

# Number Theory of Matrix Semigroups

Nicholas Baeth<sup>1</sup>

Vadim Ponomarenko<sup>2</sup>

Donald Adams<sup>3</sup>(graduate student)

Rene Ardila<sup>4</sup>(undergraduate)

David Hannasch<sup>5</sup>(undergraduate)

Audra Kosh<sup>6</sup>(undergraduate)

Hanah McCarthy<sup>7</sup>(undergraduate)

Ryan Rosenbaum<sup>8</sup>(undergraduate)

June, 2010

## Abstract

Unlike factorization theory of commutative semigroups which are well-studied, very little literature exists describing factorization properties in noncommutative semigroups. Perhaps the most ubiquitous noncommutative semigroups are semigroups of square matrices and this article investigates the factorization properties within certain subsemigroups of  $M_n(\mathbb{Z})$ , the semigroup of  $n \times n$  matrices with integer entries. Certain important invariants are calculated to give a sense of how unique or non-unique factorization is in each of these semigroups.

## 1 Introduction

Many number theoretic results rely on knowing whether or not certain algebraic structures are endowed with the property of unique factorization. This paper investigates questions of unique factorization within certain classes of integral-valued matrices. Given a class  $S$  of matrices, we call  $M \in S$  *irreducible* if it cannot be written as  $M = AB$  where  $A, B \in S$  are noninvertible  $n \times n$  matrices. We intend to answer the following questions:

- (1) Can we enumerate the set of irreducibles of  $S$ ?
- (2) Given a matrix  $A \in S$ , what can we say about the factorizations of  $A$  into irreducibles?

Such questions of matrix factorizations were studied by P. Cohn [Coh63] as early as 1963. In the context of semigroups of matrices, factorization problems were studied in 1966 by Jacobson and Wisner [JW66] and in 1985 by Ch'uan and Chuan [CC85]. Motivated by these results, we apply the concepts of contemporary factorization theory to semigroups of integral-valued matrices. The study of non-unique factorizations has been well developed over the past several decades and was unified in [GHK06]. We intend to use methods from commutative contexts to study factorizations of matrices with integer entries.

Throughout,  $\mathbb{N}$  will denote the set of all positive integers and  $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ . A semigroup is a pairing  $(S, \cdot)$  where  $S$  is a set and  $\cdot$  is an associative binary operation on  $S$ . When the binary operation is clear from context and  $A, B \in S$ , we will simply write  $AB$  instead of  $A \cdot B$ . If  $S$  contains an element  $I$  such that  $AI = IA = A$  for all  $A \in S$ , then  $I$  is the *identity* of  $S$ . An element  $A \in S$ , a semigroup with identity, is a unit of  $S$  if there

---

<sup>1</sup>Department of Mathematics and Computer Science, San Diego State University, Warrensburg, MO 64093, [baeth@ucmo.edu](mailto:baeth@ucmo.edu)

<sup>2</sup>Department of Mathematics and Statistics, University of Central Missouri, San Diego, CA 92182, [vadim@rohan.sdsu.edu](mailto:vadim@rohan.sdsu.edu)

<sup>3</sup>San Diego State University, currently at Arizona State University

<sup>4</sup>City College of New York

<sup>5</sup>University of Nevada Las Vegas, currently at University of Illinois

<sup>6</sup>University of California Santa Barbara

<sup>7</sup>Lawrence University

<sup>8</sup>San Diego State University, currently at University of Colorado

exists an element  $B \in S$  such that  $AB = BA = I$ . A nonunit  $A \in S$  is called an *atom* of  $S$  if whenever  $A = BC$  for some elements  $B, C \in S$ , either  $B$  or  $C$  is a unit of  $S$ . The semigroup  $S$  is said to be *atomic* provided each nonunit element in  $S$  can be written as a product of atoms of  $S$ .

We now briefly introduce some important invariants that we will use throughout to describe how unique factorizations are within a given semigroup. Let  $S$  denote an atomic semigroup and let  $A$  be a nonunit element of  $S$ . The set

$$\mathcal{L}(A) = \{t : A = A_1 A_2 \cdots A_t \text{ with each } A_i \text{ an atom of } S\}$$

is the *set of lengths* of  $A$ . We denote by  $L(A) = \sup \mathcal{L}(A)$  the longest (if finite) factorization length of  $A$  and  $l(A) = \min \mathcal{L}(A)$  the minimum factorization length of  $A$ . The *elasticity*, denoted  $\rho(A) = \frac{L(A)}{l(A)}$ , of  $A$  gives a coarse measure of how far away  $A$  is from having unique factorization. Indeed, if  $A$  has a unique factorization  $A = A_1 A_2 \cdots A_t$ , then  $\mathcal{L}(A) = \{t\}$  and hence  $l(A) = L(A) = t$  and  $\rho(A) = t/t = 1$ . The *elasticity* of the semigroup  $S$ ,  $\rho(S)$  is given by  $\rho(S) = \sup\{\rho(A) : A \in S\}$ . If  $\mathcal{L}(A) = \{t_1, t_2, \dots\}$  with  $t_i < t_{i+1}$  for each  $i$ , then  $\Delta(A) = \{t_{i+1} - t_i : t_i, t_{i+1} \in \mathcal{L}(A)\}$ . Then  $\Delta(S) = \bigcup_{A \in S} \Delta(A)$ .

If  $S$  is an atomic semigroup and  $T$  is an atomic semigroup with identity, a surjective semigroup homomorphism  $\phi : S \rightarrow T$  is a *transfer homomorphism* provided that whenever  $\phi(s) = xy$  with  $x$  and  $y$  nonunits of  $T$ , there exist  $a$  and  $b$  nonunits of  $S$  such that  $\phi(a) = ux$ ,  $\phi(b) = vy$  with  $u, v$  units of  $S$  and  $ab = s$ . It is well known (cf. [GHK06]) that if  $\phi : S \rightarrow T$  is a transfer homomorphism between two atomic semigroups, then  $\rho(S) = \rho(T)$  and  $\Delta(S) = \Delta(T)$ . Transfer homomorphisms will allow us, in Sections 2 and 5, to understand the factorization of certain matrix semigroups by studying factorizations of elements in certain simpler semigroups.

We say that an atomic semigroup is *factorial* if every factorization is unique up to units. Note that this differs slightly from the commutative definition since we consider  $AB = BA$  to be two distinct factorizations of the same element. An atomic semigroup is *half-factorial* provided  $L(A) = l(A)$  for each nonunit  $A \in S$ . Finally, following [AAH<sup>+</sup>09], we define an atomic semigroup to be *bifurcus* provided  $l(A) = 2$  for every nonunit nonatom  $A$  of  $S$ . We note that if  $S$  is bifurcus, then  $\rho(S) = \infty$  and  $\Delta(S) = \{1\}$ .

Finally, we introduce some basic notation pertaining to greatest common divisor of a matrix. If  $A$  is any  $m \times n$  matrix, we set  $\gcd(A)$  to be the greatest common divisor of the  $mn$  entries of  $A$ .

## 2 The Semigroups $M_n(\mathbb{Z})$ and $T_n(\mathbb{Z})$

Before considering specific subsemigroups of matrices, we use this section to consider the semigroup  $M_n(\mathbb{Z})$  of all  $n \times n$  integer valued matrices and the subsemigroup  $T_n(\mathbb{Z})$  of  $n \times n$  upper triangular integer valued matrices. Such matrices are widely studied in mathematics; see, for example [Har90] and [SS06]. In this section we will find that the factorization of a matrix with integer entries is equivalent to the factorization of its determinant in  $\mathbb{Z}$ . Thus we are able to relate factorization of matrix semigroups with the better-understood integer semigroups as studied in [Gre80]. First we give a preliminary result which we use to classify the units in  $M_n(\mathbb{Z})$  and  $T_n(\mathbb{Z})$ .

**Lemma 2.1.** *Let  $S$  denote a subsemigroup of  $M_n(\mathbb{Z})$  containing  $I_n$  and let  $A \in S$ . If  $A$  is a unit of  $S$ , then  $|\det(A)| = 1$ . Moreover, if  $S$  is closed under adjugates, then  $|\det(A)| = 1$  implies that  $A$  is a unit of  $S$ .*

*Proof.* If  $A$  is a unit, then  $AB = I_n$  for some  $B \in S$ . Since  $\det(A)\det(B) = \det(I_n) = 1$ , and since all of the entries of  $A$  are integers,  $\det(A) = \pm 1$ .

Suppose now that  $\det(A) = \pm 1$  and that  $\text{adj}(A) \in S$ . Then  $A$  is invertible in  $M_n(\mathbb{R})$  and  $A^{-1} = \frac{1}{\det(A)} \text{adj}(A) \in S$ .  $\square$

In particular, since  $M_n(\mathbb{Z})$  and  $T_n(\mathbb{Z})$  are closed under adjugates, the units of these semigroups are precisely the elements with determinant plus or minus one.

The following lemma provides transfer homomorphisms from  $M_n(\mathbb{Z})$  and  $T_n(\mathbb{Z})$  to the semigroup  $\mathbb{Z}$ , thus allowing us to study the factorization properties of a matrix  $A$  by instead studying the factorization properties of  $\det(A) \in \mathbb{Z}$ .

**Lemma 2.2.** (1) *Let  $A \in M_n(\mathbb{Z})$  such that  $\det(A) = xy$  for some integers  $x$  and  $y$ . Then there exist  $X, Y \in M_n(\mathbb{Z})$  such that  $\det(X) = x$ ,  $\det(Y) = y$  and  $XY = A$ .*

(2) *Let  $A \in T_n(\mathbb{Z})$  such that  $\det(A) = xy$  for some integers  $x$  and  $y$ . Then there exist  $X, Y \in T_n(\mathbb{Z})$  such that  $\det(X) = x$ ,  $\det(Y) = y$  and  $XY = A$ .*

*Proof.* Let  $A \in M_n(\mathbb{Z})$  and write  $A$  using the Smith Normal Form as  $A = UDV$  where  $D \in M_n(\mathbb{Z})$  is a diagonal matrix and both  $U$  and  $V$  are elements of  $M_n(\mathbb{Z})$  with determinant in the set  $\{-1, 1\}$ . Since  $\det(D) = xy$ , we can then construct  $D_1$  and  $D_2$  diagonal matrices with  $D = D_1D_2$ ,  $\det(D_1) = x$  and  $\det(D_2) = y$ . Now  $A = XY$  where  $X = UD_1$  and  $Y = D_2V$  have the desired properties, proving (1).

