Pure Mathematics 理论数学, 2024, 14(1), 341-346
Published Online January 2024 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2024.141035

Hans汉斯

$\mathbb{S}_{max}$上2 × 2拟可逆矩阵的研究

张利萍[1]，苏　瑞[2]，李思璋[1]

[1]云南财经大学，统计与数学学院，云南　昆明
[2]武汉生物工程学院，计算机科学与技术学院，湖北　武汉

收稿日期：2023年12月1日；录用日期：2023年12月14日；发布日期：2024年1月31日

摘　要

矩阵作为代数中常见的工具，与方程组、线性变换密切相关。本文将对对称max-plus半环$\mathbb{S}_{max}$上的二阶矩阵的结构进行研究，并对系数矩阵拟可逆的二元一次方程解进行讨论。

关键词

热带半环，热带矩阵，拟可逆

Study on 2 × 2 Quasi-Invertible Matrices over $\mathbb{S}_{max}$

Liping Zhang[1], Rui Su[2], Sizhuo Li[1]

[1]School of Statistics and Mathematics, Yunnan University of Finance and Economics, Kunming Yunnan
[2]School of Computer Science and Technology, Wuhan University of Bioengineering, Wuhan Hubei

Received: Dec. 1st, 2023; accepted: Dec. 14th, 2023; published: Jan. 31st, 2024

Abstract

As a common tool in algebra, matrix is closely related to equations and linear transformations. In this paper, the structure of 2 × 2 matrix on symmetric max-plus semiring $\mathbb{S}_{max}$ is studied, and the solutions of bivariate first order equations with quasi-invertible coefficient matrix are discussed.

Keywords

Tropical Semiring, Tropical Matrix, Quasi-Invertible

文章引用: 张利萍, 苏瑞, 李思璋. $\mathbb{S}_{max}$上2 × 2拟可逆矩阵的研究[J]. 理论数学, 2024, 14(1): 341-346.
DOI: 10.12677/pm.2024.141035

1. 引言

热带几何是一种建立在热带半环 $\mathbb{R}$ 上的几何。热带半环是具有加法 $\oplus$ 和乘法 $\otimes$ 两种运算的集合 $\mathbb{R}_{\max} := \mathbb{R} \cup \{-\infty\}$，其中加法为取最大，乘法为取加法。热带几何最初是在 20 世纪末的初期出现的，但围绕这个主题的基本定理和定义的整合在 90 年代才开始真正地出现。1990 年，为解决热带中的加法不可逆，Max Plus 引入 balance，将热带推广到对称 max-plus 半环 $\mathbb{S}_{\max}$ 上[1]。随后在 1992 年，Francois Baccelli 在对称 max-plus 半环中对矩阵的结构进行了推广和研究[2]。2014 年，Pascal Benchimol 建立了多面体基本点和边的热带对应概念，产生了单纯形法热带化的几何解释，并将经典线性规划的复杂度转化为热带线性规划[3]。

热带几何是一个强大的工具，因为它允许我们用线性、组合的方式分析固有的非线性问题。一般策略是先将经典非线性系统转换为热带线性系统，然后使用热带线性代数的方法来提供原始系统的信息[4]。由于在应用领域中出现的许多问题都是自然地用热带线性方程表示的，作为热带线性代数应用的直接结果，热带半环上的矩阵自 20 世纪 60 年代以来一直是积极研究的主题。在 2018 年，Zhang 首次使用热带矩阵半环作为平台来构造密码系统，提出了基于热带矩阵的公钥密码体制[5]。之后 Grigoreiv 等人进行了改进，提出了基于热带矩阵半环的半直积的公钥密码体制[6]。对此，2022 年黄华伟和李春华提出了一种攻击方法[7]，其中离不开 2×2 矩阵。

本文先对对称 max-plus 半环 $\mathbb{S}_{\max}$ 上的 2×2 矩阵的结构进行研究，得到 2×2 矩阵拟可逆的条件；再对系数矩阵拟可逆的二元一次方程解进行讨论，得出在 $A^{adj}b$ 非符号的情况下，方程 $AX \Delta b$ 的解与 $(\det A)X \Delta A^{adj}b$ 的解并不等价。

