Matrix Number Theory

Factorization in Integral Matrix Semigroups *

Donald Adams
Vadim Ponomarenko†
Ryan Rosenbaum
San Diego State University

Rene Ardila
City College of New York

David Hannasch
University of Nevada, Las Vegas

Audra Kosh
University of California, Santa Barbara

Hanah McCarthy
Lawrence University

August 18, 2008

Abstract

Factorization theory is a prominent field of mathematics; however, most previous research in this area lies in the commutative case. Noncommutative factorization theory is a relatively new topic of interest. This paper examines the factorization properties of noncommutative atomic semigroups of integral matrices. In particular, semigroups with determinant conditions, triangular matrices, rank 1 matrices, and bistochastic matrices are studied with the operation of multiplication and, in a special case, addition. The authors find invariants of interest in factorization theory such as the minimum and maximum length of atomic factorizations, elasticity of the semigroups, and the delta set of the semigroups.

*Supported by National Science Foundation Grant 0647384
†Project Director

Contents

1 Introduction

Factorization theory has become a popular field in recent years. In particular, the study of non-unique factorizations has been very well developed and unified in [8]; the study of non-unique factorization, however, has been studied primarily in commutative contexts (see references in [8]). Noncommutative factorization has been studied by Cohn as early as 1963 in [4]. Noncommutative factorization has been studed in the context of matrices by Jacobson and Wisner in [15] as well as by Ch'uan and Chuan in [2]. Motivated by these results, this paper applies the concepts of contemporary factorization theory to semigroups of integral matrices.

Throughout this paper, let $\mathbb{Z}$ represent the set of integers. Let $\mathbb{N}$ be the set of natural numbers, while $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. In the factorization theory context, the notation from [1] is used. Let S be a semigroup. If $[0] \in S$, then $S^\bullet$ denotes $\{A \in S : A \text{ is not a zero divisor}\}$. When the identity $I \in S$, define $A \in S$ to be a unit if there exists some $B \in S$ such that $AB = I$ or $BA = I$. Define $S^\times$ to be the units of S and S^* to be the nonunits of S. $A, B \in S$ are considered associates, or $A \cong B$, if there exists some unit $U \in S^\times$ such that $A = BU$. $A \in S^*$ is called an atom if $A = BC$ implies that either B or C is a unit. $\mathcal{I}(S)$ denotes the set of atoms of S. Call S atomic if each $A \in S^*$ can be written as the product of atoms.

Let S be an atomic semigroup. For $A \in S^*$, define $\mathcal{L}(A)$ to be the set of lengths of atomic factorizations of A. Formally, $\mathcal{L}(A) = \{t : A = A_1 \cdots A_t$ for some $A_i \in \mathcal{I}(S)\}$. $L(A) = \sup \mathcal{L}(A)$ denotes the maximum factorization length of A, while $\ell(A) = \min \mathcal{L}(A)$ denotes the minimum factorization length of A. Define $\rho(A) = \frac{L(A)}{\ell(A)}$ to be the elasticity of A. The elasticity of S is $\rho(S) = \sup\limits_{A \in S^*} \rho(A)$.

Define $\mathcal{L}_i(A)$ such that $\mathcal{L}_i \in \mathcal{L}(A)$ and $\mathcal{L}_i(A) < \mathcal{L}_{i+1}(A)$ for $1 \leq i < |\mathcal{L}(A)|$. Let $\Delta(A) = \{\mathcal{L}_{i+1}(A) - \mathcal{L}_i(A) : 1 \leq i < |\mathcal{L}(A)|\}$ be the delta set of A. The delta set of S is defined $\Delta(S) = \bigcup\limits_{A \in S^*} \Delta(A)$. This paper evaluates these invariants for various matrix semigroups.

An atomic semigroup S is called factorial if every factorization is unique up to units; since matrix factorization is noncommutative, consider $A = P_1 P_2 = P_2 P_1$ to be two distinct factorizations of A. Call S half-factorial if $L(A) = \ell(A)$ for each $A \in S^*$. Additionally, call S *bifurcus* if $\ell(A) = 2$ for each $A \in S^*$.

Table 1: Notation

Symbol	Definition
$\mathbb{P}$	$\{p \in \mathbb{Z} : p \text{ is prime}\}$
$\det A$	the determinant of the matrix A
$r(a)$	number of primes, counting multiplicity, in $a \in \mathbb{Z}$; $r(0) = \infty$
$r(A)$	$r(\det A)$
$\omega(a)$	number of distinct primes in $a \in \mathbb{Z}$; $\omega(0) = \infty$
$\omega(A)$	$\omega(\det A)$
$\gcd(a, b)$	greatest common divisor of the integers a and b
$\gcd(A)$	greatest common divisor of the entries of the matrix A
$\eta_k(a)$	greatest integer t such that $k^t \mid a \in \mathbb{Z}$
$\eta_k(A)$	greatest integer t such that $k^t \mid \det A$
$[a]$	matrix with all entries equal to $a \in \mathbb{Z}$
$S^\times$	$\{U \in S : U^{-1} \in S\}$
$\mathcal{I}(S)$	$\{P \in S : P \notin S^\times \text{ and } P = AB \Rightarrow \text{one of } A, B \in S^\times\}$
$\mathcal{L}(A)$	$\{t : \exists P_1, P_2, \ldots P_t \in \mathcal{I}(S)(A = P_1 P_2 \cdots P_t)\}$
$L(A)$	$\sup \mathcal{L}(A)$
$\ell(A)$	$\min \mathcal{L}(A)$
$\rho(A)$	$\frac{L(A)}{\ell(A)}$
$\rho(S)$	$\sup\limits_{A \in S} \rho(A)$
$\Delta(A)$	$\{\mathcal{L}_{i+1} - \mathcal{L}_i : 1 \leq i < \lvert\mathcal{L}(A)\rvert\}$
$\Delta(S)$	$\bigcup\limits_{A \in S} \Delta(A)$
$S^\bullet$	$\{A \in S : \forall B \in S(B \neq [0] \Rightarrow AB, BA \neq [0])\}$

Table 2: B: semigroup is bifurcus (see Corollary 2.7); F: semigroup is factorial or half-factorial (see Introduction)

Semigroup	Atoms	ℓ	L	ρ	Δ
Integer Entries	3.7	3.7	F	F	F
Triangular, $\mathbb{Z}$	3.7	3.7	F	F	F
$\det A > 1$	3.7	3.7	F	F	F
Triangular, $\det A > 1$	3.7	3.7	F	F	F
$k \mid \det A$, $k = p^h$	3.11	3.12	3.10	3.14	3.16
$k \mid \det A$, $k \neq p^h$	3.11	3.17	3.10	B	B
Composite Determinant	3.19	3.21	3.20	3.22	3.23
2×2 Triangular, $\mathbb{N}$	4.1	n/a	4.2	4.3	4.4
2×2 Triangular, $\mathbb{N}_0$	4.8	n/a	4.13	n/a	n/a
Triangular, entries divisible by k	4.16	4.17	4.15	B	B
2×2 Triangular, entries in 3 ideals	4.18	4.18	4.21	B	B
$n \times n$ Unitriangular, $\mathbb{N}$	n/a	4.27	n/a	B	B
$n \times n$ Unitriangular, $\mathbb{N}_0$	4.25	n/a	4.24	4.26	n/a
2×2 Unitriangular	4.29	4.30	F	F	F
3×3 Unitriangular, $\mathbb{N}$	4.40	4.27	4.41	B	B
3×3 Unitriangular, $\mathbb{N}_0$	4.36	4.38	4.35	4.39	4.38
4×4 Unitriangular, $\mathbb{N}$	4.42	4.42	n/a	B	B
Gauss Matrices, $\mathbb{N}$	4.43	4.44	4.44	B/F	B/F
Gauss Matrices, $\mathbb{N}_0$	4.45	4.46	F	F	F
2×2 Equal-Diagonal Triangular	4.51	4.56	4.54	4.57	4.61
Rank 1, $\mathbb{N}$	5.2	5.2	5.4	B	B
Rank 1, $m\mathbb{N}$	5.5	5.5	5.7	B	B
Rank 1 generated by a set of vectors	5.13	5.15	5.13	B	B
Rows of Zero	5.16	5.16	5.17	B	B
Single-Value, $n = p^k$	5.18	5.19	5.19	5.19	5.19
Single-Value, $n = st$ and $\gcd(st) = 1$	5.18	5.19	5.19	B	B
Bistochastic $(+)$, $\mathbb{N}$	6.2	6.3	6.1	B	B
Bistochastic $(+)$, $\mathbb{N}_0$	6.6	6.7	F	F	F
2×2 Bistochastic $(\times)$ $\det A$ odd, $\mathbb{N}$	6.9	n/a	6.10	n/a	n/a

2 General Results

Theorem 2.1. *Let S be an atomic semigroup. S is half-factorial if and only if there exists a $\phi : S \to \mathbb{N}$ such that $\phi(AB) = \phi(A) + \phi(B)$ for all $A, B \in S$ and $\phi(P) = 1$ for all atoms $P \in S$. If such a ϕ exists, then $L(A) = \ell(A) = \phi(A)$ for all $A \in S$.*

Proof. Suppose that there exists such a ϕ. Let $P_1P_2 \cdots P_m = Q_1Q_2 \cdots Q_n$ for some atoms $P_i, Q_i \in S$. Then $m = \phi(P_1P_2 \cdots P_m) = \phi(Q_1Q_2 \cdots Q_n) = n$. Hence S is half-factorial. Let $A = A_1A_2 \cdots A_t$ for some atoms $A_i \in S$. Since S is half-factorial, $L(A) = \ell(A) = t = \phi(A_1A_2 \cdots A_t) = \phi(A)$.
Suppose that S is half-factorial. Then $L(A) : S \to \mathbb{N}$ and $L(AB) = L(A)+L(B)$ for all $A, B \in S$ and $L(P) = 1$ for all atoms $P \in S$. $\square$

Theorem 2.2. *Let S be an atomic semigroup and let $\phi : S \to H$ where $H \subseteq \mathbb{Z}$ such that $\phi(AB) = \phi(A)\phi(B)$ for all $A, B \in S$. If, whenever $\phi(X) = uv$ for some $u, v \in H^*$, there exist $U, V \in S^*$ such that $\phi(U) = u$, $\phi(V) = v$, and $X = UV$, then the factorization properties of S are identical to those of H. Specifically, $\mathcal{L}(X) = \mathcal{L}(\phi(X))$.*

Proof. Suppose that $\phi(A) = h$. Since ϕ is a homomorphism, A is an atom if and only if h is an atom.
Suppose that $t \in \mathcal{L}(X)$. Then $X = X_1X_2 \cdots X_t$ for some atoms $X_i \in S$, so $\phi(X) = \phi(X_1)\phi(X_2) \cdots \phi(X_t)$, so $t \in \mathcal{L}(\phi(X))$.
Suppose that $t \in \mathcal{L}(\phi(X))$. Then $\phi(X) = x_1x_2 \cdots x_t$ for some atoms $x_i \in H$, so by assumption there exist atoms $X_1X_2 \cdots X_t$ such that $\phi(X_i) = x_i$ and $X = X_1X_2 \cdots X_t$. Hence $t \in \mathcal{L}(X)$. $\square$

Theorem 2.3. *Let $k \in \mathbb{N}$. Let S be an atomic semigroup and let $A \in S^*$. If $\ell(X) - k < \ell(XP)$ for any atom $P \mid A$ and any $X \in S^*$ such that $X \mid A$, then $\Delta(A) \subseteq \{1, 2, 3, \dots, k\}$.*

Proof. Let $t = L(A)$. Then $A = A_1A_2 \cdots A_t$ for some atoms $A_i \in S$. Let $\ell_i = \ell(A_1A_2 \cdots A_i)$. Notice that $\ell_i - k < \ell_{i+1} \leq \ell_i + 1$ by assumption, $\ell_1 = 1$ and $\ell_t = \ell(A)$. If we take the minimum length factorization of $A_1A_2 \cdots A_i$ and append $A_{i+1} \cdots A_t$, we have a factorization of A with length $L_i = \ell_i + t - i$. Thus we have a map from $\{1, 2, 3, \dots, t\}$ to $\{L(A), L(A) - 1, \dots, \ell(A)\}$. Since $\ell_i - k + t - i - 1 < \ell_{i+1} + t - i - 1 \leq \ell_i + t - i$, $L_i - k \leq L_{i+1} \leq L_i$, so there can be no gaps in the factorization lengths greater than k. Hence $\Delta(A) \subseteq \{1, 2, 3, \dots, k\}$. $\square$

Theorem 2.4. *Let $k \in \mathbb{N}$. Let S be an atomic semigroup and let $A \in S^*$. If $L(XP) < L(X) + k$ for any atom $P \mid A$ and any $X \in S^*$ such that $X \mid A$, then $\Delta(A) \subseteq \{1, 2, 3, \dots, k - 2\}$.*

Proof. Let A be an arbitrary element of S such that $A = P_1P_2 \cdots P_t$ for some atoms $P_i \in S$. Let $L_i = L(P_1P_2 \cdots P_i)$. Note that $L_1 = L(P_1) = 1$ and $L_i \geq i$ for all $2 \leq i \leq t$.

Case 1: $L_i > i$ for some $2 \le i \le t$. Let m be minimal such that $L_m > m$. Then $P_1P_2 \cdots P_m = Q_1Q_2 \cdots Q_{L_m}$, so $A = P_1P_2 \cdots P_t =$ $Q_1Q_2 \cdots Q_{L_m}P_{m+1} \cdots P_t$. Hence $t - m + L_m \in \mathcal{L}(A)$. By the minimality of m, $L_{m-1} = m-1$, so $L_m < L_{m-1} + k = m+k-1$ and thus $L_m \le m+k-2$. Hence $t-m+L_m \le t-m+m+k-2 = t+k-2$, so $t+1 \le t-m+L_m \le t+k-2$. Since there is some factorization of A with length between $t+1$ and $t+k-2$, the gap between t and the next longer factorization length of A is at most $k-2$.

Case 2: $L_i = i$ for all $2 \le i \le t$. Then $L_t = L(A)$, so there is no longer factorization of A.

Since for any factorization length t of A, the next larger length is at most $t+k-2$, $\Delta(A) \subseteq \{1, 2, 3, \ldots, k-2\}$. □

Theorem 2.5. *Let S be an atomic semigroup. If there exists a natural number k such that $\ell(A) < \ell(AX)$ for all $A \in S$ and for all $X \in S$ such that $L(X) \ge k$, then $\rho(S) \le k$.*

Proof. Let $A \in S$. Suppose for such a k we have $L(A) = kq + r$ with $0 < r < k$. Write $A = RX_1X_2 \cdots X_q$, where $L(X_i) = k$ and $L(A) = L(R) + L(X_1) + \cdots + L(X_q)$. Observe that $\ell(RX_1X_2 \cdots X_q) \ge \ell(RX_1X_2 \cdots X_{q-1}) + 1 \ge \cdots \ge \ell(R) + q$. Hence $\rho(A) \le \frac{kq+L(R)}{q+\ell(R)} < \frac{kq+k}{q+1} = k$. Now suppose $L(A) = kq$. The proof that $\rho(A) \le k$ is identical.

□

Theorem 2.6. *If $\ell(A) \le k$ for all $A \in S$, then $\rho(S) = \infty$ and $\Delta(S) \subseteq \{1, 2, 3, \ldots, k-1\}$.*

Proof. Let $P \in S$ be an atom in S. $\rho(S) \ge \lim_{i\to\infty} \rho(P^i) \ge \lim_{i\to\infty} \frac{i}{k} = \infty$.
Since $\ell(X) - k + 1 \le 1 < \ell(XP)$ for all $X \in S$ and all atoms $P \in S$, by Theorem 2.3 $\Delta(S) \subseteq \{1, 2, 3, \ldots, k-1\}$. □

Corollary 2.7. *If S is bifurcus, then $\rho(S) = \infty$ and $\Delta(S) = \{1\}$.*

Theorem 2.8. *Let R be a subsemiring of $\mathbb{Z}$ and let S be a semigroup of matrices with entries from R such that S has no units. Let $a \in R$ be nonzero; for all $A \in aS$, if $a^2 \nmid \gcd(A)$, A is an atom, and if $A = a^2B$ where $B \in S$, then A is an atom in aS if and only if B is an atom in S. Furthermore, if S is bifurcus, then aS is bifurcus.*

Proof. If $A = A_1A_2$ for $A_1, A_2 \in aS$, $A = A_1A_2 = (aB_1)(aB_2) = a^2B_1B_2$ where $B_1, B_2 \in S$, so $a^2 | \gcd(A)$. Hence if $a^2 \nmid \gcd(A)$, A is an atom.
Now let $A = a^2B$ where $B \in S$. If $B = B_1B_2$ for some $B_1, B_2 \in S$, then $A = a^2B = (aB_1)(aB_2)$, and $aB_1, aB_2 \in aS$. If $A = A_1A_2$ for some $A_1, A_2 \in aS$, then $a^2B = A = A_1A_2 = (aC_1)(aC_2)$ for some $C_1, C_2 \in S$, so $B = C_1C_2$ is reducible. Hence A is an atom if and only if B is an atom.

Let A be an arbitrary reducible matrix in aS. Then $A = A_1A_2$ for some $A_1, A_2 \in aS$, so $A = A_1A_2 = (aB_1)(aB_2)$ for some $B_1, B_2 \in S$. Since $B_1B_2 \in S$ and S is bifurcus, $A = a^2B_1B_2 = a^2P_1P_2 = (aP_1)(aP_2)$ for some atoms $P_1, P_2 \in S$.

Suppose aP_i is reducible in aS. Then $aP_i = XY$ for some $X, Y \in aS$, so $aP_i = aX'Y$ where $X' \in S$. Hence $P_i = X'Y$ where $X' \in S_R$ and $Y \in aS \subseteq S$, $\rightarrow\leftarrow$. Thus aP_i is an atom.