Now let  $A \in T_n(\mathbb{Z})$  and let  $a_1, a_2, \dots, a_n$  denote the diagonal entries of  $A$ . Note that  $\det(A) = xy = a_1a_2 \cdots a_n$  and let  $y = p_1p_2 \cdots p_m$  denote the prime factorization of  $y$  with the  $p_i$  not necessarily distinct primes. Finally, let  $k \in \{1, 2, \dots, n\}$  be the smallest positive integer such that  $p_1 \mid a_k$ . We claim that  $A$  can be factored as

$$A = \begin{bmatrix} T_1 & \mathbf{u} & V \\ 0 & a_k & W \\ 0 & 0 & T_2 \end{bmatrix} = \begin{bmatrix} T_1 & \mathbf{u}_1 & V \\ 0 & \frac{a_k}{p_1} & W \\ 0 & 0 & T_2 \end{bmatrix} \begin{bmatrix} I_{k-1} & \mathbf{u}_2 & 0 \\ 0 & p_1 & 0 \\ 0 & 0 & I_{n-k} \end{bmatrix}$$

where  $T_1 \in T_{k-1}(\mathbb{Z})$ ,  $T_2 \in T_{n-k}(\mathbb{Z})$ ,  $\mathbf{u}, \mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^{k-1}$ ,  $V \in M_{k-1, n-k}(\mathbb{Z})$ , and  $W \in M_{1, n-k}(\mathbb{Z})$ . Such a decomposition of  $A$  exists if and only if we can find vectors  $\mathbf{u}_1$  and  $\mathbf{u}_2$  such that  $T_1\mathbf{u}_2 + p_1\mathbf{u}_1 = \mathbf{u}$ . That is,

there must exist  $\mathbf{u}_1 = \begin{bmatrix} u_{1,1} \\ u_{1,2} \\ \vdots \\ u_{1,k-1} \end{bmatrix}$  and  $\mathbf{u}_2 = \begin{bmatrix} u_{2,1} \\ u_{2,2} \\ \vdots \\ u_{2,k-1} \end{bmatrix}$  such that

$$\begin{bmatrix} a_1 & a_{12} & \cdots & a_{1(k-1)} \\ 0 & a_2 & \cdots & a_{2(k-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{k-1} \end{bmatrix} \begin{bmatrix} u_{2,1} \\ u_{2,2} \\ \vdots \\ u_{2,k-1} \end{bmatrix} + p_1 \begin{bmatrix} u_{1,1} \\ u_{1,2} \\ \vdots \\ u_{1,k-1} \end{bmatrix} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_{k-1} \end{bmatrix}.$$

Since  $a_{k-1}$  and  $p_1$  are relatively prime there must exist  $u_{1,k-1}$  and  $u_{2,k-1}$  such that  $u_{k-2} = p_1u_{1,k-1} + a_{k-1}u_{2,k-1}$ . Now since  $a_{k-2}$  and  $p_1$  are relatively prime we can find  $u_{2,k-2}$  and  $u_{1,k-2}$  such that  $u_{k-2} = p_1u_{1,k-2} + a_{k-2}u_{2,k-2} + a_{k-2,k-1}u_{2,k-1}$ . We continue inductively until we achieve the above factorization

of  $A$ . Let  $B_1$  denote the matrix  $\begin{bmatrix} I_{k-1} & \mathbf{u}_2 & 0 \\ 0 & p_1 & 0 \\ 0 & 0 & I_{n-k} \end{bmatrix}$ . Then we have a factorization  $A = \hat{A}B_1$  where  $\hat{A} =$

$$\begin{bmatrix} T_1 & \mathbf{u}_1 & V \\ 0 & \frac{a_k}{p_1} & W \\ 0 & 0 & T_2 \end{bmatrix}. \text{ Following this same procedure, we may factor } A \text{ as } A = X(B_mB_{m-1} \cdots B_1) \text{ where } B_i = \begin{bmatrix} I_{k-1} & \tilde{\mathbf{u}}_i & 0 \\ 0 & p_i & 0 \\ 0 & 0 & I_{n-k} \end{bmatrix} \text{ for some appropriate vector } \tilde{\mathbf{u}}_i. \text{ By setting } Y = B_mB_{m-1} \cdots B_1 \text{ we have the desired factorization } A = XY \text{ with } \det(X) = \frac{xy}{p_mp_{m-1} \cdots p_1} = x \text{ and } \det(Y) = p_mp_{m-1} \cdots p_1 = y. \text{ This proves (2). } \square$$

The transfer homomorphism  $A \mapsto \det(A)$  provided by Lemma 2.2 together with the uniqueness of factorization in  $\mathbb{Z}$  and  $\mathbb{N}$  provide the following Theorem.

**Theorem 2.3.** *Let  $S$  be one of the following subsemigroups of  $M_n(\mathbb{Z})$ :*

- $M_n(\mathbb{Z})$ ,
- $T_n(\mathbb{Z})$ ,
- $\{A \in M_n(\mathbb{Z}) \mid \det(A) > 1\}$ , or
- $\{A \in T_n(\mathbb{Z}) \mid \det(A) > 1\}$ .

Then

- (1)  $A$  is an atom of  $S$  if and only if  $\det(A)$  is prime,
- (2)  $L(A) = l(A)$  is the number of (not necessarily distinct) prime factors of  $\det(A)$ , and
- (3)  $S$  is half-factorial.

The remaining sections will consider certain subsemigroups of  $M_n(\mathbb{Z})$  and  $T_n(\mathbb{Z})$ . As we shall see, these subsemigroups have more interesting factorization properties than the larger semigroups in which they live.

### 3 Subsemigroups of $M_n(\mathbb{Z})$

#### 3.1 Subsemigroups $M_n(\mathbb{Z})$ with determinant in $k\mathbb{Z}$

In this section we consider subsemigroups of  $M_n(\mathbb{Z})$  and  $T_n(\mathbb{Z})$  with the restriction that the determinant of each matrix is divisible by a fixed integer. We refer to these semigroups as  ${}_kM_n(\mathbb{Z})$  and  ${}_kT_n(\mathbb{Z})$  respectively. Such matrices have been considered in [CC86] and [Est91]. Throughout this section, let  $k > 1$  be a fixed positive integer and let  $S$  denote either the subsemigroup of  $M_n(\mathbb{Z})$  consisting of all matrices  $A$  with  $\det(A) \in k\mathbb{Z}$  or the subsemigroup of  $T_n(\mathbb{Z})$  consisting of all upper triangular matrices  $A$  with  $\det(A) \in k\mathbb{Z}$ . Note that since  $I_n \notin S$ ,  $S$  contains no units. For a square matrix  $B$ , we set  $\nu_r(B)$  to denote the number  $\max\{t : r^t \mid \det(B)\}$ .

**Lemma 3.1.** *Let  $k > 1$  be a positive integer and either let  $S = {}_kM_n(\mathbb{Z})$  or  $S = {}_kT_n(\mathbb{Z})$ . If  $A \in S$ , then*

- (1)  $L(A) = \nu_k(A)$  and
- (2)  $A$  is an atom of  $S$  if and only if  $k^2 \nmid \det(A)$ .

*Proof.* Suppose that  $A$  factors as  $A = A_1 A_2 \cdots A_m$  in  $S$ . By the definition of  $S$ ,  $k \mid \det(A_i)$  for all  $i$  and hence  $k^m \mid \det(A)$ . Therefore,  $L(A) \leq \nu_k(A)$ . Using Lemma 2.2, there exist matrices  $A_1, A_2, \dots, A_{\nu_k(A)} \in S$  with  $\det(A_i) = k$  for all  $i \in \{1, 2, \dots, \nu_k(A) - 1\}$  and  $\det(A_{\nu_k(A)}) = \frac{\det(A)}{k^{\nu_k(A)-1}}$ . Therefore,  $L(A) \geq \nu_k(A)$ . This proves (1), of which (2) is a consequence.  $\square$

**Lemma 3.2.** *Let  $k = p^t$  for some prime integer  $p$  and some positive integer  $t$ . Either let  $S = {}_kM_n(\mathbb{Z})$  or  $S = {}_kT_n(\mathbb{Z})$ . If  $A \in S$ , then  $l(A) = \left\lfloor \frac{\nu_p(A) + 2t - 2}{2t - 1} \right\rfloor$ .*

*Proof.* Write  $\det(A) = p^m x$  where  $m \geq t$  and  $p \nmid x$ ; that is,  $\nu_p(A) = m$ . Factor  $A$  in  $S$  as  $A = A_1 A_2 \cdots A_s$  where each  $A_i$  is an atom of  $S$  and set, for each  $i$ ,  $t_i = \nu_p(A_i)$ . Since  $\det(A) = \det(A_1) \det(A_2) \cdots \det(A_s)$ ,  $m = \sum_{i=1}^s t_i$ . Moreover, since each  $A_i$  is an atom, Lemma 3.1 gives us that  $t_i \leq 2t - 1$  for each  $i \in \{1, 2, \dots, s\}$ . Thus  $m = \sum_{i=1}^s t_i \leq s(2t - 1)$ . If  $s \leq \left\lfloor \frac{\nu_p(A) + 2t - 2}{2t - 1} \right\rfloor - 1$ , then  $s \leq \frac{\nu_p(A) - 1}{2t - 1}$  and hence  $s(2t - 1) \leq m - 1$ , a contradiction. Therefore,  $l(A) \geq \left\lfloor \frac{\nu_p(A) + 2t - 2}{2t - 1} \right\rfloor$ .

Appealing to Lemma 2.2 we see that factoring  $A$  is equivalent to factoring  $\det(A)$  in  $\mathbb{Z}$ . Write  $\nu_p(A) = q(2t - 1) + r$  where  $0 \leq r < 2t - 1$ . Then  $\left\lfloor \frac{\nu_p(A) + 2t - 2}{2t - 1} \right\rfloor = q + 1 + \left\lfloor \frac{r - 1}{2t - 1} \right\rfloor$ . Clearly,  $A$  is an atom of  $S$  if and only if  $q = 0$ . If  $A$  is not an atom then we can factor  $\det(A)$  as

$$\det(A) = \begin{cases} (p^{2t-1})(p^t)(p^{r+t-1}) & \text{if } r > 0 \\ (p^{2t-1})^{q-1}(p^{2t-1}x) & \text{if } r = 0 \end{cases}$$

giving either a factorization of length  $q + 1$  when  $r > 0$  or a factorization of length  $q$  when  $r = 0$ . This proves that  $l(A) \leq \left\lfloor \frac{\nu_p(A) + 2t - 2}{2t - 1} \right\rfloor$ .  $\square$

Using Lemma 3.2, the following Theorem gives the elasticity  $\rho(S)$  regardless of  $k$ . To see this, it is important to recall that bifurcus semigroups necessarily have infinite elasticity.