2. 预备知识

定义 1 [8]热带半环 $\mathbb{R}_{\max}$ 指在 $\mathbb{R} \cup \{-\infty\}$ 上，对于任意 $a,b \in \mathbb{R}_{\max}$，定义加法 $\oplus$ 和乘法 $\otimes$ 如下：

$$a \oplus b = \max\{a,b\}; a \otimes b = a + b.$$

显然，0 是 $\otimes$ 上的单位元；$\varepsilon := -\infty$ 是 $\oplus$ 上的零元。

性质 1 [1]对于任意 $a,b,c \in \mathbb{R}_{\max}$，有：

1) $a \otimes b = b \otimes a$;
2) $a \oplus b = b \oplus a$;
3) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$;
4) $(a \otimes b) \otimes c = a \otimes (b \otimes c)$;
5) $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

考虑基于 Dioid 结构下的 $\mathbb{R}_{\max}^2$ 代数，对于 $(x',x''),(y',y'') \in \mathbb{R}_{\max}^2$，

$$(x',x'') \oplus (y',y'') := (x' \oplus y', x'' \oplus y''),$$

$$(x',x'') \otimes (y',y'') := (x'y' \oplus x''y'', x'y'' \oplus x''y').$$

显然，$(0,\varepsilon)$ 是 $\otimes$ 上的单位元；$(\varepsilon,\varepsilon)$ 是 $\oplus$ 上的零元。

定义 2 [1]设 $x = (x',x'') \in \mathbb{R}_{\max}^2$，定义

$$\ominus x := (x'', x');$$

$$|x| := x' \oplus x'';$$

$$x^{\cdot} := (|x|, |x|).$$

性质 2 [1]对于任意 $a,b \in \mathbb{R}_{\max}^2$， $a \neq b$，有：

1) $a^{\cdot} = (\ominus a)^{\cdot}$;
2) $(a^{\cdot})^{\cdot} = a^{\cdot}$;
3) $a \otimes b^{\cdot} = (a \otimes b)^{\cdot}$;
4) $\ominus(\ominus a) = a$;
5) $\ominus(a \oplus b) = (\ominus a) \oplus (\ominus b)$;
6) $\ominus(a \otimes b) = (\ominus a) \otimes b = a \otimes (\ominus b)$;
7) $(\ominus a) \otimes (\ominus b) = a \otimes b$.

特别的，$a \ominus b = a \oplus (\ominus b)$。

定义 3 [1]设 $x = (x', x''), y = (y', y'') \in \mathbb{R}_{\max}^2$，若 $x' \oplus y'' = x'' \oplus y'$，称 $x \Delta y$。

特别地，Δ 不具有传递性，不是等价关系，我们考虑 $\mathbb{R}_{\max}^2$ 上的 $\mathcal{R}$ 关系：

$$x \mathcal{R} y \Leftrightarrow \begin{cases} x' \oplus y'' = x'' \oplus y', & \text{若 } x' \neq x'' \text{ 或 } y' \neq y'', \\ (x', x'') = (y', y''), & \text{其他情况.} \end{cases}$$

可以验证，$\mathcal{R}$ 关系是 $\mathbb{R}_{\max}^2$ 上的一种等价关系。

定义 4 [1]记 $\mathbb{S}_{\max} := \mathbb{R}_{\max}^2 / \mathcal{R}$，称为对称 max-plus 半环。对 $a,b \in \mathbb{R}_{\max}^2$，记 $\overline{(a,b)}$ 为 (a,b) 所在的等价类。

