East-West J. of Mathematics: Vol. 26, No 2 (2025) pp. 102-116
https://doi.org/10.36853/ewjm0414

SEMIGROUP OF 2×2 TROPICAL CIRCULANT MATRICES AND THE BIORDER STRUCTURE OF THEIR IDEMPOTENTS

Ardra T. Joy[1], **Prakash G. N. Shenoi**
and **A. R. Rajan**

[1] *Department of Mathematics, Maharaja's College, Ernakulam*
Park Avenue Road, Marine Drive, Kerala–682011, India
Affiliated to Mahatma Gandhi University, Kottayam..
Email:ardratjoy17@gmail.com

Abstract

Tropical circulant matrix is a circulant matrix which operates within the tropical algebra framework where addition is replaced by the minimum and multiplication by the ordinary addition. These matrices have found applications in areas like cryptography and graph theory. In this paper we are dealing with $C_2(\overline{\mathbb{R}})$, the multiplicative semigroup of 2×2 circulant matrices over tropical semiring $\overline{\mathbb{R}} = (\mathbb{R} \cup \{\infty\}, \min, +)$. The semigroup $M_2(\overline{\mathbb{R}})$ of all 2×2 tropical matrices are known to be a regular semigroup. We show that the subsemigroup $C_2(\overline{\mathbb{R}})$ of circulant matrices is an inverse semigroup, that is, a regular semigroup in which every element has a unique inverse. It is known that the set of idempotents of an inverse semigroup is a semi-lattice and this semi-lattice of idempotents provides a way to understand and analyze the structure and behavior of inverse semigroups. So the semi-lattice $E(C_2)$ of idempotents of $C_2(\overline{\mathbb{R}})$ plays a crucial role in the structure of $C_2(\overline{\mathbb{R}})$. Also we determine the biorder structure of the set of idempotents and describe the sandwich sets associated with the idempotents. A description of the associated inductive groupoid is also given.

Keywords: Semigroups, Tropical matrices, Idempotents, Biorder relations, Biorder ideals.
2000 AMS Mathematics Subject Classification:15A80, 16Y60, 20M10.

Introduction

The algebra of real numbers augmented with ∞ under the operations of addition and minimum is known as tropical algebra, sometimes referred to as min-plus algebra. Since the 1970s, it has been a subject of active research in its own right. Because of its applicability in other scientific and mathematical fields, researchers in these fields have independently rediscovered many of its fundamental properties. Tropical algebra is largely concerned with matrices since many of the issues that occur in application areas are naturally represented in terms of linear equations. Thus the algebraic structure of the semigroup of all square matrices of a given order over the tropical semiring, $(\mathbb{R} \cup \{\infty\}, \min, +)$, becomes the subject of considerable study and a systematic understanding of this using the tools of semigroup theory was initiated by Johnson and Kambites [**?**] and independently by Izhakian and Margolis [**?**].

Tropical mathematics, especially tropical matrices, are used widely in tropical cryptography these days. Tropical cryptography, a relatively new and promising area in cryptography, is aiming to use various structures of tropical mathematics to redefine the classical public key exchange protocols in cryptography. An obvious advantage of using tropical algebra is high efficiency because, in tropical schemes, one does not have to perform any multiplication of numbers since tropical multiplication is the usual addition. However, tropical powers of an element exhibit some patterns, even if such an element is a matrix over a tropical algebra. Also since tropical public-key cryptosystems adopt a public matrix to construct commutative semirings or the presence of tropical matrix addition operation in the systems, most of the tropical public-key cryptosystems have security defects. So, recently [**?**] and [**?**], provides new public-key cryptosystems based on tropical circulant matrices. Therefore, applying semigroup theory methods to gain a deeper grasp of this algebraic structure will be beneficial for future research in this field.

In semigroup theory, the biordered set structure provides a powerful tool for analyzing and classifying semigroups by focusing on their idempotent elements. Specifically, K. S. S. Nambooripad introduced them to characterize the set of idempotents in regular semigroups, while Easdown demonstrated that the idempotents of arbitrary semigroups can also be described by biordered sets, [**?**]. In this paper we are studying about, $C_2(\overline{\mathbb{R}})$, the multiplicative semigroup of 2×2 circulant matrices over tropical semiring $\overline{\mathbb{R}} = (\mathbb{R} \cup \{\infty\}, \min, +)$, using the biorder relations on its idempotents. The semigroup $M_2(\overline{\mathbb{R}})$ of all 2×2 tropical matrices are known to be a regular semigroup while we show that the subsemigroup $C_2(\overline{\mathbb{R}})$ of circulant matrices is an inverse semigroup. Also, we determine the biorder structure of the set of idempotents and describe the sandwich sets associated with the idempotents.

1 Preliminaries

This section provides a brief summary of the background information from tropical algebra [**?**], semigroup theory and biordered sets [**?**] used in this paper.