**Theorem 3.3.** *Let  $k > 1$  be a positive integer and either let  $S = {}_kM_n(\mathbb{Z})$  or  $S = {}_kT_n(\mathbb{Z})$ .*

- (1) *If  $k = p^t$  for some prime  $p$  and some positive integer  $t$ , then  $\rho(S) = \frac{2t-1}{t}$ .*
- (2) *If  $k = st$  with  $s, t > 1$  and  $\gcd(s, t) = 1$ , then  $S$  is bifurcus.*
- (3)  *$S$  is half-factorial if and only if  $k$  is prime.*

*Proof.* Suppose that  $k = p^t$  for some prime  $p$  and some positive integer  $t$ . By Lemma 3.1, for any  $A \in S$  we have that

$$\rho(A) = \frac{\left\lfloor \frac{\nu_p(A)}{t} \right\rfloor}{\left\lfloor \frac{\nu_p(A) + 2t - 2}{2t - 1} \right\rfloor} \leq \frac{\frac{\nu_p(A)}{t}}{\frac{\nu_p(A)}{2t - 1}} = \frac{2t - 1}{t}.$$

Therefore,  $\rho(S) \leq \frac{2t-1}{t}$ . However, this elasticity is achieved by any element  $A \in S$  with  $\det(A) = (p^t)^{2t-1} = (p^{2t-1})^t$  and hence  $\rho(S) = \frac{2t-1}{t}$ .

Suppose that  $k = st$  with  $s, t > 1$  and  $\gcd(s, t) = 1$ . If  $A \in S$  can be written as the product of two elements in  $S$ , then by Lemma 3.1  $(st)^2 \mid \det(A)$  and hence  $\det(A) = (st)^m x_1 x_2$  where  $m \geq 2$ ,  $s \nmid x_1$  and  $t \nmid x_2$ . Writing  $\det(A) = (s^{m-1} t x_2)(st^{m-1} x_1)$ , we see by either Lemma 2.2 or Lemma 2.2 that there exist matrices  $B$  and  $C$  in  $S$  such that  $\det(B) = s^{m-1} t x_2$ ,  $\det(C) = st^{m-1} x_1$  and  $A = BC$ . Since the determinants of  $B$  and  $C$  are not divisible by  $(st)^2$ , by Lemma 3.1  $B$  and  $C$  are atoms of  $S$  and hence  $l(A) = 2$ .

If  $k = st$  where  $\gcd(s, t) = 1$  then  $S$  is bifurcus and hence  $S$  is not half-factorial. If  $k = p^t$  for some prime  $p$  and some positive integer  $k$ , then  $\rho(S) = \frac{2t-1}{t}$  and hence  $S$  is half-factorial if and only if  $t = 1$ ; i.e.,  $k$  is prime.  $\square$

### 3.2 Subsemigroups of $M_n(\mathbb{Z})$ with Composite Determinant

We conclude this section by considering the larger subsemigroup  $S$  of  $n \times n$  integer matrices with composite determinant. We note that since  $I_n \notin S$ ,  $S$  contains no units. For convenience, we let  $r(A)$  denote the number of prime divisors of  $\det(A)$  counted with multiplicity and note that if  $X, Y \in S$ , then  $r(XY) = r(X) + r(Y)$ . Also note that if  $A \in S$ , then  $r(A) \geq 2$ . The following lemma is an analog of Lemmas 2.2 and 2.2 which will be allow us to compute both  $\rho(S)$  and  $\Delta(S)$ .

**Lemma 3.4.** *Let  $S$  denote the subsemigroup of all matrices in either  $M_n(\mathbb{Z})$  or  $T_n(\mathbb{Z})$  with composite determinant and let  $A \in S$ .*

- (1)  $A$  is an atom of  $S$  if and only if  $r(A) \leq 3$ .
- (2) If  $r(A) = x + y$  with  $x, y \geq 2$ , then there exist  $X, Y \in S$  with  $r(X) = x$ ,  $r(Y) = y$  and  $A = XY$ .

*Proof.* Suppose that  $A$  factors as  $A = BC$  in  $S$ . Since  $B, C \in S$ , we have that  $r(B), r(C) \geq 2$ . Then  $r(A) = r(B) + r(C) \geq 2 + 2 = 4$ .

Now suppose that  $r(A) \geq 4$ . Then we can write  $r(A) = x + y$  with  $x, y \geq 2$ . Factor the determinant of  $A$  as  $\det(A) = p_1 \cdots p_x p_{x+1} \cdots p_{x+y}$  where the  $p_i$  are not necessarily distinct primes. From either Lemma 2.2 or 2.2 there exist matrices  $X$  and  $Y$  with  $\det(X) = p_1 \cdots p_x$  and  $\det(Y) = p_{x+1} \cdots p_{x+y}$  and  $A = XY$ . Since  $x, y \geq 2$   $\det(X)$  and  $\det(Y)$  are composite and hence  $X, Y \in S$ . Moreover,  $A$  is not an atom of  $S$ .  $\square$

**Theorem 3.5.** *Let  $S$  denote the subsemigroup of all matrices in either  $M_n(\mathbb{Z})$  or  $T_n(\mathbb{Z})$  with composite determinant and let  $A$  be a non-atom of  $S$ . Then*

- (1)  $L(A) = \left\lfloor \frac{r(A)}{2} \right\rfloor$ ,
- (2)  $l(A) = \left\lceil \frac{r(A)}{3} \right\rceil$ ,
- (3)  $\rho(S) = \frac{3}{2}$ , and
- (4)  $\Delta(S) = 1$ .

*Proof.* Write  $r(A) = 2 \left\lfloor \frac{r(A)}{2} \right\rfloor + x$  where  $x \in \{0, 1\}$ . Suppose that  $A = A_1 A_2 \cdots A_s$  where each  $A_i$  is an atom of  $S$ . Then  $r(A) = \sum_{i=1}^s r(A_i)$ . As  $r(A_i) \geq 2$  for each  $i$ ,  $r(A) \geq 2s$ . Therefore,  $L(A) \leq \left\lfloor \frac{r(A)}{2} \right\rfloor$ . From Lemma 3.4 we know that since  $r(A) = 2 \left\lfloor \frac{r(A)}{2} \right\rfloor + x \geq 2$ , we can factor  $A$  as  $A_1 A_2 \cdots A_{\left\lfloor \frac{r(A)}{2} \right\rfloor}$  where  $r(A_i) = 2$  for all  $i \in \{1, \dots, \left\lfloor \frac{r(A)}{2} \right\rfloor - 1\}$  and  $r\left(A_{\left\lfloor \frac{r(A)}{2} \right\rfloor}\right) = 2 + x$ . Therefore,  $L(A) = \left\lfloor \frac{r(A)}{2} \right\rfloor$ .

Write  $r(A) = 3 \left\lfloor \frac{r(A)}{3} \right\rfloor + x$  where  $x \in \{0, 1, 2\}$ . We will consider two cases. First, suppose that  $x = 0$  and factor  $A$  as  $A = A_1 A_2 \cdots A_{\left\lfloor \frac{r(A)}{3} \right\rfloor}$  where  $r(A_i) = 3$  for all  $i \in \{1, \dots, \left\lfloor \frac{r(A)}{3} \right\rfloor\}$ . This gives  $l(A) \leq \left\lceil \frac{r(A)}{3} \right\rceil$ . Next, suppose that  $x \in \{1, 2\}$  and factor  $A$  as  $A = A_1 A_2 \cdots A_{\left\lfloor \frac{r(A)}{3} \right\rfloor} A_{\left\lfloor \frac{r(A)}{3} \right\rfloor + 1}$  where  $r(A_i) = 3$  for all  $i \in \{1, \dots, \left\lfloor \frac{r(A)}{3} \right\rfloor\}$ ,  $r\left(A_{\left\lfloor \frac{r(A)}{3} \right\rfloor}\right) = 1 + x$  and  $r\left(A_{\left\lfloor \frac{r(A)}{3} \right\rfloor + 1}\right) = 2$ . This gives  $l(A) \leq \left\lfloor \frac{r(A)}{3} \right\rfloor + 1 = \left\lceil \frac{r(A)}{3} \right\rceil$ . Now

factor  $A$  as  $A_1 \cdots A_s$  where each  $A_i$  is an atom of  $S$ . Since  $r(A_i) \leq 3$  for each  $i$ ,  $r(A) \leq 3s$ . With  $s = l(A)$ ,  $\frac{r(A)}{3} \leq l(A)$ . Since  $l(A) \in \mathbb{Z}$ ,  $l(A) \geq \left\lceil \frac{r(A)}{3} \right\rceil$ .

We now have that

$$\rho(A) = \frac{\left\lfloor \frac{r(A)}{2} \right\rfloor}{\left\lceil \frac{r(A)}{3} \right\rceil} \leq \frac{\frac{r(A)}{2}}{\frac{r(A)}{3}} = \frac{3}{2}.$$

Whenever  $6 \mid r(A)$  this elasticity is achieved and hence  $\rho(S) = 3/2$ .

Write  $A = A_1 A_2 \cdots A_s$  where each  $A_i$  is an atom of  $S$  and such that  $s > l(A)$ . That is,  $s \geq \left\lceil \frac{r(A)}{3} \right\rceil + 1$ . Let  $x$  denote the number of  $A_i$  with  $r(A_i) = 2$ . Then  $r(A) = \sum_{i=1}^s r(A_i) = 2x + 3(s - x) = 3s - x$  and hence  $s \geq \left\lceil \frac{r(A)}{3} \right\rceil + 1 = \left\lceil \frac{3s - x}{3} \right\rceil + 1 = s + 1 + \left\lceil \frac{-x}{3} \right\rceil$ . Therefore  $-1 \geq \left\lceil \frac{-x}{3} \right\rceil$  and so  $x \geq 3$ . Without loss of generality, assume that  $r(A_1) = r(A_2) = r(A_3) = 2$ . Then  $r(A_1 A_2 A_3) = 3 + 3$  and hence there are atoms  $B_1, B_2$  in  $S$  with  $A_1 A_2 A_3 = B_1 B_2$ . Therefore,  $A = B_1 B_2 A_4 \cdots A_s$  is the product of  $s - 1$  atoms of  $S$ . As this holds for any non-atom  $A \in S$ ,  $\Delta(S) = \{1\}$ .  $\square$

## 4 Subsemigroups of $T_n(\mathbb{Z})$

Upper triangular matrices are well-studied, in part because their determinants are easy to compute and because any integer valued matrix can be put in Hermite Normal Form. Moreover, being able to factor matrices in  $T_n(\mathbb{Z})$  plays an important role in the Post correspondence problem (cf. [Kro85] and [HH07]). In this section we investigate factorization properties of certain subsemigroups of  $T_n(\mathbb{Z})$ . In particular, we consider  $T_2(\mathbb{N})$ ,  $T_2(\mathbb{N}_0)$ ,  $T_n(k\mathbb{N})$  for  $k > 1$ , and unitriangular matrices — elements of  $T_n(\mathbb{N}_0)$  whose diagonal elements are all 1's.

