arXiv:2601.03206v1 [math.GR] 6 Jan 2026

有理矩阵有限不可约半群大小上界的一个简短证明

BENJAMIN STEINBERG

Abstract. 我给出一个简短证明，证明 Kiefer 和 Ryzhikov 最近得到的结果：由 $n \times n$ 矩阵构成的有限不可约半群，其基数至多为 3^{n^2}。

1. Introduction

Kiefer 和 Ryzhikov [KR26] 最近证明，由有理数域上的 $n \times n$ 矩阵构成的不可约半群，其基数至多为 3^{n^2}。这一上界较此前的上界 [BHK+20]有了重大改进，他们的证明也提出了许多新颖思路。不过，利用有限半群的已知表示理论，可以大大简化这个证明。本文给出一个简短证明，其思路与闵可夫斯基证明有限群情形的方法非常接近。相比之下，Kiefer 和 Ryzhikov 通过组合学上的非凡壮举，将问题归结为闵可夫斯基定理。我的证明中的一个关键点是 Rhodes 的结果：不可约的有限矩阵半群（含零元）在其（0-）极小理想 [Rho69]上左右作用忠实。

2. The main result

矩阵半群若没有非平凡不变子空间，则称为不可约。设 S 是由 $\mathbb{Q}$ 上的 $n \times n$ 阶矩阵构成的不可约子半群。不失一般性，假设 $0 \in S$，因为将其添入不会改变不可约性。为避免平凡情况，我默认 $S \neq 0$。

含零半群的理想若不包含真非零理想，则称为 0-极小。若含零半群具有一个 0-极小理想 I，使得 S 在 I的左侧和右侧都忠实作用，则称其为广义群映射；在这种情况下，I 必为 0-单半群，且是 S唯一的 0-极小理想。含零半群 S 若 $S^2 \neq 0$ 和 S 没有真非零理想，则称其为 0-单半群。参见 [KRT68] 或 [RS09，第 4]章。每个 0-单半群

Date：2026年1月7日。2020 *Mathematics Subject Classification.* 20M30，20M35。
Key words and phrases. 不可约半群。作者获得了美国国家科学基金会 DMS-2452324 项目、Simons 基金会合作资助（编号 849561）、澳大利亚研究理事会 DP230103184 项目以及 Marsden 基金MFP-VUW2411 的支持。

S 包含 $S \setminus \{0\}$ 中的一个极大子群 G（即在作为群这一性质下极大的子半群），且任意两个极大子群都同构 [RS09，附录 A]。

回顾一下，若半群中的两个元素生成相同的主双边理想（分别为相同的主右理想、相同的主左理想），则称它们是 $\mathscr{J}$-等价（分别是 $\mathscr{R}$-等价、 $\mathscr{L}$-等价）。记作 $\mathscr{H} = \mathscr{R} \cap \mathscr{L}$。注意，每个极大子群都是一个 [RS09, Appendix A] 中的 $\mathscr{H}$-类。有限半群是稳定的，这意味着

$$sx \ \mathscr{J} \ s \iff sx \ \mathscr{R} \ s \text{ and } xs \ \mathscr{J} \ s \iff xs \ \mathscr{L} \ s.$$

参见 [RS09, Theorem A.2]。

引理 1 (Rhodes [Rho69, Lemma 1.5])。设 S 是域 K 上含有 0 的有限不可约半群。那么 S 是广义群映射。

证明。设 I 是 S 的任意一个 0-极小理想。 S 的 K-张成空间 A 是一个单代数 [CP61, Theorem 5.7]。 I 的 K-张成空间是 A 的一个理想，因此根据单性，它是 A 。但是 A 含有单位矩阵 1 [CP61, Lemma 5.32]。因此，1 属于 I 的 K-张成空间，例如 $1 = \sum_{i=1}^{k} c_i s_i$ ，其中 $c_i \in K$、 $s_i \in I$。如果 s 和 t 在 I 的左侧作用相同，那么

$$s = s1 = \sum_{i=1}^{k} c_i s s_i = \sum_{i=1}^{k} c_i t s_i = t1 = t$$

右侧的情况对偶地成立。因此 S 是广义群映射。 □

以下是 [KRT68]第 8 章命题 3.28 的一个特例。

命题 2。 设 S 是有限广义群映射半群，其0-极小理想为 I。设 G 是 $I \setminus \{0\}$ 的一个极大子群。那么，同态 $\varphi\colon \ S \to T$ 是单射，当且仅当 $\varphi(I) \cap \varphi(0) = \emptyset$ 且 $\varphi|_G$ 是单射。