1.1 Tropical matrices

Our basic object of study is the class of matrices over a tropical semiring $\overline{\mathbb{R}} = (\mathbb{R} \cup \{\infty\}, \oplus, \odot)$. The basic arithmetic operations of addition and multiplication of real numbers are transformed in this case as follows;

$$x \oplus y = \min\{x, y\} \text{ and } x \odot y = x + y.$$

Throughout this paper our tropical semiring is,

$$\overline{\mathbb{R}} = (\mathbb{R} \cup \{\infty\}, \oplus, \odot).$$

We write $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ also. In this case ∞ is the identity element for $\oplus$ and 0 is the identity element for $\odot$. We also note the following relations involving the two identity elements;

$$x \odot \infty = \infty \text{ and } x \oplus 0 = \begin{cases} 0 & \text{if } x \geq 0 \\ x & \text{if } x < 0\,. \end{cases}$$

Tropical matrices are matrices over $\overline{\mathbb{R}}$. For any two tropical matrices, $A = (a_{ij})_{n\times n}$ and $B = (b_{ij})_{n\times n}$, tropical matrix addition is,

$$A \oplus B = (m_{ij})_{n\times n};\ m_{ij} = a_{ij} \oplus b_{ij} = \min\{a_{ij}, b_{ij}\}$$

and tropical matrix multiplication is,

$$A \odot B = (m_{ij})_{n\times n};\ m_{ij} = \min_{k=1,2,\ldots,n} \{a_{ik} + b_{kj}\}.$$

Clearly, $(M_n(\overline{\mathbb{R}}), \oplus, \odot)$ has a semiring structure. But we are interested in the multiplicative semigroup of tropical matrices, that is, $(M_n(\overline{\mathbb{R}}), \odot)$, which is also denoted as $M_n(\overline{\mathbb{R}})$. The identity matrix in $M_n(\overline{\mathbb{R}})$ is,

$$\begin{bmatrix} 0 & \infty & \cdots & \infty \\ \infty & 0 & \cdots & \infty \\ \cdots & & & \\ \infty & \infty & \cdots & 0 \end{bmatrix}$$

and the zero matrix is

$$\begin{bmatrix} \infty & \infty & \cdots & \infty \\ \infty & \infty & \cdots & \infty \\ \cdots & & & \\ \infty & \infty & \cdots & \infty \end{bmatrix},$$

which is denoted as $(\infty)_{n\times n}$.
Hence the identity matrix in $M_2(\overline{\mathbb{R}})$ is $\begin{bmatrix} 0 & \infty \\ \infty & 0 \end{bmatrix}$ and zero matrix is $\begin{bmatrix} \infty & \infty \\ \infty & \infty \end{bmatrix}$.

1.2 Biordered sets

Biordered sets were introduced by K. S. S. Nambooripad [**?**, Definition 3.1] as an order structure to characterize the structure of the set of idempotents in a semigroup. A semigroup S is said to be regular if for every $x \in S$ there is $a \in S$ such that $xax = x$ and a semigroup S is called an inverse semigroup if every element in S has a unique inverse, that is, there exist $x \in S$ such that $axa = a$ and $xax = x$. Note that an inverse semigroup is regular. The theorem below gives some useful characterization of inverse semigroups. Recall that a semi-lattice is a commutative semigroup of idempotents.

Proposition 1.2.1. *[**?**, Theorem 2.44.] The following conditions on a semigroup S are equivalent.*

(i) S is regular and the set of all idempotents in S, $E(S)$, is a sub semi-lattice of S;

(ii) S is an inverse semigroup.

Several properties of regular semigroups are directly reflected in the properties of biordered sets.

In [**?**, Theorem 3.2], it is shown that biordered sets are structures that affords representation as a partial algebra and since the partial algebra representation simplifies the presentation significantly we are using it as the definition of the biordered set here.

A partial algebra on a set X is a triple $(X, D_X, \circ)$ where $D_X \subseteq X \times X$ and $\circ : D_X \to X$. Here $\circ$ is called the partial binary operation on X and D_X is called the domain of the partial binary operation. Often we denote a partial algebra as a pair (X, D_X). For $x, y \in X$ we write $xy = z$ to mean that $(x, y) \in D_X$ and $x \circ y = z$.