**Remark 4.1.** Note that each of the results in this section pertaining to subsemigroups of  $T_n(\mathbb{Z})$  of upper triangular matrices can be restated for subsemigroups of  $L_n(\mathbb{Z})$  of lower triangular matrices.

### 4.1 $T_n(k\mathbb{Z})$

In this section we take  $S$  to be the subsemigroup of all nonzero upper triangular  $n \times n$  integer valued matrices whose entries are a multiple of some integer  $k > 1$ . Since  $S$  does not contain the identity matrix,  $S$  contains no units. Recall that if  $x$  is an integer, divisible by  $k$ , then  $\nu_k(x)$  is the largest integer  $t$  such that  $k^t \mid x$ .

**Lemma 4.2.** *Let  $k > 1$  be an integer and let  $S$  denote the semigroup of all nonzero matrices in  $T_n(k\mathbb{Z})$ . Let  $A \in S$ .*

$$(1) \ L(A) = \nu_k(\gcd(A)).$$

$$(2) \ A \text{ is an atom of } S \text{ if and only if } \nu_k(\gcd(A)) = 1.$$

*Proof.* First note that if  $k^u$  divides all entries of an  $n \times n$  matrix  $B$  and  $k^v$  divides all entries of an  $n \times n$  matrix  $C$ , then  $k^{u+v}$  divides all the entries of their product  $BC$ . Thus, if  $A = A_1 A_2 \cdots A_t$  with each  $A_i$  an element of  $S$ , then  $k^t$  divides all entries of  $A$  and so  $t \leq \nu_k(\gcd(A))$ . That is, taking each  $A_i$  to be an atom of  $S$ ,  $L(A) \leq \nu_k(\gcd(A))$ . Note that  $kI_n \in S$  and that  $A = (kI_n)^{\nu_k(\gcd(A))-1} A'$  for some  $A' \in S$ . Therefore,  $L(A) \geq \nu_k(\gcd(A))$  proving (1).

Since  $A$  is an atom of  $S$  if and only if  $L(A) = 1$ , (2) follows immediately.  $\square$

**Theorem 4.3.** *Let  $k > 1$  be an integer and let  $S$  denote the semigroup of all nonzero matrices in  $T_n(k\mathbb{Z})$  where  $n \geq 2$ . Then  $S$  is bifurcus.*

*Proof.* Write  $A$  as  $A = [\mathbf{u} \ B]$  where  $\mathbf{u}$  is a column vector and  $B$  is an  $n \times (n - 1)$  matrix. If  $\nu = \nu_k(\gcd(\mathbf{u}))$ , then we can factor  $A$  as

$$A = [\mathbf{u} \ B] = \left[ \left( \frac{1}{k^{\nu-1}} \right) \mathbf{u} \ \frac{1}{k} B \right] \begin{bmatrix} k^{\nu-1} & 0 \\ 0 & kI_{n-1} \end{bmatrix}$$

where  $\begin{bmatrix} k^{\nu-1} & 0 \\ 0 & kI_{n-1} \end{bmatrix}$  is a  $4 \times 4$  block matrix with the non-diagonal blocks consisting of only zero entries. By Lemma 4.2, each of these factors is an atom of  $S$  and hence  $S$  is bifurcus.  $\square$

## 4.2 Unitriangular Matrices

In this section we consider  $S$  to be the subsemigroup of  $T_n(\mathbb{N}_0)$  with ones along the diagonal — that is the set of unitriangular matrices with nonnegative entries. We restrict to nonnegative entries since every unitriangular matrix over the integers is a unit thus making factorization questions trivial. In [GMSGP06], it was shown that the group of  $n \times n$  upper triangular matrix over a semiring is the semidirect product of the group of diagonal matrices and the monoid of unitriangular matrices. The complexity of the set of  $n \times n$  unitriangular matrices over a finite field was studied in [Kra07]. Thus we have motivation to study factorization properties in the family of unitriangular matrices.

We will first consider the entire semigroup and then restrict to the subsemigroup consisting only of matrices with nonzero entries above the diagonal. For a matrix  $A \in S$ , let  $\Sigma(A)$  denote the sum of the off diagonal entries in  $A$ . Note that since matrices in  $S$  contain no negative entries, if  $A, B \in S$ , then  $\Sigma(AB) \geq \Sigma(A) + \Sigma(B)$ . Therefore, the only unit of  $S$  is the  $n \times n$  identity matrix  $I_n$ . Indeed, if  $AB = I_n$ , then  $0 \leq \Sigma(A) \leq \Sigma(AB) = \Sigma(I_n) = 0$  and hence  $\Sigma(A) = 0$ .

For  $i$  and  $j$  with  $i < j$ , let  $E_{i,j} \in M_n(\mathbb{N}_0)$  (not in  $S$ ) denote the matrix whose only nonzero entry is  $e_{i,j} = 1$ . Note that  $E_{i_1,j_1}E_{i_2,j_2}$  is nonzero if and only if  $j_1 = i_2$ .

**Lemma 4.4.** *Let  $m \in \{1, 2, \dots, n\}$ . Suppose  $A$  and  $B$  are unitriangular upper triangular matrices with entries in  $\mathbb{N}_0$  with  $a_{i,j} = 0$  whenever  $i < m$  and  $i \neq j$  and  $b_{i,j} = 0$  whenever  $i > m$  and  $j \neq i$ . Then  $AB = A + B - I$ .*

*Proof.* Write  $A$  and  $B$  as

$$A = \begin{bmatrix} I & 0 & 0 \\ 0 & 1 & \mathbf{u} \\ 0 & 0 & A' \end{bmatrix}, \quad B = \begin{bmatrix} I & 0 & B' \\ 0 & 1 & \mathbf{v} \\ 0 & 0 & I \end{bmatrix}$$

where  $\mathbf{u}$  and  $\mathbf{v}$  are column vectors in  $\mathbb{N}_0^n$ . Then

$$AB = \begin{bmatrix} I & 0 & 0 \\ 0 & 1 & \mathbf{u} \\ 0 & 0 & A' \end{bmatrix} \begin{bmatrix} I & 0 & B' \\ 0 & 1 & \mathbf{v} \\ 0 & 0 & I \end{bmatrix} = \begin{bmatrix} I & 0 & B' \\ 0 & 1 & \mathbf{u} + \mathbf{v} \\ 0 & 0 & A' \end{bmatrix} = A + B - I.$$

□

**Theorem 4.5.** *Let  $S$  denote the subsemigroup of  $T_n(\mathbb{N}_0)$  of unitriangular matrices and let  $A \in S$ . Then  $L(A) = \Sigma(A)$ .*

*Proof.* Suppose that  $A = A_1 A_2 \cdots A_t$  where each  $A_i$  is a nonunit of  $S$  ( $A_i \neq I_n \forall i$ ). Then  $\Sigma(A) \geq t$  and hence  $L(A) \leq \Sigma(A)$ . Using Lemma 4.4, we now write  $A$  as

$$A = I + \sum_{i=1}^{n-1} \left( \sum_{j=1+i}^n a_{i,j} E_{i,j} \right) = \prod_{i=1}^{n-1} \left( \prod_{j=i+1}^n (I + E_{i,j})^{a_{i,j}} \right)$$

giving a factorization of  $A$  of length  $\Sigma(A)$  and hence  $L(A) \geq \Sigma(A)$ . □

The following result, which follows trivially from Theorem 4.5, gives a classification of the atoms of  $S$ .

**Corollary 4.6.** *Let  $S$  denote the semigroup of  $T_n(\mathbb{N}_0)$  of unitriangular matrices and let  $A \in S$ . Then  $A$  is an atom of  $S$  if and only if  $\Sigma(A) = 1$ .*

**Theorem 4.7.** *Let  $S$  denote the semigroup of  $T_n(\mathbb{N}_0)$  of unitriangular matrices.*

(1) *If  $n = 2$ , then  $S$  is factorial.*

(2) *If  $n \geq 3$ , then  $\rho(S) = \infty$ .*

*Proof.* If  $n = 2$ , then the only unit in  $S$  is  $I_2$  and the only atom of  $S$  is  $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ . If  $B \in S$  is a nonunit,

then  $B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$  with  $b \geq 1$ . The only factorization of  $B$  is  $B = A^b$  and hence  $S$  is factorial.

Now suppose  $n \geq 3$  and write  $A = (I + E_{1,2})^a (I + E_{2,3})^a = I + aE_{1,2} + aE_{2,3} + a^2 E_{1,3}$ . Thus  $l(A) = 2a$ . Moreover,  $L(A) = 2a + a^2$  and hence  $\rho(S) \geq \lim_{a \rightarrow \infty} \rho(A) \geq \lim_{a \rightarrow \infty} \frac{2a + a^2}{2a} = \infty$ . □

We conclude this section by considering the subsemigroup  $S$  of  $T_n(\mathbb{N})$  of unitriangular matrices. Note that we now require all entries above the diagonal to be positive. We now show that  $S$  is bifurcus and hence has infinite elasticity.

**Theorem 4.8.** *Let  $n \geq 4$  and let  $S$  denote the semigroup of  $T_n(\mathbb{N})$  of unitriangular matrices. Then  $S$  is bifurcus.*

*Proof.* First note that if  $X \in S$  can be factored as the product of two elements of  $S$ , then each of the superdiagonal entries of  $X$  is at least two. Consequently, if any of the superdiagonal entries of  $X$  are one, then  $X$  is an atom of  $S$ . Now, suppose that  $A \in S$  can be written as the product of two elements  $B, C \in S$ . That is,

$$A = \begin{bmatrix} 1 & a_{1,2} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & a_{n-1,n} \\ 0 & \cdots & \cdots & 1 \end{bmatrix} = \begin{bmatrix} 1 & b_{1,2} & \cdots & b_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & b_{n-1,n} \\ 0 & \cdots & \cdots & 1 \end{bmatrix} \begin{bmatrix} 1 & c_{1,2} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & c_{n-1,n} \\ 0 & \cdots & \cdots & 1 \end{bmatrix} = BC.$$

Let  $U = I + (1 - b_{1,2})E_{1,2} + c_{n-1,n}E_{n-1,n}$  and  $V = I + (b_{1,2} - 1)E_{1,2} + (1 - c_{n-1,n})E_{n-1,n}$ ; that is,

$$U = \begin{bmatrix} 1 & 1 - b_{1,2} & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \cdots & & 1 & c_{n-1,n} - 1 \\ 0 & \cdots & \cdots & & 1 \end{bmatrix} \text{ and } V = \begin{bmatrix} 1 & b_{1,2} - 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \cdots & & 1 & 1 - c_{n-1,n} \\ 0 & \cdots & \cdots & & 1 \end{bmatrix}.$$

Note that  $U$  and  $V$  are not elements of  $S$ . However, since  $UV = I_n$ ,  $A = BC = B(UV)C = (BU)(VC)$ . Moreover,  $BU, VC \in S$  are atoms since they each possess a one as a superdiagonal entry. Thus  $A$  can be factored as the product of two atoms of  $S$  and hence  $S$  is bifurcus.  $\square$

### 4.3 $T_2(\mathbb{N})$

Throughout this section  $S$  will denote the semigroup of all  $2 \times 2$  upper triangular matrices with positive integer entries; that is, if  $A \in S$ , then  $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$  for some positive integers  $a, b$  and  $c$ . Since  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin S$ ,  $S$  contains no units. The following lemma classifies all atoms of  $S$ .

