向量群分解的算法与应用

陈经纬

中国数学会 2022 年学术年会 @ 武汉

2023 年 2 月 19 日

提纲

1. 向量群分解问题
2. 离散情形
3. 非离散情形

提纲

1. 向量群分解问题
2. 离散情形
3. 非离散情形

向量群的定义

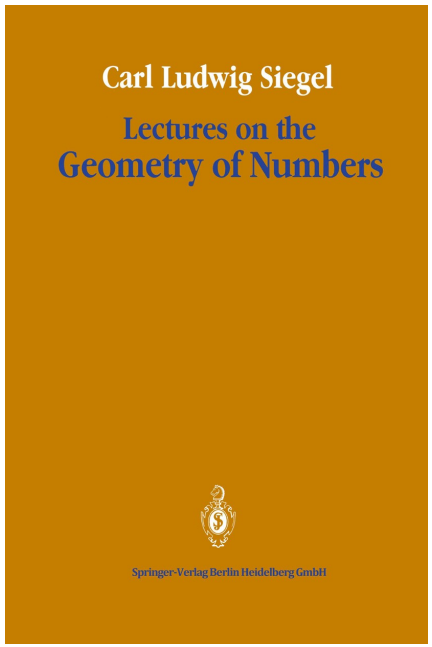
称 m 维欧氏空间 $\mathbb{R}^m$ 中的子集 G 是一个向量群，若

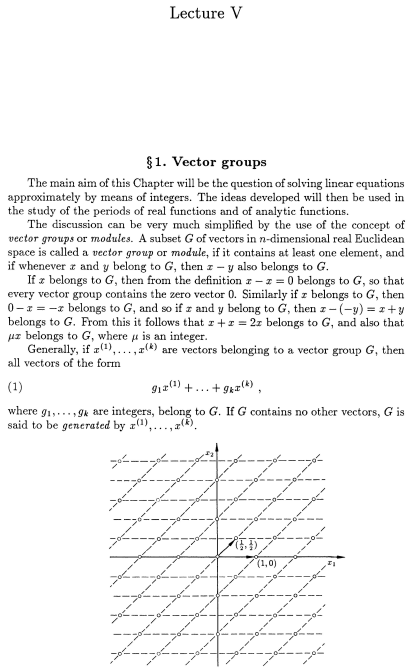
- G 非空；
- 当 $\boldsymbol{x}, \boldsymbol{y} \in G$ 时有 $\boldsymbol{x} - \boldsymbol{y} \in G$ 成立.

向量群的定义

称 m 维欧氏空间 $\mathbb{R}^m$ 中的子集 G 是一个向量群，若

- G 非空；
- 当 $x, y \in G$ 时有 $x - y \in G$ 成立.





Lecture V

§1. Vector groups

The main aim of this Chapter will be the question of solving linear equations approximately by means of integers. The ideas developed will then be used in the study of the periods of real functions and of analytic functions.

The discussion can be very much simplified by the use of the concept of *vector groups* or *modules*. A subset G of vectors in n-dimensional real Euclidean space is called a *vector group* or *module*, if it contains at least one element, and if whenever x and y belong to G, then $x - y$ also belongs to G.

If x belongs to G, then from the definition $x - x = 0$ belongs to G, so that every vector group contains the zero vector 0. Similarly if x belongs to G, then $0 - x = -x$ belongs to G, and so if x and y belong to G, then $x - (-y) = x + y$ belongs to G. From this it follows that $x + x = 2x$ belongs to G, and also that μx belongs to G, where μ is an integer.

Generally, if $x^{(1)}, \ldots, x^{(k)}$ are vectors belonging to a vector group G, then all vectors of the form

$$g_1 x^{(1)} + \ldots + g_k x^{(k)} , \tag{1}$$

where $g_1, \ldots, g_k$ are integers, belong to G. If G contains no other vectors, G is said to be *generated* by $x^{(1)}, \ldots, x^{(k)}$.

向量群的生成元

设 G 是 $\mathbb{R}^m$ 中的一个向量群.

- $\mathbf{0} \in G$;
- 若 $\boldsymbol{x} \in G$，则 $-\boldsymbol{x} \in G$;
- 若 $\mu \in \mathbb{Z}$ 且 $\boldsymbol{x} \in G$，则 $\mu \cdot \boldsymbol{x} \in G$;
- 若 $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \in G$，则所有的向量

$$\mu_1 \boldsymbol{x}_1 + \cdots + \mu_k \boldsymbol{x}_k \tag{1}$$

都属于向量群 G，其中 $\mu_1, \ldots, \mu_k \in \mathbb{Z}$.

向量群的生成元

设 G 是 $\mathbb{R}^m$ 中的一个向量群.

- $\mathbf{0} \in G$;
- 若 $\boldsymbol{x} \in G$，则 $-\boldsymbol{x} \in G$;
- 若 $\mu \in \mathbb{Z}$ 且 $\boldsymbol{x} \in G$，则 $\mu \cdot \boldsymbol{x} \in G$;
- 若 $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \in G$，则所有的向量

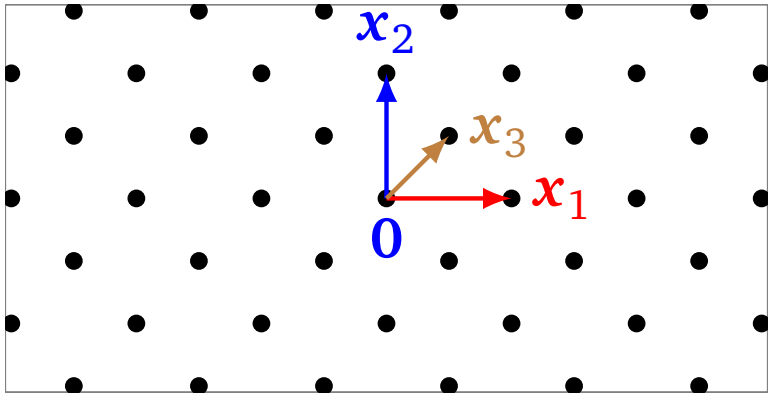
$$\mu_1 \boldsymbol{x}_1 + \cdots + \mu_k \boldsymbol{x}_k \tag{1}$$

都属于向量群 G，其中 $\mu_1, \ldots, \mu_k \in \mathbb{Z}$.

若 G 的所有元素都有 (1) 的形式，则称 G 是由 $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ 生成的. 记为 $G = \langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \rangle$.