Definition 1.2.2. *[**?**, Theorem 3.2] Let $\mathbb{E} =< E, D_E >$ be a partial algebra where $D_E \subseteq E \times E$ is the domain of the partial binary operation on E. Define relations ω^r and ω^l on E as follows. For all $e, f \in E$,*

$$\begin{array}{lll} e\,\omega^r\,f & \text{if} & fe = e, \text{ and} \\ e\,\omega^l\,f & \text{if} & ef = e. \end{array}$$

Then E is a biordered set if it satisfies the following axioms and their duals. Let e, g, f, etc., denote arbitrary elements in E and

$$\mathcal{R} = \omega^r \cap (\omega^r)^{-1},\ \mathcal{L} = \omega^l \cap (\omega^l)^{-1} \text{ and } \omega = \omega^l \cap \omega^r.$$

B_1. *(a)* ω^l *and* ω^r *are quasiorders on* E.
(b) $D_E = \omega^r \cup \omega^l \cup (\omega^r)^{-1} \cup (\omega^l)^{-1}$

B_2. *(a) If* $e\,\omega^r\,f$ *then* $e\,\mathcal{R}\,ef\,\omega\,f$.
(b) If $g\,\omega^r\,f\,\omega^r\,e$ *then* $gf = (ge)f$.

B_3. *If* $g, f \in \omega^r(e)$, $g\,\omega^l\,f$ *then* $ge\,\omega^l\,fe$ *and* $(fg)e = (fe)(ge)$.

B_4. *If* $f, g \in \omega^r(e)$ *and* $ge\,\omega^l\,fe$, *then there exists* $g_1 \in \omega^r(e)$ *such that* $g_1\,\omega^l\,f$ *and* $g_1e = ge$.

Remark 1.2.1. *We observe that* $\omega = \omega^l \cap \omega^r$ *is a partial order and for the elements* $e, f \in E$, *whenever* $e\,\omega\,f$, *we write* $e \leqslant f$.

For a semigroup S, the set $E(S)$ of idempotents of S has the structure of a biordered set. The details are in the following theorem:

Theorem 1.2.2. *[?, Theorem 3.3] For a semigroup* S, *let* $E(S) = \{e \in S : e^2 = e\}$ *be the set of idempotents in* S. *Let*

$$D_E = \{(e, f) \in E(S) \times E(S) : ef \in \{e, f\} \text{ or } fe \in \{e, f\}\}.$$

Then $E(S) =< E(S), D_E >$ *is a biordered set with respect to the restriction of the product in* S *to* D_E.

A subset E' of a biordered set E is said to be a biordered subset of E if E' is a biordered set with respect to the restriction of the partial binary operation on E as the biordered set operation. Now we give some properties of biordered subsets of a biordered set.

Proposition 1.2.3. *[?, Proposition 3.13] Let* E' *be a subset of a biordered set* E. *Then* E' *is a biordered subset of* E *if and only if* E' *satisfies the following conditions and their duals;*

(i) For all $e', f' \in E'$, $(e', f') \in D_E$ *implies* $e'f' \in E'$.

(ii) If $e' \in E'$, $f', g' \in \omega^r(e') \cap E'$ *and* $g'e'\,\omega^l\,f'e'$ *then there exists* $g'_1 \in E' \cap \omega^l(f') \cap \omega^r(e')$ *such that* $g'_1e' = g'e'$.

Corollary 1.2.3. *[?, Corollary 3.14] Let* $\{E_i : i \in I\}$ *be a family of biordered subsets of* E. *Then*

$$E' = \bigcap_{i \in I} E_i$$

is a biordered subset of E.

Remark 1.2.4. *For $e \in E$, the biordered subset $\omega^r(e)$ called the ω^r ideal, $\omega^l(e)$ called the ω^l ideal and $\omega(e)$, the ω-ideal of E generated by e are described as follows:*

$$\begin{aligned} \omega^r(e) &= \{f \in E : f\,\omega^r\, e, \text{ that is, } ef = f\}, \\ \omega^l(e) &= \{f \in E : f\,\omega^l\, e, \text{ that is, } fe = f\} \text{ and} \\ \omega(e) &= \omega^l(e) \cap \omega^r(e). \end{aligned}$$

The sandwich set $\mathcal{S}(e, f)$ for e, f in a biordered set E is a subset of $\mathcal{M}(e, f) = \omega^l(e) \cap \omega^r(f)$ defined as follows:

Definition 1.2.4. *[?, Definition 3.3] Let E be a biordered set. For $e, f \in E$ define a relation $\leqslant$ on $\mathcal{M}(e, f)$ as follows. For $g, h \in \mathcal{M}(e, f)$,*

$$g \leqslant h \text{ if } eg\ \omega^r\ eh \text{ and } gf\,\omega^l\, hf.$$

The sandwich set of e and f is defined as

$$\mathcal{S}(e, f) = \{h \in \mathcal{M}(e, f) : g \leqslant h \text{ for all } g \in \mathcal{M}(e, f)\}.$$

Definition 1.2.5. *[?, Definition 3.4] A biordered set E is said to be regular if $\mathcal{S}(e, f) \neq \emptyset$ for all $e, f \in E$.*

Now we give a different description of sandwich sets for biordered sets of idempotents of a semigroup. In the following, we write $x \perp y$ for elements x, y of a semigroup S to mean that x is a generalized inverse of y.