**Lemma 4.9.** *Let  $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in S$ . Then  $A$  is an atom of  $S$  if and only if  $b = 1$ .*

*Proof.* If  $b > 1$  then we can write  $b = m + n$  with  $m, n \geq 1$ . Thus we can factor  $A$  as

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} 1 & m \\ 0 & c \end{bmatrix} \begin{bmatrix} a & n \\ 0 & 1 \end{bmatrix}$$

and hence  $A$  is a non-atom. Conversely, suppose that  $A$  can be written as the product of two elements of  $S$  as

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} s & m \\ 0 & u \end{bmatrix} \begin{bmatrix} t & n \\ 0 & v \end{bmatrix}.$$

Then  $b = sn + mv > 1$ .  $\square$

**Theorem 4.10.** *Let  $S$  be the semigroup of all  $2 \times 2$  upper triangular matrices with positive integer entries and let  $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in S$ . Then*

- (1)  $L(A) = b$ .
- (2)  $\rho(S) = \infty$ .



(3) For every prime  $p$ ,  $p - 1 \in \Delta(S)$ .

*Proof.* Consider  $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in S$ . If  $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \cdots \begin{bmatrix} a_s & b_s \\ 0 & c_s \end{bmatrix}$ , then  $b \geq b_1 + b_2 + \cdots + b_s$  and hence  $s \leq b$ . That is,  $L(A) \leq b$ . If  $b = 1$ , then  $A$  is an atom by Lemma 4.9  $k = 1$  and thus has a factorization of length  $b = 1$ . If  $b \geq 2$ , then we can factor  $A$  as

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & c \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{b-2} \begin{bmatrix} a & 1 \\ 0 & 1 \end{bmatrix}$$

and hence (again by Lemma 4.9)  $A$  has a factorization of length  $b$ .

Let  $n$  be a positive integer and consider the following matrix  $B = \begin{bmatrix} 2^n & 2^{n+1} \\ 0 & 2^n \end{bmatrix} \in S$ . Since  $B = \begin{bmatrix} 2^n & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 2^n \end{bmatrix}$   $l(B) = 2$  by Lemma 4.9. From (1),  $L(B) = 2^{n+1}$ . Therefore,  $\rho(B) = \frac{2^{n+1}}{2}$ . Taking the limit as  $n$  approaches infinity gives us that  $\rho(S) = \infty$ .

Let  $p$  be a prime and consider the matrix  $P = \begin{bmatrix} p & p+1 \\ 0 & 1 \end{bmatrix} \in S$ . Since  $p$  is prime, if

$$P = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix},$$

then  $a_1, a_2 \in \{1, p\}$  and  $c_1 = c_2 = 1$ . Thus, by Lemma 4.9, the only atoms that can appear in a factorization of  $P$  are  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and  $\begin{bmatrix} p & 1 \\ 0 & 1 \end{bmatrix}$ . Furthermore, the matrix  $\begin{bmatrix} p & 1 \\ 0 & 1 \end{bmatrix}$  must appear exactly once in any factorization of  $P$ . Thus, the only factorizations of  $P$  have the form

$$P = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^m \begin{bmatrix} p & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{t-m-1}$$

where  $t$  is the length of the factorization and  $0 \leq m \leq t-1 \leq p$ . If  $t-m-1 = 0$ , then  $t = p+1$ . If  $t-m-1 \geq 1$ , then

$$P = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^m \begin{bmatrix} p & p(t-m-1)+1 \\ 0 & 1 \end{bmatrix}$$

and hence  $p(t-m-1)+1 \leq p+1$  which implies that  $t-m-1 = 1$ ; i.e.,  $t = 2$ . Therefore, all factorizations of  $P$  have length 2 or  $p+1$  and hence  $\Delta(P) = \{p-1\}$ .  $\square$

#### 4.4 $T_2(\mathbb{N}_0)$

In this section we consider the semigroup  $S$  of upper triangular  $2 \times 2$  matrices with nonnegative entries and non-zero determinant; that is, if  $A \in S$  then  $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$  where  $a, c \in \mathbb{N}$  and  $b \in \mathbb{N}_0$ . Note that in this case  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  is the only unit of  $S$ . As in the previous section, we first classify the atoms of  $S$ .

**Lemma 4.11.** *Let  $S$  denote the subsemigroup of invertible matrices in  $T_2(\mathbb{N}_0)$ . The set of atoms of  $S$  consists of the matrix  $X = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and the matrices — for each prime  $p$  —  $Y_p = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$  and  $Z_p = \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}$ .*

*Proof.* Suppose that  $X = X_1 X_2$  for some  $X_1, X_2 \in S$ . Since  $\det(X) = 1$ ,  $\det(X_1) = \det(X_2) = 1$  and we can write

$$X_1 X_2 = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

where  $m+n=1$ . Thus either  $X_1$  or  $X_2$  is the identity and hence  $X$  is an atom.

Suppose now that  $p$  is prime and  $Y_p = Y_1 Y_2$  for some  $Y_1, Y_2 \in S$ . Since  $p$  is prime, either

$$Y_1 Y_2 = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & p \end{bmatrix}$$

with  $0 = n + mp$  or

$$Y_1 Y_2 = \begin{bmatrix} 1 & n \\ 0 & p \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$$

with  $0 = n + m$ . In either case,  $m = 0$  and hence  $Y_p$  is an atom of  $S$ . Similarly one can see that each  $Z_p$  is an atom of  $S$ .

Finally, we show that these are the only atoms of  $S$ . Let  $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in S$ . Following the proof of Lemma 4.9, we see that if  $b \geq 2$  then  $A$  is a non-atom of  $S$ . Suppose  $A = \begin{bmatrix} a & 1 \\ 0 & c \end{bmatrix}$  and note that we can factor  $A$  as

$$A = \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} \begin{bmatrix} a & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & c \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus  $A$  is an atom if and only if  $a = c = 1$ ; that is,  $A = X$ . Now suppose  $A = \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix}$  and note that  $A$  can be factored as

$$A = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & 1 \end{bmatrix}$$

where  $a_1$  and  $a_2$  are factors of  $a$  and  $c_1$  and  $c_2$  are factors of  $c$ . Thus  $A$  is an atom if and only if  $A = Y_p$  or  $A = Z_p$  for some prime  $p$ .  $\square$

Throughout the remainder of this section we let  $r(A)$  denote the number of (not necessarily distinct) prime factors of  $\det(A)$ .

**Lemma 4.12.** *If  $A$  can be factored as  $A = A_1 A_2 \cdots A_t$  with each  $A_i$  an atom of  $S$ , then  $t = r(A) + k$  where  $k = \left| \left\{ i : A_i = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\} \right|$ .*

*Proof.* For each  $i$ ,  $A_i$  is an atom and thus  $\det(A_i)$  is either 1 or is prime. Since  $\det(A) = \det(A_1) \det(A_2) \cdots \det(A_t)$ ,  $|\{i : \det(A_i) \text{ is prime}\}| = r(A)$ . If  $k = |\{i : \det(A_i) = 1\}|$  then the length of the factorization is

$$t = |\{i : \det(A_i) \text{ is prime}\}| + |\{i : \det(A_i) = 1\}| = r(A) + k.$$

$\square$

**Theorem 4.13.** *Let  $S$  denote the subsemigroup of invertible matrices in  $T_2(\mathbb{N}_0)$  and let  $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in S$ .*

(1) *If  $b = 0$ , then  $l(A) = r(A)$ .*

(2) *If  $b|ac$ , then  $l(A) = r(A) + 1$ .*

(3)  *$L(A) = r(A) + b$ .*

*Proof.* Suppose that  $b = 0$  and write  $l(A) = r(A) + k$  as in Lemma 4.12. If  $k \geq 1$  then any factor containing  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  cannot have two nonzero entries. This contradicts  $b = 0$  and hence  $k = 0$ . That is,  $l(A) = r(A)$ .

Now suppose that  $b|ac$ . Again write  $l(A) = r(A) + k$  as in Lemma 4.12. Since  $b > 0$ ,  $k \geq 1$  and hence  $l(A) \geq r(A) + 1$ . Write  $a = ma'$ ,  $c = nc'$  and  $b = a'c'$  and factor  $A$  as

$$A = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix} \begin{bmatrix} a' & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & c' \end{bmatrix} \begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix}.$$

Therefore,

$$\begin{aligned} l(A) &\leq l\left(\begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}\right) + l\left(\begin{bmatrix} a' & 0 \\ 0 & 1 \end{bmatrix}\right) + l\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) + l\left(\begin{bmatrix} 1 & 0 \\ 0 & c' \end{bmatrix}\right) + l\left(\begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix}\right) \\ &= r(n) + r(a') + 1 + r(c') + r(m) \\ &= r(na'c'm) + 1 \\ &= r(A) + 1. \end{aligned}$$

Note that for any matrix  $\begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} \in S$ ,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^r \begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^s = \begin{bmatrix} a' & d \\ 0 & c' \end{bmatrix}$$

with  $d \geq r + s$ . Thus, if  $A = A_1 A_2 \cdots A_t$  with each  $A_i$  an atom of  $S$ ,  $b \geq |\{i : \det(A_i) = 1\}|$ . By Lemma 4.12,  $l(A) = r(A) + k$  with  $b \geq k$ . Thus  $L(A) \leq r(A) + b$ . Since

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^b \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix},$$

we have that

$$\begin{aligned} L(A) &\geq l\left(\begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix}\right) + b \cdot l\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) + l\left(\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}\right) \\ &= r(c) + b + r(a) \\ &= r(A) + b. \end{aligned}$$

□

**Corollary 4.14.** *Let  $S$  denote the subsemigroup of invertible matrices in  $T_2(\mathbb{N}_0)$  and let  $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in S$ .*

(1) *If  $b = 0$ , then  $\rho(A) = 1$ .*

(2) *If  $b|ac$ , then  $\rho(A) = \frac{r(A)+b}{r(A)+1}$ .*

(3)  *$\rho(S) = \infty$ .*

*Proof.* The proofs of (1) and (2) follow immediately from Theorem 4.13.