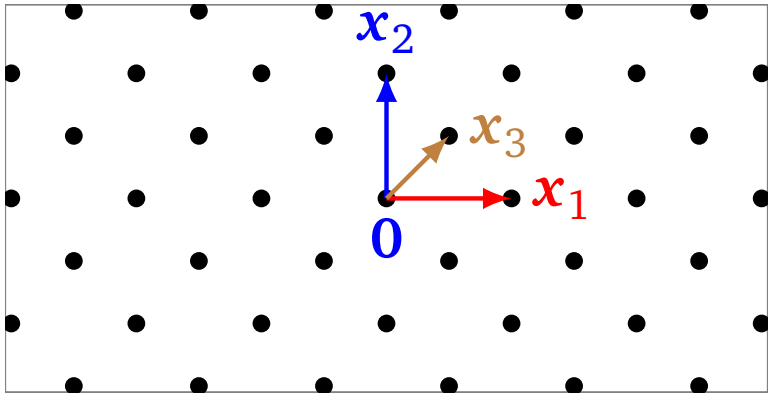
两个例

例 1: $G = \langle \boldsymbol{x}_1 = (1,0), \boldsymbol{x}_2 = (0,1), \boldsymbol{x}_3 = (1/2, 1/2) \rangle \subseteq \mathbb{R}^2$.



两个例

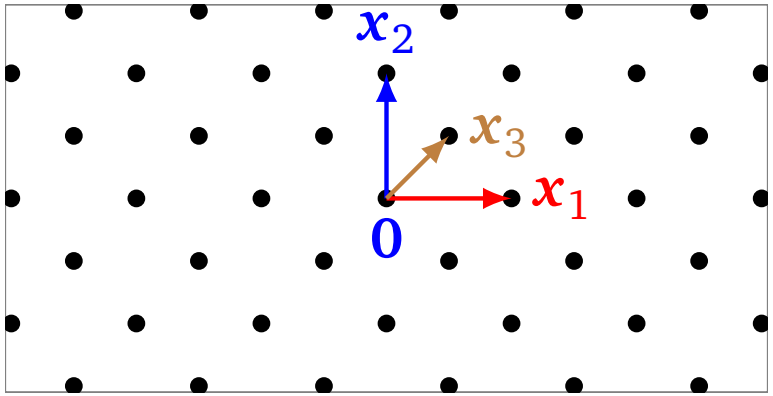
例 1: $G = \langle \boldsymbol{x}_1 = (1,0), \boldsymbol{x}_2 = (0,1), \boldsymbol{x}_3 = (1/2, 1/2) \rangle \subseteq \mathbb{R}^2$.



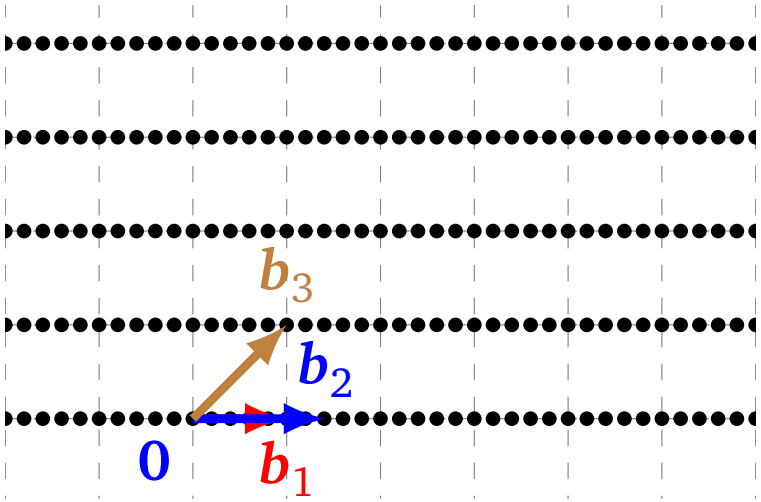
例 2: $G = \langle \boldsymbol{b}_1 = (1,0), \boldsymbol{b}_2 = (\sqrt{2},0), \boldsymbol{b}_3 = (1,1) \rangle \subseteq \mathbb{R}^2$.

两个例

例 1: $G = \langle \boldsymbol{x}_1 = (1,0), \boldsymbol{x}_2 = (0,1), \boldsymbol{x}_3 = (1/2, 1/2) \rangle \subseteq \mathbb{R}^2$.



例 2: $G = \langle \boldsymbol{b}_1 = (1,0), \boldsymbol{b}_2 = (\sqrt{2}, 0), \boldsymbol{b}_3 = (1,1) \rangle \subseteq \mathbb{R}^2$.



向量群的性质 (I)

定理 (Siegel's book, Lec. V, Th. 2.1)

若向量群 G 中不包含长度任意小的向量，则存在 G 中的有限个向量使得 G 由这组向量生成.

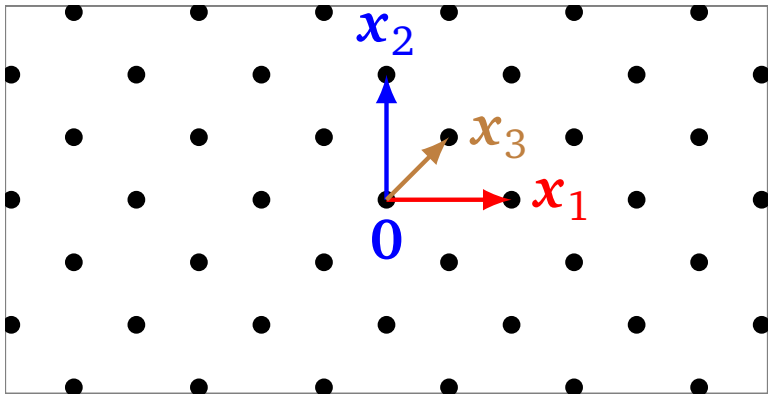
- 称 G 为一个离散向量群 (也常被称作欧几里得格，简称格).
- 这组生成元被称作 G 的基.
- 基向量的个数被称作 G 的秩，记为 $\mathrm{rank}(G)$.

向量群的性质 (I)

定理 (Siegel's book, Lec. V, Th. 2.1)

若向量群 G 中不包含长度任意小的向量，则存在 G 中的有限个向量使得 G 由这组向量生成.

- 称 G 为一个离散向量群 (也常被称作欧几里得格，简称格).
- 这组生成元被称作 G 的基.
- 基向量的个数被称作 G 的秩，记为 $\mathrm{rank}(G)$.



- 例 1 (续)：(x_1, x_3) 和 (x_2, x_3) 均是 G 的基；$\mathrm{rank}(G) = 2$.

向量群的性质 (II)

定理 (Siegel's book, Lec. VI, Th. 2.6)

设 G 是向量群. 则它的闭包 $\overline{G}$ 可被唯一分解为 $\overline{G} = \Lambda \oplus E$，其中

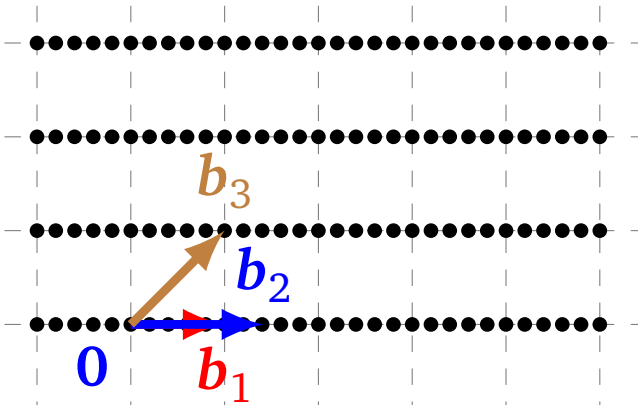
- Λ：格，被称作 G 的格分支；
- E：向量空间，E 的维数被称为 G 的局部秩；
- $\mathrm{Span}(\Lambda) \perp E$.