性质 3 [1]对 $t \in \mathbb{R}_{\max}$，如下结论成立：

$$\overline{(t, \varepsilon)} = \{(t, x''); x'' < t\};$$

$$\overline{(\varepsilon, t)} = \{(x', t); x' < t\};$$

$$\overline{(t,t)} = \{t^{\cdot} = (t,t)\}.$$

记

$$\mathbb{R}_{\max}^{\oplus} := \{\overline{(t, \varepsilon)} \mid t \in \mathbb{R}_{\max}\};$$

$$\mathbb{R}_{\max}^{\ominus} := \{\overline{(\varepsilon, t)} \mid t \in \mathbb{R}_{\max}\};$$

$$\mathbb{R}_{\max}^{\cdot} := \{\overline{(t,t)} \mid t \in \mathbb{R}_{\max}\}.$$

显然，$\mathbb{S}_{\max} = \mathbb{R}_{\max}^{\oplus} \cup \mathbb{R}_{\max}^{\ominus} \cup \mathbb{R}_{\max}^{\cdot}$，$\mathbb{R}_{\max}^{\oplus} \cap \mathbb{R}_{\max}^{\ominus} \cap \mathbb{R}_{\max}^{\cdot} = \{(\varepsilon, \varepsilon)\}$。特别地，映射 $\mathbb{R}_{\max} \to \mathbb{R}_{\max}^{\oplus}$：$a \mapsto \overline{(a, \varepsilon)}$ 定义了 $\mathbb{R}_{\max}$ 到 $\mathbb{R}_{\max}^{\oplus}$ 的同构映射。为方便起见，后面将用 $\mathbb{R}_{\max}$ 表示 $\mathbb{R}_{\max}^{\oplus}$。另外，对任意 $s \in \mathbb{R}_{\max}$，都有 $|s| = |\ominus s| = |s^{\cdot}| = s \in \mathbb{R}_{\max}$。

易验证，对于任意 $a,b \in \mathbb{S}_{\max}$，有

$$a \oplus b = \begin{cases} a, & \text{若 } |a| > |b| \text{ 或 } a = b; \\ b, & \text{若 } |a| < |b|; \\ |a|^{\cdot}, & \text{若 } |a| = |b| \text{ 且 } a \neq b. \end{cases}$$

性质 4 [1]记 $\mathbb{R}_{\max}^{\vee} := \mathbb{R}_{\max}^{\oplus} \cup \mathbb{R}_{\max}^{\ominus}$，有 $\mathbb{R}_{\max}^{\vee} \setminus \{\varepsilon\} = \mathbb{S}_{\max} \setminus \mathbb{R}_{\max}^{\cdot}$。若 $a \in \mathbb{R}_{\max}^{\vee}$，称 a 是符号的。

定义 4 [1]设 n 阶矩阵 $A\in Mat_{n\times n}\left(\mathbb{S}_{\max}\right)$，$A$ 的行列式为

$$\det A=\oplus_{\sigma}\operatorname{sgn}(\sigma)\otimes_{i=1}^{n}a_{i\sigma(i)},$$

其中 σ 是一种排列。当 σ 为奇排列时，$\operatorname{sgn}(\sigma)=\ominus 0$；当 σ 为偶排列时，$\operatorname{sgn}(\sigma)=0$。

定义 5 设矩阵 $A\in Mat_{n\times n}\left(\mathbb{S}_{\max}\right)$，若 $\det A\notin\mathbb{R}_{\max}^{\cdot}$，则称 A 是拟可逆的，否则称 A 是非拟可逆的。

3. 2 × 2 拟可逆矩阵

性质 5 矩阵 $\begin{bmatrix}a & b\\ c & d\end{bmatrix}\in Mat_{2\times 2}\left(\mathbb{S}_{\max}\right)$ 拟可逆当且仅当下列条件之一成立：

(i) $|ad|>|bc|$ 且 $a,d\notin\mathbb{R}_{\max}^{\cdot}$，

(ii) $|ad|<|bc|$ 且 $b,c\notin\mathbb{R}_{\max}^{\cdot}$，

(iii) $|ad|=|bc|$，$a,b,c,d\notin\mathbb{R}_{\max}^{\cdot}$ 且 $ad=\ominus bc$。

证明 对任意矩阵 $A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$，行列式 $\det A=ad\ominus bc$，有以下三种情况：