Consider, for each prime  $p$  the matrix  $A_p = \begin{bmatrix} p & p \\ 0 & p \end{bmatrix}$ . By (2),  $\rho(A_p) = \frac{p+2}{3}$ . Allowing  $p$  to tend towards infinity, we see that  $\rho(S) = \infty$ . □

## 5 Gaussian Matrices

In this section we investigate the factorization properties of semigroups of  $n \times n$  Gaussian matrices — matrices differing from the identity matrix  $I_n$  only in the  $j$ th column which has the form

$$\begin{bmatrix} 0 & \cdots & 0 & 1 & a_{j+1,j} & a_{j+2,j} & \cdots & a_{n,j} \end{bmatrix}^T$$

for some  $j$ ,  $1 \leq j \leq n-1$ . Gaussian elimination of column  $j$  of a matrix is achieved by multiplication by a Gaussian matrix with nonzero off diagonal entries in the  $j$ th column. This type of matrix is essential in  $LU$  factorizations and thus have a wide array of applications in both pure and applied mathematics (cf. [GL96], [SH00] and [Fru87]).

Note that when two Gaussian matrices are multiplied, the only entries affected are the off diagonal entries. Furthermore, if  $A = BC$  where  $A, B, C$  are Gaussian matrices with all nonzero off diagonal entries in fixed column  $j$ , then

$$\begin{bmatrix} a_{j+1,j} \\ a_{j+2,j} \\ \vdots \\ a_{n,j} \end{bmatrix} = \begin{bmatrix} b_{j+1,j} \\ b_{j+2,j} \\ \vdots \\ b_{n,j} \end{bmatrix} + \begin{bmatrix} c_{j+1,j} \\ c_{j+2,j} \\ \vdots \\ c_{n,j} \end{bmatrix}.$$

This immediately yields the following lemma.

**Lemma 5.1.** *Let  $S$  denote the semigroup of  $n \times n$  Gaussian matrices differing from the identity matrix  $I_n$  only in the  $j$ th column which has the form  $\begin{bmatrix} 0 & \cdots & 0 & 1 & a_{j+1,j} & a_{j+2,j} & \cdots & a_{n,j} \end{bmatrix}^T$  for some  $j$ ,  $1 \leq j \leq n-1$ .*

(1) If  $a_{k,j} \in \mathbb{N}$  for all  $k \in \{j+1, \dots, n\}$ , then let  $T = \{0\} \cup \mathbb{N}^{n-j}$ .

(2) If  $a_{k,j} \in \mathbb{N}_0$  for all  $k \in \{j+1, \dots, n\}$ , then let  $T = \mathbb{N}_0^{n-j}$ .

There exists a transfer homomorphism  $\phi : (S, \cdot) \rightarrow (T, +)$  defined by  $[\mathbf{a}_1 \ \cdots \ \mathbf{a}_n] \mapsto [a_{j+1,j} \ a_{j+2,j} \ \cdots \ a_{n,j}]^T$ . In particular,  $S$  is commutative.

The following two theorems give factorization properties of Gaussian matrices over  $\mathbb{N}$  and over  $\mathbb{N}_0$  in which we see a dramatic difference in uniqueness of factorization depending on whether or not entries of the  $j$ th column below the diagonal are allowed to be zero.

**Theorem 5.2.** *Let  $S$  denote the subsemigroup of  $M_n(\mathbb{N})$  of Gaussian matrices with nonzero off diagonal entries in column  $j$  and let  $A \in S$ .*

- (1)  $A$  is an atom if and only if 1 is an off diagonal entry of  $A$ .
- (2)  $L(A)$  is equal to the minimal positive off diagonal entry of  $A$ .
- (3) If  $j = n - 1$ , then  $S$  is factorial.
- (4) If  $j \neq n - 1$ , then  $S$  is bifurcus.

*Proof.* In light of Lemma 5.1 we consider, instead, factorizations in  $T = \{0\} \cup \mathbb{N}^{n-j}$ . Suppose that  $\mathbf{a} = \mathbf{b} + \mathbf{c}$  for some  $\mathbf{a}, \mathbf{b}, \mathbf{c} \in T$ . Let  $a_i$  denote a positive entry of  $\mathbf{a}$ . Then  $a_i = b_i + c_i > 1$ . Assume now that  $a := a_i > 1$  is the minimal entry of  $\mathbf{a}$ . Then  $a_i - (a - 1) = 1$  and hence we can factor  $\mathbf{a}$  as

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-j} \end{bmatrix} = a \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} + \begin{bmatrix} a_1 - (a - 1) \\ a_2 - (a - 1) \\ \vdots \\ a_{n-j} - (a - 1) \end{bmatrix}.$$

Therefore,  $\mathbf{a}$  is an atom of  $T$  if and only if  $a_i = 1$  for some  $i$ . Moreover,  $L(\mathbf{a})$  is at least the minimal positive entry of  $\mathbf{a}$ . However, if  $L(\mathbf{a}) > a$ , then  $a_i \geq L(\mathbf{a}) > a = a_i$ , a contradiction. Therefore,  $L(\mathbf{a})$  is equal to the minimal positive entry of  $\mathbf{a}$ .

Suppose that  $j = n - 1$ . Then  $T = \mathbb{N}_0$  has a unique factorization and hence both  $T$  and  $S$  are half-factorial.

Suppose now that  $j \neq n - 1$ . If  $\mathbf{a}$  is not an atom of  $T$  then  $a_k \geq 2$  for all  $k \in \{1, 2, \dots, n - j\}$ . Thus we can write

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n-j} \end{bmatrix} = \begin{bmatrix} 1 \\ a_2 - 1 \\ a_3 - 1 \\ \vdots \\ a_{n-j} - 1 \end{bmatrix} + \begin{bmatrix} a_1 - 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

and hence  $\mathbf{a}$  can be written as the sum of two atoms. That is,  $T$ , and hence  $S$  is bifurcus.  $\square$

**Theorem 5.3.** *Let  $S$  denote the subsemigroup of  $M_n(\mathbb{N}_0)$  of Gaussian matrices with nonnegative off diagonal entries in column  $j$  and let  $A \in S$ .*

- (1)  $A$  is an atom if and only if all entries in column  $j$  are zero except for  $a_{j,j} = a_{k,j} = 1$  for some  $k \in \{j+1, j+2, \dots, n\}$ .
- (2)  $S$  is factorial.

*Proof.* Again, in light of Lemma 5.1, we consider factorization in  $T = \mathbb{N}_0^{n-j}$ . Assume first that all entries of an element  $\mathbf{a}$  are zero except one single entry. Assume that  $a_i = 1$  for some  $i \in \{1, 2, \dots, n - j\}$ . If  $\mathbf{a} = \mathbf{b} + \mathbf{c}$  for some  $\mathbf{b}, \mathbf{c} \in T$ , then  $b_i + c_i = 1$  and  $b_k + c_k = 0$  for all  $k \in \{1, 2, \dots, n - j\} \setminus \{i\}$ . Thus either  $\mathbf{a} = \mathbf{b}$  and  $\mathbf{c} = \mathbf{0}$  or

$\mathbf{a} = \mathbf{c}$  and  $\mathbf{b} = \mathbf{0}$ . Either way, we see that  $\mathbf{a}$  is an atom of  $T$ . Now suppose that  $\mathbf{a}$  has more than one positive entry. Without loss of generality, assume that  $a_1, a_2 > 0$ . Then

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n-j} \end{bmatrix} = \begin{bmatrix} 1 \\ a_2 - 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} a_1 - 1 \\ 1 \\ a_3 \\ \vdots \\ a_{n-j} \end{bmatrix}$$

and hence  $\mathbf{a}$  is not an atom of  $T$ .

Note that each element  $\mathbf{a}$  of  $T$  can be uniquely factored as

$$\mathbf{a} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-j} \end{bmatrix} = a_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + a_2 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + a_{n-j} \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

and hence  $T$  is factorial.  $\square$

## 6 Rank One Matrices

Rank one matrices have been intensely studied from many different perspectives and have a wide array of applications (cf. [Son05], [wLdZ06] and [SK03]). Throughout this section, let  $n \geq 2$  and let  $S$  denote the subsemigroup of  $M_n(\mathbb{N})$  of matrices with rank one. Note that  $S$  contains no identity and no units. We recall that if  $A \in M_n(\mathbb{N})$  has rank one, then  $A = \mathbf{u}\mathbf{v}^T$  for some vectors  $\mathbf{u}, \mathbf{v} \in \mathbb{N}^n$ . The following lemma will be useful in studying factorizations in  $S$ .

### 6.1 Preliminaries

**Lemma 6.1.** *Let  $\mathbf{u}$  and  $\mathbf{v}$  be vectors in  $\mathbb{N}^n$  and set  $A = \mathbf{u}\mathbf{v}^T$ . Then  $\gcd(A) = \gcd(\mathbf{u})\gcd(\mathbf{v})$ .*

*Proof.* Note that  $\frac{1}{\gcd(\mathbf{u})\gcd(\mathbf{v})}A = \left(\frac{1}{\gcd(\mathbf{u})}\mathbf{u}\right)\left(\frac{1}{\gcd(\mathbf{v})}\mathbf{v}^T\right)$  and thus we may assume that  $\gcd(\mathbf{u}) = \gcd(\mathbf{v}) = 1$ . Suppose that  $m \mid \gcd(A)$  for some  $m > 1$ . Then  $m$  divides each entry of  $A$  and in particular each entry in column  $i$  of  $A$  for each  $i \in \{1, 2, \dots, n\}$ . However, the  $i$ th column of  $A$  is the vector  $v_i\mathbf{u}$ . Since  $\gcd(\mathbf{u}) = 1$ ,  $m \mid v_i$ . As this holds for all  $i \in \{1, 2, \dots, n\}$ ,  $m \mid \gcd(\mathbf{v})$ , a contradiction. Thus  $\gcd(A) = 1$ .  $\square$

**Theorem 6.2.** *Let  $S$  denote the subsemigroup of  $M_n(\mathbb{N})$  consisting of all matrices with rank one and let  $A \in S$ .*