Hence any matrix in aS may be factored into two atoms, so aS is bifurcus. $\square$

Theorem 2.9. *Let S be an atomic matrix semigroup and let $S^T = \{A^T : A \in S\}$. Then the factorization properties of S^T are identical to those of S. Specifically, $\mathcal{L}(A^T) = \mathcal{L}(A)$.*

Proof. Let $U \in S$ be a unit in S. Since $U^{-1} \in S$, $(U^T)^{-1} = (U^{-1})^T \in S^T$, so U^T is a unit in S^T. Let $A \in S$ be reducible. Then $A = BC$ for some nonunits $B, C \in S$, $A^T = C^T B^T$ for some nonunits $C^T, B^T \in S^T$.
Suppose that $t \in \mathcal{L}(A)$. Then $A = A_1 A_2 \cdots A_t$ for some atoms $A_i \in S$, so $A^T = A_t^T \cdots A_2^T A_1^T$. Hence $t \in \mathcal{L}(A^T)$.
Suppose that $t \in \mathcal{L}(A^T)$. Then $A^T = B_1 B_2 \cdots B_t$ for some atoms $B_i \in S^T$, so $A = B_t^T \cdots B_2^T B_1^T$. Hence $t \in \mathcal{L}(A)$. $\square$

Because of this result, when considering triangular matrices it is not important to draw distinctions between upper triangular matrices and the corresponding lower triangulars; the factorization properties will be identical.

3 Determinant Conditions

The determinant is a crucial property of any matrix. The multiplicatve property of the determinant (namely, that $\det AB = \det A \det B$) provides a useful tool for studying factorization properties of matrices. Matrices with integer entries, and hence integral determinants, are of wide interest in mathematics [22][13]. Additionally, matrices with conditions on their determinant are also of interest. For example, factorization of integral matrices with prime determinants has previously been studied [3]. Other determinant conditions, such as determinant divisible by a fixed number, arise in mathematics as well [6].

3.1 Factorization of Determinants

Let S denote the semigroup of $n \times n$ matrices with integer entries and non-zero determinant.

Theorem 3.1. *A is a unit in S if and only if $|\det A| = 1$.*

Proof. If A is a unit, there exists $B \in Z$ such that $AB = BA = I$. Hence $\det A \cdot \det B = \det I = 1$. Since A has integral entries, $\det A$ must be an integer, so $\det A = \det B = \pm 1$. Let C be the cofactor matrix of A such that c_{ij} is the cofactor of a_{ij}. C has integral entries since the cofactor of an entry in a matrix with integral entries is always an integer. Then by the cofactor expansion method of finding inverses, $A^{-1} = \frac{1}{\det A} C^T$. And if $|\det A| = 1$, $A^{-1} \in S$. $\square$

Theorem 3.2. *If A is an $n \times n$ matrix with integer entries and $\det A = xy$, then there exists matrices X and Y with integer entries such that $A = XY$, $\det X = x$, and $\det Y = y$.*

Proof. Let $A = UDV$ be the Smith Normal Form of A, where D is diagonal, U and V are both unimodular. All matrices have integer entries. Since $\det D = xy$ there exists integral diagonal matrices D_1, D_1 such that $D = D_1D_2$ and $\det D_1 = x$ and $\det D_2 = y$. Thus, $A = UD_1D_2V = (UD_1)(D_2V)$. So let $X = UD_1$ and $Y = D_2V$. □

Corollary 3.3. *For any semigroup S where $A \in S$ if and only if $\det A \in H$ where $H \subseteq \mathbb{Z}$, the factorization properties of S are identical to those of H.*

Proof. The result follows from Theorem 3.2 and 2.2. □

This result relates many matrix semigroups to the better-understood integer semigroups, which have been previously studied in papers such as [11].

Corollary 3.4. *If A is an $n \times n$ matrix with entries from $m\mathbb{Z}$ and $\frac{1}{m^2}A$ has integer entries then $\det A = m^{2n}xy$ and there exists X,Y with entries in $m\mathbb{Z}$ such that $A = XY$ and $\det X = m^n x$ and $\det Y = m^n y$.*

Proof. Let $A = m^2\hat{A}$. Then $\hat{A}$ has entries from $\mathbb{Z}$. Thus, by Theorem 3.2, $\hat{A} = XY$ where $\det X = x$ and $\det Y = y$. So $A = m^2\hat{A} = m^2XY = (mX)(mY)$. Let $S = mX$ and $T = mY$. □

The following theorems show a similar result to Theorem 3.2 for triangular matrices with integer entries. Let S^T denote the semigroup of $n \times n$ upper triangular integral matrices.

Theorem 3.5. *A is a unit in S^T if and only if $|\det A| = 1$.*

Proof. By Theorem 3.1, if A is a unit, then $|\det A| = 1$. Again, let C be the cofactor matrix of A such that c_{ij} is the cofactor of a_{ij}. Since A is upper triangular, C is lower triangular, and thus C^T is upper triangular. Also, C has integral entries since the cofactor of an entry in a matrix with integral entries is always an integer. Then by the cofactor expansion method of finding inverses, $A^{-1} = \frac{1}{\det A}C^T$. And if $|\det A| = 1$, $A^{-1} \in S^T$. □

Theorem 3.6. *If A is an $n\times n$ upper triangular matrix with integer entries and $\det A = xy$, then there exists upper triangular matrices X and Y with integer entries such that $A = XY$, $\det X = x$, and $\det Y = y$.*

Proof. Let $\det A = xy = a_1a_2\cdots a_n$ where the a_i's are the diagonal entries of A. Also, let $y = p_1p_2\cdots p_m$ where the p_j's are the not necessarily distinct primes of y. Let a_k be the first diagonal entry such that $p_1 \mid a_k$. Then $A = \begin{pmatrix} a_1 & a_{12} & \dots & a_{1n} \\ 0 & a_2 & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix} = \begin{pmatrix} T_1 & u & v \\ 0 & a_k & z \\ 0 & 0 & T_2 \end{pmatrix}$. Where $T_1, T_2, u, v,$ and f are all block matrices corresponding to the entries of A, and a_k is the first diagonal entry such that $p_1 \mid a_k$. Then $\begin{pmatrix} T_1 & u & v \\ 0 & a_k & z \\ 0 & 0 & T_2 \end{pmatrix}$ $= \begin{pmatrix} T_1 & u_1 & y \\ 0 & \frac{a_k}{p_1} & z \\ 0 & 0 & T_2 \end{pmatrix} \begin{pmatrix} I & u_2 & 0 \\ 0 & p_1 & 0 \\ 0 & 0 & I \end{pmatrix}$. Now we must solve for u_1 and u_2, so $T_1u_2 + p_1u_1 = u$. So $T_1u_2 + p_1u_1 = \begin{pmatrix} a_1 & a_{12} & \dots & a_{1k-1} \\ 0 & a_2 & \dots & a_{2k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{k-1} \end{pmatrix} \begin{pmatrix} u_{2_1} \\ u_{2_2} \\ \vdots \\ u_{2_{k-1}} \end{pmatrix} +$ $p_1 \begin{pmatrix} u_{1_1} \\ u_{1_2} \\ \vdots \\ u_{1_{k-1}} \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_{k-1} \end{pmatrix}$. So consider $u_{k-1} = p_1u_{1_{k-1}} + a_{k-1}u_{2_{k-1}}$. Since $\gcd(a_{k-1}, p_1) = 1$, we can find $u_{1_{k-1}}$ and $u_{2_{k-1}}$. Then $u_{k-2} = p_1u_{1_{k-2}} + a_{k-2}u_{2_{k-2}} + a_{k-2,k-1}u_{2_{k-1}}$. Since $u_{2_{k-1}}$, $a_{k-2,k-1}$ and u_{k-2} are all defined and $\gcd(p_1, a_{k-2}) = 1$, we can find $u_{2_{k-2}}$ and $u_{1_{k-2}}$ such that $u_{k-2} - a_{k-2,k-1}u_{2_{k-1}} = p_1u_{1_{k-2}} + a_{k-2}u_{2_{k-2}}$. We can continue this back-substitution until we find all values of u_1 and u_2. Now we have $A = \hat{A}B_1$ where $\det \hat{A} = \frac{xy}{p_1}$ and $\det B_1 = p_1$. We can do the same process until all factors of y are factored out of the diagonal entries of A. Then we have $A = X(B_1B_2 \cdots B_m)$ where $\det B_i = p_i$. Let $Y = \prod_{i=1}^{m} B_i$.

$\square$

Corollary 3.7. *In following semigroups with integer entries and non-zero determinant:*

1. *$n \times n$ matrices with entries from $\mathbb{Z}$*
2. *$n \times n$ triangular matrices with entries from $\mathbb{Z}$*
3. *$n \times n$ matrices with determinant greater than 1*
4. *$n \times n$ triangular matrices with determinant greater than 1*

A is an atom if and only if $\det A \in \mathbb{P}$ and $L(A) = \ell(A) = r(A)$.

Proof. The result follows immediately from Theorem 3.2, Theorem 3.6, and Theorem 2.1. $\square$

If A is a 2×2 matrix with determinant xy, then the factorization $A = XY$ where $\det X = x$ and $\det Y = y$ can be easily found in an algorithmic way without using the Smith Normal Form. Before exhibiting this algorithm, however, we first show how to easily factor a 2×2 upper triangular matrix $T, \det T = xy$, such that $T = XY$ and $\det X = x, \det Y = y$. Let $T = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$ where $a'c' = xy$.

Lemma 3.8. *If $y \mid a'c'$, then there exist α, γ such that $\alpha \mid a'$, $\gamma \mid c'$, $\alpha\gamma = y$, and* $\gcd(\gamma, \frac{a'}{\alpha}) = 1$.

Proof. Let $g = \gcd(\gamma, \frac{a'}{\alpha})$. If $g > 1$, we can replace α with $g\alpha$ and γ with $\frac{\gamma}{g}$. Hence, without loss of generality, $\gcd(\gamma, \frac{a'}{\alpha}) = 1$. □

Theorem 3.9. *If $T = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$ where $a', b', c' \in \mathbb{Z}$ and $\det T = xy$, then there exist X, Y such that $T = XY$, $\det X = x$ and $\det Y = y$.*

Proof. Since $y \mid a'c'$, by Lemma 3.8 let $y = \alpha\gamma$ where $\alpha \mid a'$ and $\gamma \mid c'$ and $\gcd(\gamma, \frac{a'}{\alpha}) = 1$. Factor $T = \begin{pmatrix} \frac{a'}{\alpha} & b_1 \\ 0 & \frac{c'}{\gamma} \end{pmatrix} \begin{pmatrix} \alpha & b_2 \\ 0 & \gamma \end{pmatrix}$ where $b' = \frac{a'}{\alpha} b_2 + \gamma b_1$. □

Now that we have shown any upper triangular 2×2 matrix T with $\det T = xy$ can be factored $T = XY$ where $\det X = x$ and $\det Y = y$, apply the following algorithm for 2×2 matrices, not necessarily triangular. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $ad - bc = xy$.

1. Let $r, s \in \mathbb{Z}$ such that $ar + cs = \gcd(a, c) = g$. Note that since $\gcd(r, s) \gcd(a, c) \mid ar + cs = \gcd(a, c)$, $\gcd(r, s) = 1$.

2. Pick $z, w \in \mathbb{Z}$ such that $rz + sw = 1$.

3. Now let $B = \begin{pmatrix} r & s \\ -w & z \end{pmatrix}$ and note that $\det B = rz + sw = 1$. So now
$$BA = \begin{pmatrix} r & s \\ -w & z \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ra + sc & rb + sd \\ -wa + zc & -wb + zd \end{pmatrix}.$$

4. Let $u = ra + sc, v = -wa + zc$ and observe that $u \mid v$, so let $E = \begin{pmatrix} 1 & 0 \\ \frac{-v}{u} & 1 \end{pmatrix}$. Note that $\det E = 1$.

5. Now EBA is upper triangular with $\det(EBA) = xy$, so by Theorem 3.9 factor $EBA = X'Y'$ where $\det X' = x$ and $\det Y' = y$.

6. Now let $X = B^{-1}E^{-1}X'$ and $Y = Y'$ so $A = XY$ where $\det X = x$ and $\det Y = y$.

Similarly, although Theorem 3.12 and Theorem 3.10, together with Theorem 3.2 and Theorem 3.6, show the existence of the minimum and maximum length factorizations, these theorems do not provide the factorization into matrices. However, when A is a 2×2 upper triangular matrix, it is not difficult to explicitly construct the minimum and maximum length factorizations. The following factorizations show one direction of the equality, and readers can refer to Theorem 3.10, Theorem 3.12, and Theorem 3.17 for the other direction of the equality. First consider when $\det A = p^h$. Let $A = \begin{pmatrix} p^m a & b \\ 0 & p^n c \end{pmatrix}$ be an arbitrary element of S where $m+n \geq h$, $p \nmid a$, and $p \nmid c$.

For the maximum length factorization of A, let $m = q_1 h + r_1$ and let $n = q_2 h + r_2$. Recall that by Theorem 3.10, $L(A) = \eta_k(A) = \lfloor \frac{m+n}{h} \rfloor$.

Case 1: $h \leq r_1 + r_2 < 2h$. Factor $A = \begin{pmatrix} p^m a & b \\ 0 & p^n c \end{pmatrix}$
$= \begin{pmatrix} 1 & 0 \\ 0 & p^h \end{pmatrix}^{q_2} \begin{pmatrix} p^{r_1} a & b \\ 0 & p^{r_2} c \end{pmatrix} \begin{pmatrix} p^h & 0 \\ 0 & 1 \end{pmatrix}^{q_1}$. Hence $L(A) \geq q_1 + q_2 + 1 = \frac{q_1 h}{h} + \frac{q_2 h}{h} + \lfloor \frac{r_1+r_2}{h} \rfloor = \lfloor \frac{q_1 h + q_2 h + r_1 + r_2}{h} \rfloor = \lfloor \frac{m+n}{h} \rfloor$.

Case 2: $r_1 + r_2 < h$. Since $q_1 + q_2 \geq 1$, one of q_1, q_2 is at least 1. Without loss of generality, assume $q_1 \geq 1$. Factor $A = \begin{pmatrix} p^m a & b \\ 0 & p^n c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p^h \end{pmatrix}^{q_2} \begin{pmatrix} p^{r_1+h} a & b \\ 0 & p^{r_2} c \end{pmatrix} \begin{pmatrix} p^h & 0 \\ 0 & 1 \end{pmatrix}^{q_1-1}$. Hence $L(A) \geq q_1 + q_2 = \frac{q_1 h}{h} + \frac{q_2 h}{h} + \lfloor \frac{r_1+r_2}{h} \rfloor = \lfloor \frac{q_1 h + q_2 h + r_1 + r_2}{h} \rfloor = \lfloor \frac{m+n}{h} \rfloor$.

For the minimum length factorization of A, recall that by Theorem 3.12, $\ell(A) = \left\lfloor \frac{\eta_p(A)+2h-2}{2h-1} \right\rfloor$. Let $m = q_1(2h-1) + r_1$ and let $n = q_2(2h-1) + r_2$. Let $\ell(A) = \lambda = \left\lfloor \frac{m+n+2k-2}{2k-1} \right\rfloor$

Case 1: $r_1 + r_2 = 0$. Factor $A = \begin{pmatrix} p^m a & b \\ 0 & p^n c \end{pmatrix}$
$= \begin{pmatrix} 1 & 0 \\ 0 & p^{2h-1} \end{pmatrix}^{q_2-1} \begin{pmatrix} a & b \\ 0 & p^{2h-1} c \end{pmatrix} \begin{pmatrix} p^{2h-1} & 0 \\ 0 & 1 \end{pmatrix}^{q_1}$
$= \begin{pmatrix} 1 & 0 \\ 0 & p^{2h-1} \end{pmatrix}^{q_2} \begin{pmatrix} p^{2h-1} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} p^{2h-1} & 0 \\ 0 & 1 \end{pmatrix}^{q_1-1}$. Since $r_1 = r_2 = 0$ and $m+n \geq h > 0$, at least one of q_1, q_2 must be greater than zero, so at least one of these factorizations is valid. Hence $\ell(A) \leq q_1 + q_2 = \frac{q_1(2h-1)}{2h-1} + \frac{q_2(2h-1)}{2h-1} + \lfloor \frac{2h-2}{2h-1} \rfloor = \lfloor \frac{m}{2h-1} + \frac{m}{2h-1} + \frac{2h-2}{2h-1} \rfloor = \lambda$.

Case 2: $1 \leq r_1 + r_2 < h$. Factor $A = \begin{pmatrix} p^m a & b \\ 0 & p^n c \end{pmatrix}$
$= \begin{pmatrix} 1 & 0 \\ 0 & p^{2h-1} \end{pmatrix}^{q_2-1} \begin{pmatrix} p^{r_1} a & b \\ 0 & p^{r_2+2h-1} c \end{pmatrix} \begin{pmatrix} p^{2h-1} & 0 \\ 0 & 1 \end{pmatrix}^{q_1}$
$= \begin{pmatrix} 1 & 0 \\ 0 & p^{2h-1} \end{pmatrix}^{q_2} \begin{pmatrix} p^{r_1+2h-1} a & b \\ 0 & p^{r_2} c \end{pmatrix} \begin{pmatrix} p^{2h-1} & 0 \\ 0 & 1 \end{pmatrix}^{q_1-1}$. Since $r_1 + r_2 < h$ and $m+n \geq h$, at least one of q_1, q_2 must be greater than zero, so at least one of these factorizations is valid. Since $r_1 + r_2 + 2h - 1 \geq 2h$, the central matrix is reducible by Lemma 3.11. Furthermore, by Theorem 3.10 its maximum factorization length is $\lfloor \frac{r_1+r_2+2h-1}{h} \rfloor \leq \lfloor \frac{3h-2}{h} \rfloor \leq 2$. Hence these factorizations are of length $q_1 + q_2 - 1 + 2 = q_1 + q_2 + 1$, so $\ell(A) \leq q_1 + q_2 + 1 = \frac{q_1(2h-1)}{2h-1} + \frac{q_2(2h-1)}{2h-1} + \lfloor \frac{r_1+r_2-1}{2h-1} \rfloor + \frac{2h-1}{2h-1} = \lambda$.