1) 当 $|ad|>|bc|$ 时，$\det A=ad$，

(i) 若 a,d 至少有一个属于 $\mathbb{R}_{\max}^{\cdot}$，$\det A=ad\in\mathbb{R}_{\max}^{\cdot}$，$A$ 非拟可逆；

(ii) 若 a,d 都不属于 $\mathbb{R}_{\max}^{\cdot}$，$\det A=ad\notin\mathbb{R}_{\max}^{\cdot}$，$A$ 拟可逆。

2) 当 $|ad|<|bc|$ 时，$\det A=\ominus bc$，

(i) 若 b,c 至少有一个属于 $\mathbb{R}_{\max}^{\cdot}$，$\det A=\ominus bc\in\mathbb{R}_{\max}^{\cdot}$，$A$ 非拟可逆；

(ii) 若 b,c 都不属于 $\mathbb{R}_{\max}^{\cdot}$，$\det A=\ominus bc\notin\mathbb{R}_{\max}^{\cdot}$，$A$ 拟可逆。

3) 当 $|ad|=|bc|$ 时，

(i) 若 a,b,c,d 中至少有一个属于 $\mathbb{R}_{\max}^{\cdot}$，由性质 2，$\det A\in\mathbb{R}_{\max}^{\cdot}$，$A$ 非拟可逆；

(ii) 若 a,b,c,d 中全不属于 $\mathbb{R}_{\max}^{\cdot}$，

若 a,b,c,d 全属于 $\mathbb{R}_{\max}^{\ominus}$，即 $ad=bc$，$\det A=ad\ominus bc\in\mathbb{R}_{\max}^{\cdot}$，$A$ 非拟可逆；

若 a,b,c,d 中有三个属于 $\mathbb{R}_{\max}^{\ominus}$，即 $ad=\ominus bc$，$\det A=ad=\ominus bc\notin\mathbb{R}_{\max}^{\cdot}$，$A$ 拟可逆；

若 a,b,c,d 中有两个属于 $\mathbb{R}_{\max}^{\ominus}$，即 $ad=bc$，$\det A\in\mathbb{R}_{\max}^{\cdot}$，$A$ 非拟可逆；

若 a,b,c,d 中有一个属于 $\mathbb{R}_{\max}^{\ominus}$，即 $ad=\ominus bc$，$\det A\notin\mathbb{R}_{\max}^{\cdot}$，$A$ 拟可逆；

若 a,b,c,d 全属于 $\mathbb{R}_{\max}$，即 $ad=\ominus bc$，$\det A\in\mathbb{R}_{\max}^{\cdot}$，$A$ 非拟可逆。

综上所述，性质成立。

例 1

1) $\begin{vmatrix}5 & 2\\ 3^{\cdot} & \ominus 1\end{vmatrix}=5\otimes\ominus 1\ominus 2\otimes 3^{\cdot}=\ominus 6\notin\mathbb{R}_{\max}^{\cdot}$，矩阵拟可逆，此时 $|5\otimes 1|>|2\otimes 3|$ 且 $5,\ominus 1\notin\mathbb{R}_{\max}^{\cdot}$，符合条件(i)；

2) $\begin{vmatrix}1^{\cdot} & 2\\ 7 & \ominus 3\end{vmatrix}=1^{\cdot}\otimes\ominus 3\ominus 2\otimes 7=\ominus 9\notin\mathbb{R}_{\max}^{\cdot}$，矩阵拟可逆，此时 $|7\otimes 2|>|1\otimes 3|$ 且 $7,2\notin\mathbb{R}_{\max}^{\cdot}$，符合条件(ii)；

3) $\begin{vmatrix}3 & 6\\ 4 & \ominus 7\end{vmatrix}=3\otimes\ominus 7\ominus 4\otimes 6=\ominus 10\notin\mathbb{R}_{\max}^{\cdot}$，矩阵拟可逆，此时 $|7\otimes 3|=|4\otimes 6|$，$3,6,4,\ominus 7\notin\mathbb{R}_{\max}^{\cdot}$ 且 $3\otimes\ominus 7=\ominus 4\otimes 6$，符合条件(iii)；