(1)  *$A$  is an atom of  $S$  if and only if  $\gcd(A) < n$ .*

(2)  *$S$  is bifurcus.*

*Proof.* Suppose that  $A = A_1A_2$  for  $A_1, A_2 \in S$ . Since  $A_1$  and  $A_2$  have rank one, there exist vectors  $\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_1, \mathbf{v}_2 \in \mathbb{N}^n$  such that  $A_1 = \mathbf{u}_1\mathbf{v}_1^T$  and  $A_2 = \mathbf{u}_2\mathbf{v}_2^T$ . Since  $\mathbf{v}_1^T\mathbf{u}_2$  is a scalar, we have that

$$A = (\mathbf{u}_1\mathbf{v}_1^T)(\mathbf{u}_2\mathbf{v}_2^T) = \mathbf{u}_1(\mathbf{v}_1^T\mathbf{u}_2)\mathbf{v}_2^T = (\mathbf{v}_1^T\mathbf{u}_2)(\mathbf{u}_1\mathbf{v}_2^T).$$

Since the entries of  $\mathbf{v}_1^T$  and  $\mathbf{u}_2$  are positive integers,  $\gcd(A) \geq (\mathbf{v}_1^T\mathbf{u}_2) \geq n$ . Now suppose that  $\gcd(A) \geq n$  and write  $A = \gcd(A)B$  where  $B$  is an atom of  $S$ . Write  $B = \mathbf{u}\mathbf{v}^T$  for some vectors  $\mathbf{u}$  and  $\mathbf{v}$ . Since  $\gcd(A) \geq n$ , write  $\gcd(A) = \mathbf{x}^T\mathbf{y}$  where  $\mathbf{x} = [\gcd(A) - n + 1 \quad 1 \quad 1 \quad \cdots \quad 1]^T$  and  $\mathbf{y} = [1 \quad 1 \quad \cdots \quad 1]^T$ . Then

$$A = \gcd(A)B = (\mathbf{x}^T\mathbf{y})(\mathbf{u}\mathbf{v}^T) = \mathbf{u}(\mathbf{x}^T\mathbf{y})\mathbf{v}^T = (\mathbf{u}\mathbf{x}^T)(\mathbf{y}\mathbf{v}^T).$$

Since  $B = \mathbf{u}\mathbf{v}^T$  and  $\gcd(B) = 1$ ,  $\gcd(\mathbf{u}) = \gcd(\mathbf{v}) = 1$  by Lemma 6.1. Again applying Lemma 6.1, we see that  $\mathbf{u}\mathbf{x}^T$  and  $\mathbf{y}\mathbf{v}^T$  are atoms of  $S$ . Thus  $A$  is an atom of  $S$  if and only if  $\gcd(A) = 1$ . Moreover, we have shown that  $S$  is bifurcus as every nonatom can be factored as the product of two atoms of  $S$ .  $\square$

The following theorem gives a formula for  $L(A)$  where  $A \in S$  and shows that computing  $L(A)$  is an NP-complete problem. First, we define, for integers  $n$  and  $m$ ,  $\Psi_n(m)$  to be the greatest integer  $k$  such that there exist integers  $m_1, m_2, \dots, m_k, r$  such that  $m = m_1 m_2 \cdots m_k r$  with  $r < n \leq m_i$  for each  $i$ . We note that  $\Psi_n(m)$  is at most the number of primes counting multiplicity in the prime factorization of  $m$ , with equality if  $n=2$ .

**Theorem 6.3.** *Let  $S$  denote the subsemigroup of  $M_n(\mathbb{N})$  consisting of all matrices with rank one and let  $A \in S$ .*

- (1) *Then  $L(A) = \Psi_n(\gcd(A)) + 1$ .*
- (2) *Calculating  $L(A)$  is a NP-complete problem*

*Proof.* Assume that  $A$  has some factorization of length  $t$  and write  $A = \prod_{i=1}^t A_i = \prod_{i=1}^t \mathbf{u}_i \mathbf{v}_i^T$  where each  $A_i = \mathbf{u}_i \mathbf{v}_i^T$  is an atom of  $S$ . We can rewrite this product as

$$A = \prod_{i=1}^t \mathbf{u}_i \mathbf{v}_i^T = \mathbf{u}_1 \mathbf{v}_1^T \prod_{i=1}^{t-1} \langle \mathbf{v}_i, \mathbf{u}_{i+1} \rangle$$

where  $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x} \mathbf{y}^T$  denotes the standard inner product of vectors  $\mathbf{x}$  and  $\mathbf{y}$ . Since each  $\langle \mathbf{v}_i, \mathbf{u}_{i+1} \rangle$  is the sum of  $n$  positive integers,  $\langle \mathbf{v}_i, \mathbf{u}_{i+1} \rangle \geq n$  for each  $i \in \{1, 2, \dots, t-1\}$ . By Lemma 6.1,  $\gcd(A) = \gcd(\mathbf{u}_1) \gcd(\mathbf{v}_t) \prod_{i=1}^{t-1} \langle \mathbf{v}_i, \mathbf{u}_{i+1} \rangle$  and hence

$$\Psi_n(\gcd(A)) = \Psi_n \left( \gcd(\mathbf{u}_1) \gcd(\mathbf{v}_t) \prod_{i=1}^{t-1} \langle \mathbf{v}_i, \mathbf{u}_{i+1} \rangle \right) \geq \Psi_n \left( \prod_{i=1}^{t-1} \langle \mathbf{v}_i, \mathbf{u}_{i+1} \rangle \right) \geq t-1.$$

Therefore,  $L(A) \leq \Psi_n(\gcd(A)) + 1$ .

Now suppose that  $\Psi_n(A) = k$  and write  $\gcd(A) = r m_1 m_2 \cdots m_k$  for some integers  $r, m_1, m_2, \dots, m_k$  with  $r < n \leq m_i$  for each  $i \in \{1, 2, \dots, k\}$ . For each  $i \in \{1, 2, \dots, k\}$  we can write  $A = r m_1 m_2 \cdots m_i B_i$  for an appropriate matrix  $B_i \in S$ . Since  $\gcd(m_i B_i) \geq m_i \geq n$ ,  $m_i B_i$  is not an atom of  $S$  and thus we can write  $m_i B_i = B_{i-1} C_i$  for some atom  $C_i \in S$ . Therefore,

$$A = r m_1 m_2 \cdots m_k B_k = (r B_0) C_1 C_2 \cdots C_k.$$

Therefore  $A$  has a factorization of length at least  $k+1$  and consequently  $L(A) \geq \Psi_n(\gcd(A)) + 1$ .

If  $m = p_1 p_2 \cdots p_t$  with each  $p_i$  prime, then  $\Psi_n(m)$  is equal to the maximum number of disjoint subsets  $\{a_1, a_2, \dots, a_s\}$  of  $\{1, 2, \dots, t\}$  such that  $p_{a_1} p_{a_2} \cdots p_{a_s} \geq n$ . Thus  $\log(p_{a_1}) + \log(p_{a_2}) + \cdots + \log(p_{a_s}) \geq \log(n)$  and hence finding  $\Psi_n(m)$  is equivalent to solving a bin-covering problem. Therefore, calculating  $\Psi_n(m)$  is a NP-complete problem.  $\square$

## 6.2 Rank One Matrices with Entries in $m\mathbb{N}$

In this section we restrict to the subsemigroup  $S_m$  of rank one matrices in  $M_n(m\mathbb{N})$  where  $m \geq 1$  is an integer. The following lemma allows us to apply factorization information gleaned from  $S_1$  (Theorem 6.2) to the semigroup  $S_m$ .

**Lemma 6.4.** *Let  $m \geq 1$  be an integer, let  $S_m$  denote the subsemigroup of rank one matrices in  $M_n(m\mathbb{N})$  and let  $A \in S_m$ .*

- (1) *If  $m^2 \nmid \gcd(A)$  then  $A$  is an atom of  $S_m$ .*
- (2) *If  $A = m^2 B$  with  $B \in S_1$ , then  $A$  is an atom of  $S_m$  if and only if  $B$  is an atom of  $S_1$ .*

*Proof.* Suppose that  $A = A_1 A_2$  with  $A_1, A_2 \in S_m$ . Then  $A = (m B_1)(m B_2) = m^2 B_1 B_2$  for some  $B_1, B_2 \in S_1$ . Thus if  $m^2 \nmid \gcd(A)$ , then  $A$  is an atom of  $S_m$ .

Now suppose that  $A = m^2 B$  for some  $B \in S_1$ . If  $B = B_1 B_2$  for some  $B_1, B_2 \in S_1$  then  $A = m^2 B = (m B_1)(m B_2)$  with  $m B_1, m B_2 \in S_m$ . If  $A = A_1 A_2$  with  $A_1, A_2 \in S_m$  then  $m^2 B = A = A_1 A_2 = (m C_1)(m C_2)$  for some  $C_1, C_2 \in S_1$  and hence  $B = C_1 C_2$ . Thus  $A$  is an atom of  $S_m$  if and only if  $B$  is an atom of  $S_1$ .  $\square$

**Theorem 6.5.** *Let  $m \geq 1$  be an integer and let  $S_m$  denote the subsemigroup of rank one matrices in  $M_n(m\mathbb{N})$ . Then  $S_m$  is bifurcus.*

*Proof.* Let  $A \in S_m$  be a nonatom and factor  $A$  as  $A = A_1 A_2$  for some  $A_1, A_2 \in S_m$ . By Lemma 6.4,  $A = (mB_1)(mB_2)$  for some  $B_1, B_2 \in S_1$ . By Theorem 6.2,  $S_1$  is bifurcus and so  $A = m^2 B_1 B_2 = m^2 P_1 P_2 = (mP_1)(mP_2)$  for some atoms  $P_1, P_2 \in S_1$ . If  $mP_i = XY$  for  $X, Y \in S_m$  then  $mP_i = mX'Y$  with  $X' \in S_1$  and hence  $P_i = X'Y$  with  $X', Y \in S_1$ , contradicting that  $P_i$  is an atom of  $S_1$ . Therefore,  $A$  can be factored as the product of two atoms in  $S_m$  and hence  $S_m$  is bifurcus.  $\square$

### 6.3 The Semiring of Single-Valued Matrices

In this section we consider a specific class of rank one matrices — the class of  $n \times n$  matrices in which all entries are identical. Jacobson [Jac65] considered the  $2 \times 2$  case and was able to classify the atoms of this semigroup and give examples of nonunique factorization. We extend these results to  $n \times n$  single-valued matrices over  $\mathbb{N}$ ,  $\mathbb{N}_0$  and  $\mathbb{Z}$ . We adopt Jacobson's notation and let  $[a]$  denote the  $n \times n$  matrix for which every entry is  $a$ . The simple observation that if  $[a]$  and  $[b]$  are  $n \times n$  matrices, then  $[a][b] = [nab]$  allows us to classify the atoms and to compute various factorization invariants. The following theorems are stated for the semigroup  $S$  of nonzero single-valued matrices with integer entries, but the results hold if we restrict to nonnegative entries or to only positive entries. In either case, it is easy to see that  $S$  has no units.