Proposition 1.2.6. *[?, Proposition 3.4] Let $E = E(S)$ be the biordered set of a semigroup S. For $e, f \in E$ define*

$$\mathcal{S}_1(e, f) = \{h \in \mathcal{M}(e, f) : ehf = ef\} \tag{1}$$

and

$$\mathcal{S}_2(e, f) = \{h \in \mathcal{M}(e, f) : h \perp ef\}. \tag{2}$$

Then we have $\mathcal{S}_1(e, f) = \mathcal{S}_2(e, f) \subseteq \mathcal{S}(e, f)$.
Moreover, ef is a regular element in S if and only if

$$\mathcal{S}_1(e, f) = \mathcal{S}_2(e, f) = \mathcal{S}(e, f) \neq \emptyset.$$

Remark 1.2.5. *From the above proposition it follows that whenever S is a regular semigroup the biordered set $E(S)$ is regular.*

Proposition 1.2.7. *[?, Proposition 3.12] Let $e\,\mathcal{L}\,e'$ and $f\,\mathcal{R}\,f'$ where $e, e', f, f' \in E$. Then $\mathcal{M}(e, f) = \mathcal{M}(e', f')$. Consequently, $\mathcal{S}(e, f) = \mathcal{S}(e', f')$.*

2 The semigroup $C_2(\overline{\mathbb{R}})$

A circulant matrix is a square matrix in which all rows are composed of the same elements and each row is rotated one element to the right relative to the preceding row. A $n \times n$ circulant matrix, C, takes the form

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \dots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \dots & c_{n-2} \\ \vdots & \ddots & c_0 & \ddots & \vdots \\ c_2 & & \ddots & \ddots & c_1 \\ c_1 & c_2 & \dots & c_{n-1} & c_0 \end{bmatrix}.$$

So clearly C is fully specified by one vector, which appears as the first row of C.

2.1 Properties of $C_2(\overline{\mathbb{R}})$

In this paper, we consider only 2×2 tropical circulant matrices. Hence, a matrix $A \in M_2(\overline{\mathbb{R}})$ is a circulant matrix then it will be of the form

$$A = \begin{bmatrix} a & b \\ b & a \end{bmatrix}; a, b \in \overline{\mathbb{R}}.$$

The set of all these circulant matrices then forms a commutative subsemigroup of $M_2(\overline{\mathbb{R}})$ as shown in the following result.

Proposition 2.1.1. *The set of all* 2×2 *circulant matrices,* $C_2(\overline{\mathbb{R}})$*, forms a commutative subsemigroup of* $M_2(\overline{\mathbb{R}})$*.*

Proof. Let $A = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix}$ and $B = \begin{bmatrix} b_1 & b_2 \\ b_2 & b_1 \end{bmatrix}$ be two elements in $C_2(\overline{\mathbb{R}})$. Then,

$$AB = \begin{bmatrix} \min(a_1 + b_1, a_2 + b_2) & \min(a_1 + b_2, a_2 + b_1) \\ \min(a_1 + b_2, a_2 + b_1) & \min(a_1 + b_1, a_2 + b_2) \end{bmatrix} \in C_2(\overline{\mathbb{R}})$$

and clearly $AB = BA$. Hence the proof.

□

From now onwards we are considering $C_2(\overline{\mathbb{R}})$ itself as the semigroup. The semigroup $M_2(\overline{\mathbb{R}})$ of all 2×2 tropical matrices are known to be a regular semigroup [**?**, corollary 2.4]. So while studying about the regularity of circulant semigroups we have ended with finding a generalized inverse for each element in $C_2(\overline{\mathbb{R}})$ as seen in the following result.

Theorem 2.1.1. $C_2(\overline{\mathbb{R}})$ *is a regular semigroup.*

Proof. Let $A = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix}$ be any element in $C_2(\overline{\mathbb{R}})$.

- Case 1: $a_1 \leq a_2$ and $a_1 \neq \infty$.
  For $X = \begin{bmatrix} -a_1 & a_2 - 2a_1 \\ a_2 - 2a_1 & -a_1 \end{bmatrix}$, we have $AXA = A$ and $XAX = X$.
- Case 2: $a_1 \geq a_2$ and $a_2 \neq \infty$.
  For $X = \begin{bmatrix} a_1 - 2a_2 & -a_2 \\ -a_2 & a_1 - 2a_2 \end{bmatrix}$, we have $AXA = A$ and $XAX = X$.
- Case 3: $a_1 = a_2 = \infty$.
  Then $X = A = \begin{bmatrix} \infty & \infty \\ \infty & \infty \end{bmatrix}$ itself gives the result.

Hence the proof. □

2.2 Idempotents in $C_2(\overline{\mathbb{R}})$

Here we describe all idempotent elements in $C_2(\overline{\mathbb{R}})$.