Case 3: $h \le r_1 + r_2 < 2h$. Factor $A = \begin{pmatrix} p^m a & b \\ 0 & p^n c \end{pmatrix}$ $= \begin{pmatrix} 1 & 0 \\ 0 & p^{2h-1} \end{pmatrix}^{q_2} \begin{pmatrix} p^{r_1} a & b \\ 0 & p^{r_2} c \end{pmatrix} \begin{pmatrix} p^{2h-1} & 0 \\ 0 & 1 \end{pmatrix}^{q_1}$. Hence $\ell(A) \le q_1 + q_2 + 1 = \frac{q_1(2h-1)}{2h-1} + \frac{q_2(2h-1)}{2h-1} + \lfloor \frac{r_1+r_2-1}{2h-1} \rfloor + \frac{2h-1}{2h-1} = \lambda$.

Case 4: $2h \le r_1 + r_2 < 3h$. Factor $A = \begin{pmatrix} p^m a & b \\ 0 & p^n c \end{pmatrix}$ $= \begin{pmatrix} 1 & 0 \\ 0 & p^{2h-1} \end{pmatrix}^{q_2} \begin{pmatrix} p^{r_1} a & b \\ 0 & p^{r_2} c \end{pmatrix} \begin{pmatrix} p^{2h-1} & 0 \\ 0 & 1 \end{pmatrix}^{q_1}$. Since $r_1 + r_2 \ge 2h$, the central matrix is reducible by Lemma 3.11. Furthermore, by Theorem 3.10 its maximum factorization length is $\lfloor \frac{r_1+r_2}{h} \rfloor \le 2$. Hence this factorization is of length q_1+q_2+2, so $\ell(A) \le q_1+q_2+2 = \frac{q_1(2h-1)}{2h-1} + \frac{q_2(2h-1)}{2h-1} + \lfloor \frac{r_1+r_2-1}{2h-1} \rfloor + \frac{2h-1}{2h-1} = \lambda$.

Case 5: $3h \le r_1 + r_2 \le 4h - 4$. Since $r_2 \le 2h - 2$, $r_1 + 2h - 2 \ge r_1 + r_2 \ge 3h$, so $r_1 \ge h + 2$. Similarly, $r_2 \ge h + 2$. Factor $A = \begin{pmatrix} p^m a & b \\ 0 & p^n c \end{pmatrix}$ $= \begin{pmatrix} 1 & 0 \\ 0 & p^{2h-1} \end{pmatrix}^{q_2} \begin{pmatrix} 1 & 0 \\ 0 & p^{r_2} \end{pmatrix} \begin{pmatrix} p^{r_1} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} p^{2h-1} & 0 \\ 0 & 1 \end{pmatrix}^{q_1}$. Since $r_1 \le 2h - 2 < 2h$ and $r_2 \le 2h - 2 < 2h$, this factorization is of length $q_1 + q_2 + 2$. Hence $\ell(A) \le q_1 + q_2 + 2 = \frac{q_1(2h-1)}{2h-1} + \frac{q_2(2h-1)}{2h-1} + \lfloor \frac{r_1+r_2-1}{2h-1} \rfloor + \frac{2h-1}{2h-1} = \lambda$.

Similarly, now consider when $\det A = st$, $\gcd(s,t) = 1$. Recall that by Theorem 3.17, this semigroup is bifurcus. So, to find a factorization of length 2, let z be maximal such that $s^2 t^z | ac$. By 3.8, pick α, γ such that $\alpha | a$, $\gamma | c$, and $\alpha\gamma = st^{z-1}$. Let $g = \gcd(\alpha, \frac{c}{\gamma})$. If $g > 1$, we can replace α with $\frac{\alpha}{g}$ and γ with $g\gamma$. Hence, without loss of generality, $\gcd(\alpha, \frac{c}{\gamma}) = 1$. Factor $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} \alpha & x \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} \frac{a}{\alpha} & y \\ 0 & \frac{c}{\gamma} \end{pmatrix}$ where $b = y\alpha + x\frac{c}{\gamma}$. Since $\gcd(\alpha, \frac{c}{\gamma}) = 1$, there are infinitely many such $x, y \in \mathbb{Z}$. Since $\alpha\gamma = st^{z-1}$ and $\gcd(s,t) = 1$, $k = st | \alpha\gamma$ but $k^2 = s^2t^2 \nmid \alpha\gamma$, so the left matrix is an atom in S. Since $s^2t^z | ac$, $k = st | \frac{ac}{\alpha\gamma}$, but $k^2 = s^2t^2 \nmid \frac{ac}{\alpha\gamma}$ by the maximality of z, so the right matrix is an atom in S.

Again, the maximum length factorization can be constructed as well. The construction into the maximum length is shown by induction.
Let $w = \eta_k(A)$. Suppose $w = 1$. Then A is an atom by Theorem 3.11, so $L(A) = 1 = w$. Now assume that $L(A) \ge \eta_k(A)$ for all $\eta_k(A) \le i$. Let $w = i+1$. Since $k | ac$, by Lemma 3.8 there exist α, γ such that $\alpha | a$, $\gamma | c$, $\alpha\gamma = k$, and $\gcd(\alpha, \frac{c}{\gamma}) = 1$. Factor $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} \alpha & x \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} \frac{a}{\alpha} & y \\ 0 & \frac{c}{\gamma} \end{pmatrix}$ where $b = y\alpha + x\frac{c}{\gamma}$. Since $\eta_k(\frac{ac}{\alpha\gamma}) = w - 1 = i$, $L(A) \ge 1 + i = w$.

Now one could look at the factorization of matrices in comparison to the integers. By the Fundamental Theorem of Arithmetic, factorization of the integers is unique up to units and order. However, if we look at the semigroup of all matrices with integer entries, we lose something. All the atoms of this semigroup have prime determinant and the units are anything with determinant 1, but any matrix with determinant p are associates of each other. Namely, by the Smith Normal Form, any matrix A with $\det A = p$ there exists unimodular U_1 and V_1 and diagonal D such that $A = U_1 D V_1$. Also, for any other matrix B with $\det B = p$, then we can find unimodular U_2 and V_2 such that $B = U_2 D V_2$. Thus $D = U_2^{-1} B V_2^{-1}$, and $A = U_1 U_2^{-1} B V_2^{-1} V_1$ so A and B differ only by multiplication by units. However, since matrix multiplication is non-commutative, the order of the factorization is important. Now, looking at the semigroup of upper triangular matrices something interesting happens. The atoms are any matrix with determinant p and the units of this semigroup are anything with determinant 1. So if we have a matrix $A = \begin{pmatrix} p & b_1 \\ 0 & 1 \end{pmatrix}$ there exist no units U_1, U_2 in the semigroup such that $U_1 A U_2 = \begin{pmatrix} 1 & b_2 \\ 0 & p \end{pmatrix}$. This is because $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & b_2 \\ 0 & p \end{pmatrix}$. Therefore, we have atoms of the same determinant that are not associates of each other, but if there are no factors of the same type B then there cannot be any factors of that type. Since the diagonal entries of the product of two upper triangular matrices are the product of the diagonal entries, then the order of the factors is important but they are all associates of each other.

3.2 Semigroups with Determinant in $k\mathbb{Z}$

By Theorem 3.2 and 3.6, factorization properties of $n \times n$ matrices (either non-triangular or triangular) are the same as factorization properties of the determinant over the integers. Hence, the following results factor the determinant of the desired matrix and apply Theorem 3.2 and 3.6 to show the existence of matrices with the desired determinant. Consequently, the semigroups mentioned in Sections 3.2 and 3.3 apply to both semigroups with non-triangular matrices and semigroups with triangular matrices.

Let S be the semigroup of $n \times n$ matrices with entries from $\mathbb{Z}$ and nonzero determinant divisible by some $k \in \mathbb{N}$ where $k > 1$. Note that S has no identity and no units.

Theorem 3.10. $L(A) = \eta_k(A)$

Proof. Let $A = A_1 A_2 \cdots A_t$. Since $k \mid \det A_i$, $k^t \mid \det A$. Hence $L(A) \leq \eta_k(A)$. Let $g = \eta_k(A)$. By Theorem 3.2 for triangular matrices, there exist upper triangular matrices $A_1, A_2, \ldots, A_g$ such that $A = A_1 A_2 \cdots A_g$ where $\det A_i = k$ for all $1 \leq i \leq g-1$ and $\det A_g = \frac{\det A}{k^{g-1}}$. Hence $L(A) \geq g = \eta_k(A)$. □

Corollary 3.11. *A is an atom if and only if $k^2 \nmid \det A$.*

The remaining factorization properties of S change substantially depending on the value of k. We will now show that if k is a prime, then S is half-factorial; if $k = st$ where $\gcd(s,t) = 1$, then S is bifurcus; and if k is a power a prime, then S is neither half-factorial or bifurcus. First consider when k is a power of a prime, $k = p^h$.

Theorem 3.12. *If $k = p^h$, then $\ell(A) = \left\lfloor \frac{\eta_p(A)+2h-2}{2h-1} \right\rfloor$.*

Proof. Let A be an arbitrary element of S where $\det A = p^m x, m \geq h$, and $p \nmid x$. Let $m = \eta_p(A)$ and let $\lambda = \left\lfloor \frac{m+2h-2}{2h-1} \right\rfloor$.
Let $A = A_1 A_2 \cdots A_s$ and let $t_i = \eta_{A_i}(A)$. Since $\det A = \det A_1 \det A_2 \cdots \det A_s$, $m = t = \sum_{i=1}^{s} t_i \leq s(2h-1)$. If $s \leq \lambda - 1 = \left\lfloor \frac{m-1}{2h-1} \right\rfloor \leq \frac{m-1}{2h-1}$, $s(2h-1) \leq m-1$, $\rightarrow\leftarrow$. Hence $s \geq \lambda$, so $\ell(A) \geq \lambda$.
By Theorem 3.2, factoring $\det A$ is equivalent to factoring A. Let $m = q(2h-1) + r$ where $0 \leq r < 2h-1$. Then $\lambda = \left\lfloor \frac{q(2h-1)+r+2h-2}{2h-1} \right\rfloor = q + \left\lfloor \frac{r-1+2h-1}{2h-1} \right\rfloor = q + 1 + \left\lfloor \frac{r-1}{2h-1} \right\rfloor$.

Case 1: $r = 0$. Factor $\det A = (p^{2h-1})^{q-1}(p^{2h-1}x)$. Since $r = 0$ and $m \geq 2h, q > 1$, so this factorization is valid. Hence $\ell(A) \leq q = q + 1 + \left\lfloor \frac{r-1}{2h-1} \right\rfloor = \lambda$.

Case 2: $1 \leq r < h$. Factor $\det A = (p^{2h-1})^{q-1}(p^{r+2h-1}x)$. Since $r < h$ and $m \geq 2h$, again $q > 1$, so this factorizations is valid. Since $r + 2h - 1 \geq 2h$, the matrix with determinant $p^{r+2h-1}x$ is reducible by Corollary 3.11. Furthermore, by Theorem 3.10 its maximum factorization length is $\lfloor \frac{r+2h-1}{h} \rfloor \leq \lfloor \frac{3h-2}{h} \rfloor \leq 2$. Hence these factorizations are of length $q - 1 + 2 = q + 1$, so $\ell(A) \leq q + 1 = q + 1 + \left\lfloor \frac{r-1}{2h-1} \right\rfloor = \lambda$.

Case 3: $h \leq r < 2h-1$. Factor $\det A = (p^{2h-1})^q (p^r x)$. Hence $\ell(A) \leq q+1 = q + 1 + \left\lfloor \frac{r-1}{2h-1} \right\rfloor = \lambda$. □

Lemma 3.13. $\lfloor \frac{a}{b} \rfloor \geq \frac{a-b+1}{b}$.

Proof. Let $a = qb + r$ where $0 \leq r \leq b-1$. $\lfloor \frac{a}{b} \rfloor = q = \frac{a-r}{b} \geq \frac{a-b+1}{b}$. □

Theorem 3.14. $\rho(S) = \frac{2h-1}{h}$.

Proof. For any $A \in S$, $\rho(A) = (\lfloor \frac{\eta_p(A)}{h} \rfloor)/(\left\lfloor \frac{\eta_p(A)+2h-2}{2h-1} \right\rfloor) \leq (\frac{\eta_p(A)}{h})/(\frac{\eta_p(A)}{2h-1}) = \frac{2h-1}{h}$ by Lemma 3.13. Thus $\rho(S) \leq \frac{2h-1}{h}$. This elasticity is achieved by any element $A \in S$ such that $\det A = (p^h)^{2h-1} = (p^{2h-1})^h$, since then $L(A) = 2h-1$ and $\ell(A) = h$. □

Corollary 3.15. *S is half-factorial if and only if k is prime.*

Proof. By Theorem 3.14, $h = 1$ if and only if $\rho(S) = \frac{2h-1}{h} = 1$, so $L(A) = \ell(A)$. Clearly, S is not factorial because integers commute, so the determinant of a given matrix A can be factored in multiple ways, and hence the matrices in the factorization of A can also be rearranged in different ways. □

Corollary 3.16. *If $h = 1$, then $\Delta(S) = \emptyset$. Otherwise, $\Delta(S) = \{1\}$.*

Proof. Let X be an arbitrary element of S and let $t = \eta_p(X)$. Let P be an arbitrary atom of S and let $u = \eta_p(P)$. Since $\ell(X) = \left\lfloor \frac{t+2h-2}{2h-1} \right\rfloor \leq \left\lfloor \frac{t+u+2h-2}{2h-1} \right\rfloor = \ell(XP)$, by the Theorem 2.3, $\Delta(S) \subseteq \{1\}$.
If $h = 1$, S is half-factorial by Corollary 3.15 and $\Delta(S) = \emptyset$. If $h > 1$, S is not half-factorial and $\Delta(S) \neq \emptyset$, so $\Delta(S) = \{1\}$. □

Now consider when k is neither a prime or a power of a prime; that is, $k = st$ where $\gcd(s,t) = 1$.

Theorem 3.17. *If $k = st$ where $\gcd(s,t) = 1$, then S is bifurcus.*

Proof. Suppose $A \in S$ is reducible. Then, by Corollary 3.11, $(st)^2 \mid \det A$. So $\det A = (st)^m x_1 x_2$ where $m > 1$ and $s \nmid x_1, t \nmid x_2$. Since $\det A = (s^{m-1}tx_2)(st^{m-1}x_1)$, by Theorem 3.2, there exist matrices $B', C' \in S$ such that $\det B' = s^{m-1}tx_2$, $\det C' = st^{m-1}x_1$, and $A = B'C'$. Note that both B' and C' are atoms since their determinant is not divisible by $(st)^2$, so $\ell(A) = 2$. □

3.3 Semigroup of Matrices with Composite Determinant

Let S be the semigroup of $n \times n$ matrices with integer entries and composite determinant. Note that S has no identity and hence no units. Let $A \in S$. Observe that $r(XY) = r(X) + r(Y)$.

Lemma 3.18. *If $r(A) = x + y$, then there exist $X, Y \in S$ such that $r(X) = x$, $r(Y) = y$, and $XY = A$.*

Proof. Let $\det A = p_1 p_2 \cdots p_{r(A)}$ where $p_i \in \mathbb{P}$. By Theorem 3.2, there exist $X, Y \in S$ such that $\det X = p_1 p_2 \cdots p_x$, $\det Y = p_{x+1} \cdots p_{r(A)}$, and $XY = A$. □

Theorem 3.19. *A is an atom in S if and only if $r(A) \leq 3$.*

Proof. Suppose $A = BC$. Since $B, C \in S$, $r(B) \geq 2$ and $r(C) \geq 2$. Hence $r(A) \geq 4$. Now suppose $r(A) \geq 4$. Factor $A = B'C'$ where $r(B'), r(C') \geq 2$. □

Theorem 3.20. $L(A) = \lfloor \frac{r(A)}{2} \rfloor$.

Proof. Let $r(A) = 2q + x$ where $x \in \{0, 1\}$. Note that $q = \lfloor \frac{r(A)}{2} \rfloor$. Suppose $A = A_1 A_2 \cdots A_t$ for some atoms A_i. Then $r(A) = r(A_1) + r(A_2) + \cdots + r(A_t)$, so since $r(A_i) \geq 2$, $r_A \geq 2t$. Hence $L(A) \leq q$.
Factor $A = A_1 A_2 \cdots A_q$ where for $1 \leq i < q$, $r(A_i) = 2$, and $r(A_q) = 2 + x$. Hence $L(A) \geq q$. □

Theorem 3.21. $\ell(A) = \lceil \frac{r(A)}{3} \rceil$.

Proof. Let $r(A) = 3q + x$ where $x \in \{0, 1, 2\}$.

Case 1: $x = 0$. Factor $A = A_1 A_2 \cdots A_q$ where $r(A_i) = 3$ for $1 \leq i \leq q$. Hence $\ell(A) \leq q = \lceil \frac{r_A}{3} \rceil$.

Case 2: $1 \leq x \leq 2$. Factor $A = A_1 A_2 \cdots A_q A_{q+1}$ where $r(A_i) = 3$ for $1 \leq i < q$, $r(A_q) = 1 + x$, and $r(A_{q+1}) = 2$. Hence $\ell(A) \leq q + 1 = \lfloor \frac{r(A)}{3} \rfloor + 1 = \lceil \frac{r(A)}{3} \rceil$. Now let $A = A_1 \cdots A_t$ for some atoms A_i. Since $r(A_i) \leq 3$, $r(A) \leq 3t$. Taking $t = \ell(A)$, $\frac{r(A)}{3} \leq \ell(A)$. And since $\ell(A) \in \mathbb{Z}, \ell(A) \geq \lceil \frac{r(A)}{3} \rceil$. □

Theorem 3.22. $\rho(S) = \frac{3}{2}$.