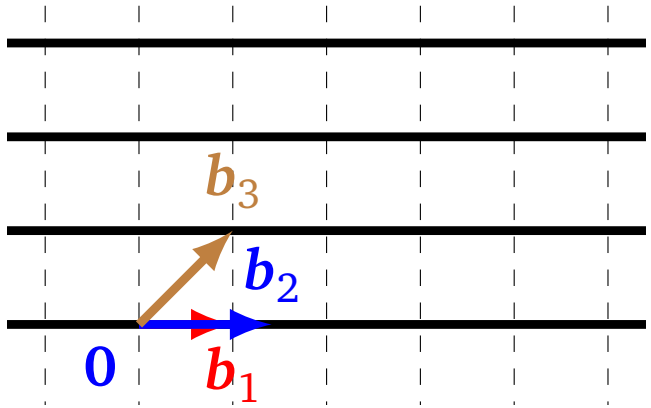
向量群的性质 (II)

定理 (Siegel's book, Lec. VI, Th. 2.6)

设 G 是向量群. 则它的闭包 $\overline{G}$ 可被唯一分解为 $\overline{G} = \Lambda \oplus E$，其中

- Λ：格，被称作 G 的格分支；
- E：向量空间，E 的维数被称为 G 的局部秩；
- $\mathrm{Span}(\Lambda) \perp E$.





- 例 2 (续)：$\overline{G} = \mathbb{Z} \cdot (0,1) \oplus \mathbb{R} \cdot (1,0)$；$G$ 的局部秩为 1.

向量群分解问题

定理 (Siegel's book, Lec. VI, Th. 2.6)

设 G 是向量群. 则它的闭包 $\overline{G}$ 可被唯一分解为 $\overline{G} = \Lambda \oplus E$，其中

- Λ：格，被称作 G 的格分支；
- E：向量空间，E 的维数被称为 G 的局部秩；
- $\mathrm{Span}(\Lambda) \perp E$.

向量群分解问题

给定向量群 G 的一组生成元，如何计算上述分解?

向量群分解问题

定理 (Siegel's book, Lec. VI, Th. 2.6)

设 G 是向量群. 则它的闭包 $\overline{G}$ 可被唯一分解为 $\overline{G} = \Lambda \oplus E$，其中

- Λ：格，被称作 G 的格分支；
- E：向量空间，E 的维数被称为 G 的局部秩；
- $\mathrm{Span}(\Lambda) \perp E$.

向量群分解问题

给定向量群 G 的一组生成元，如何计算上述分解？特别地，

- 如何确定 G 的局部秩？

向量群分解问题

定理 (Siegel's book, Lec. VI, Th. 2.6)

设 G 是向量群. 则它的闭包 $\overline{G}$ 可被唯一分解为 $\overline{G} = \Lambda \oplus E$，其中

- Λ：格，被称作 G 的格分支；
- E：向量空间，E 的维数被称为 G 的局部秩；
- $\mathrm{Span}(\Lambda) \perp E$.

向量群分解问题

给定向量群 G 的一组生成元，如何计算上述分解？特别地，

- 如何确定 G 的局部秩？
  - [Babai, et al. '88]：(在解析计算树模型下)不可判定！

向量群分解问题

定理 (Siegel's book, Lec. VI, Th. 2.6)

设 G 是向量群. 则它的闭包 $\overline{G}$ 可被唯一分解为 $\overline{G} = \Lambda \oplus E$，其中

- Λ：格，被称作 G 的格分支；
- E：向量空间，E 的维数被称为 G 的局部秩；
- $\mathrm{Span}(\Lambda) \perp E$.

向量群分解问题

给定向量群 G 的一组生成元，如何计算上述分解？特别地，

- 如何确定 G 的局部秩？
  - [Babai, et al. '88]：(在解析计算树模型下)不可判定！
- 给定 G 的局部秩，如何得到 G 的格分支的一组基？

向量群分解问题

定理 (Siegel's book, Lec. VI, Th. 2.6)

设 G 是向量群. 则它的闭包 $\overline{G}$ 可被唯一分解为 $\overline{G} = \Lambda \oplus E$，其中

- Λ：格，被称作 G 的格分支；
- E：向量空间，E 的维数被称为 G 的局部秩；
- $\mathrm{Span}(\Lambda) \perp E$.

向量群分解问题

给定向量群 G 的一组生成元，如何计算上述分解？特别地，

- 如何确定 G 的局部秩？
  - [Babai, et al. '88]：(在解析计算树模型下)不可判定！
- 给定 G 的局部秩，如何得到 G 的格分支的一组基？
  - 局部秩为零：离散情形；
  - 局部秩非零：非离散情形.

提纲

1. 向量群分解问题
2. 离散情形
3. 非离散情形

离散情形 (I)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

- 得到的基向量足够“短”
- 效率足够高

离散情形 (I)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

- 得到的基向量足够“短”
- 效率足够高

意义

- 近年来，格的理论与算法是热门的研究方向，因为
  - 格为数学、理论计算机科学、密码学等学科提供有力工具；
  - 基于格的密码学被普遍认为可抵御量子计算机的攻击；
  - ……
- 几乎所有格算法的输入都是以格的一组基为输入的.
- 很多应用中，仅能提取出格的一组生成元.

离散情形 (I)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

- 得到的基向量足够“短”
- 效率足够高

算法概览

- [Lenstra, et al. ’82]：基于 LLL 算法及其改进 (较短、较快)
- [Storjohann ’00]：Hermite 标准型 (HNF)
- [Storjohann ’00]：Smith 标准型 (SNF)
- [Li, Nguyen ’19]：HNF + 对偶基 (稍长、更快)
- [Li, Storjohann ’22]：特殊情形 $m = n + 1$
- ……

离散情形 (II)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

基于 LLL 算法的格基算法新分析 [C., Stehlé, Villard '18]

- LLL 算法：输入格的一组基，返回该格质量更“好”的一组基.