Theorem 2.2.1. *A non - zero matrix $A \in C_2(\overline{\mathbb{R}})$ is an idempotent if and only if A is of the form $\begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix}$, where $a \in \overline{\mathbb{R}}$ and $a \geq 0$.*

Proof. Assume that $A = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix}$ be an idempotent element in $C_2(\overline{\mathbb{R}})$. Then,

$$A^2 = \begin{bmatrix} \min(2a_1, 2a_2) & a_1 + a_2 \\ a_1 + a_2 & \min(2a_1, 2a_2) \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix}$$

That is, $a_1 + a_2 = a_2$ implies $a_1 = 0$ and hence from $\min(2a_1, 2a_2) = a_1$, we have $a_2 \geq 0$. So, $A = \begin{bmatrix} 0 & a_2 \\ a_2 & 0 \end{bmatrix}$; $a_2 \geq 0$.

Hence the result. □

Remark 2.2.2. *Denote the set of all idempotent elements in $C_2(\overline{\mathbb{R}})$ by $E(C_2)$, we have*

$$E(C_2) = \left\{ \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} ; a \geq 0 \text{ and } a \in \overline{\mathbb{R}} \right\} \cup \left\{ \begin{bmatrix} \infty & \infty \\ \infty & \infty \end{bmatrix} \right\}.$$

3 Biorder relations on $E(C_2)$

As seen in preliminaries, Theorem 1.2.2, the set of idempotents of a semigroup is a biordered set. Hence, $E(C_2)$ is a biordered set. Since, $C_2(\overline{\mathbb{R}})$ is a commutative semigroup, the quasi orders, ω^l and ω^r, are equal to the partial order, ω, associated with the biorder structure. That is, for any $e \in E(C_2)$,

$$\omega^l(e) = \omega^r(e) = \omega(e).$$

3.1 Characterization of the partial order ω

In this section, we characterize this partial order, ω, associated with the biorder structure.

Theorem 3.1.1. *Let* $e_1 = \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} : a \geq 0$ *and* $e_2 = \begin{bmatrix} 0 & b \\ b & 0 \end{bmatrix} : b \geq 0$ *be in* $E(C_2)$. *Then the following are equivalent.*

(i) $e_1 \, \omega \, e_2$.

(ii) $a \leq b$.

Proof. (a) $(i) \implies (ii)$

Without loss of generality assume that for given e_1 and e_2, $e_1 \, \omega^l \, e_2$, then $e_1 e_2 = e_1$. That is,

$$\begin{bmatrix} \min(0, a+b) & \min(a,b) \\ \min(a,b) & \min(0, a+b) \end{bmatrix} = \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix}.$$

Since $\min(a, b) = a$ we have $a \leq b$. Hence (ii) holds.

(b) $(ii) \implies (i)$

Assume the relation in (ii), then

$$e_1 e_2 = \begin{bmatrix} \min(0, a+b) & \min(a,b) \\ \min(a,b) & \min(0, a+b) \end{bmatrix} = e_1.$$

That is, $e_1 \, \omega^l \, e_2$. Then by commutativity of these matrices, we have $e_2 e_1 = e_1$. That is, $e_1 \, \omega^r \, e_2$. Hence (i) holds.

Hence the proof. □

Corollary 3.1.2. *Let* $e_1, e_2 \in E(C_2)$. *Then either* $e_1 \leq e_2$ *or* $e_2 \leq e_1$.

Proof. Let $e_1 = \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} : a \geq 0$ and $e_2 = \begin{bmatrix} 0 & b \\ b & 0 \end{bmatrix} : b \geq 0$ be in $E(C_2)$. Then

$$e_1 e_2 = \begin{bmatrix} \min(0, a+b) & \min(a,b) \\ \min(a,b) & \min(0, a+b) \end{bmatrix} = \begin{bmatrix} 0 & \min(a,b) \\ \min(a,b) & 0 \end{bmatrix}.$$

Hence based on the values of a and b, we have either $e_1 e_2 = e_1$ or $e_1 e_2 = e_2$. Hence the proof.

□

Using the Remark 1.2.4 and Theorem 3.1.1 we can prove the following lemma.

Lemma 3.1.3. *For* $e = \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} \in E(C_2)$, *we have,*

$$\omega(e) = \left\{ \begin{bmatrix} 0 & x \\ x & 0 \end{bmatrix} : x \leq a, x \geq 0 \right\} \cup \left\{ \begin{bmatrix} \infty & \infty \\ \infty & \infty \end{bmatrix} \right\}.$$

The following observation on idempotents is important in the study of the semigroup structure.

Theorem 3.1.4. *The biordered set $E(C_2)$ has the property that for any e_1 and e_2 in $E(C_2)$,*

$$\omega(e_1) \cap \omega(e_2) = \omega(e_3)$$

for some $e_3 \in E(C_2)$, where e_3 is either e_1 or e_2.