Proof. $\rho(A) = \lfloor \frac{r(A)}{2} \rfloor / \lceil \frac{r(A)}{3} \rceil \leq \frac{r(A)}{2} / \frac{r(A)}{3} = \frac{3}{2}$. Whenever $6 \mid r(A)$, this elasticity is achieved, so $\rho(S) = \frac{3}{2}$. □

Theorem 3.23. $\Delta(S) = \{1\}$

Proof. Suppose that $A = A_1 A_2 \cdots A_t$ for some atoms A_i where $t > \ell(A) = \lceil \frac{r(A)}{3} \rceil$, so $t \geq \lceil \frac{r(A)}{3} \rceil + 1$. Let x denote the number of A_i such that $r(A_i) = 2$. Then $r(A) = \sum_{i=1}^{t} r(A_i) = 2x + 3(t - x) = 3t - x$. Hence $t \geq \lceil \frac{r(A)}{3} \rceil + 1 = \lceil \frac{3t-x}{3} \rceil + 1 = t + 1 + \lceil -\frac{x}{3} \rceil$, so $-1 \geq \lceil -\frac{x}{3} \rceil$. Thus $x \geq 3$. Since we have at least three A_j such that $r(A_j) = 2$, we can recombine these three into two B_j such that $r(B_j) = 3$. Hence $A = B_1 B_2 \cdots B_{t-1}$ for some atoms B_i. Therefore $\Delta(S) = \{1\}$. □

4 Triangular Matrices

Upper triangular matrices are very useful because of their determinant properties. Also, since it is very easy to put any integral matrix into upper triangular form using the Hermite Normal Form, it is useful to study these matrices. Such things as the Post correspondence problem refer the the factors of 3×3 upper triangular matrices [17]. At first the problem was proven using matrices with determinant equal to 1. Later, the problem was generalized to any nonsigular upper triangular matrix [12]. These problems, which rely heavily on upper triangular matrices, show the importance of studying factorization properties of such a class of matrices.

4.1 2×2 Triangular Matrices, $\mathbb{N}$

Let S be the semigroup of 2×2 upper triangular matrices with positive integer entries and non-zero determinant. Let $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in S$. Note that S has no identity and hence no units.

Theorem 4.1. *$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ is an atom if and only if $b = 1$.*

Proof. If $b > 1$, factor A as A=$\begin{pmatrix} 1 & m \\ 0 & c \end{pmatrix}\begin{pmatrix} a & n \\ 0 & 1 \end{pmatrix}$ so that $m+n=b$. If A is reducible, then $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} s & m \\ 0 & u \end{pmatrix}\begin{pmatrix} t & n \\ 0 & v \end{pmatrix}$ where $a = st$, $c = uv$, and $b = sn + mv$. Since b is a sum of products of positive integers, $b > 1$. ☐

Theorem 4.2. $L(A) = b$.

Proof. Since each multiplication must increase the value of b, no A $\in S$ can have a factorization of length greater than b. Furthermore, every matrix A has a factorization of length b, as we can show by induction:
If b=1, then by Lemma 4.1 A is an atom, so $L(A) = 1$. For $b > 1$, suppose that for any $M \in S$, $M = \begin{pmatrix} m_{11} & b-1 \\ 0 & m_{22} \end{pmatrix}$ has $L(M) = b - 1$. Then $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ $= \begin{pmatrix} 1 & b-1 \\ 0 & c \end{pmatrix}\begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix}$ has $L(A) = b - 1 + 1 = b$. ☐

Corollary 4.3. $\rho(S) = \infty$

Proof. Observe that $A = \begin{pmatrix} 2^h & 2^{h+1} \\ 0 & 2^h \end{pmatrix} = \begin{pmatrix} 2^h & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 2^h \end{pmatrix}$ has $\ell(A) = 2$ by Theorem 4.1 and $L(A) = 2^{h+1}$ by Theorem 4.2. So $\rho(A) = 2^h$ and hence $\rho(S) \geq \lim_{h\to\infty} 2^h = \infty$. ☐

Theorem 4.4. *For every* $p \in \mathbb{P}, p - 1 \in \Delta(S)$.

Proof. Let $\begin{pmatrix} p & p+1 \\ 0 & 1 \end{pmatrix} = A_1A_2\cdots A_t$ for some atoms $A_i \in S$. Then
$\begin{pmatrix} p & p+1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \begin{pmatrix} p & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{t-m-1}$ where $m \leq t - 1$, so $t - m - 1 \geq 0$.

Case 1: $t - m - 1 = 0$. Then $m = t - 1$, so $A_1A_2\cdots A_t$ $= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{t-1}\begin{pmatrix} p & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & t \\ 0 & 1 \end{pmatrix}$. Hence $t = p + 1$.

Case 2: $t - m - 1 \geq 1$. Then $\begin{pmatrix} p & p+1 \\ 0 & 1 \end{pmatrix} = A_1A_2\cdots A_t$
$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \begin{pmatrix} p & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{t-m-1}$
$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \begin{pmatrix} p & p(t-m-1)+1 \\ 0 & 1 \end{pmatrix}$, so $p(t-m-1)+1 \leq p+1$ and thus $t - m - 1 \leq 1$. Hence $t - m - 1 = 1$, so $\begin{pmatrix} p & p+1 \\ 0 & 1 \end{pmatrix}$
$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \begin{pmatrix} p & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \begin{pmatrix} p & p+1 \\ 0 & 1 \end{pmatrix}$, and thus $m = 0$. Since $t - m - 1 = 1$, $t = m + 2 = 2$.

Consequently, the only possible factorization lengths of $\begin{pmatrix} p & p+1 \\ 0 & p \end{pmatrix}$ are $p+1$ and 2. Since $\mathcal{L}\begin{pmatrix} p & p+1 \\ 0 & p \end{pmatrix} = \{2, p+1\}$, $\Delta\begin{pmatrix} p & p+1 \\ 0 & p \end{pmatrix} = \{p-1\}$. $\square$

The gaps between factorization lengths of a matrix A appear to correspond to the gaps in the linear combinations of the prime factors of the determinant minus one.

Conjecture 4.5. *If $p, q \in \mathbb{P}$ and $b > pq$, then $\Delta\begin{pmatrix} p & b \\ 0 & q \end{pmatrix} = \Delta(\{(p-1)x + (q-1)y : x, y \in \mathbb{N}_0\})$.*

Lemma 4.6. *Let $a, b \in \mathbb{N}$ such that $a - b = \gcd(a, b) = g$. Let $W = \{ax + by : x, y \in \mathbb{N}_0\}$. Then $\Delta(W) = \{g, 2g, 3g, \ldots, b\}$.*

Proof. Let $W_i = \{ax + by \in W : x + y = i\}$. Note that $\max(W_i) = ai$ and $\min(W_i) = ib$. Now, if $i < \frac{b}{g}$ then $ia < (i+1)b$. Equivalently, every element of W_i is less than every element of W_{i+1}.
$W_i = \{w_0, w_1, w_2, \ldots, w_j, \ldots, w_i\}$ where $w_j = ja + (i-j)b$. Since $w_{j+1} - w_j = g$, $\Delta(W_i) = \{g\}$. Now, $\min(W_{i+1}) - \max(W_i) = (i+1)b - ia = b - ig$ for $0 \le i < \frac{b}{g}$. Thus $g, 2g, 3g, \ldots, b \in \Delta(W)$. Moreover, since all linear combinations of a and b must be divisible by $\gcd(a, b)$, every element of $\Delta(W)$ must also be divisble by g. Hence, since nothing greater than b can be in $\Delta(W)$, $\Delta(W) = \{g, 2g, 3g, \ldots, b\}$. $\square$

If Conjecture 4.5 is true for $p = q+2$, then $\{2, 4, 6, \ldots, q-1\} = \Delta\begin{pmatrix} p & b \\ 0 & q \end{pmatrix} \subset \Delta(S)$.

Conjecture 4.7. *If the Twin Prime Conjecture is true, then $2\mathbb{N} \subset \Delta(S)$.*

4.2 2×2 Triangular Matrices, $\mathbb{N}_0$

Let S be the semigroup of upper triangular 2×2 matrices with non-negative entries and non-zero determinant. Notice that the only unit in S is the identity matrix. Let $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in S$.

Theorem 4.8. *The atoms of S are $X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $Y = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, and $Z = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ where p is prime.*

Proof. Suppose $X = X_1X_2$. Since $\det X = 1$, X_1 and X_2 must also have determinant 1. So write $X_1X_2 = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ where $m + n = 1$. But then WLOG $m = 0$ and X_1 is the identity. Now suppose $Y = Y_1Y_2$. By the multiplicative property of the determinant, there are only two possible

factorizations. First, $Y_1Y_2 = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & p \end{pmatrix}$ where $0 = n + mp$. But then we must have $m = 0$ and hence Y_1 is the identity. Second, we could have $Y_1Y_2 = \begin{pmatrix} 1 & n \\ 0 & p \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ where $0 = n + m$. Hence $m = 0$ and Y_2 is the identity. Similarly for Z.
We will now show that these are the only atoms. By 4.1, if $b \geq 2$, then A is reducible over the positive integers and hence A is also reducible over the non-negative integers. So let $b = 1$.
Factor $A = \begin{pmatrix} a & 1 \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & c \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. At least one of these factorizations contains two non-units unless $a = c = 1$. And if $a = c = 1$, then A itself is an atom.

□

Theorem 4.9. *Let $A = P_1P_2 \cdots P_t = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in S$ where P_i is an atom for $1 \leq i \leq t$. Then $t = r(A) + k$ where $k = |\{i : P_i = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\}|$.*

Proof. Since P_i is an atom, recall that $\det P_i$ is either prime or 1. Now $\det A = \det P_1 \det P_2 \cdots \det P_t$. So $|\{i : \det P_i \text{ is prime }\}| = r(A)$ and then let $k = |\{i : \det P_i = 1\}|$. Now $t = |\{i : \det P_i \text{ is prime }\}| + |\{i : \det P_i = 1\}| = r(A) + k$. □

Lemma 4.10. *Let $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $A = A_1A_2 \cdots A_\lambda$ where $A_i = \begin{pmatrix} a_i & b_i \\ 0 & c_i \end{pmatrix}$. Then $b \geq \sum_{i=1}^{\lambda} b_i$.*

Proof. When $\lambda = 1$, $b = b \geq b$. Now suppose the result holds for all $\alpha < \lambda$. So let $A_1A_2 \cdots A_{\lambda-1} = \begin{pmatrix} a'_{\lambda-1} & b'_{\lambda-1} \\ 0 & c'_{\lambda-1} \end{pmatrix}$. By the hypothesis, $b'_{\lambda-1} \geq \sum_{i=1}^{\lambda-1} b_i$. Now $A = \begin{pmatrix} a'_{\lambda-1} & b'_{\lambda-1} \\ 0 & c'_{\lambda-1} \end{pmatrix}\begin{pmatrix} a_\lambda & b_\lambda \\ 0 & c_\lambda \end{pmatrix} = \begin{pmatrix} a'_{\lambda-1}a_\lambda & a'_{\lambda-1}b_\lambda + b'_{\lambda-1}c_\lambda \\ 0 & c'_{\lambda-1}c_\lambda \end{pmatrix}$. And since $a'_{\lambda-1}, c_\lambda \in \mathbb{N}$, $a'_{\lambda-1}b_\lambda + b'_{\lambda-1}c_\lambda \geq b_\lambda + b'_{\lambda-1}$. □

Lemma 4.11. *If $A = \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix}$ where $p \nmid r$, then $\ell(A) = 1 + r$.*

Proof. As in Lemma 4.9, write $\ell(A) = r(A) + k = 1 + k$. So we have one copy of the atom $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ and k copies of the atom $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in any factorization of A, in particular the factorization of A of minimum length. So, either $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ or $A = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k$. The first factorization violates the assumption $p \nmid r$, so we must have $A = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}$, so $k = r$ and hence $\ell(A) = 1 + r$. □

Theorem 4.12. *Let $M \in S$. If $b = 0$, then $\ell(M) = r(M)$. If $b|ac$, then $\ell(M) = r(M) + 1$.*

Proof. Suppose $b = 0$ and write $\ell(M) = r(M) + k$ as in Theorem 4.9 and suppose $k \geq 1$. So the factorization of M contains at least one copy of the atom $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, but then by Lemma 4.10 $b \geq 1$. So $k = 0$ and $\ell(M) = r(M)$. Now suppose $b|ac$. Again by Theorem 4.9, write $\ell(M) = r(M) + k$. Since $b > 0$ we have $k \geq 1$ and then $\ell(M) \geq r(M) + 1$. Now write $a = ma'$ and $c = nc'$ such that $a'c' = b$. Factor $A = \begin{pmatrix} ma' & a'c' \\ 0 & nc' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}\begin{pmatrix} a' & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & c' \end{pmatrix}\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$. Now $\ell(M) \leq$
$\ell(\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}) + \ell(\begin{pmatrix} a' & 0 \\ 0 & 1 \end{pmatrix}) + \ell(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) + \ell(\begin{pmatrix} 1 & 0 \\ 0 & c' \end{pmatrix}) + \ell(\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}) =$
$r(n) + r(a') + 1 + r(c') + r(m) = r(na'cm') + 1 = r(M) + 1$. □

Theorem 4.13. *$L(M) = r(M) + b$.*

Proof. Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b+c \\ 0 & c \end{pmatrix}$ and $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b+a \\ 0 & c \end{pmatrix}$, each multiplication of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ increases the value of the upper right entry in the matrix. So $b \geq |\{i : \det A_i = 1\}|$. By Theorem 4.9 we can write $L(M) = r(M) + k$ where $k = |\{i : \det A_i = 1\}|$. Since $b \geq k$, $L(M) \leq r(M) + b$. Now factor $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^b\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. Then L$(M) \geq L(\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}) + L(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^b) + L(\begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix}) = r(c) + b + r(a) = r(M) + b$. □

Conjecture 4.14. *If $A = \begin{pmatrix} p & pq+r \\ 0 & p \end{pmatrix}$ where p is prime, $q \in \mathbb{Z}$, and $0 \leq r < p$, then $\ell(A) = q + r + 2$.*

Proof. $\ell(A) \leq q+r+2$: Factor $A = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}$. This factorization has length $1 + r + q + 1 = q + r + 2$. □

4.3 Entries Divisible by k

Let S be the semigroup of $n \times n$ upper triangular matrices with entries divisible by $k > 1$. Let $S^\bullet$ be S without the zero matrix. Let $A \in S^\bullet$. Notice that $S^\bullet$ does not have the identity matrix. Thus $S^\bullet$ does not have units.

$$A = \begin{pmatrix} kx_{1,1} & kx_{1,2} & \cdots & kx_{1,n} \\ & kx_{2,2} & \cdots & kx_{2,n} \\ & & \ddots & \vdots \\ 0 & & & kx_{n,n} \end{pmatrix}, \text{ where } x_{1,1}, x_{1,2}, \cdots, x_{n,n} \in \mathbb{Z}.$$

Theorem 4.15. $L(A) = \eta_k(gcd(A))$.

Proof. Let $m = \eta_k(gcd(A))$. Let $A = A_1A_2\cdots A_t$. For any $B, C \in S^\bullet$, if k^u divides all entries of B and k^v divides all entries of C, then k^{u+v} must divide all entries of BC. Thus, since k divides all entries of each A_i, each multiplication must increase the power of k, so $m \geq t$. Hence $m \geq L(A)$.
For any $A \in S^\bullet$, we can write $A = k^{m-1}A'$ where $A' \in S^\bullet$. Thus $A = (kI)^{m-1}A'$, so $L(A) \geq m$. $\square$

Corollary 4.16. *A is an atom of S if and only if $\eta_k(gcd(A)) = 1$.*

Proof. The result follows immediately from Theorem 4.15. $\square$

Theorem 4.17. *$S^\bullet$ is bifurcus.*

Proof. Let $\kappa = \begin{pmatrix} kI & 0 \\ 0 & k^{w-1} \end{pmatrix}$. Note that κ, when multiplied on the left, multiplies each row except the nth by k and multiplies the nth row by k^{w-1}. Then $A = \begin{pmatrix} & & B & \\ 0 & 0 & \cdots & k^w a_{n,n} \end{pmatrix} = \kappa \begin{pmatrix} & & B' & \\ 0 & 0 & \cdots & ka_{n,n} \end{pmatrix}$ where $B = kB'$. $\square$

Note that these results also apply to lower triangular matrices.

4.4 Entries in Three Ideals

Let S be the semigroup of 2×2 upper triangular matrices with entries in three integral ideals. Let $S^\bullet$ be S without the zero matrix. Let $A \in S^\bullet$. Notice that $S^\bullet$ does not contain the identity matrix. Thus $S^\bullet$ does not have units.
$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} {k_1}^{m_1}s & k_2t \\ 0 & {k_3}^{m_3}u \end{pmatrix}$, where $s \not\equiv 0 \pmod{k_1}, u \not\equiv 0 \pmod{k_3}$ and $k_1, k_2, k_3 > 1$.