离散情形 (II)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

基于 LLL 算法的格基算法新分析 [C., Stehlé, Villard '18]

- LLL 算法：输入格的一组基，返回该格质量更"好"的一组基.
- 启发式地，当 $K > 2^{\Omega(m)} \cdot \|\boldsymbol{A}\|^{\frac{n}{m-n}}$ (其中 $\|\boldsymbol{A}\| := \max|a_{i,j}|$) 时：

$$\begin{pmatrix} K \cdot \boldsymbol{A} \\ \boldsymbol{I} \end{pmatrix} \xrightarrow{\text{LLL}} \begin{pmatrix} \mathbf{0} & K \cdot \boldsymbol{B} \\ * & * \end{pmatrix}.$$

离散情形 (II)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

基于 LLL 算法的格基算法新分析 [C., Stehlé, Villard '18]

- LLL 算法：输入格的一组基，返回该格质量更"好"的一组基.
- 启发式地，当 $K > 2^{\Omega(m)} \cdot \|\boldsymbol{A}\|^{\frac{n}{m-n}}$ (其中 $\|\boldsymbol{A}\| := \max|a_{i,j}|$) 时：

$$\begin{pmatrix} K \cdot \boldsymbol{A} \\ \boldsymbol{I} \end{pmatrix} \xrightarrow{\text{LLL}} \begin{pmatrix} \mathbf{0} & K \cdot \boldsymbol{B} \\ * & * \end{pmatrix}.$$

- LLL 迭代次数的经典结果：$O(n^2(\log K + \log \|\boldsymbol{A}\|))$.

离散情形 (II)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

基于 LLL 算法的格基算法新分析 [C., Stehlé, Villard '18]

- LLL 算法：输入格的一组基，返回该格质量更"好"的一组基.
- 启发式地，当 $K > 2^{\Omega(m)} \cdot \|\boldsymbol{A}\|^{\frac{n}{m-n}}$ (其中 $\|\boldsymbol{A}\| := \max|a_{i,j}|$) 时：

$$\begin{pmatrix} K \cdot \boldsymbol{A} \\ \boldsymbol{I} \end{pmatrix} \xrightarrow{\text{LLL}} \begin{pmatrix} \boldsymbol{0} & K \cdot \boldsymbol{B} \\ * & * \end{pmatrix}.$$

- LLL 迭代次数的经典结果：$O(n^2(\log K + \log \|\boldsymbol{A}\|))$.
- 新工具：$\Pi_k(\boldsymbol{A}) = \sum_{j=1}^{n-1} (n-j) \log \|\boldsymbol{a}_{\ell_j}^*\| - \sum_{i=1}^{m-n} i \log \|\boldsymbol{a}_{s_i}^*\| + \sum_{i=1}^{m-n} s_i.$

离散情形 (II)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

基于 LLL 算法的格基算法新分析 [C., Stehlé, Villard '18]

- LLL 算法：输入格的一组基，返回该格质量更"好"的一组基.
- 启发式地，当 $K > 2^{\Omega(m)} \cdot \|\boldsymbol{A}\|^{\frac{n}{m-n}}$ (其中 $\|\boldsymbol{A}\| := \max|a_{i,j}|$) 时：

$$\begin{pmatrix} K \cdot \boldsymbol{A} \\ \boldsymbol{I} \end{pmatrix} \xrightarrow{\text{LLL}} \begin{pmatrix} \boldsymbol{0} & K \cdot \boldsymbol{B} \\ * & * \end{pmatrix}.$$

- LLL 迭代次数的经典结果：$O(n^2(\log K + \log \|\boldsymbol{A}\|))$.
- 新工具：$\Pi_k(\boldsymbol{A}) = \sum_{j=1}^{n-1} (n-j) \log \|\boldsymbol{a}^*_{\ell_j}\| - \sum_{i=1}^{m-n} i \log \|\boldsymbol{a}^*_{s_i}\| + \sum_{i=1}^{m-n} s_i$.
- LLL 迭代次数：$O(n^3 + n(m-n)(1 + \log \|\boldsymbol{A}\|))$，与 K 无关！

离散情形 (III)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

- 需要计算一个幺模矩阵 $\boldsymbol{U} \in \mathrm{GL}_m(\mathbb{Z})$ 使得 $\boldsymbol{A} \cdot \boldsymbol{U} = (\boldsymbol{0}, \boldsymbol{B})$.

离散情形 (III)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

- 需要计算一个幺模矩阵 $\boldsymbol{U} \in \mathrm{GL}_m(\mathbb{Z})$ 使得 $\boldsymbol{A} \cdot \boldsymbol{U} = (\boldsymbol{0}, \boldsymbol{B})$.

幺模矩阵的随机生成 [C., Feng, Liu, Wu '21]

给定一个本原矩阵 $\boldsymbol{V} \in \mathbb{Z}^{k \times n}$，存在一个 Las Vegas 算法将 $\boldsymbol{V}$ 扩充为一个 $n \times n$ 的幺模矩阵 $\boldsymbol{U}$ 使得：

离散情形 (III)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

- 需要计算一个幺模矩阵 $\boldsymbol{U} \in \mathrm{GL}_m(\mathbb{Z})$ 使得 $\boldsymbol{A} \cdot \boldsymbol{U} = (\boldsymbol{0}, \boldsymbol{B})$.

幺模矩阵的随机生成 [C., Feng, Liu, Wu '21]

给定一个本原矩阵 $\boldsymbol{V} \in \mathbb{Z}^{k \times n}$，存在一个 Las Vegas 算法将 $\boldsymbol{V}$ 扩充为一个 $n \times n$ 的幺模矩阵 $\boldsymbol{U}$ 使得：

- 幺模矩阵规模：$\|\boldsymbol{U}\| \leq n^{O(1)} \|\boldsymbol{A}\|$，

离散情形 (III)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

- 需要计算一个幺模矩阵 $\boldsymbol{U} \in \mathrm{GL}_m(\mathbb{Z})$ 使得 $\boldsymbol{A} \cdot \boldsymbol{U} = (\boldsymbol{0}, \boldsymbol{B})$.

幺模矩阵的随机生成 [C., Feng, Liu, Wu '21]

给定一个本原矩阵 $\boldsymbol{V} \in \mathbb{Z}^{k \times n}$，存在一个 Las Vegas 算法将 $\boldsymbol{V}$ 扩充为一个 $n \times n$ 的幺模矩阵 $\boldsymbol{U}$ 使得：

- 幺模矩阵规模：$\|\boldsymbol{U}\| \leq n^{O(1)} \|\boldsymbol{A}\|$，
- 期望位复杂度：$O(n^{\omega+\varepsilon} \log^{1+\varepsilon} \|\boldsymbol{A}\|)$.

离散情形 (III)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

- 需要计算一个幺模矩阵 $\boldsymbol{U} \in \mathrm{GL}_m(\mathbb{Z})$ 使得 $\boldsymbol{A} \cdot \boldsymbol{U} = (\boldsymbol{0}, \boldsymbol{B})$.

幺模矩阵的随机生成 [C., Feng, Liu, Wu '21]

给定一个本原矩阵 $\boldsymbol{V} \in \mathbb{Z}^{k \times n}$，存在一个 Las Vegas 算法将 $\boldsymbol{V}$ 扩充为一个 $n \times n$ 的幺模矩阵 $\boldsymbol{U}$ 使得：

- 幺模矩阵规模：$\|\boldsymbol{U}\| \leq n^{O(1)} \|\boldsymbol{A}\|$，
- 期望位复杂度：$O(n^{\omega+\varepsilon} \log^{1+\varepsilon} \|\boldsymbol{A}\|)$.
- ⋆ 先前已知位复杂度：$O((n-k) n^{\omega+\varepsilon} \log^{1+\varepsilon} \|\boldsymbol{A}\|)$.