4) $\begin{vmatrix}5 & 6\\ 6 & 7\end{vmatrix}=5\otimes 7\ominus 6\otimes 6=12^{\cdot}\in\mathbb{R}_{\max}^{\cdot}$，矩阵非拟可逆，此时 $|5\otimes 7|=|6\otimes 6|$，$5,6,7\notin\mathbb{R}_{\max}^{\cdot}$，但 $5\otimes 7\neq\ominus 6\otimes 6$，不符合任一个条件。

4. 系数矩阵拟可逆的二元一次方程解

对于二元一次方程组

$$AX \Delta b,$$

其中，$A=\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$，$b=\begin{bmatrix} e \\ f \end{bmatrix}$，$X=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$。

1) 若 A 拟可逆(即 $\det A \notin \mathbb{R}_{\max}^{\cdot}$)，$A^{adj}b$ 是符号的(即 $A^{adj}b \in \mathbb{R}_{\max}^{\vee}$)，对于方程 $AX \Delta b$，左乘 A^{adj}，有 $A^{adj}AX \Delta A^{adj}b$，由 $A^{adj}A \Delta \det A \cdot I$，得 $(\det A)X \Delta A^{adj}b$。即 Cramer 法则[1]，方程 $AX \Delta b$ 有唯一符号解

$$X=(\det A)^{-1}A^{adj}b.$$

2) 若 A 拟可逆，$A^{adj}b$ 非符号的，此时方程 $AX \Delta b$ 与方程 $(\det A)X \Delta A^{adj}b$ 的解并不等价。

例 2 对方程

$$\begin{cases} 5x \oplus 1y \Delta 0 \\ 2x \oplus 5y \Delta 4 \end{cases}.$$

解 $\det A=\begin{vmatrix} 5 & 1 \\ 2 & 5 \end{vmatrix}=10 \notin \mathbb{R}_{\max}^{\cdot}$，

对于

$$(\det A)X \Delta A^{adj}b \to 10\begin{bmatrix} x \\ y \end{bmatrix} \Delta \begin{bmatrix} 5 & \ominus 1 \\ \ominus 2 & 5 \end{bmatrix}\begin{bmatrix} 0 \\ 4 \end{bmatrix} \to 10\begin{bmatrix} x \\ y \end{bmatrix} \Delta \begin{bmatrix} 5^{\cdot} \\ 9 \end{bmatrix},$$

方程有解 $\begin{cases} x=t, t \in \mathbb{R}_{\max}^{\cdot} \\ y=-1 \end{cases}$。取一组解 $\begin{cases} x=1^{\cdot} \\ y=-1 \end{cases}$ 带入方程 $\begin{cases} 5x \oplus 1y \Delta 0 \\ 2x \oplus 5y \Delta 4 \end{cases}$，有

$$\begin{cases} 5 \otimes 1^{\cdot} \oplus 1 \otimes (-1) \Delta 6^{\cdot} \\ 2 \otimes 1^{\cdot} \oplus 5 \otimes (-1) \Delta 4 \end{cases},$$

不成立。

而方程的解为

$$\begin{cases} x=t, |t|<-5, t \in \mathbb{S}_{\max} \text{ 或 } x=-5 \\ y=-1 \end{cases},$$

两者解集有交集。

例 3 对方程

$$\begin{cases} 3x \oplus 4y \Delta 2^{\cdot} \\ 1^{\cdot}x \oplus \ominus 3y \Delta 0 \end{cases}.$$

解 由 $\begin{vmatrix} 3 & 4 \\ 1^{\cdot} & \ominus 3 \end{vmatrix}=\ominus 6 \notin \mathbb{R}_{\max}^{\cdot}$，

对于方程

$$(\det A)X \Delta A^{adj}b \to \ominus 6\begin{bmatrix} x \\ y \end{bmatrix} \Delta \begin{bmatrix} \ominus 3 & \ominus 4 \\ 1^{\cdot} & 3 \end{bmatrix}\begin{bmatrix} 2^{\cdot} \\ 0 \end{bmatrix} \to \ominus 6\begin{bmatrix} x \\ y \end{bmatrix} \Delta \begin{bmatrix} 5^{\cdot} \\ 3^{\cdot} \end{bmatrix},$$