Proof. Let $e_1 = \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix}$ and $e_2 = \begin{bmatrix} 0 & b \\ b & 0 \end{bmatrix}$ be in $E(C_2)$.

- Case 1: $e_1 \leq e_2$.
  By above lemma, we have:

$$\omega(e_1) \cap \omega(e_2) = \left\{ \begin{bmatrix} 0 & x \\ x & 0 \end{bmatrix} : x \leq a \text{ and } x \geq 0 \right\} \cup \left\{ \begin{bmatrix} \infty & \infty \\ \infty & \infty \end{bmatrix} \right\} = \omega(e_1). \tag{3}$$

  Now, required $e_3 = e_1$.

- Case 2: $e_2 \leq e_1$.
  Hence, we have by above lemma,

$$\omega(e_1) \cap \omega(e_2) = \left\{ \begin{bmatrix} 0 & x \\ x & 0 \end{bmatrix} : x \leq b \text{ and } x \geq 0 \right\} \cup \left\{ \begin{bmatrix} \infty & \infty \\ \infty & \infty \end{bmatrix} \right\} = \omega(e_2). \tag{4}$$

  Now, required $e_3 = e_2$.

Hence the proof. □

3.2 Sandwich set associated with the idempotents

Now, we have the biordered set $E(C_2)$ is arising from an inverse semigroup, $C_2(\overline{\mathbb{R}})$, hence the different descriptions about the sandwich sets in Proposition 1.2.6 coincide and for every pair of idempotents, the sandwich set is non-empty in $E(C_2)$. Here we use the definition of $\mathcal{S}_1(e, f)$ in Eq.(1) for sandwich sets.

Theorem 3.2.1. *Let $e_1 = \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix}$ and $e_2 = \begin{bmatrix} 0 & b \\ b & 0 \end{bmatrix}$ be in $E(C_2)$. Then*

$$\mathcal{S}(e_1, e_2) = \left\{ \begin{bmatrix} 0 & c \\ c & 0 \end{bmatrix} \right\} \subseteq E(C_2), \text{ where } c = \min(a, b).$$

Proof. Let $e_1 = \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix}$ and $e_2 = \begin{bmatrix} 0 & b \\ b & 0 \end{bmatrix}$ be in $E(C_2)$.

- Case 1: $e_1 \leq e_2$.
  Then by Eq.(3),

$$\mathcal{M}(e_1, e_2) = \left\{ \begin{bmatrix} 0 & x \\ x & 0 \end{bmatrix} : x \leq a \text{ and } x \geq 0 \right\} \cup \left\{ \begin{bmatrix} \infty & \infty \\ \infty & \infty \end{bmatrix} \right\}.$$

  For all $h \in \mathcal{M}(e_1, e_2)$, we have $e_1 h e_2 = h e_2 = h$, by Theorem 3.1.1 and $e_1 e_2 = e_1$. Hence,

$$\mathcal{S}(e_1, e_2) = \{h \in \mathcal{M}(e_1, e_2) : e_1 h e_2 = e_1 e_2\} = \{e_1\}.$$

- Case 2: $e_2 \leq e_1$.
  Then by Eq.(4),

$$\mathcal{M}(e_1, e_2) = \left\{ \begin{bmatrix} 0 & x \\ x & 0 \end{bmatrix} : x \leq b \text{ and } x \geq 0 \right\} \cup \left\{ \begin{bmatrix} \infty & \infty \\ \infty & \infty \end{bmatrix} \right\}.$$

  For all $h \in \mathcal{M}(e_1, e_2)$, we have $e_1 h e_2 = h e_2 = h$, by Theorem 3.1.1 and $e_1 e_2 = e_2$. Hence,

$$\mathcal{S}(e_1, e_2) = \{h \in \mathcal{M}(e_1, e_2) : e_1 h e_2 = e_1 e_2\} = \{e_2\}.$$

Hence the proof. □

3.3 Semi-lattice structure of $E(C_2)$

Since, $C_2(\overline{\mathbb{R}})$ is an inverse semigroup, from Proposition 1.2.1, we have $E(C_2)$ has a semi-lattice structure. Next result says that $E(C_2)$ is itself a commutative subsemigroup and hence a sub semi-lattice of $C_2(\overline{\mathbb{R}})$ and we can identify $E(C_2)$ with $\mathbb{R}^+$, the set of positive real numbers including 0.

Proposition 3.3.1. *The set of all non zero idempotents in* $C_2(\overline{\mathbb{R}})$*,* $E(C_2)^*$*, has a semi-lattice structure isomorphic to the set of positive real numbers. That is,*

$$(E(C_2)^*, \leq) \cong (\mathbb{R}^+, \leq).$$

Proof. For any e_1 and e_2 in $E(C_2)$, we have either $e_1 e_2 = e_1$ or $e_1 e_2 = e_2$ and by Theorem 2.1.1 we have $E(C_2)^*$ has a semi-lattice structure.
Consider, $f : E(C_2)^* \to \mathbb{R}^+$ defined by

$$f\Big(\begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} \Big) = a \,; \text{ for every } a \in [0, \infty].$$

Clearly, f is an isomorphism. Hence the proof.