离散情形 (III)

格基计算问题

给定 $\boldsymbol{A} \in \mathbb{Z}^{n \times m}$，如何计算 $\Lambda = \langle \boldsymbol{A} \rangle$ 的一组基 $\boldsymbol{B}$?

- 需要计算一个幺模矩阵 $\boldsymbol{U} \in \mathrm{GL}_m(\mathbb{Z})$ 使得 $\boldsymbol{A} \cdot \boldsymbol{U} = (\boldsymbol{0}, \boldsymbol{B})$.

幺模矩阵的随机生成 [C., Feng, Liu, Wu '21]

给定一个本原矩阵 $\boldsymbol{V} \in \mathbb{Z}^{k \times n}$，存在一个 Las Vegas 算法将 $\boldsymbol{V}$ 扩充为一个 $n \times n$ 的幺模矩阵 $\boldsymbol{U}$ 使得：

- 幺模矩阵规模：$\|\boldsymbol{U}\| \leq n^{O(1)} \|\boldsymbol{A}\|$，
- 期望位复杂度：$O(n^{\omega+\varepsilon} \log^{1+\varepsilon} \|\boldsymbol{A}\|)$.
- ⋆ 先前已知位复杂度：$O((n-k) n^{\omega+\varepsilon} \log^{1+\varepsilon} \|\boldsymbol{A}\|)$.

公开问题一

- 如何将随机算法的思想融入格基计算的算法设计与分析?

提纲

1. 向量群分解问题
2. 离散情形
3. 非离散情形

向量群的分解问题

定理 (Siegel's book, Lec. VI, Th. 2.6)

设 G 是向量群. 则它的闭包 $\overline{G}$ 可被唯一分解为 $\overline{G} = \Lambda \oplus E$，其中

- Λ：格，被称作 G 的格分支；
- E：向量空间，E 的维数被称为 G 的局部秩；
- $\mathrm{Span}(\Lambda) \perp E$.

向量群的分解问题

给定向量群 G 的一组生成元，如何计算上述分解？特别地，

- 如何确定 G 的局部秩？
  - [Babai, et al. '88]：不可判定！
- 给定 G 的局部秩，如何得到 G 的格分支的一组基？
  - 局部秩为零：离散情形；
  - 局部秩非零：非离散情形.

向量群的对偶

设 G 是一个向量群. 定义 G 的对偶为如下集合：

$$G^{\vee} = \{\boldsymbol{x} \in \mathrm{Span}(G) : \forall \boldsymbol{y} \in G, \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}\}.$$

向量群的对偶

设 G 是一个向量群. 定义 G 的对偶为如下集合：

$$G^\vee = \{\boldsymbol{x} \in \mathrm{Span}(G) : \forall \boldsymbol{y} \in G, \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}\}.$$

- $G^\vee$ 是一个格.

向量群的对偶

设 G 是一个向量群. 定义 G 的对偶为如下集合：

$$G^\vee = \{x \in \mathrm{Span}(G) : \forall y \in G, \langle x, y\rangle \in \mathbb{Z}\}.$$

- $G^\vee$ 是一个格.
- 若 G 的闭包有唯一分解 $\overline{G} = \Lambda \oplus E$，则 $G^\vee = \Lambda^\vee$.

对偶和投影

向量群的对偶

设 G 是一个向量群. 定义 G 的对偶为如下集合：

$$G^\vee = \{x \in \mathrm{Span}(G) : \forall y \in G, \langle x, y\rangle \in \mathbb{Z}\}.$$

- $G^\vee$ 是一个格.
- 若 G 的闭包有唯一分解 $\overline{G} = \Lambda \oplus E$，则 $G^\vee = \Lambda^\vee$.

格到向量空间的正交投影

设 Λ 是格，E 是向量空间. 记 $\pi(\Lambda, E)$ 为 Λ 到 E 上的正交投影.

对偶和投影

向量群的对偶

设 G 是一个向量群. 定义 G 的对偶为如下集合：

$$G^\vee = \{x \in \mathrm{Span}(G) : \forall y \in G, \langle x, y\rangle \in \mathbb{Z}\}.$$

- $G^\vee$ 是一个格.
- 若 G 的闭包有唯一分解 $\overline{G} = \Lambda \oplus E$，则 $G^\vee = \Lambda^\vee$.

格到向量空间的正交投影

设 Λ 是格，E 是向量空间. 记 $\pi(\Lambda, E)$ 为 Λ 到 E 上的正交投影.

- $\pi(\Lambda, E)$ 是一个向量群.
- 对任意向量群 G 都存在格 Λ 和向量空间 E 使得 $G = \pi(\Lambda, E)$.

对偶和投影

向量群的对偶

设 G 是一个向量群. 定义 G 的对偶为如下集合：

$$G^\vee = \{x \in \mathrm{Span}(G) : \forall y \in G, \langle x, y\rangle \in \mathbb{Z}\}.$$

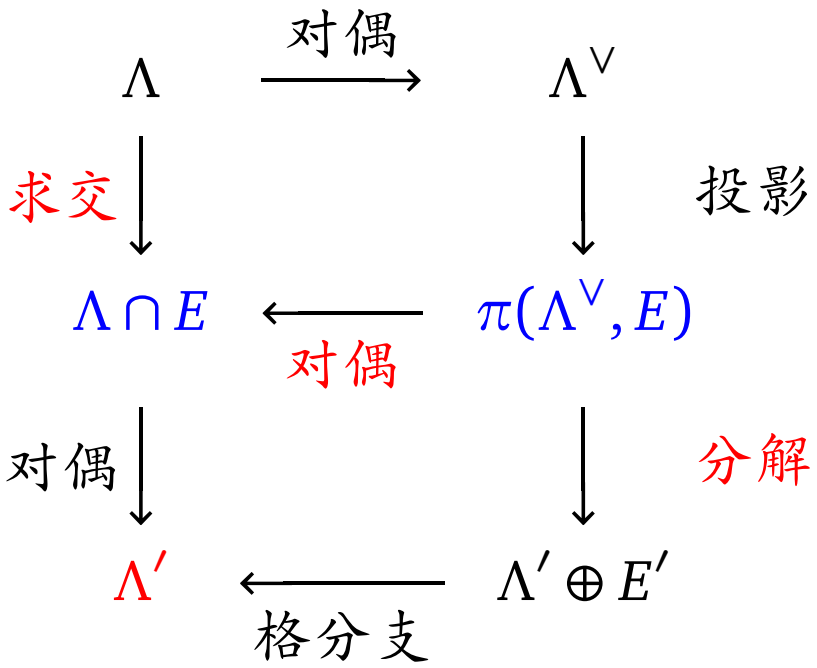
- $G^\vee$ 是一个格.
- 若 G 的闭包有唯一分解 $\overline{G} = \Lambda \oplus E$，则 $G^\vee = \Lambda^\vee$.

