. Legat 和 J. P. Vielma. Jump 1.0：面向数学优化建模语言的最新改进。《数学规划计算》，2023。doi:10.1007/s12532-023-00235-5。[17] A. Lubotzky 和 I. Pak. 乘积替换算法与 Kazhdan 性质（T）。《美国数学会杂志》，14(2):347–363，2001。doi:10.1090/S0894-0347-00-00356-8。[18]M. Marcinkowski 和 P. Mizerka. pra_complexity. https://github.com/piotrmizerka/pra_complexity，2025。GitHub 仓库。[19] M. Marcinkowski 和 P. Mizerka. “有限群元素采样：带累加器的乘积替换算法的效率”的复现详情，2025。doi:10.5281/zenodo.17981235。[20] T. Netzer 和 A. Thom. 通过半定优化研究 Kazhdan 性质（T）。《实验数学》，24(3):371–374，2015。doi:10.1080/10586458.2014.999149。[21] P. M. Neumann 和 C. E. Praeger. 特殊线性群的识别算法。《伦敦数学会会刊》，s3-65(3):555–603，1992 年 11 月。arXiv:https://academic.oup.com/plms/ article-pdf/s3-65/3/555/4456828/s3-65-3-555.pdf, doi:10.1112/plms/s3-65.3.555。

[22] M. Nitsche. 关于性质 (T) 的计算机证明与半定规划对偶性。https://arxiv.org/abs/2009.05134，2022 年。 arXiv:2009.05134。[23] B. O'Donoghue、E. Chu、N. Parikh 和 S. Boyd. 通过算子分裂和齐次自对偶嵌入进行锥优化。《优化理论与应用杂志》，169(3):1042–1068，2016 年 6 月。doi:10.1007/s10957-016-0892-3。[24] N. Ozawa. Kazhdan 性质 (T) 的非交换实代数几何。《*Jussieu* 数学研究所杂志》，15(1):85–90，2016 年。 doi:10.1017/S1474748014000309。[25] I. Pak. 我们对乘积替换算法了解多少？见《群与计算》第三卷（俄亥俄州哥伦布市，*1999* 年），第 8 卷，载于俄亥俄州立大学数学研究所出版物，第 301–347 页。德古意特，柏林，2001 年。[26] I. Pak 和 A. Żuk. 关于 Kazhdan 常数与随机游走混合。《国际数学研究通知》，(36):1891–1905，2002 年。doi:10.1155/S1073792802206017。[27] D. P. Sanders、L. Benet、L. Ferranti、K. Agarwal、B. Richard、J. Grawitter、E. Gupta、M. Forets、M. F. Herbst、yashrajgupta、E. Hanson、B. van Dyk、C. Rackauckas、R. Vasani、S. Micluţa-Câmpeanu、S. Olver、T. Koolen、C. Wormell、D. Karrasch、D. Widmann、F. A. Vázquez、G. Dalle、J. Sarnoff、J. TagBot、K. O'Bryant、K. Carlsson、M. Piibeleht、M. Giordano、Q. Zhang 和 R. Deits. JuliaInter- vals/IntervalArithmetic.jl：v0.20.9，2023 年。doi:10.5281/zenodo.8037734。[28] Á.Seress. 置换群算法。剑桥数学专著丛书。剑桥大学出版社，2003 年。

波兰弗罗茨瓦夫大学数学系

电子邮箱地址：michal.marcinkowski@math.uni.wroc.pl

波兰波兹南亚当·密茨凯维奇大学数学与计算机科学学院

电子邮箱地址：piotr.mizerka@amu.edu.pl