□

Remark 3.3.1. *The zero idempotent* $\begin{bmatrix}\infty & \infty\\ \infty & \infty\end{bmatrix}$ *in* $E(C_2)$ *can be identify with* $-\infty$ *as it is the minimum element among the set* $E(C_2)$.

Remark 3.3.2. *In short, we have the semigroup of all* 2×2 *circulant matrices,* $C_2(\overline{\mathbb{R}})$*, has the following properties:*

1. $C_2(\overline{\mathbb{R}})$ *is an inverse semigroup.*
2. $E(C_2)$ *is a semi-lattice with the property that if* $e_1 \leq e_2$ *then*

$$e_1e_2 = e_2e_1 = e_1.$$

3. $(E(C_2)^*, \otimes) \cong ([0,\infty], \leq)$.

4 Inductive groupoid

The inductive groupoid $G(S)$ associated with an inverse semigroup S is described as

$$G(S) = \{(x, x^{-1}) : x \in S\}.$$

Here, for (x, x^{-1}), $(y, y^{-1}) \in G(S)$ the composition is defined by,

$$(x, x^{-1})(y, y^{-1}) = \begin{cases}(xy, y^{-1}x^{-1})\,;\ \text{if } x^{-1}x = yy^{-1}\\ \text{Not defined}\ ;\ \text{otherwise}\end{cases} \tag{5}$$

Further we know that [**?**] the groupoid composition extends to a full binary operation on $G(S)$ by defined

$$(x, x^{-1})(y, y^{-1}) = (xh, hx^{-1})(hy, y^{-1}h),\ \text{where } h = x^{-1}x.yy^{-1}. \tag{6}$$

4.1 Inductive groupoid associated with $C_2(\overline{\mathbb{R}})$

Now we describe the inductive groupoid $G(C_2)$ associated with the semigroup $C_2(\overline{\mathbb{R}})$. For convenience we avoid the zero matrix $\begin{bmatrix}\infty & \infty\\ \infty & \infty\end{bmatrix}$ from the semigroup but the resulting semigroup is also denoted by $C_2(\overline{\mathbb{R}})$. We describe the inductive groupoid $\varphi : \overline{\mathbb{R}} \times \overline{\mathbb{R}} \to \overline{\mathbb{R}} \times \overline{\mathbb{R}}$ using an involution map given by,

$$\varphi(a_1, a_2) = \begin{cases}(-a_1, a_2 - 2a_1); a_1 \leq a_2\\ (a_1 - 2a_2, -a_2); a_2 \leq a_1.\end{cases}$$

Also we write for $A = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix}$,

$$\varphi(A) = \begin{cases} \begin{bmatrix} -a_1 & a_2 - 2a_1 \\ a_2 - 2a_1 & -a_1 \end{bmatrix}; \, a_1 \leq a_2 \\ \\ \begin{bmatrix} a_1 - 2a_2 & -a_2 \\ -a_2 & a_1 - 2a_2 \end{bmatrix}; \, a_2 \leq a_1. \end{cases}$$

Theorem 4.1.1. *The inductive groupoid* $G(C_2(\overline{\mathbb{R}}))$ *is isomorphic to the groupoid* G_2 *described as follows:*

$$G_2 = \{((a_1, a_2), \varphi(a_1, a_2)) : a_1, a_2 \in \overline{\mathbb{R}} \text{ with either } a_1 \neq \infty \text{ or } a_2 \neq \infty\}.$$

Product is given by,

(1) $a_1 \leq a_2$ *and* $b_1 \leq b_2$ $((a_1, a_2), \varphi(a_1, a_2))((b_1, b_2), \varphi(b_1, b_2)) =$

$$= \begin{cases} ((a_1 + b_1, a_1 + b_2), (-a_1 - b_1, a_2 - 2a_1 - b_1)) \text{ if } a_2 - a_1 = b_2 - b_1 \\ \text{Not defined ; otherwise.} \end{cases}$$

(2) $a_1 \leq a_2$ *and* $b_2 \leq b_1$ $((a_1, a_2), \varphi(a_1, a_2))((b_1, b_2), \varphi(b_1, b_2)) =$

$$= \begin{cases} ((a_1 + b_1, a_1 + b_2), (a_2 - 2a_1 - b_2, -a_1 - b_2)) \\ \qquad ; \text{ if } a_2 - a_1 = b_1 - b_2 \\ \text{Not defined ; otherwise.} \end{cases}$$