格到向量空间的正交投影

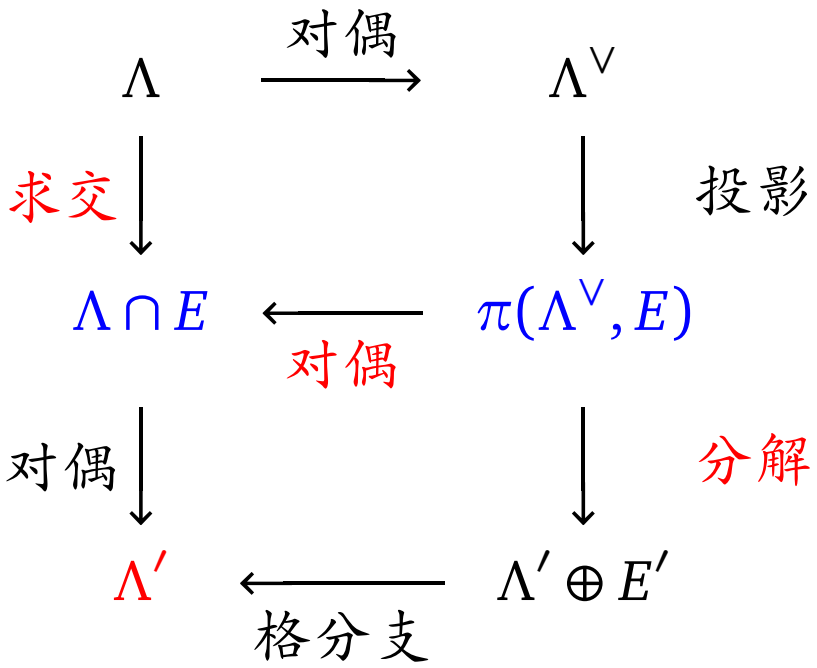
设 Λ 是格，E 是向量空间. 记 $\pi(\Lambda, E)$ 为 Λ 到 E 上的正交投影.

- $\pi(\Lambda, E)$ 是一个向量群.
- 对任意向量群 G 都存在格 Λ 和向量空间 E 使得 $G = \pi(\Lambda, E)$.
- 关键关系：$\pi(\Lambda^\vee, E)^\vee = \Lambda \cap E$.

分解与求交


对偶
Λ
$\Lambda^\vee$
求交
投影
$\Lambda \cap E$
$\pi(\Lambda^\vee, E)$
对偶
对偶
分解
Λ'
$\Lambda' \oplus E'$
格分支

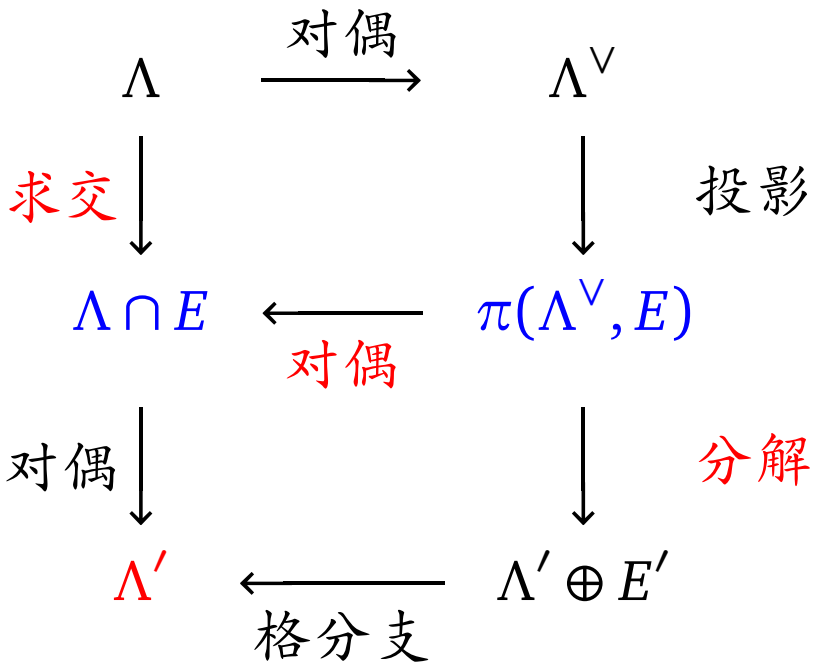
分解与求交



通过格与向量空间的交分解向量群 [C., Stehlé, Villard '13]

- 方法：整数关系探测 (HJLS、PSLQ 算法等)
  - 被 SIAM 评为“二十世纪十大算法”之一.

分解与求交



通过格与向量空间的交分解向量群 [C., Stehlé, Villard '13]

- 方法：整数关系探测 (HJLS、PSLQ 算法等)
  - 被 SIAM 评为"二十世纪十大算法"之一.
- 问题 1: 算法复杂度分析是在精确实数计算模型下完成的.
- 问题 2: 算法分析方法或可进一步优化.

PSLQ 算法的数值稳定性分析

PSLQ 算法：输入：$\boldsymbol{x} \in \mathbb{R}^n$；输出：$\boldsymbol{m} \in \mathbb{Z}^n \cap \boldsymbol{x}^{\perp}$.

- 提取向量群 $\pi(\mathbb{Z}^n, \boldsymbol{x}^{\perp})$ 的一组生成元，其矩阵记为 $\boldsymbol{H}_x$.
- 以 $\boldsymbol{H}_x$ 为输入，计算 $\pi(\mathbb{Z}^n, \boldsymbol{x}^{\perp})$ 的格分支.

PSLQ 算法的数值稳定性分析

PSLQ 算法：输入：$\boldsymbol{x} \in \mathbb{R}^n$；输出：$\boldsymbol{m} \in \mathbb{Z}^n \cap \boldsymbol{x}^\perp$.

- 提取向量群 $\pi(\mathbb{Z}^n, \boldsymbol{x}^\perp)$ 的一组生成元，其矩阵记为 $\boldsymbol{H}_x$.
- 以 $\boldsymbol{H}_x$ 为输入，计算 $\pi(\mathbb{Z}^n, \boldsymbol{x}^\perp)$ 的格分支.