Theorem 4.18. *A is an atom of $S^\bullet$ if and only if ${k_1}^2 \nmid a$ or ${k_3}^2 \nmid c$ or $\gcd(k_1, k_3) \nmid \frac{b}{k_2}$. Moreover, $S^\bullet$ is bifurcus.*

Proof. Assume A is reducible. Then a is a product of two multiples of k_1 and c is a product of two multiples of k_3. Thus ${k_1}^2 \mid a$ and ${k_3}^2 \mid c$.
Since A is reducible, $b = (k_1\alpha)(k_2\beta_1) + (k_2\beta_2)(k_3\gamma)$ where $\alpha, \beta_1, \beta_2, \gamma, \in \mathbb{Z}$. Hence $\gcd(k_1, k_3) \mid \frac{b}{k_2}$.
For the converse, assume ${k_1}^2 \mid a$ and ${k_3}^2 \mid c$ and $\gcd(k_1, k_3) \mid \frac{b}{k_2}$, so there exist $x, y \in \mathbb{Z}$ such that $\frac{b}{k_2} = k_1x + k_3y$. So $b = k_1(k_2x) + k_3(k_2y)$. Then
$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} k_1 & k_2y \\ 0 & \frac{c}{k_3} \end{pmatrix} \begin{pmatrix} \frac{a}{k_1} & k_2x \\ 0 & k_3 \end{pmatrix}$. $\square$

Theorem 4.19. *If $\gcd(k_1, c) = 1$ or $\gcd(k_3, a) = 1$, then $L(A) = \min(m_1, m_3)$.*

Table 3: Notation for Unitriangular Matrices

Symbol	Definition
$E_{i,j}$	the matrix with the i,jth entry equal to 1 and other entries 0
$\Sigma(A)$	the sum of all off-diagonal entries of A
$\Lambda(x,y,z)$	greatest k such that $k < x$, $k < y$, and $\frac{k(k+3)}{2} < z$

Proof. Let $A = A_1A_2\cdots A_t$. Since each multiplication increases m_1 and m_3, $m_1, m_3 \geq t$. Hence $L(A) \leq \min(m_1, m_3)$.
If $\gcd(k_1, c) = 1$, then a matrix in S is an atom if and only if $\min(m_1, m_3) = 1$. Let $\min(m_1, m_3) = i+1$. Factor $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} k_1 & b_1 \\ 0 & k_3 \end{pmatrix} \begin{pmatrix} \frac{a}{k_1} & b_2 \\ 0 & \frac{c}{k_3} \end{pmatrix}$ where $b = k_1b_2 + \frac{c}{k_3}b_1$. By the inductive hypothesis, the maximum length of the right matrix is $\min(m_1-1, m_3-1) = \min(m_1, m_3) - 1$, so $L(A) \geq \min(m_1, m_3)$. Similarly, if $\gcd(k_3, a) = 1$, then $L(A) \geq \min(m_1, m_3)$. $\square$

Theorem 4.20. *Let $g = \gcd(k_1, k_3)$. If $g \mid k_2$, then $L(A) \leq \min(m_1, m_3, \eta_g(b)+1)$.*

Proof. Define $\gamma(A) = \eta_g(b)$. Let $A = A_1A_2\cdots A_t$. Let $B_i = A_1A_2\cdots A_i$. For the base step, $\gamma(B_1) \geq 0 = 1-1$. Now assume that $\gamma(B_i) \geq i-1$ for all $i \leq j$. $B_{j+1} = B_jA_{j+1} = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\begin{pmatrix} a_{j+1} & b_{j+1} \\ 0 & c_{j+1} \end{pmatrix} = \begin{pmatrix} a'a_{j+1} & a'b_{j+1} + b'c_{j+1} \\ 0 & c'c_{j+1} \end{pmatrix}$. Since $g \mid k_2$, $g^{j+1} \mid {k_1}^j k_2 \mid a'b_{j+1}$. By the inductive hypothesis, $g^{j-1} \mid b'$, so since $g \mid k_3 \mid c_{i+1}$, $g^j \mid b'c_{j+1}$. Hence $\gamma(B_{j+1}) \geq j$, so $\gamma(A) = \gamma(B_t) \geq t-1$. $\square$

Conjecture 4.21. $L(A) = \min(m_1, m_3, \eta_g(b)+1)$

4.5 Unitriangular Matrices

Throughout this section, let S be the semigroup of $n \times n$ unitriangular matrices. If $A \in S$ then

$$A = \begin{pmatrix} 1 & a_{1,2} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & a_{n-1,n} \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$$

with all entries a_{ij} with $i > j$ from $\mathbb{N}_0$ or $\mathbb{N}$ (depending on the case being explored). It seems natural to look at unitriangular matrices over $\mathbb{Z}$ as well but this case proves insignificant. On inspection, allowing negative integers into the matrices changes every matrix in $S_{\mathbb{Z}}$ to a unit (all inverses are within the semigroup). Thus making the properties of $S_{\mathbb{Z}}$ trivial, it is more meaningful merely to focus on $\mathbb{N}_0$ and $\mathbb{N}$.

Unitriangular matrices have been applied by previous authors such as Gomes, Sezinardo, Pin, and Kambites. In [10], Gomes', Sezinardo's, and Pin's use of unitriangulars involve the decomposition of $n \times n$ upper triangular matrices over a semiring k. They explore the fact that an $n \times n$ upper triangular matrix over a semiring is the semidirect product of the group of diagonal matrices and the monoid of unitriangular matrices over that semiring [10].

Kambites also explores the unitriangular matrix, however not for the sake of decomposition. In [16], Kambites finds the complexity of all $n \times n$ unitriangular matrices over a finite field k. [16] Rather than unitrainagular matrices used in factorization and decomposition, the latter uses them in a linear algebraic sense. Clearly the interest in this specific semigroup proves interesting and useful not only in this paper. Used by other applications and mathematicians, this inspires the study of the unitriangular factorization properties which follow.

4.5.1 $n \times n$ Unitriangular Matrices

Let $E_{i,j}$ denote the matrix with all entries above the diagonal 0 except the entry in the ith row and jth column, which is 1.

$n \times n$ with $\mathbb{N}_0$ Let S be the semigroup of $n \times n$ unitriangular matrices with entries from $\mathbb{N}_0$. Let A be an arbitrary element of S. Define $\Sigma(A)$ to be the sum of the off-diagonal entries of A.

Lemma 4.22. *A is a unit if and only if $\Sigma(A) = 0$.*

Proof. Suppose $AB = I$ for some $B \in S$. By Lemma 4.32, $\Sigma(A) \leq \Sigma(A) + \Sigma(B) \leq \Sigma(AB) = \Sigma(I) = 0$. Hence $\Sigma(A) = 0$.
Suppose $\Sigma(A) = 0$. Then $A = I$. □

Lemma 4.23. *For any $w_1, w_2, \ldots, w_m \geq y$, $(I + \sum_{i=1}^{m} c_i E_{w_i,x_i})(I + dE_{y,z}) = I + \sum_{i=1}^{m} c_i E_{w_i,x_i} + dE_{y,z}$.*

Proof. Note that $E_{i_1,j_1}E_{i_2,j_2} \neq [0]$ if and only if $j_1 = i_2$. Let $w_1, w_2, \ldots, w_m \geq y$. Then $(I + c_1E_{w_1,x_1} + c_2E_{w_2,x_2} + \cdots + c_mE_{w_m,x_m})(I + dE_{y,z}) = I + c_1E_{w_1,x_1} + c_2E_{w_2,x_2} + \cdots + c_mE_{w_m,x_m} + dE_{y,z} + (c_1E_{w_1,x_1} + c_2E_{w_2,x_2} + \cdots + c_mE_{w_m,x_m})dE_{y,z}$. Since $x_i > w_i \geq y$, $(c_iE_{w_i,x_i})(dE_{y,z}) = (c_id)(E_{w_i,x_i}E_{y,z}) = [0]$, so $(I + c_1E_{w_1,x_1} + c_2E_{w_2,x_2} + \cdots + c_mE_{w_m,x_m})(I + dE_{y,z}) = I + c_1E_{w_1,x_1} + c_2E_{w_2,x_2} + \cdots + c_mE_{w_m,x_m} + dE_{y,z}$. □

Theorem 4.24. *$L(A) = \Sigma(A)$*

Proof. Let $A = A_1A_2 \cdots A_t$ where $A_i \neq I$. By Lemma 4.32, $\Sigma(A) \geq t$. Hence $L(A) \leq \Sigma(A)$.

By Lemma 4.23, for any $w_1, w_2, \ldots, w_m \geq y$, $(I + \sum_{i=1}^{m} c_i E_{w_i,x_i})(I + dE_{y,z}) = I + \sum_{i=1}^{m} c_i E_{w_i,x_i} + dE_{y,z}$. Therefore $\prod_{i=n-1}^{1} \left(\prod_{j=n}^{i+1} (I + E_{i,j})^{A_{i,j}} \right)$

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

$= I + \sum_{i=n-1}^{1}\sum_{j=n}^{i+1} A_{i,j}E_{i,j} = A$. Thus we can factor $A = \prod_{i=n-1}^{1}\left(\prod_{j=n}^{i+1}(I + E_{i,j})^{A_{i,j}}\right)$, so $L(A) \geq \Sigma(A)$. ☐

Corollary 4.25. *A is an atom if and only if $\Sigma(A) = 1$.*

Theorem 4.26. *If $n \geq 3$, then $\rho(S) = \infty$.*

Proof. Let $A \in S$ such that $A = \prod_{i=1}^{n-1}(I + E_{i,i+1})^a = \prod_{i=1}^{n-1}(I + aE_{i,i+1})$ where $a \in \mathbb{N}$. Since $(I + aE_{1,2})(I + aE_{2,3}) = I + aE_{1,2} + aE_{2,3} + a^2E_{1,3}$, if $n \geq 3$, then $\Sigma(A) \geq a^2$, so by Theorem 4.24 $L(A) \geq a^2$. Since $A = \prod_{i=1}^{n-1}(I + E_{i,i+1})^a$, $\ell(A) \leq (n-1)a$. Hence $\rho(S) \geq \lim_{a\to\infty} \rho(A) \geq \lim_{a\to\infty} \frac{a^2}{(n-1)a} = \lim_{a\to\infty} \frac{a}{n-1} = \infty$. ☐

$n \times n$ with $\mathbb{N}$ Let S be the set of $n \times n$ unitriangular matrices over the positive integers.

Theorem 4.27. *S is bifurcus.*

Proof. Suppose that $X \in S$ is reducible. Then each superdiagonal entry of X is a sum of positive integers, so each is at least 2. Thus, for any $X \in S$, if $\min(X) = 1$, then X is an atom.

Assume $A \in S$ is reducible. Then $A = \begin{pmatrix} 1 & a_{1,2} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & a_{n-1,n} \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$

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

Let $U_1 = I + (1 - b_{1,2})E_{1,2} + (c_{n-1,n} - 1)E_{n-1,n}$ and let $U_2 = I + (b_{1,2} - 1)E_{1,2} + (1 - c_{n-1,n})E_{n-1,n}$. Then $U_1 = \begin{pmatrix} 1 & 1 - b_{1,2} & 0 & \cdots & & 0 \\ 0 & 1 & 0 & \cdots & & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & \cdots & & & 1 & c_{n-1,n} - 1 \\ 0 & \cdots & & & \cdots & 1 \end{pmatrix}$ and let $U_2 = \begin{pmatrix} 1 & b_{1,2} - 1 & 0 & \cdots & & 0 \\ 0 & 1 & 0 & \cdots & & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & \cdots & & & 1 & 1 - c_{n-1,n} \\ 0 & \cdots & & & \cdots & 1 \end{pmatrix}$. Note that $U_1U_2 = I$. Thus

$A = BC = BIC = (BU_1)(U_2C)$. Note that all entries of U_1 are nonnegative except $1 - b_{1,2}$; this will be multiplied only by 1 and the corresponding cell of BU_1 will be the sum $b_{1,2} + 1 - b_{1,2} = 1$. Hence $BU_1 \in S$, and since $\min(BU_1) = 1$, BU_1 is an atom. Similarly, all entries of U_2 are nonnegative except $1 - c_{n-1,n}$; this will be multiplied only by 1 and the corresponding cell of U_2C will be the sum $c_{n-1,n} + 1 - c_{n-1,n} = 1$. Hence $U_2C \in S$, and since $\min(U_2C) = 1$, U_2C is an atom. Consequently, $\ell(A) = 2$. □

It is interesting to explore this proof further. As can be seen, the atoms for unitriangular $n \times n$ matrices over the positive integers have yet to be discovered. However, it is still possible to prove this semigroup is bifurcus. The reason this can be done is it *is* known those matrices containing an off diagonal entry $A_{i,j} = 1$ are atoms (if reducible, then $A_{i,j}$ must be at least the sum of two positive integers, implying $A_{i,j} \geq 2$). Since every $A \in S$ can be the product of two atoms of this type, the semigroup is bifurcus, although all atoms have yet to be identified.

This is not *all* that is known about unitriangular matrices, merely for the $n \times n$ cases. Much more has been discovered in the smaller dimension matrices that follow.

4.5.2 2×2 Unitriangulars

2×2 with $\mathbb{N}_0$ Let S be the semigroup of 2×2 unitriangular matrices with entries from $\mathbb{N}_0$. Let $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ be an arbitrary element of S.

Lemma 4.28. *A is a unit if and only if $A = I$.*

Proof. This follows from Lemma 4.22. □

Lemma 4.29. *A is an atom if and only if $a = 1$.*

Proof. This follows from Corollary 4.25. □

Lemma 4.30. $L(A) = \ell(A) = a$

Proof. Let $A = P_1P_2 \cdots P_t$ where P_i are atoms in S. Then $P_i = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, so $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$. Hence $t = a$. □

Corollary 4.31. *S is factorial.*

Proof. Since there is only one atom in S, all atomic factorizations of A must be the same up to units. □

2×2 with $\mathbb{N}$ Let S' be the semigroup of 2×2 unitriangular matrices with entries from $\mathbb{N}$. Since $S' = S \backslash \{I\}$, the factorization properties of S' are identical to those of S.

4.5.3 3×3 Unitriangular Matrices

Let S be a semigroup of 3×3 unitriangular matrices. Let $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ be an arbitrary element of S. Let $s(A) = a+c$ denote the sum of the superdiagonal of A. The following lemmas, Lemma 4.32 and Lemma 4.33, state properties of products of two matrices in this semigroup. They will be referred to later within this subsection.

Lemma 4.32. *$\Sigma(AX) = \Sigma(A) + \Sigma(X) + A_{1,2}X_{2,3}$ for any $X \in S$. Specifically, $(AX)_{1,2} = A_{1,2} + X_{1,2}$, $(AX)_{2,3} = A_{2,3} + X_{2,3}$, and $(AX)_{13} = A_{13} + X_{13} + A_{1,2}X_{2,3}$.*

Proof. Let $X = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$ be an arbitrary element of S. Since $AX = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{pmatrix}$, $\Sigma(AX) = a+b+c+x+y+z+az = \Sigma(A) + \Sigma(X) + A_{1,2}X_{2,3}$. □

Lemma 4.33. *If $A = A_1A_2\cdots A_t$, then $\Sigma(A) = \sum_{i=1}^{t}\Sigma(A_i) + \sum_{i=1}^{t}(\sum_{j=1}^{i-1} a_j)c_i$.*

Proof. Let $A = A_1A_2\cdots A_t$ where $A_i = \begin{pmatrix} 1 & a_i & b_i \\ 0 & 1 & c_i \\ 0 & 0 & 1 \end{pmatrix}$. Let $B_i = A_1A_2\cdots A_i$. $\Sigma(B_1) = \Sigma(A_1) = \sum_{i=1}^{1}\Sigma(A_i) + \sum_{i=1}^{1}(\sum_{j=1}^{i-1} a_j)c_i$. Suppose $\Sigma(B_i) = \sum_{j=1}^{i}\Sigma(A_j) + \sum_{j=1}^{i}(\sum_{k=1}^{j-1} a_k)c_j$ for all $i \le m$. $\Sigma(B_{m+1}) = \Sigma(B_mA_{m+1}) = \Sigma(B_m) + \Sigma(A_{m+1}) + (\sum_{i=1}^{m} a_i)c_{m+1}$ by Lemma 4.32, so by the inductive hypothesis $\Sigma(B_{m+1})$
$= \sum_{j=1}^{m}\Sigma(A_j) + \sum_{j=1}^{m}(\sum_{k=1}^{j-1} a_k)c_j + \Sigma(A_{m+1}) + (\sum_{i=1}^{m} a_i)c_{m+1}$
$= \sum_{j=1}^{m+1}\Sigma(A_j) + \sum_{j=1}^{m+1}(\sum_{k=1}^{j-1} a_k)c_j$. Hence $\Sigma(A) = \sum_{i=1}^{t}\Sigma(A_i) + \sum_{i=1}^{t}(\sum_{j=1}^{i-1} a_j)c_i$. □

3×3 with $\mathbb{N}_0$ Let S be the semigroup of 3×3 unitriangular matrices with entries from $\mathbb{N}_0$. While first discussing matrices over $\mathbb{N}_0$, it shall be seen that in comparison to $\mathbb{N}$ the factorization properties are drastically different.

Lemma 4.34. *A is a unit if and only if $\Sigma(A) = 0$.*

Proof. This follows from Lemma 4.22. □

Theorem 4.35. $L(A) = \Sigma(A)$

Proof. This follows directly from Corollary 4.25. $\square$

Corollary 4.36. *A is an atom if and only if* $\Sigma(A) = 1$.

Corollary 4.37. *If* $A = A_1A_2\cdots A_t$ *and* A_i *are atoms, then* $\Sigma(A) = t + \sum_{i=1}^{t}(\sum_{j=1}^{i} a_j)c_i$.

Proof. The result follows directly from Lemma 4.33 and Theorem 4.35. $\square$

Theorem 4.38. $\ell(A) = \Sigma(A) - \min(b, ac)$ *and* $\Delta(S) = 1$.

Proof. Let $A = A_1A_2\cdots A_t$ where A_i are atoms. Since $\sum_{i=1}^{t}(\sum_{j=1}^{i} a_j)c_i \leq ac$, by Corollary 4.37 $t \geq \Sigma(A) - ac$. Meanwhile, by Lemma 4.32 $\sum_{i=1}^{t}(\sum_{j=1}^{i} a_j)c_i \leq b$, so by Corollary 4.37 $t \geq \Sigma(A) - b$. Consequently, $\ell(A) \geq \Sigma(A) - \min(b, ac)$.
To achieve the length $\Sigma(A) - k$ where $0 < k \leq \min(b, ac)$, let $k = qa + r$ where $0 < r \leq a$ and factor $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$
$= (I + E_{2,3})^{c-q-1}(I + E_{1,2})^{r}(I + E_{2,3})(I + E_{1,2})^{a-r}(I + E_{2,3})^{q}(I + E_{1,3})^{b-k}$.
Thus $\ell(A) \leq \Sigma(A) - \min(b, ac)$ and $\Delta(S) = 1$. $\square$

Note the order of the matrices are important to achieve the minimum length. This semigroup is *not* commutative. For example: $(I + E_{2,3})(I + E_{1,2}) = I + E_{2,3} + E_{1,2} \neq (I + E_{1,2})(I + E_{2,3}) = I + E_{1,2} + E_{2,3} + E_{1,3}$. Recall how the minimum length was not noted for the $n \times n$ case. This precise order, as seen in the 3×3, surely does exist for $n \times n$ matrices, but that which was difficult in a 3×3 matrix, is ever more daunting to find for an $n \times n$ matrix.