证明。对于非平凡方向，假设 $\varphi(s) = \varphi(s')$。注意， $s = s'$属于 S 当且仅当对所有 $x, y \in I$ 都有 $xsy = xs'y$ （见引理 4.6.23 [RS09]），因为若 $s \neq s'$，则由右作用的忠实性，存在 $x \in I$ 使得 $xs \neq xs'$ ；此时由左作用的忠实性，存在 $y \in I$ 使得$xsy \neq xs'y$。因此，设 $x, y \in I$。由于 $\varphi(xsy) = \varphi(xs'y)$，关于 φ的假设保证了 $xsy = 0 = xs'y$ 或 $xsy, xs'y \in I$。在后一种情况下，$xsy \ \mathscr{J} \ x \ \mathscr{J} \ y \ \mathscr{J} \ xs'y$，故由稳定性可得 $xsy \ \mathscr{H} \ xs'y$。但根据 Green 引理 [RS09，引理 A.3.1], ，存在 a, b ，使得 $r \mapsto arb$ 是从 xsy的 $\mathscr{H}$-类到 G的双射。于是， $\varphi(axsyb) = \varphi(axs'yb)$意味着 $axsyb = axs'yb$ ，因为 $\varphi|_G$ 是单射。但这就有 $xsy = xs'y$，正如所需。因此 φ 是单射。□

最后，我们在此记录一个众所周知的引理，至少对于群而言是如此。

引理 3。 设 S 是 $M_n(\mathbb{Q})$ 的有限子半群。那么 S 共轭于 $M_n(\mathbb{Z})$ 的一个子半群。

证明。设 b_1，……，b_n 是 $\mathbb{Q}^n$的一组基。由于 S是有限的，子群 $L = \langle \{b_1, \ldots, b_n\} \cup Sb_1 \cup \cdots \cup Sb_n \rangle$ 是一个 S-不变的有限生成子群，并且因此是自由阿贝尔群。此外，它的秩为 n，且张成 $\mathbb{Q}^n$，因为它包含 b_1，……，b_n。于是，相对于 L的任意整基，S均可表示为整数矩阵。□

现在我证明 [KR26] 的上界。我将使用闵可夫斯基的一项经典结果：对于 p 奇素数，映射 $GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}/p\mathbb{Z})$ 的核是无挠的。为完整起见，我将简述证明。

定理 4 (闵可夫斯基**)。** 设 p 是奇素数。那么 $\ker(\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}))$ 是无挠的。

证明。如果它不是无挠的，那么它有一个 A 素数阶为 q的元素。因此$A^q = 1$ 且 $A = 1 + p^k C$，其中 $C \not\equiv 0$ 模 p 且 $k \geq 1$。因此，

$$1 = (1 + p^k C)^q = 1 + qp^k C + \sum_{i=2}^{q} \binom{q}{i} p^{ik} C^i,$$

因此 $qC = -\sum_{i=2}^{q} \binom{q}{i} p^{k(i-1)} C^i \equiv 0$ 模 p。于是 $q = p$ 如 $C \not\equiv 0$ 模 p。两边除以 p，得到 $C = -\sum_{i=2}^{p-1} \binom{p}{i} p^{k(i-1)-1} C^i - p^{k(p-1)-1} C^p$。由于当 $1 < i < p$ 时 $p \mid \binom{p}{i}$，因此 $C \equiv -p^{k(p-1)-1} C^p$ 模 p，这与$C \not\equiv 0$ 模 p 如 $p > 2$矛盾。□

为了稍微改进这个界，我还将利用当 $p = 2$ 时核只有 2-挠这一事实（见 [Ser07]）。回顾一下，如果一个半群的所有极大子群都是平凡的，则称它是无周期的。