扰动理论 [Feng, C., Wu '19]

对 $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$，若

- $\boldsymbol{H}_x \in \mathbb{R}^{n \times (n-1)}$：下梯形，行构成 $\pi(\mathbb{Z}^n, \boldsymbol{x}^\perp)$ 的一组生成元，
- $\overline{\boldsymbol{H}_x} \in \mathbb{R}^{n \times (n-1)}$：$\|\boldsymbol{H}_x - \overline{\boldsymbol{H}_x}\|_F < \varepsilon_1$，
- $\boldsymbol{H} = \boldsymbol{U}\overline{\boldsymbol{H}_x}\boldsymbol{Q}$：$\boldsymbol{H}$ 下梯形，$\boldsymbol{U}$ 幺模，$\boldsymbol{Q}$ 正交，$|h_{n,n-1}| < \varepsilon_2$，
- $\boldsymbol{m}$ 是 $\boldsymbol{U}^{-1}$ 的第 $(n-1)$ 列，则存在 C 使得

$$|\langle \boldsymbol{x}, \boldsymbol{m} \rangle| < C \cdot (\|\boldsymbol{m}\|_2 \cdot \varepsilon_1 + x_n \varepsilon_2).$$

PSLQ 算法的数值稳定性分析

PSLQ 算法：输入：$\boldsymbol{x} \in \mathbb{R}^n$；输出：$\boldsymbol{m} \in \mathbb{Z}^n \cap \boldsymbol{x}^\perp$.

- 提取向量群 $\pi(\mathbb{Z}^n, \boldsymbol{x}^\perp)$ 的一组生成元，其矩阵记为 $\boldsymbol{H}_x$.
- 以 $\boldsymbol{H}_x$ 为输入，计算 $\pi(\mathbb{Z}^n, \boldsymbol{x}^\perp)$ 的格分支.

扰动理论 [Feng, C., Wu '19]

对 $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$，若

- $\boldsymbol{H}_x \in \mathbb{R}^{n\times(n-1)}$：下梯形，行构成 $\pi(\mathbb{Z}^n, \boldsymbol{x}^\perp)$ 的一组生成元，
- $\overline{\boldsymbol{H}_x} \in \mathbb{R}^{n\times(n-1)}$：$\|\boldsymbol{H}_x - \overline{\boldsymbol{H}_x}\|_F < \varepsilon_1$，
- $\boldsymbol{H} = \boldsymbol{U}\overline{\boldsymbol{H}_x}\boldsymbol{Q}$：$\boldsymbol{H}$ 下梯形，$\boldsymbol{U}$ 幺模，$\boldsymbol{Q}$ 正交，$|h_{n,n-1}| < \varepsilon_2$，
- $\boldsymbol{m}$ 是 $\boldsymbol{U}^{-1}$ 的第 $(n-1)$ 列，则存在 C 使得

$$|\langle \boldsymbol{x}, \boldsymbol{m} \rangle| < C \cdot (\|\boldsymbol{m}\|_2 \cdot \varepsilon_1 + x_n \varepsilon_2).$$

公开问题二

- 如何基于上述分析设计高效的向量群分解的符合数值算法？

PSLQ 算法迭代次数分析

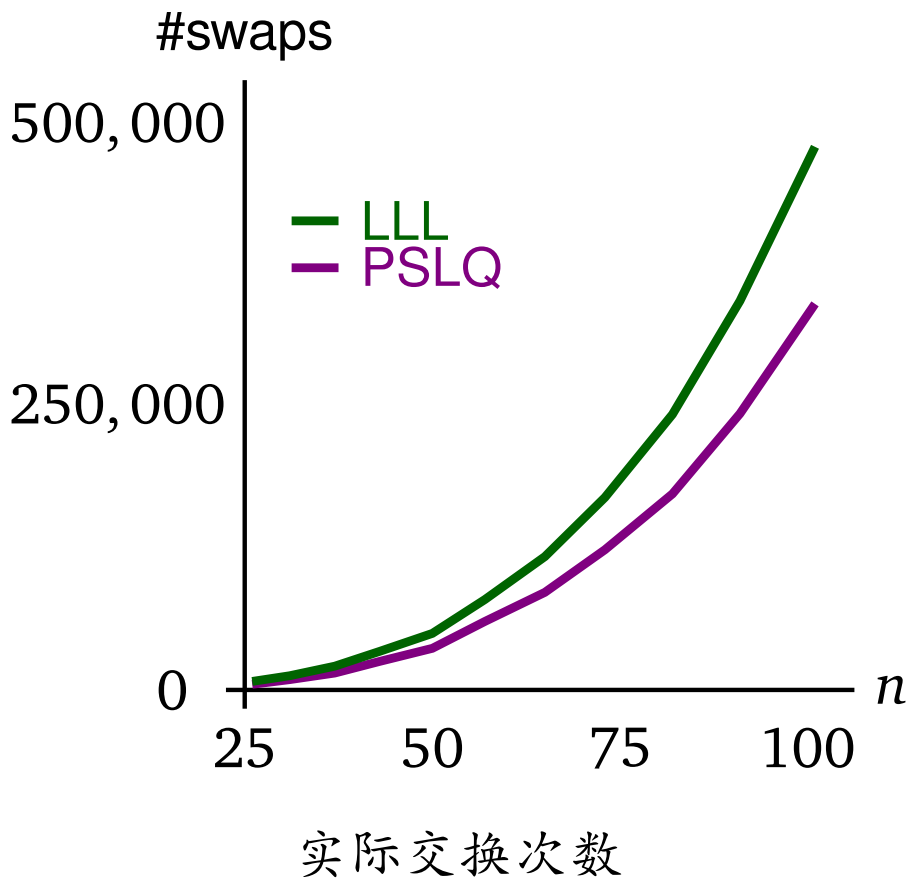
LLL vs PSLQ (当 $\boldsymbol{x} \in \mathbb{Z}^n$ 时)

- 交换规则：Lovász 交换 vs Bergman 交换 (局部vs 全局)
- 理论交换次数：$O(n + n\log\|\boldsymbol{x}\|)$ vs $O(n^2(n + \log\|\boldsymbol{x}\|))$

PSLQ 算法迭代次数分析

LLL vs PSLQ (当 $\boldsymbol{x} \in \mathbb{Z}^n$ 时)

- 交换规则：Lovász 交换 vs Bergman 交换 (局部vs 全局)
- 理论交换次数：$O(n + n\log\|\boldsymbol{x}\|)$ vs $O(n^2(n + \log\|\boldsymbol{x}\|))$



$x \mapsto Ax + b$

- 若 $I - A$ 可逆，则存在不动点 $x^* = (I - A)^{-1} b$.
- 令 $x = x^* + e$. 则该系统可被重写为 $e \mapsto Ae$.
- 若 $\|A\|_p \leq 1 - \delta$，则运行该系统 t 次后 $\|A^t e\|_p \leq \mathrm{e}^{-\delta \cdot t} \|e\|_p$.
- 若考虑坐标变换 $y = Dx$，D 可逆且 $\|DAD^{-1}\|_p \leq 1 - \varepsilon$，则

$$\|A^t e\|_p \leq \mathrm{e}^{-\delta \cdot t} \kappa_p(D) \|e\|_p, \quad \kappa_p(D) = \|D\|_p \cdot \|D^{-1}\|_p.$$