Corollary 4.39. $\rho(S) = \infty$

Proof. $\rho(S) \geq \lim_{a\to\infty} \rho \begin{pmatrix} 1 & a & a^2 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} = \lim_{a\to\infty} \frac{a^2+2a}{2a} = \lim_{a\to\infty} \frac{a+2}{2} = \infty$ by Theorems 4.35 and 4.38. $\square$

3×3 with $\mathbb{N}$ Let S be the semigroup of 3×3 unitriangular matrices with entries from $\mathbb{N}$. Note that S has no identity and no units.

Lemma 4.40. *If* $a = 1$ *or* $c = 1$ *or* $b \leq 2$*, then A is an atom. Otherwise, A is reducible and* $\ell(A) = 2$.

Proof. Suppose $A = BC$ for some $B, C \in S$. Then a and c are sums of two positive integers, so $a, c \geq 2$. Further, b is a sum of three positive integers, so $b \geq 3$.

Suppose $a, c \geq 2$ and $b \geq 3$. Factor $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 1 & b_1 \\ 0 & 1 & c-1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a-1 & b_2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ where $b = b_2 + 1 + b_1$. □

Define $\Lambda(x, y, z)$ to be the greatest k such that $k < x$, $k < y$, and $\frac{k(k+3)}{2} < z$.

Lemma 4.41. $L(A) = \Lambda(a, c, b) + 1$.

Proof. Let $A = A_1 A_2 \cdots A_t$. Let $T_1 = I + \sum_{i=1}^{n} \sum_{j=i+1}^{n} E_{ij}$. Entrywise,

$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = A = A_1 A_2 \cdots A_t \geq T_1^t = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^t$

$= \begin{pmatrix} 1 & t & \frac{t(t+1)}{2} \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}$ by Lemma 4.33. Hence $a \geq t > t-1$ and $c \geq t > t-1$.

Similarly, $b \geq \frac{t(t+1)}{2} = \frac{t^2+t}{2} > \frac{t^2+t-2}{2} = \frac{(t-1)(t+2)}{2}$, and therefore $t - 1 \leq \Lambda(a, c, b)$. Thus $t \leq \Lambda(a, c, b) + 1$, so $L(A) \leq \Lambda(a, c, b) + 1$.

Let $\lambda = \Lambda(a, c, b)$. Then $\lambda < a$, $\lambda < c$, and $\frac{\lambda(\lambda+3)}{2} < b$. Factor $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & c-\lambda \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^{\lambda-1} \begin{pmatrix} 1 & a-\lambda & b - \frac{\lambda(\lambda+3)}{2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Thus $L(A) \geq \lambda + 1 = \Lambda(a, c, b) + 1$. □

4.5.4 4×4 Unitriangular Matrices

4×4 with $\mathbb{N}$ Let S be the semigroup of 4×4 unitriangular matrices with entries from $\mathbb{N}$. Let $A = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix}$ be an arbitrary element of S. Note that S has no identity and no units.

Theorem 4.42. *A is an atom if and only if $a < 2$, $d < 2$, $f < 2$, $b < 3$, $e < 3$, $c < 4$, or $b + e < d + 4$. Moreover, S is bifurcus.*

Proof. Suppose A is reducible. Than $\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix} = A = A_1 A_2$

$$= \begin{pmatrix} 1 & a_1 & b_1 & c_1 \\ 0 & 1 & d_1 & e_1 \\ 0 & 0 & 1 & f_1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & b_2 & c_2 \\ 0 & 1 & d_2 & e_2 \\ 0 & 0 & 1 & f_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & a_1+a_2 & b_1+b_2+a_1d_2 & c_1+c_2+a_1e_2+b_1f_2 \\ 0 & 1 & d_1+d_2 & e_1+e_2+d_1f_2 \\ 0 & 0 & 1 & f_1+f_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$ Hence $a \geq 2$, $d \geq 2$, $f \geq 2$, $b \geq 3$, $e \geq 3$, and $c \geq 4$. Also, $b+e = b_1+b_2+a_1d_2+e_1+e_2+d_1f_2 \geq 4+a_1d_2+d_1f_2 \geq 4+d_1+d_2 = 4+d$.

Suppose that $a \geq 2$, $d \geq 2$, $f \geq 2$, $b \geq 3$, $e \geq 3$, $c \geq 4$, and $b+e \geq d+4$. Factor

$$A = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & d_1 & e-d_1-1 \\ 0 & 0 & 1 & f-1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a-1 & b-d_2-1 & c-3 \\ 0 & 1 & d_2 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$ Hence A is reducible and $\ell(A) = 2$. □

4.6 Gauss Matrices

A Gauss matrix (also called a Frobenius matrix) is a lower unitriangular matrix, where all of the off diagonal entries are zero, except for the entries in one column. That is, a matrix of the form:

$$\begin{pmatrix} 1 & & & & & & & 0 \\ 0 & \ddots & & & & & & \\ 0 & \ddots & 1 & & & & & \\ 0 & \ddots & 0 & 1 & & & & \\ & & 0 & a_{j+1,j} & 1 & & & \\ \vdots & & 0 & a_{j+2,j} & 0 & \ddots & & \\ & & \vdots & \vdots & \vdots & \ddots & 1 & \\ 0 & \dots & 0 & a_{n,j} & 0 & \dots & 0 & 1 \end{pmatrix}$$

Gaussian elimination of column j is described by multiplication with a Gauss matrix that has the non zero entries on the jth column. Since this type of matrices are essential in LU factorizations, they have wide applications in pure and applied mathematics. See [9], [21], [7] for more information on Gauss(Frobenius) matrices.

When two Gauss matrices are multiplied, the only entries that change are the off diagonal entries. Furthermore, these off diagonal entries are added. Let S be the semigroup of $n \times n$ Gauss matrices with a fixed non zero column. Let j

be the column with non zero diagonal entries. Then we can express $A = BC$, the product of two Gauss matrices as:

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

4.6.1 Entries from $\mathbb{N}$

Let S^1 be the semigroup of $n \times n$ Gauss matrices with a fixed nonzero column of positive entries. Let $A \in S^1$. Notice that S^1 does not have the identity matrix. Thus S does not have units.
Let $m = \min\{a_{i,j} : a_{i,j} \text{ is a positive off diagonal entry of } A\}$.

Theorem 4.43. *A is an atom of S^1 if and only if 1 is an off diagonal entry of A. Furthermore, $L(A) = m$.*

Proof. Let $a_{i,j}$ be a positive off diagonal entry of A. If A is the product of two matrices $B, C \in S^1$, then $a_{i,j} = b_{i,j} + c_{i,j}$. where $b_{i,j}, c_{i,j}$ are positive off diagonal entries, $b_{i,j} \in B$ and $c_{i,j} \in C$. Thus $a_{i,j} \neq 1$. For the converse, assume that $a_{i,j} > 1$. WLOG, assume $m = a_{n,j}$. Then A can be factored into m atoms:

$$A = \begin{pmatrix} a_{j+1,j} \\ \vdots \\ a_{n-1,j} \\ a_{n,j} \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix}^{m-1} \begin{pmatrix} a_{j+1,j} - (m-1) \\ \vdots \\ a_{n-1,j} - (m-1) \\ 1 \end{pmatrix}.$$

Assume to the contrary that $L(A) = t > m$. Then $a_{n,j} \geq t > m = a_{n,j}$. Contradiction. $\square$

Corollary 4.44. *If $j \neq n-1$, then S^1 is bifurcus. Otherwise, S^1 is factorial. Moreover, $L(A) = \ell(A) = a_{n,n-1}$.*

Proof. Case 1: $j \neq n-1$
If A is reducible, then

$$A = \begin{pmatrix} a_{j+1,j} \\ a_{j+2,j} \\ a_{j+3,j} \\ \vdots \\ a_{n,j} \end{pmatrix} = \begin{pmatrix} 1 \\ a_{j+2,j} - 1 \\ a_{j+3,j} - 1 \\ \vdots \\ a_{n,j} - 1 \end{pmatrix} \begin{pmatrix} a_{j+1,j} - 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Case 2: $j = n-1$
If $j = n-1$, then $a_{n,n-1}$ is the only off diagonal entry. Since $a_{n,n-1} = a_{n,n-1}(1)$, the only possible factorization of A into atoms is:
$A = \begin{pmatrix} a_{n,n-1} \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix}^{a_{n,n-1}}$. $\square$

4.6.2 Entries from $\mathbb{N}_0$

Let S^0 be the semigroup of $n \times n$ Gauss matrices with a fixed nonzero column of non negative entries. Let $A \in S^0$. The identity matrix I is the only unit of S^0, since it is the only element with an inverse.

Theorem 4.45. *A is an atom of S^0 if and only if the the off diagonal entries of the jth column are zero, except for one single 1 entry.*

Proof. Assume the off diagonal entries of the jth column of A are zero, except for one single 1 entry. WLOG, assume $a_{j+1,j}$ is the 1 entry. If $A = BC$, then the only possible factorization of A is:

$$A = \begin{pmatrix} a_{j+1,j} \\ a_{j+2,j} \\ \vdots \\ a_{n,j} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

That is, $A = AI$. Thus A is an atom. For the converse, assume A has more than one off diagonal non zero entry. WLOG, assume $a_{j+1,j}, a_{j+2,j} > 0$. Then

$$A = \begin{pmatrix} a_{j+1,j} \\ a_{j+2,j} \\ a_{j+3,j} \\ \vdots \\ a_{n,j} \end{pmatrix} = \begin{pmatrix} a_{j+1,j} - 1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ a_{j+2,j} - 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Now assume A has one off diagonal entry greater than 1. WLOG, assume $a_{j+1,j} > 1$. Then

$$A = \begin{pmatrix} a_{j+1,j} \\ a_{j+2,j} \\ \vdots \\ a_{n,j} \end{pmatrix} = \begin{pmatrix} a_{j+1,j} - 1 \\ a_{j+2,j} \\ \vdots \\ a_{n,j} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

□

Theorem 4.46. *S^0 is factorial. Furthermore, $L(A) = \ell(A) = \sum_{k=j+1}^{n} a_{k,j}$.*

Proof. $A = \begin{pmatrix} a_{j+1,j} \\ a_{j+2,j} \\ \vdots \\ a_{n,j} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}^{a_{j+1,j}} \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}^{a_{j+2,j}} \cdots \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}^{a_{n,j}}.$

Assume to the contrary that A has a different factorization. Then one of the exponents in the previous factorization is different. WLOG, assume $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ has an exponent $t \neq a_{j+1,j}$. Since multiplication of matrices in S^0 implies addition of the off diagonal entries, then we have $a_{j+1,j} = t \neq a_{j+1,j}$. Contradiction.

□

4.6.3 Entries from $\mathbb{Z}$

Let S be the semigroup of $n \times n$ Gauss matrices with a fixed nonzero column of integer entries. Let $A \in S$. Then

$$A = \begin{pmatrix} a_{j+1,j} \\ a_{j+2,j} \\ \vdots \\ a_{n,j} \end{pmatrix} = \begin{pmatrix} a_{j+1,j} - 1 \\ a_{j+2,j} - 1 \\ \vdots \\ a_{n,j} - 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Thus S does not have atoms.

4.7 Equal-Diagonal Triangular Matrices

Now we will consider a generalization of unitriangular matrices, equal-diagonal triangular matrices. An equal-diagonal triangular matrix has all diagonal entries equal.

Let S be the commutative semigroup of 2×2 upper triangular matrices with entries from $\mathbb{Z}$ and diagonal entries equal and nonzero determinant. Let $A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, $a \neq 0$ be an arbitrary element of S. Let $d_A = \sqrt{\det A}$ denote the (repeated) diagonal entry of A.

Lemma 4.47. *Let $a, b, c \in \mathbb{Z}$.* $\gcd(a, bc) \mid \gcd(a, b)\gcd(a, c)$.

Proof. Let $g = \gcd(a, bc)$. Since $g|bc$, $g = g_1 g_2$ where $g_1|b$ and $g_2|c$. $g_1|g|a$, so $g_1|\gcd(a, b)$. $g_2|g|a$, so $g_2|\gcd(a, c)$. Thus $g = g_1 g_2|\gcd(a, b)\gcd(a, c)$. □

Lemma 4.48. *Let $B, C \in S$. If* $\gcd(d_B, d_C) = 1$, *then* $\gcd(BC) = \gcd(B)\gcd(C)$.

Proof. Let $B = \begin{pmatrix} d_B & \beta \\ 0 & d_B \end{pmatrix}$ and $C = \begin{pmatrix} d_C & \gamma \\ 0 & d_C \end{pmatrix}$, so $BC = \begin{pmatrix} d_B d_C & d_B\gamma + d_C\beta \\ 0 & d_B d_C \end{pmatrix}$. Let $g = \gcd(BC) = \gcd(d_B d_C, d_B\gamma + d_C\beta)$. Since $g \mid d_B d_C$, $g = g_1 g_2$ where $g_1 \mid d_B$ and $g_2 \mid d_C$. $g_1 \mid d_B \mid d_B\gamma$ and $g_1 \mid g \mid d_B\gamma + d_C\beta$, so $g_1 \mid d_C\beta$. Hence $g_1 \mid \gcd(d_B, d_C\beta) \mid \gcd(d_B, d_C)\gcd(d_B, \beta) = \gcd(B)$ by Lemma 4.47. Similarly, $g_2 \mid d_C\beta$ and $g_2 \mid d_B\gamma + d_C\beta$, so $g_2 \mid d_B\gamma$ and $g_2 \mid \gcd(C)$. Thus $g = g_1 g_2 \mid \gcd(B)\gcd(C)$.
Since $\gcd(B)$ divides all entries of B, $\gcd(C)$ divides all entries of C, and all entries of BC are sums of products of entries of B and C, $\gcd(B)\gcd(C) \mid \gcd(BC)$. □

Lemma 4.49. *Let $B, C \in S$.* $\gcd(d_B, d_C)|\gcd(BC)$ *and* $\gcd(B)\gcd(C)|\gcd(BC)$.

Proof. Let $BC = \begin{pmatrix} d_B & \beta \\ 0 & d_B \end{pmatrix} \begin{pmatrix} d_C & \gamma \\ 0 & d_C \end{pmatrix} = \begin{pmatrix} d_B d_C & d_B\gamma + d_C\beta \\ 0 & d_B d_C \end{pmatrix}$.
$\gcd(d_B, d_C)$ divides $d_B d_C$ and $d_B\gamma + d_C\beta$, so it divides $\gcd(BC)$. Similarly, $\gcd(B)\gcd(C)$ divides $d_B d_C$ and $d_B\gamma + d_C\beta$, so it divides $\gcd(BC)$. □

Lemma 4.50. *A is a unit if and only if $|\det A| = 1$.*

Proof. Suppose A is a unit. Then there exists some $B \in S$ such that $AB = I$, so $\det A \det B = \det I = 1$. Hence $|\det A| = 1$.
Suppose $|\det A| = 1$. Then $A^{-1} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \frac{1}{\det A}\begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} \in S$. $\square$

Theorem 4.51. *If $\sqrt{\det A} \in \mathbb{P}$ or $A = \begin{pmatrix} p^m & b \\ 0 & p^m \end{pmatrix}$ where $p \nmid b$ for some $p \in \mathbb{P}$, then A is an atom. Otherwise, A is reducible.*

Proof. Suppose A is reducible. Then $A = BC$ for some nonunits $B, C \in S$, so $\det A = \det B \det C = (d_B)^2(d_C)^2$. Hence $\sqrt{\det A} = d_B d_C$, so since $|d_B|, |d_C| > 1$, $\sqrt{\det A} \notin \mathbb{P}$. Thus if $\sqrt{\det A} \in \mathbb{P}$, then A is an atom.
Suppose that $d_A = p^m$ and $A = BC$ for some nonunits $B, C \in S$. Then $d_B = p^{m_1}$ and $d_C = p^{m_2}$ where $m_1 + m_2 = m$, and since $|d_B|, |d_C| > 1$, $m_1, m_2 > 0$. Hence $A = \begin{pmatrix} p^m & b \\ 0 & p^m \end{pmatrix} = BC = \begin{pmatrix} p^{m_1} & b_1 \\ 0 & p^{m_1} \end{pmatrix}\begin{pmatrix} p^{m_2} & b_2 \\ 0 & p^{m_2} \end{pmatrix} = \begin{pmatrix} p^m & p^{m_1}b_2 + p^{m_2}b_1 \\ 0 & p^m \end{pmatrix}$, so since $m_1, m_2 > 0$, $p \mid p^{m_1}b_2 + p^{m_2}b_1 = b$. Thus if $A = \begin{pmatrix} p^m & b \\ 0 & p^m \end{pmatrix}$ where $p \nmid b$, then A is an atom.
Now suppose that neither condition is satisfied.

Case 1: $A = \begin{pmatrix} p^m & b \\ 0 & p^m \end{pmatrix}$ where $p \mid b$. Since $\gcd(p, p^{m-1}) = p \mid b$, there exist $b_1, b_2 \in \mathbb{Z}$ such that $b = pb_2 + p^{m-1}b_1$. Factor $A = \begin{pmatrix} p^m & b \\ 0 & p^m \end{pmatrix} = \begin{pmatrix} p & b_1 \\ 0 & p \end{pmatrix}\begin{pmatrix} p^{m-1} & b_2 \\ 0 & p^{m-1} \end{pmatrix}$.