定理 5. 设 $S \subseteq M_n(\mathbb{Q})$ 不可约。则 $|S| \leq 3^{n^2}$。若 S 的唯一（0-）极小理想的极大子群 G 为奇数阶（例如，若 S 无周期），则 $|S| \leq 2^{n^2}$。

证明。不失一般性，假设 S 包含 0，并由引理 3 得 $S \subseteq M_n(\mathbb{Z})$。由引理 1，$S$ 是广义群映射，且有唯一的 0-极小理想 I。设 G为 I 的极大子群，$0 \neq e$ 为其单位元。若 G 为奇数阶，令 $p = 2$；若 G 为偶数阶，令 $p = 3$。假设 e 的秩为 r。则 $e\mathbb{Z}^n$ 是秩为 r的自由阿贝尔群，并且$\mathbb{Z}^n = e\mathbb{Z}^n \oplus (1 - e)\mathbb{Z}^n$。因此，选择一个适配此直和的 $\mathbb{Z}^n$ 的整基后，不失一般性可假设

$$e = \begin{bmatrix} 1_r & 0_{r,n-r} \\ 0_{n-r,r} & 0_{n-r} \end{bmatrix}.$$

那么典范投影 $\pi\colon\ M_n(\mathbb{Z}) \to M_n(\mathbb{Z}/p\mathbb{Z})$ 满足 $\pi(e) \neq 0$，因此 π 将 0 与 I 分离（因为 I 是 0-极小的，且 $\pi^{-1}(0) \cap I$ 是一个理想）。注意，G随后包含于

$$\begin{bmatrix} GL_r(\mathbb{Z}) & 0_{r,n-r} \\ 0_{n-r,r} & 0_{n-r} \end{bmatrix}$$

因此， $\pi|_G$ 可以视为投影 $GL_r(\mathbb{Z}) \to GL_r(\mathbb{Z}/p\mathbb{Z})$ 的限制。闵可夫斯基定理（或其 $p = 2$ 变体）于是推出 $\pi|_G$是单射。因此，根据命题 2， $\pi|_S$ 是单射，所以 $|S| \leq p^{n^2}$，正如所要求的。□

References

[BHK+20] Georgina Bumpus、Christoph Haase、Stefan Kiefer、Paul-Ioan Stoienescu 和 Jonathan Tanner。《有限有理矩阵半群的大小》。载于 *47th International Colloquium on Automata, Languages, and Programming*，第 168 卷，*LIPIcs. Leibniz Int. Proc. Inform.*，第 115 号文章，共 13 页。达格施图尔城堡。莱布尼茨信息学中心，瓦德恩，2020 年。[CP61] A. H. Clifford 和 G. B. Preston。*The algebraic theory of semigroups. Vol. I*。《数学调查丛书》，第 7 号。美国数学会，普罗维登斯，罗得岛州，1961 年。[KR26] Stefan Kiefer 和 Andrew Ryzhikov。《有理矩阵有限不可约半群的渐近大小》，2026 年。arXiv:2601.01236。[KRT68] K. Krohn、J. Rhodes 和 B. Tilson。*Algebraic theory of machines, languages, and semigroups*。Michael A. Arbib 编。Kenneth Krohn 和 John L. Rhodes 作出重要贡献。学术出版社，纽约，1968 年。第 1、5–9 章。[Rho69] John Rhodes。《有限半群的特征与复杂度》。*J. Combinatorial Theory* 6 67 85, 1969，：–。[RS09] John Rhodes 和 Benjamin Steinberg。*The q-theory of finite semigroups*。《施普林格数学专著》。施普林格，纽约，2009 年。[Ser07] Jean-Pierre Serre。《 $G(k)$ 的有限子群阶数的界》。载于 *Group representation theory*，第 405–450 页。洛桑联邦理工学院出版社，洛桑，2007 年。

（B. Steinberg） Department of Mathematics, City College of New York, Convent Avenue at 138th Street, New York, New York 10031, USA*Email address*: bsteinberg@ccny.cuny.edu