$x \mapsto Ax + b$

- 若 $I - A$ 可逆，则存在不动点 $x^* = (I - A)^{-1} b$.
- 令 $x = x^* + e$. 则该系统可被重写为 $e \mapsto Ae$.
- 若 $\|A\|_p \leq 1 - \delta$，则运行该系统 t 次后 $\|A^t e\|_p \leq \mathrm{e}^{-\delta \cdot t} \|e\|_p$.
- 若考虑坐标变换 $y = Dx$，D 可逆且 $\|DAD^{-1}\|_p \leq 1 - \varepsilon$，则

$$\|A^t e\|_p \leq \mathrm{e}^{-\delta \cdot t} \kappa_p(D) \|e\|_p, \quad \kappa_p(D) = \|D\|_p \cdot \|D^{-1}\|_p.$$

- 为使 $\|A^t e\|_p < \varepsilon$，仅需迭代次数 t 满足

$$t \geq \frac{1}{\delta} \left(\ln \frac{1}{\varepsilon} + \ln \kappa_p(D) + \ln \|e\|_p \right).$$

PSLQ 算法迭代的动力系统分析 [C., Feng, Liu, Wu '23]

- 从 PSLQ 算法迭代提取动力系统模型 $\boldsymbol{z} \mapsto \boldsymbol{A}\boldsymbol{z} + \boldsymbol{b}$，其中

$$a_{i,j} = \begin{cases} 2^{j-i-2} & 1 \le j \le i+1 \le n, \\ 0 & \text{其他}, \end{cases}$$

$$\boldsymbol{b} = (0, \ldots, 0, -1/2) \in \mathbb{Q}^{n-3}.$$

PSLQ 算法迭代的动力系统分析 [C., Feng, Liu, Wu '23]

- 从 PSLQ 算法迭代提取动力系统模型 $\boldsymbol{z} \mapsto \boldsymbol{A}\boldsymbol{z} + \boldsymbol{b}$，其中

$$a_{i,j} = \begin{cases} 2^{j-i-2} & 1 \le j \le i+1 \le n, \\ 0 & \text{其他}, \end{cases}$$

$$\boldsymbol{b} = (0, \ldots, 0, -1/2) \in \mathbb{Q}^{n-3}.$$

- 该系统的不动点为：$\boldsymbol{z}^* = (z_i^*)_{i \le n-3}$，$x_i^* = -\dfrac{i+1}{n-1}$.

PSLQ 算法迭代的动力系统分析 [C., Feng, Liu, Wu '23]

- 从 PSLQ 算法迭代提取动力系统模型 $\boldsymbol{z} \mapsto \boldsymbol{A}\boldsymbol{z} + \boldsymbol{b}$，其中

$$a_{i,j} = \begin{cases} 2^{j-i-2} & 1 \le j \le i+1 \le n, \\ 0 & \text{其他}, \end{cases}$$

$$\boldsymbol{b} = (0, \ldots, 0, -1/2) \in \mathbb{Q}^{n-3}.$$

- 该系统的不动点为：$\boldsymbol{z}^* = (z_i^*)_{i \le n-3}$，$x_i^* = -\dfrac{i+1}{n-1}$.
- 引入变换矩阵 $\boldsymbol{D} = \mathrm{diag}\left((n-1)/((i+1)(n-i-2))\right)_{i \le n-3}$ 后

$$\|\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^{-1}\|_\infty \le 1 - \left(1 + \frac{n^2}{8}\right)^{-1}.$$

PSLQ 算法迭代的动力系统分析 [C., Feng, Liu, Wu '23]

- 从 PSLQ 算法迭代提取动力系统模型 $\boldsymbol{z} \mapsto \boldsymbol{A}\boldsymbol{z} + \boldsymbol{b}$，其中

$$a_{i,j} = \begin{cases} 2^{j-i-2} & 1 \le j \le i+1 \le n, \\ 0 & \text{其他}, \end{cases}$$

$$\boldsymbol{b} = (0, \ldots, 0, -1/2) \in \mathbb{Q}^{n-3}.$$

- 该系统的不动点为：$\boldsymbol{z}^* = (z_i^*)_{i \le n-3}$，$x_i^* = -\dfrac{i+1}{n-1}$.
- 引入变换矩阵 $\boldsymbol{D} = \mathrm{diag}\left((n-1)/((i+1)(n-i-2))\right)_{i \le n-3}$ 后

$$\|\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^{-1}\|_\infty \le 1 - \left(1 + \frac{n^2}{8}\right)^{-1}.$$

- 迭代次数：$t \ge \left(1 + \dfrac{n^2}{8}\right) \cdot \left(\ln \dfrac{1}{\varepsilon} + \ln\left(\dfrac{(n-1)^2}{4(n-2)} \|\boldsymbol{e}\|_\infty\right)\right)$.

PSLQ 算法迭代的动力系统分析 [C., Feng, Liu, Wu '23]

- 从 PSLQ 算法迭代提取动力系统模型 $\boldsymbol{z} \mapsto \boldsymbol{A}\boldsymbol{z} + \boldsymbol{b}$，其中

$$a_{i,j} = \begin{cases} 2^{j-i-2} & 1 \le j \le i+1 \le n, \\ 0 & \text{其他}, \end{cases}$$

$$\boldsymbol{b} = (0, \ldots, 0, -1/2) \in \mathbb{Q}^{n-3}.$$

- 该系统的不动点为：$\boldsymbol{z}^* = (z_i^*)_{i \le n-3}$，$x_i^* = -\dfrac{i+1}{n-1}$.
- 引入变换矩阵 $\boldsymbol{D} = \mathrm{diag}\left((n-1)/((i+1)(n-i-2))\right)_{i \le n-3}$ 后

$$\|\boldsymbol{D}\boldsymbol{A}\boldsymbol{D}^{-1}\|_\infty \le 1 - \left(1 + \frac{n^2}{8}\right)^{-1}.$$

- 迭代次数：$t \ge \left(1 + \dfrac{n^2}{8}\right) \cdot \left(\ln \dfrac{1}{\varepsilon} + \ln\left(\dfrac{(n-1)^2}{4(n-2)} \|\boldsymbol{e}\|_\infty\right)\right)$.

公开问题三

- 能否将上述分析方法应用于高效向量群分解的算法设计？

总结

- 向量群的定义、性质和向量群分解问题
- 离散向量群分解 $\Leftrightarrow$ 格基计算
- 非离散向量群分解 $\Leftrightarrow$ 格与向量空间求交
- 几个公开问题

总结

- 向量群的定义、性质和向量群分解问题
- 离散向量群分解 $\Leftrightarrow$ 格基计算
- 非离散向量群分解 $\Leftrightarrow$ 格与向量空间求交
- 几个公开问题
- 未涉及：代数向量群及其分解

总结

- 向量群的定义、性质和向量群分解问题
- 离散向量群分解 $\Leftrightarrow$ 格基计算
- 非离散向量群分解 $\Leftrightarrow$ 格与向量空间求交
- 几个公开问题
- 未涉及：代数向量群及其分解