Case 2: $d_A = st$ where $\gcd(s,t) = 1$. Factor $A = \begin{pmatrix} st & b \\ 0 & st \end{pmatrix}$ $= \begin{pmatrix} s & b_1 \\ 0 & s \end{pmatrix}\begin{pmatrix} t & b_2 \\ 0 & t \end{pmatrix}$ where $b = sb_2 + tb_1$. $\square$

Lemma 4.52. *If $\gcd(A) = 1$, then $L(A) = \ell(A) = \omega(d_A)$.*

Proof. Let $A = P_1P_2 \cdots P_t$ for some atoms $P_i \in S$. For any $1 \le i, j \le t$, $\gcd(P_i^0, P_j^0) \mid \gcd(A) = 1$, so $\gcd(P_i^0, P_j^0) = 1$. Thus $L(A) \le \omega(d_A)$. Meanwhile, since all P_i are atoms, $\omega(P_i^0) = 1$. Hence $\ell(A) \ge \omega(d_A)$. $\square$

Lemma 4.53. *If $\omega(d_A) = 1$, then $L(A) = r(\gcd(A)) + \omega(\frac{d_A}{\gcd(A)})$.*

Proof. Let $B = \begin{pmatrix} p^m & \beta \\ 0 & p^m \end{pmatrix} \in S$ such that $L(pB) = t$. Then $pB = P_1P_2 \cdots P_t$ for some atoms $P_i \in S$. Let $C = P_{t-1}P_t$. By Lemma 4.49, $p \mid \gcd(C)$, so $C = pD$. Hence $pB = pP_1P_2 \cdots P_{t-2}D$, so $B = P_1P_2 \cdots P_{t-2}D$. Thus, for any such B, $L(pB) \le L(B) + 1$, and so since $L(pB) = L((pI)B) \ge L(B) + 1$,

$L(pB) = L(B) + 1$.
Let $\omega(d_A) = 1$ and let $A = \gcd(A)A'$. Then by the above $L(A) = L(A') + r(\gcd(A))$. Since $\gcd(A') = 1$, by Lemma 4.52 $L(A') = \omega(d_{A'}) = \omega(\frac{d_A}{\gcd(A)})$, so $L(A) = r(\gcd(A)) + \omega(\frac{d_A}{\gcd(A)})$. □

Theorem 4.54. $L(A) = r(\gcd(A)) + \omega(\frac{d_A}{\gcd(A)})$

Proof. Let $A = P_1 P_2 \cdots P_t$ for some atoms $P_i \in S$ where $t = L(A)$. Group the atoms by the primes on their diagonals so that $A = Q_1 Q_2 \cdots Q_{\omega(d_A)}$ where $d_{Q_i} = q_i^{\eta_{q_i}(d_A)}$ and $L(A) = \sum_{i=1}^{\omega(d_A)} L(Q_i)$. By Lemma 4.53, $L(Q_i) = r(\gcd(Q_i)) + \omega(\frac{d_{Q_i}}{\gcd(Q_i)})$, so $L(A) = \sum_{i=1}^{\omega(d_A)} L(Q_i) = \sum_{i=1}^{\omega(d_A)} r(\gcd(Q_i)) + \sum_{i=1}^{\omega(d_A)} \omega(\frac{d_{Q_i}}{\gcd(Q_i)}) = r(\prod_{i=1}^{\omega(d_A)} \gcd(Q_i)) + \omega(\prod_{i=1}^{\omega(d_A)} \frac{d_{Q_i}}{\gcd(Q_i)}) = r(\gcd(A)) + \omega(\frac{d_A}{\gcd(A)})$ by Lemma 4.48. □

Lemma 4.55. *If $\omega(d_A) = 1$, then $1 \le \ell(A) \le 4$. Furthermore, if $2 \nmid d_A$, then $1 \le \ell(A) \le 3$.*

Proof. If $\omega(d_A) = 1$, $A = \begin{pmatrix} p^m & p^n b \\ 0 & p^m \end{pmatrix}$ where $p \in \mathbb{P}$ and $p \nmid b$ unless $b = 0$. If $b = 0$, let $n = 17m + 3221$. If $m = 1$ or $n = 0$, then A is an atom and $\ell(A) = 1$. Assume $m > 1$ and $n > 0$. Further, if $n = 1$, then $A = (pI)A'$ where A' is an atom, so $\ell(A) = 2$. Assume $n > 1$.

Case 1: $m > 2n$. Factor $A = \begin{pmatrix} p^m & p^n b \\ 0 & p^m \end{pmatrix}$
$= \begin{pmatrix} p^{m-n} & b_1 \\ 0 & p^{m-n} \end{pmatrix} \begin{pmatrix} p^n & b_2 \\ 0 & p^n \end{pmatrix}$ where $p^n b = p^{m-n} b_2 + p^n b_1$, so $b = b_1 + p^{m-2n} b_2$. $p \mid p^{m-2n} b_2$ and $p \nmid b$, so $p \nmid b_1$ for any solution (b_1, b_2), and if $p \mid b_2$ we can replace b_1 with $b_1 + p^{m-2n}$ and b_2 with $b_2 - 1$, so that $p \nmid b_2$. Thus $\ell(A) = 2$.

Case 2a: $m = 2n$ and $p = 2$. If $A = BC$, then $A = \begin{pmatrix} 2^{2n} & 2^n b \\ 0 & 2^{2n} \end{pmatrix} = BC = \begin{pmatrix} 2^{m_1} & b_1 \\ 0 & 2^{m_1} \end{pmatrix} \begin{pmatrix} 2^{m_2} & b_2 \\ 0 & 2^{m_2} \end{pmatrix}$ where $2^n b = 2^{m_1} b_2 + 2^{m_2} b_1$ and $m_1 + m_2 = 2n$. Without loss of generality, $m_1 \le m_2$, so $m_1 \le n$ and $2^{n-m_1} b = b_2 + 2^{m_2 - m_1} b_1$. If $m_1 = m_2 = n$, then $b = b_1 + b_2$ is odd, so b_1 and b_2 cannot both be odd, so since $m_1 = m_2 = n > 1$, one of the factors must be reducible. If $m_1 < n$, then b_2 must be even, so since $m_2 > n > m_1 \ge 1$, the right matrix is reducible. Thus $\ell(A) > 2$. However, since $n > 0$ we can factor $A = \begin{pmatrix} 2^{2n} & 2^n b \\ 0 & 2^{2n} \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2^{2n-1} & 2^{n-1} b \\ 0 & 2^{2n-1} \end{pmatrix}$. Since $2n - 1 > 2n - 2 = 2(n-1)$, by Case 1 $\ell(A) \le 1 + 2 = 3$, so $\ell(A) = 3$.

Case 2b: $m = 2n$ and $p \ne 2$. Factor $A = \begin{pmatrix} p^{2n} & p^n b \\ 0 & p^{2n} \end{pmatrix}$

$= \begin{pmatrix} p^n & b_1 \\ 0 & p^n \end{pmatrix} \begin{pmatrix} p^n & b_2 \\ 0 & p^n \end{pmatrix}$ where $p^n b = p^n b_1 + p^n b_2$, so $b = b_1 + b_2$. If b_1 or b_2 is divisible by p, we can replace b_1 with $b_1 + \alpha$ and b_2 with $b_2 - \alpha$ where $\alpha \not\equiv -b_1$ (mod p) and $\alpha \not\equiv b_2$ (mod p) so that p divides neither. Thus $\ell(A) = 2$.

Case 3a: $m < 2n$ and m is even. Factor $A = \begin{pmatrix} p^m & p^n b \\ 0 & p^m \end{pmatrix}$ $= \begin{pmatrix} p^{\frac{m}{2}} & b_1 \\ 0 & p^{\frac{m}{2}} \end{pmatrix} \begin{pmatrix} p^{\frac{m}{2}} & b_2 \\ 0 & p^{\frac{m}{2}} \end{pmatrix}$ where $p^n b = p^{\frac{m}{2}} b_1 + p^{\frac{m}{2}} b_2 = p^{\frac{m}{2}}(b_1 + b_2)$. Since $\gcd(p^{\frac{m}{2}}, p^{\frac{m}{2}}) = p^{\frac{m}{2}} \mid p^n b$, there exist infinitely many such $b_1, b_2 \in \mathbb{Z}$. If b_1 or b_2 is divisible by p, we can replace b_1 with $b_1 + \alpha$ and b_2 with $b_2 - \alpha$ where $\alpha \not\equiv -b_1$ (mod p) and $\alpha \not\equiv b_2$ (mod p) so that p divides neither. Since $p \mid b_1 + b_2$, there will be an α even when $p = 2$. Hence $\ell(A) = 2$.

Case 3b: $m < 2n$ and m is odd. If $A = BC$, then $A = \begin{pmatrix} p^m & p^n b \\ 0 & p^m \end{pmatrix} =$ $BC = \begin{pmatrix} p^{m_1} & b_1 \\ 0 & p^{m_1} \end{pmatrix} \begin{pmatrix} p^{m_2} & b_2 \\ 0 & p^{m_2} \end{pmatrix}$ where $p^n b = p^{m_1} b_2 + p^{m_2} b_1$. Without loss of generality, $m_1 < m_2$, so $m_1 < n$ and $p^{n-m_1} b = b_2 + p^{m_2 - m_1} b_1$. Hence $p \mid b_2$, so since $m_2 > m_1 \geq 1$, the right matrix is reducible. Thus $\ell(A) > 2$. However, since $n > 0$ we can factor $A = \begin{pmatrix} p^m & p^n b \\ 0 & p^m \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} p^{m-1} & p^{n-1} b \\ 0 & p^{m-1} \end{pmatrix}$.

- If $m < 2n - 1$, then $m - 1 < 2n - 2 = 2(n-1)$, so since $m - 1$ is even, by Case 3a $\ell(A) = 3$.
- If $m = 2n - 1$ and $p \neq 2$, then $m - 1 = 2n - 2 = 2(n-1)$ and by Case 2b $\ell(A) = 3$.
- If $m = 2n - 1$ and $p = 2$, then by Case 2a $\ell(A) \leq 4$. Further, if $n \geq 4$, then since $b \neq 0$ as $n < 17m + 3221$, $b - 2^{n-3} - 2$ is odd, so since $A = \begin{pmatrix} 2^m & 2^n b \\ 0 & 2^m \end{pmatrix}$ $= \begin{pmatrix} 2^2 & 1 \\ 0 & 2^2 \end{pmatrix} \begin{pmatrix} 2^{n-2} & 1 \\ 0 & 2^{n-2} \end{pmatrix} \begin{pmatrix} 2^{n-1} & b - 2^{n-3} - 2 \\ 0 & 2^{n-1} \end{pmatrix}$, $\ell(A) = 3$.
  However, if $n = 3$, then if $A = BC$, $A = \begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix} = BC =$ $\begin{pmatrix} 2^{m_1} & b_1 \\ 0 & 2^{m_1} \end{pmatrix} \begin{pmatrix} 2^{m_2} & b_2 \\ 0 & 2^{m_2} \end{pmatrix}$ where $2^3 b = 2^{m_1} b_2 + 2^{m_2} b_1$ and $m_1 + m_2 = 5$. Without loss of generality, $m_1 < m_2$, so $m_1 < 3$ and $2^{3-m_1} b = b_2 + 2^{m_2 - m_1} b_1$. Since $m_2 \geq 3$, $2^{3-m_1} \mid b_2$. If $m_1 = 1$, then $4b = b_2 + 8b_1$, so $4 \mid b_2$ and $8 \nmid b_2$. Hence by Case 2a the minimum length of the right matrix is 3. If $m_1 = 2$, then $2b = b_2 + 2b_1$, so b_2 is even. Thus the right matrix is reducible. If $b_2 \equiv 0 \mod 4$, then by the above the minimum length of the right matrix is 3. Since $b_2 + 2b_1 = 2b \equiv 2 \mod 4$, if $b_2 \equiv 2 \mod 4$ then $2b_1 \equiv 0 \mod 4$, so b_1 is even and both matrices are reducible. Consequently, $\ell(A) = 4$.

□

Theorem 4.56. $\omega(d_A) \le \ell(A) \le 3\omega(d_A) + 1$

Proof. Let $A = P_1 P_2 \cdots P_t$ for some atoms $P_i \in S$ where $t = \ell(A)$. Group the atoms by the primes on their diagonals so that $A = Q_1 Q_2 \cdots Q_{\omega(d_A)}$ where $d_{Q_i} = q_i^{\eta_{q_i}(d_A)}$ and $\ell(A) = \sum_{i=1}^{\omega(d_A)} \ell(Q_i)$. By Lemma 4.55, $1 \le \ell(Q_i) \le 3$ for each $q_i \ne 2$, and $1 \le \ell(Q_i) \le 4$ if $q_i = 2$. Hence $\omega(d_A) \le \ell(A) \le 3\omega(d_A) + 1$. □

Corollary 4.57. $\rho(S) = \infty$

Proof. $\rho(S) \ge \lim_{m\to\infty} \begin{pmatrix} p^{2m} & 0 \\ 0 & p^{2m} \end{pmatrix} = \lim_{m\to\infty} \frac{2m}{2} = \infty$ by Lemmas 4.53 and 4.55. □

Lemma 4.58. *If $M = AX = BY$ where $d_A = d_B$, $\omega(d_A) = \omega(d_B) = 1$, and $\omega(d_X) = \omega(d_Y) = \omega(d_M) - 1$, then $A \cong B$ and $X \cong Y$.*

Proof. Let $M = \begin{pmatrix} d & e \\ 0 & d \end{pmatrix} = AX = \begin{pmatrix} p^m & b_1 \\ 0 & p^m \end{pmatrix}\begin{pmatrix} \frac{d}{p^m} & b_2 \\ 0 & \frac{d}{p^m} \end{pmatrix} = BY = \begin{pmatrix} p^m & b_3 \\ 0 & p^m \end{pmatrix}\begin{pmatrix} \frac{d}{p^m} & b_4 \\ 0 & \frac{d}{p^m} \end{pmatrix}$ where $e = p^m b_2 + \frac{d}{p^m} b_1 = p^m b_4 + \frac{d}{p^m} b_3$. Since $\gcd(p^m, \frac{d}{p^m}) = 1 \mid e$, the solutions to this equation are described by $(b_1 + kp^m, b_2 - k\frac{d}{p^m})$. Since b_3 is a solution to this equation, $b_3 = b_1 + kp^m$ for some $k \in \mathbb{Z}$. Let $U = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$. Then $B = \begin{pmatrix} p^m & b_1 + kp^m \\ 0 & p^m \end{pmatrix}$
$= \begin{pmatrix} p^m & b_1 \\ 0 & p^m \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = AU$. Since $A \cong B$ and $AX = BY$, $X \cong Y$. □

Lemma 4.59. *For all $A \in S$ and all atoms $P \in S$, $\ell(AP) \ge \ell(A) - 2$. Furthermore, If $\ell(AP) = \ell(A) - 2$, then $A = M \begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix}$ for some odd b and some $M \in S$ such that $2 \nmid \det M$ and $2 \mid \det P$.*

Proof. Let $A = A_1 A_2 \cdots A_{\ell(A)}$ for some atoms $A_i \in S$. Group the atoms by the primes on their diagonals so that $A = B_1 B_2 \cdots B_{\omega(d_A)}$ where $d_{B_i} = b_i^{\mathrm{gde}(d_A, b_i)}$ and $\ell(A) = \sum_{i=1}^{\omega(d_A)} \ell(B_i)$. Let $AP = P_1 P_2 \cdots P_{\ell(AP)}$ for some atoms $P_i \in S$. Again, group the atoms by the primes on their diagonals so that $AP = Q_1 Q_2 \cdots Q_{\omega(d_{AP})}$ where $d_{Q_i} = q_i^{\mathrm{gde}(d_{AP}, q_i)}$ and $\ell(AP) = \sum_{i=1}^{\omega(d_{AP})} \ell(Q_i)$. Without loss of generality, $P \mid Q_{\omega(d_{AP})}$.
Since $d_{Q_1} = d_{B_1}$, by Lemma 4.58 $Q_1 \cong B_1$. Now suppose that $Q_i \cong B_i$ for all $i \le m$. Since all Q_i, B_i have nonzero determinant and $B_1 B_2 \cdots B_{\omega(d_A)} P = AP = Q_1 Q_2 \cdots Q_{\omega(d_{AP})}$, $B_{m+1} \cdots B_{\omega(d_A)} P \cong Q_{m+1} \cdots Q_{\omega(d_{AP})}$. Hence by Lemma 4.58 $Q_{m+1} \cong B_{m+1}$. Thus, for $1 \le i < \omega(d_{AP})$, $Q_i \cong B_i$. Hence $\ell(Q_i) = \ell(B_i)$ for all $1 \le i < \omega(d_{AP})$, so $\ell(AP) = \sum_{i=1}^{\omega(d_{AP})} \ell(Q_i) = \sum_{i=1}^{\omega(d_{AP})-1} \ell(B_i) + \ell(Q_{\omega(d_{AP})})$.

Case 1: $\gcd(d_P, d_A) = 1$. Then $\omega(d_{AP}) = \omega(d_A) + 1$. Since $P \mid AP$, $Q_{\omega(d_{AP})} \mid AP$, and $d_{Q_{\omega(d_{AP})}} = d_P$, by Lemma 4.58 $Q_{\omega(d_{AP})} \cong P$, so $\ell(AP) = \sum_{i=1}^{\omega(d_{AP})-1} \ell(B_i) + \ell(Q_{\omega(d_{AP})}) = \sum_{i=1}^{\omega(d_A)} \ell(B_i) + \ell(P) = \ell(A) + 1 > \ell(A) - 3$.

Case 2: $\gcd(d_P, d_A) > 1$. Then $\omega(d_{AP}) = \omega(d_A)$, so since $Q_i \cong B_i$ for $1 \leq i < \omega(d_{AP}) = \omega(d_A)$, $B_{\omega(d_A)}P \cong Q_{\omega(d_A)}$. Meanwhile, $\ell(AP) = \sum_{i=1}^{\omega(d_{AP})-1} \ell(B_i) + \ell(Q_{\omega(d_{AP})}) = \sum_{i=1}^{\omega(d_A)-1} \ell(B_i) + \ell(Q_{\omega(d_A)}) = \ell(A) - \ell(B_{\omega(d_A)}) + \ell(Q_{\omega(d_A)})$

Case 2a: $B_{\omega(d_A)} \neq \begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix}$ for any odd b. Then $\ell(AP) = \ell(A) - \ell(B_{\omega(d_A)}) + \ell(Q_{\omega(d_A)}) \geq \ell(A) - 3 + 2 = \ell(A) - 1$ by Lemma 4.55. Hence $\ell(AP) \geq \ell(A) - 1 > \ell(A) - 2$.