方程只有 $\mathbb{R}_{\max}^{\cdot}$ 解，解为 $\{x \mid x \in \mathbb{R}_{\max}^{\cdot}\}$，$\{y \mid y \in \mathbb{R}_{\max}^{\cdot}\}$。但这并不是方程 $\begin{cases} 3x \oplus 4y \Delta 2^{\cdot} \\ 1^{\cdot}x \oplus \ominus 3y \Delta 0 \end{cases}$ 的解，取一组解

$\begin{cases} x=1^{\cdot} \\ y=0^{\cdot} \end{cases}$ 带入，有

$$\begin{cases} 3\otimes 1^{\cdot}\oplus 4\otimes 0^{\cdot}\,\Delta\, 4^{\cdot} \\ 1^{\cdot}\otimes 1^{\cdot}\oplus\ominus 3\otimes 0^{\cdot}\,\Delta\, 3^{\cdot} \end{cases},$$

不成立。而方程 $\begin{cases} 3x\oplus 4y\,\Delta\, 2^{\cdot} \\ 1^{\cdot}x\oplus\ominus 3y\,\Delta\, 0 \end{cases}$ 无解。

对于二元一次方程组 $AX\,\Delta\, b$，若 A 拟可逆，$A^{adj}b$ 符号，那么方程 $AX\,\Delta\, b$ 的解与 $(\det A)X\,\Delta\, A^{adj}b$ 的解等价，且有唯一符号解 $X=(\det A)^{-1}A^{adj}b$；而 $A^{adj}b$ 非符号时，方程 $AX\,\Delta\, b$ 的解与 $(\det A)X\,\Delta\, A^{adj}b$ 的解并不等价，且两者解暂无关系，这就需要进一步讨论“Δ”的相关性质及传递条件。同时，这些结果为后续探究 n 元一次方程组解提供帮助。

基金项目

云南财经大学研究生创新基金项目(2023YUFEYC072)。

参考文献

[1] Plus, M. (1990) Linear Systems in (Max, +)-Algebra. *Proceedings of the 29th Conference on Decision and Control*, Honolulu, December 1990, 6 p. https://www.researchgate.net/publication/224657696_Linear_systems_in_max_algebra

[2] Baccelli, F., Cohen, G., Olsder, G.J., *et al.* (1992) Synchronization and Linearity: An Algebra for Discrete Event Systems. John Wiley & Sons, New York.

[3] Benchimol, P. (2014) Tropical Aspects of Linear Programming. Ecole Polytechnique. https://pasteur.hal.science/INRIA/tel-01198482

[4] Simon, I. (1988) Recognizable Sets with Multiplicities in the Tropical Semiring. In: Chytil, M.P., Koubek, V. and Janiga, L., Eds., *Lecture Notes in Computer Science*, Vol. 324, Springer, Berlin, Heidelberg, 107-120. https://doi.org/10.1007/BFb0017135

[5] Zhang, Y. (2018) Cryptanalysis of a Key Exchange Protocol Based on the Ring $Ep(m)$. *Applicable Algebra in Engineering, Communication and Computing*, **29**, 103-112. https://doi.org/10.1007/s00200-017-0332-0

[6] Grigoriev, D. and Shpilrain V. (2019) Tropical Cryptography II: Extensions by Homomorphisms. *Communications in Algebra*, **47**, 4224-4229. https://doi.org/10.1080/00927872.2019.1581213

[7] 黄华伟, 李春华. 一种基于热带半环的密钥建立协议的安全性分析[J]. 计算机科学, 2022, 49(z1): 571-574.

[8] Cuninghame-Green, R. (1979) Minimax Algebra. In: Fandel, G. and Trockel, W., Eds., *Lecture Notes in Economics and Mathematical Systems*, Springer, Berlin, Heidelberg, 13-15. https://doi.org/10.1007/978-3-642-48708-8