**Lemma 6.6.** *Let  $S$  denote the semigroup of nonzero single-valued  $n \times n$  matrices with integer entries and let  $[a] \in S$ . Then  $[a]$  is an atom of  $S$  if and only if  $n \nmid a$ .*

*Proof.* If  $[a]$  factors as  $[a] = [s][t]$ , then  $[a] = [s][t] = [nst]$  and hence  $n \mid a$ . Conversely, if  $n \mid a$  then we can factor  $[a]$  as  $[a] = [nst] = [s][t]$ .  $\square$

Recall that  $\nu_n(a)$  denotes the largest integer  $k$  such that  $a$  is divisible by  $n^k$ .

**Theorem 6.7.** *Let  $n \geq 2$  and let  $S$  denote the semigroup of nonzero single-valued  $n \times n$  matrices with integer entries. Let  $[a] \in S$ .*

- (1)  $L([a]) = \nu_n(a) + 1$ .
- (2) If  $n = p^k$  for some prime  $p$ , then  $l([a]) = \left\lceil \frac{\nu_p(a)+k}{2k-1} \right\rceil$  and  $\rho(S) = \frac{2k-1}{k}$ .
- (3) If  $n$  is not the power of a prime, then  $S$  is bifurcus.
- (4) If  $n$  is prime, then  $S$  is half-factorial.
- (5) If  $n$  is not prime, then  $\Delta(S) = \{1\}$ .

*Proof.* Suppose that  $[a]$  can be factored as  $[a] = [a_1][a_2] \cdots [a_t]$  with each  $[a_i] \in S$ . Then  $[a] = [n^{t-1}a_1 a_2 \cdots a_t]$  and hence  $\nu_n(a) \geq t - 1$ . Therefore,  $L([a]) \leq \nu_n(a) + 1$ . Since  $[a]$  can be factored as  $[a] = [1]^{\nu_n(a)} \left[ \frac{a}{n^{\nu_n(a)}} \right]$ ,  $L([a]) \geq \nu_n(a) + 1$ .

Assume now that  $n = p^k$  for some prime  $p$ . Write  $a = p^m y$  with  $p \nmid y$  and suppose that  $[a]$  has a factorization of length  $d$ . Then

$$[a] = [p^m y] = [p^{m_1} y_1][p^{m_2} y_2] \cdots [p^{m_d} y_d]$$

where  $y = y_1 y_2 \cdots y_d$  and  $m = m_1 + m_2 + \cdots + m_d + k(d-1)$ . Since we are assuming each  $[p^{m_i} y_i]$  is an atom of  $S$ ,  $0 \leq m_i \leq k-1$  for each  $i \in \{1, 2, \dots, d\}$ . Let  $c$  be the nonnegative integer such that  $m_1 + m_2 + \cdots + m_d = d(k-1) - c$ . Then

$$d = \frac{m - d(k-1) + c}{k} + 1 = \frac{m + c + k}{2k-1} \geq \left\lceil \frac{m+k}{2k-1} \right\rceil.$$

Therefore,  $l([a]) = \left\lceil \frac{m+k}{2k-1} \right\rceil$ .

Observe that for any  $[p^m y] \in S$ ,

$$\rho([p^m y]) = \frac{\left\lfloor \frac{m}{k} \right\rfloor + 1}{\left\lceil \frac{m+k}{2k-1} \right\rceil} \leq \frac{\frac{m}{k} + 1}{\frac{m+k}{2k-1}} = \frac{2k-1}{k}.$$

This elasticity is achieved since  $[p^{2k(k-1)}] = [1]^{2k-1} = [p^{k-1}]^k$ .

If  $n$  is prime, then  $\rho(S) = 1$  by (2), hence half-factorial. If  $n = p^k$  for some  $k > 1$  then writing

$$[a] = [p^m y] = [p^{m_1} y_1][p^{m_2} y_2] \cdots [p^{m_d} y_d]$$

where  $y = y_1 y_2 \cdots y_d$  and  $m = m_1 + m_2 + \cdots + m_d + k(d-1)$  we see that  $m_1 + m_2 + \cdots + m_d$  can take all integer values between 0 and  $n(k-1)$ . Thus,  $\Delta([a]) = \{1\}$  for all  $[a] \in S$  and hence  $\Delta(S) = \{1\}$ .

Finally, assume that  $n = st$  with  $s, t > 1$  and  $\gcd(s, t) = 1$ . Then if  $[a]$  is not an atom of  $S$  we can write  $[a] = [n^{\nu_n(a)} y]$  where  $n \nmid y$ . Without loss of generality, assume that  $s \nmid y$ . Then we can factor  $[a]$  as

$$[a] = [n^{\nu_n(a)} y] = [s^{\nu_n(a)} t^{\nu_n(a)} y] = [s^{\nu_n(a)-1}] [t^{\nu_n(a)-1} y]$$

and hence  $l([a]) = 2$ . Therefore,  $S$  is bifurcus and  $\Delta(S) = \{1\}$ . □

## 7 Open Problems

We conclude with a list of open problems.

- (1) Let  $S = T_2(\mathbb{N})$  and let  $A \in S$ .
  - (a) Determine a formula for  $l(A)$ .
  - (b) Determine a formula for  $\rho(A)$ .
  - (c) Calculate  $\Delta(S)$ .
- (2) Let  $S = T_2(\mathbb{N}_0)$  and let  $A \in S$ .
  - (a) Determine a general formula for  $l(A)$ .
  - (b) Determine a formula for  $\rho(A)$ .
  - (c) Calculate  $\Delta(S)$ .
- (3) Let  $S = T_n(\mathbb{N})$  for  $n > 2$  and let  $A \in S$ .
  - (a) Determine a formula for  $l(A)$  and  $L(A)$ .
  - (b) Determine a general formula for  $\rho(A)$ .
  - (c) Calculate  $\Delta(S)$  and  $\rho(S)$ .
- (4) Let  $S = T_n(\mathbb{N}_0)$  for  $n > 2$  and let  $A \in S$ .
  - (a) Determine a formula for  $l(A)$  and  $L(A)$ .
  - (b) Determine a general formula for  $\rho(A)$ .
  - (c) Calculate  $\Delta(S)$  and  $\rho(S)$ .
- (5) Let  $S$  denote the subsemigroup of  $M_n(\mathbb{N}_0)$  of unitriangular matrices and let  $A \in S$ .
  - (a) Determine a formula for  $l(A)$ .
  - (b) Determine a general formula for  $\rho(A)$ .
  - (c) Calculate  $\Delta(S)$ .
- (6) Let  $S$  denote the subsemigroup of  $T_n(\mathbb{N}_0)$  of triangular unitriangular matrices and let  $A \in S$ .
  - (a) Enumerate the atoms of  $S$ .
  - (b) Determine a formula for  $l(A)$  and  $L(A)$ .
  - (c) Determine a general formula for  $\rho(A)$ .



## References

- [AAH<sup>+</sup>09] D. Adams, R. Ardila, D. Hannasch, A. Kosh, H. McCarthy, V. Ponomarenko, and R. Rosenbaum, *Bifurcus semigroups and rings*, INVOLVE **2** (2009), no. 3, 351–356.
- [CC85] Jèn Chung Ch’uan and Wai Fong Chuan, *Factorizations in a semigroup of integral matrices*, Linear and Multilinear Algebra **18** (1985), no. 3, 213–223.
- [CC86] ———, *Factorability of positive-integral matrices of prime determinants*, Bull. Inst. Math. Acad. Sinica **14** (1986), no. 1, 11–20.
- [Coh63] P. M. Cohn, *Noncommutative unique factorization domains*, Trans. Amer. Math. Soc. **109** (1963), 313–331.
- [Est91] Dennis R. Estes, *Factorization in hereditary orders*, Linear Algebra Appl. **157** (1991), 161–164.
- [Fru87] M. A. Frumkin, *Fast computations with Frobenius matrices*, Computational processes and systems, no. 5, 1987, pp. 302–311.
- [GHK06] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics, Chapman & Hall/CRC, 2006.
- [GL96] Gene H. Golub and Charles F. Van Loan, *Matrix computations*, third ed., Johns Hopkins Studies in the Mathematical Sciences, Johns Hopkins University Press, 1996.
- [GMSGP06] Helena Sezinando Gracinda M. S. Gomes and Jean-Eric Pin, *Presentations of the Schützenberger product of  $n$  groups*, Comm. Algebra **34** (2006), no. 4, 1213–1235.
- [Gre80] Gebhard Greiter, *Nonunique factorization in subsemigroups of semigroups with unique prime factorization*, Amer. Math. Monthly **87** (1980), no. 6, 473–474.
- [Har90] Glyn Harman, *Approximation of real matrices by integral matrices*, J. Number Theory **34** (1990), no. 1, 63–81.
- [HH07] Vesa Halava and Tero Harju, *On Markov’s undecidability theorem for integer matrices*, Semigroup Forum **75** (2007), no. 1, 173–180.
- [Jac65] Bernard Jacobson, *Classroom Notes: Matrix number theory: An example of nonunique factorization*, Amer. Math. Monthly **72** (1965), no. 4, 399–402.
- [JW66] Bernard Jacobson and Robert J. Wisner, *Matrix number theory i. factorization of  $2 \times 2$  unimodular matrices*, Publ. Math. Debrecen **13** (1966), 67–72.
- [Kra07] Mark Krambites, *On the Krohn-Rhodes complexity of semigroups of upper triangular matrices*, Internat. J. Algebra Comput. **17** (2007), no. 1, 187–201.
- [Kro85] Melven Krom, *An unsolvable problem with products of matrices*, Math. System **18** (1985), no. 3, 213–223.
- [SH00] Richard Shell and Ernest Hall, *Handbook of industrial automation*, CRC Press, 2000.
- [SK03] Seok-Zun Song and Kyung-Tae Kang, *Rank and perimeter preserver of rank-1 matrices over max algebra*, Discuss. Math. Gen. Algebra Appl. **23** (2003), no. 2, 125–137.
- [Son05] Seok-Zun Song, *Separability of distinct boolean rank-1 matrices*, J. Appl. Math. Comput. **18** (2005), no. 1-2, 197–204.
- [SS06] V. N. Shevchenko and S. V. Sidorov, *On the similarity of second-order matrices over the ring of integers*, Izv. Vyssh. Uchebn. Zaved. Mat. **4** (2006), 57–64.
- [wLdZ06] Shao wu Liu and Guo dong Zhang, *Maps preserving rank 1 matrices over fields*, Heilongjiang Daxue Ziran Kexue Xuebao **23** (2006), no. 1, 138–140.