(3) $a_2 \leq a_1$ *and* $b_1 \leq b_2$

$((a_1, a_2), \varphi(a_1, a_2))((b_1, b_2), \varphi(b_1, b_2)) =$

$$\begin{cases} ((a_1 + b_1, a_1 + b_2), (a_1 - 2a_2 - b_1, -a_2 - b_1)) \\ \qquad ; \text{ if } a_1 - a_2 = b_2 - b_1 \\ \text{Not defined ; otherwise.} \end{cases}$$

(4) $a_2 \leq a_1$ *and* $b_2 \leq b_1$ $((a_1, a_2), \varphi(a_1, a_2))((b_1, b_2), \varphi(b_1, b_2)) =$

$$\begin{cases} ((a_2 + b_2, a_1 + b_2), (-a_2 - b_2, a_1 - 2a_2 - b_2)) \\ \text{if } a_1 - a_2 = b_1 - b_2 \\ \text{Not defined ; otherwise.} \end{cases}$$

Proof. Let $A = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix}$ and $B = \begin{bmatrix} b_1 & b_2 \\ b_2 & b_1 \end{bmatrix}$ be in $C_2(\overline{\mathbb{R}})$ and without loss of generality assume that $a_1 \leq a_2$ and $b_1 \leq b_2$. Then by Eq. 5,

$$(A, \varphi(A))(B, \varphi(B)) = \begin{cases} (AB, \varphi(A)\varphi(B)) \text{ ; if } \varphi(A)A = B\varphi(B) \\ \text{Not defined ; otherwise.} \end{cases}$$

We have,

$$\varphi(A)A = B\varphi(B) \text{ implies } a_2 - a_1 = b_2 - b_1,$$

$$AB = \begin{bmatrix} a_1 + b_1 & a_1 + b_2 \\ a_1 + b_2 & a_1 + b_1 \end{bmatrix} \text{ and}$$

$$\varphi(B)\varphi(A) = \begin{bmatrix} -a_1 - b_1 & a_2 - 2a_1 - b_1 \\ a_2 - 2a_1 - b_1 & -a_1 - b_1 \end{bmatrix}.$$

Hence we have the required result. The other cases can be proved similarly. Hence the proof.

□

Now we can prove that the semigroup product in $C_2(\overline{\mathbb{R}})$ can be recovered from the groupoid. Here we describe it only for one of the case as follows;

Theorem 4.1.2. *The groupoid composition in C_2 can be extended to a semigroup product, for (a_1, a_2) and (b_1, b_2) with $a_1 \leq a_2$ and $b_1 \leq b_2$, by*

$$((a_1, a_2), \varphi(a_1, a_2))((b_1, b_2), \varphi(b_1, b_2))$$

$$= \begin{cases} ((a_1, a_2), (-a_1, a_2 - 2a_1))((b_1, a_2 - a_1 + b_1), (-b_1, -b_1 + a_2 - a_1)) \\ \qquad\qquad ; \text{ if } a_2 - a_1 \leq b_2 - b_1 \\ ((a_1, a_1 + b_2 - b_1), (-a_1, b_2 - b_1 - a_1))((b_1, b_2), (-b_1, b_2 - 2b_1)) \\ \qquad\qquad ; \text{ if } b_2 - b_1 \leq a_2 - a_1 \end{cases}$$

Proof. Using the Eq. 6 we can easily calculate this, here

$$h = \varphi(a_1, a_2)(a_1, a_2).(b_1, b_2)\varphi(b_1, b_2) = (0, \min(a_2 - a_1, b_2 - b_1)).$$

Hence the proof. □

Remark 4.1.3. *The other three cases of the above theorem depending on the values of a_1, a_2, b_1 and b_2 can be calculated similarly.*

References

[1] Huawei Huang, Weisha Kong, and Ting Xu, *Asymmetric cryptography based on the tropical jones matrix,* Symmetry, 16(4):456, 2024.

[2] Huawei Huang, Chunhua Li, and Lunzhi Deng *Public-key cryptography based on tropical circular matrices,* Applied Sciences, 12(15):7401, 2022.

[3] Zur Izhakian and Stuart Margolis, *Semigroup identities in the monoid of 2 × 2 tropical matrices,* Semigroup forum, 80:191–218, 2010.

[4] Marianne Johnson and Mark Kambites, *Multiplicative structure of 2 × 2 tropical matrices,* Linear algebra and its applications, 435(7):1612–1625, 2011.

[5] Diane Maclagan and Bernd Sturmfels, *Introduction to tropical geometry,* volume 161, American Mathematical Society, 2021.

[6] K. S. S. Nambooripad, *Structure of regular semigroups,* in Mem. American Mathematical Society, 224, 1979.

[7] Boris M Schein, *On the theory of inverse semigroups and generalized grouds. Twelve papers in logic and algebra,* AMS Translations, Ser, 2(113):89–123,