Case 2b: $B_{\omega(d_A)} = \begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix}$ for some odd b. Then $\ell(AP) = \ell(A) - \ell(B_{\omega(d_A)}) + \ell(Q_{\omega(d_A)}) \geq \ell(A) - 4 + 2 = \ell(A) - 2$ by Lemma 4.55. Hence $\ell(AP) \geq \ell(A) - 2 > \ell(A) - 3$. Moreover, since $\begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix} P = B_{\omega(d_A)}P \cong Q_{\omega(d_A)}$ and $\omega(Q_{\omega(d_A)}) = 1$, d_P must be a power of 2. $\square$

Lemma 4.60. *Let $b \in \mathbb{Z}$ be odd. At least one of $3, 4 \in \mathcal{L}(\begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix} P)$ for any atom $P \in S$ such that $2 \mid \det P$.*

Proof. Let $d_P = 2^h$.

Case 1: $h = 1$. Then $P = \begin{pmatrix} 2 & \beta \\ 0 & 2 \end{pmatrix}$ for some $\beta \in \mathbb{Z}$, so

$\begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix} P = \begin{pmatrix} 2^6 & 2^5\beta + 2^4 b \\ 0 & 2^6 \end{pmatrix}$

$= \begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 4 & -1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 4 & 2\beta + b \\ 0 & 4 \end{pmatrix}$, so $3 \in \mathcal{L}(\begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix} P)$.

Case 2: $h \geq 2$. Then $P = \begin{pmatrix} 2^h & \beta \\ 0 & 2^h \end{pmatrix}$ for some $\beta \in \mathbb{Z}$, and β must be odd. Hence $\begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix} P = \begin{pmatrix} 2^{h+5} & 2^5\beta + 2^{h+3} b \\ 0 & 2^{h+5} \end{pmatrix}$

$= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 4 & -1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 2^h & \beta + 2^{h-2} b \\ 0 & 2^h \end{pmatrix}$, so

$4 \in \mathcal{L}(\begin{pmatrix} 2^5 & 2^3 b \\ 0 & 2^5 \end{pmatrix} P)$. $\square$

Theorem 4.61. $\Delta(S) = \{1, 2\}$

Proof. Let $A \in S^*$ and let $t = L(A)$. Then $A = A_1 A_2 \cdots A_t$ for some atoms $A_i \in S$. Let $\ell_i = \ell(A_1 A_2 \cdots A_i)$. Notice that $\ell_i - 2 \leq \ell_{i+1} \leq \ell_i + 1$ by Lemma 4.59, $\ell_1 = 1$ and $\ell_t = \ell(A)$. If we take the minimum length factorization of $A_1 A_2 \cdots A_i$

and append $A_{i+1}\cdots A_t$, we have a factorization of A with length $L_i = \ell_i + t - i$. Thus we have a map from $\{1, 2, 3, \ldots, t\}$ to $\{L(A), L(A)-1, \ldots, \ell(A)\}$. Since $\ell_i - 2 + t - i - 1 \leq \ell_{i+1} + t - i - 1 \leq \ell_i + t - i$, $L_i - 3 \leq L_{i+1} \leq L_i$, so there can be no gaps in the factorization lengths greater than 3. Hence $\Delta(A) \subseteq \{1, 2, 3\}$.

Case 1: $L_i - 2 \leq L_{i+1}$ for $1 \leq i \leq t$. Then $\Delta(A) \subseteq \{1, 2\}$.

Case 2: $L_m - 3 = L_{m+1}$ for some $1 \leq m \leq t$. Then $\ell_m - 2 = \ell_{m+1}$. By Lemma 4.59 there can be only one such m, and we have that: $A_{m-3}A_{m-2}A_{m-1}A_m = \begin{pmatrix} 2^5 & 2^3b \\ 0 & 2^5 \end{pmatrix}$ for some odd b, $2 \nmid \det(A_1A_2\cdots A_{m-4})$, and $2 \mid \det A_{m+1}$. Let $A_1A_2\cdots A_m = B_1B_2\cdots B_{\ell_m}$ where B_i are atoms in S. Since $\eta_2(B_1B_2\cdots B_{\ell_m}) = 10$, we can shuffle the B_i so that $B_1B_2\cdots B_{\ell_m} = BX$ for some $X \in S$ such that $d_X = 2^5$ and $\ell_m = \ell(B) + \ell(X)$. Since $A_1A_2\cdots A_m = BX = A_1A_2\cdots A_{m-4}\begin{pmatrix} 2^5 & 2^3b \\ 0 & 2^5 \end{pmatrix}$, by Lemma 4.58, $B \cong A_1A_2\cdots A_{m-4}$ and $X \cong \begin{pmatrix} 2^5 & 2^3b \\ 0 & 2^5 \end{pmatrix}$, so $\ell_m = \ell(B) + \ell(X) = \ell_{m-4} + 4$.

By Lemma 4.60, at least one of $3, 4 \in \mathcal{L}(\begin{pmatrix} 2^5 & 2^3b \\ 0 & 2^5 \end{pmatrix} A_{m+1})$. Let $c \in \{3, 4\}$. Since $A = A_1A_2\cdots A_t = A_1A_2\cdots A_{m-4}\begin{pmatrix} 2^5 & 2^3b \\ 0 & 2^5 \end{pmatrix} A_{m+1}\cdots A_t$, $\ell_{m-4} + c + t - (m+1) \in \mathcal{L}(A)$. Since $\ell_{m-4} + c + t - (m+1) = \ell_m + t - m - 5 + c = L_m - 5 + c \in \{L_m - 2, L_m - 1\}$, this factorization length lies in the gap between L_m and L_{m+1}, that is, $L_{m+1} = L_m - 3 < L_m - 5 + c < L_m$. Hence $3 \notin \Delta(A)$, so $\Delta(A) \subseteq \{1, 2\}$.

Consequently, $\Delta(A) \subseteq \{1, 2\}$ for any $A \in S^*$, so $\Delta(S) \subseteq \{1, 2\}$.

$\begin{pmatrix} 8 & -1 \\ 0 & 8 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 32 & 4 \\ 0 & 32 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 8 & 1 \\ 0 & 8 \end{pmatrix}$. Thus $1 \in \Delta(S)$.

Suppose $\begin{pmatrix} 81 & 0 \\ 0 & 81 \end{pmatrix} = C_1C_2C_3$. Without loss of generality, $d_{C_1} = 9$, so $\begin{pmatrix} 81 & 0 \\ 0 & 81 \end{pmatrix} = \begin{pmatrix} 9 & b_1 \\ 0 & 9 \end{pmatrix}\begin{pmatrix} 3 & b_2 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 3 & b_3 \\ 0 & 3 \end{pmatrix}$ $= \begin{pmatrix} 81 & 27b_3 + 27b_2 + 9b_1 \\ 0 & 81 \end{pmatrix}$. Since $27 \mid 0 = 27b_3 + 27b_2 + 9b_1$ and $27 \mid 27b_3 + 27b_2$, $27 \mid 9b_1$, so $3 \mid b_1$. Hence C_1 is reducible, so $3 \notin \mathcal{L}\begin{pmatrix} 81 & 0 \\ 0 & 81 \end{pmatrix}$. Meanwhile, $\begin{pmatrix} 9 & 1 \\ 0 & 9 \end{pmatrix}\begin{pmatrix} 9 & -1 \\ 0 & 9 \end{pmatrix} = \begin{pmatrix} 81 & 0 \\ 0 & 81 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}^4$. Thus $2 \in \Delta(S)$. $\square$

5 Rank One Matrices

Rank 1 matrices have been intensely studied from many different perspectives. For examples of such different approaches, see [23], [18] and [24]. In this section we study the factorization properties of several semigroups of $n \times n$ rank 1 matrices.

5.1 Semigroup of $n \times n$ Matrices with Rank 1 and Entries from $\mathbb{N}$

Let S be the semigroup of $n \times n$ matrices with rank 1 and entries from $\mathbb{N}$. Let $A \in S$. Recall that if a matrix A has rank 1, then there exist column vectors u, v such that $A = uv^T$. Note that S has no identity and no units.

Lemma 5.1. $\gcd(uv^T) = \gcd(u)\gcd(v)$.

Proof. Since every entry in uv^T is the product of an entry of u and an entry of v, $\gcd(u)\gcd(v)$ divides each entry of uv^T. Thus $\gcd(u)\gcd(v) \mid \gcd(uv^T)$. Since $\gcd(u) \mid \gcd(u)\gcd(v) \mid \gcd(uv^T)$, $\gcd(uv^T) = k\gcd(u)$ for some $k \in \mathbb{Z}$. Notice that $uv^T = [v_1 u \; v_2 u \; v_3 u \; \cdots \; v_n u]$, so $k\gcd(u) = \gcd(uv^T)$ divides each entry in $v_1 u$. By the maximality of $\gcd(u)$, for no prime $p \mid k$ can $p\gcd(u)$ divide all the entries of u. Hence $k \mid v_1$. Similarly, $k \mid v_2, v_3, \ldots, v_n$, so $k \mid \gcd(v)$. Thus $\gcd(uv^T) = k\gcd(u) \mid \gcd(v)\gcd(u)$, so $\gcd(uv^T) = \gcd(u)\gcd(v)$. □

Theorem 5.2. *A is an atom if and only if $\gcd(A) < n$. Moreover, S is bifurcus.*

Proof. Suppose A is reducible and write $A = A_1 A_2$. Since A_1, A_2 have rank 1, write $A_1 = u_1 v_1^T$ and $A_2 = u_2 v_2^T$ where u_i and v_i and column vectors of length n. Then $A = u_1 v_1^T u_2 v_2^T = u_1(v_1^T u_2)v_2^T = (v_1^T u_2)v_1^T u_2$. Since $v_1^T u_2 \in \mathbb{N}$ is a sum of n positive integers, $v_1^T u_2 \geq n$. Thus, since $v_1^T u_2 \mid \gcd(A)$, $\gcd(A) \geq v_1^T u_2 \geq n$. Now suppose $\gcd(A) \geq n$ and write $A = \gcd(A)B$. Notice that $\gcd(B) = 1$, so B is an atom. Since $\mathrm{rank}(B) = 1$, write $B = uv^T$ where u, v are column vectors. Since $\gcd(A) \geq n$, write $\gcd(A) = x^T y$ where $x = [(\gcd(A) - n + 1), 1, 1, \ldots, 1]^T$ and $y = [1, 1, 1, \ldots, 1]^T$ so that $A = \gcd(A)B = (x^T y)uv^T = (ux^T)(yv^T)$. Since $B = uv^T$, by Lemma 5.1 $\gcd(u) | \gcd(B) = 1$, so $\gcd(u) = 1$ and similarly $\gcd(v) = 1$. Hence by Lemma 5.1 $\gcd(ux^T) = \gcd(yv^T) = 1$, so ux^T and yv^T are atoms, and consequently $\ell(A) = 2$. □

Define $\Psi_n(g)$ to be the greatest integer k such that there exist $g_1, g_2, g_3, \ldots, g_k, r \in \mathbb{Z}$ such that $g = g_1 g_2 g_3 \cdots g_k r$ where $r < n \leq g_i$ for $1 \leq i \leq k$. Note that $\Psi_2(g) = r(g)$.

Theorem 5.3. *Calculating $\Psi_n(g)$ is NP-complete.*

Proof. Factor $g = p_1 p_2 \cdots p_t$ where $p_i \in \mathbb{P}$. $\Psi_n(g)$ is equal to the maximum number of disjoint subsets of $\{1, 2, 3, \ldots, t\}$ such that for each subset $\{a_1, a_2, \ldots, a_j\}$, $p_{a_1} p_{a_2} \cdots p_{a_j} \geq n$. Then $\log(p_{a_1}) + \log(p_{a_2}) + \cdots + \log(p_{a_j}) \geq \log(n)$. Hence finding $\Psi_n(g)$ is equivalent to solving a bin-covering problem, which is NP-complete. □

Theorem 5.4. $L(A) = \Psi_n(\gcd(A)) + 1$.

Proof. Assume A has some factorization of length t. Let $A = \prod_{i=1}^{t} A_i = \prod_{i=1}^{t} u_i v_i^T = u_1 \prod_{i=1}^{t-1} \langle v_i, u_{i+1}\rangle v_t^T = u_1 v_t^T \prod_{i=1}^{t-1} \langle v_i, u_{i+1}\rangle$. Since each $\langle v_i, u_{i+1}\rangle$ is a sum of n positive integers, each must be at least n. By Lemma 5.1,
$\gcd(A) = \gcd(u_1)\gcd(v_t)\prod_{i=1}^{t-1}\langle v_i, u_{i+1}\rangle$, so $\Psi_n(\gcd(A)) =$
$\Psi_n\left(\gcd(u_1)\gcd(v_t)\prod_{i=1}^{t-1}\langle v_i, u_{i+1}\rangle\right) \geq \Psi_n\left(\prod_{i=1}^{t-1}\langle v_i, u_{i+1}\rangle\right) \geq t-1$. Hence
$L(A) \leq \Psi_n(\gcd(A)) + 1$.

Now let $\Psi_n(\gcd(A)) = k$. Then $\gcd(A) = rg_1g_2g_3\cdots g_k$ for some $r, g_1, g_2, g_3, \ldots, g_k$ where $r < n \leq g_i$ for $1 \leq i \leq k$. Write $A = \gcd(A)B_k = rg_1g_2g_3\cdots g_kB_k$.

For any i, by Lemma 5.2 we can write $g_iB_i = B_{i-1}C_i$ since $\gcd(g_iB_i) \geq g_i \geq n$. Hence $rg_1g_2g_3\cdots g_{i-1}g_iB_i = rg_1g_2g_3\cdots g_{i-1}B_{i-1}C_i$. Thus $A = rg_1g_2g_3\cdots g_kB_k = (rB_0)C_1C_2C_3\cdots C_k$, so A has a factorization of length at least $k+1$ and consequently $L(A) \geq \Psi_n(\gcd(A)) + 1$. □

5.2 Semigroup of $n \times n$ matrices with Rank 1 and Entries from $m\mathbb{N}$.

Let $m \in \mathbb{N}$ and let S_m be the semigroup of $n \times n$ matrices with rank 1 and entries from $m\mathbb{N}$. Let $A \in S_m$.

Lemma 5.5. *If $m^2 \nmid \gcd(A)$, then A is an atom. If $A = m^2B$ where $B \in S_1$, then A is an atom in S_m if and only if B is an atom in S_1. Moreover, S_m is bifurcus.*

Proof. The result follows from Theorem 2.8. □

Lemma 5.6. $a - (b-1)\lceil \frac{a+1}{b} \rceil < \lfloor \frac{a+1}{b} \rfloor$.

Proof. Let $a+1 = bq+r$ where $r < b$. Then $a-(b-1)\lceil \frac{a+1}{b} \rceil = a-(b-1)(q+1) = a+1-bq-b+q = r-b+q < q = \lfloor \frac{a+1}{b} \rfloor$. □

Theorem 5.7. *Let $\gcd(A) = m^kq$ where $m \nmid q$.*
$L(A) = \max\{t : t \leq \Psi_n(m^{k-t}q) + 1\}$.

Proof. Let $A = A_1A_2\cdots A_t$ where $A_i \in S_m$ are atoms. Then $A = A_1A_2\cdots A_t = mB_1mB_2\cdots mB_t = m^tB_1B_2\cdots B_t$ where $B_i \in S_1$. Since $\Psi_n(\gcd(B_1B_2\cdots B_t)) + 1 = L(B_1B_2\cdots B_t) \geq t$ and $\gcd(B_1B_2\cdots B_t) = \frac{\gcd(A)}{m^t} = m^{k-t}q$, $t \leq \Psi_n(m^{k-t}q)+1$. Hence $L(A) \leq \max\{t : t \leq \Psi_n(m^{k-t}q)+1\}$.

Let $\tau = \max\{t : t \leq \Psi_n(m^{k-t}q) + 1\}$. Write $A = m^\tau B$ where $B \in S_1$. By Lemma 5.4, we can factor $B = B_1B_2\cdots B_\lambda$ where $\lambda = \Psi_n(m^{k-\tau}q) + 1$.

$\tau \leq \lambda$, so $A = m^\tau B = (mB_1)(mB_2)\cdots(mB_\tau B_{\tau+1}\cdots B_\lambda)$, so $L(A) \geq \tau = \max\{t : t \leq \Psi_n(m^{k-t}q) + 1\}$. □

Corollary 5.8. *Let* $\gcd(A) = m^k q$ *where* $m \nmid q$*. If* $k \leq \Psi_n(q) + 1$*, then* $L(A) = k$*.*

Proof. By Theorem 5.7, $L(A) = \max\{t : t \leq \Psi_n(m^{k-t}q) + 1\} = k$. □

Corollary 5.9. *Let* $\gcd(A) = m^k q$ *where* $m \nmid q$*. If* $k \geq \Psi_n(q) + 1$ *and* $m = p_1 p_2 \cdots p_s$ *where* $n \leq p_i \in \mathbb{P}$*, then* $L(A) = \left\lfloor \frac{r(m)k+\Psi_n(q)+1}{r(m)+1} \right\rfloor$*.*

Proof. Let $\mu = \left\lfloor \frac{r(m)k+\Psi_n(q)+1}{r(m)+1} \right\rfloor$. Since $\mu \leq \frac{r(m)k+\Psi_n(q)+1}{r(m)+1}$, $r(m)k + \Psi_n(q) + 1 - r(m)\mu \geq \mu$, so $\Psi_n(m^{k-\mu}q) + 1 = r(m)k - r(m)\mu + \Psi_n(q) + 1 \geq \mu$. Hence $\mu \in \{t : t \leq \Psi_n(m^{k-t}q) + 1\}$.

Let $\tau > \mu$, so $\tau \geq \mu + 1 \geq \left\lceil \frac{r(m)k+\Psi_n(q)+1}{r(m)+1} \right\rceil$. Then $\Psi_n(m^{k-\tau}q) + 1 = r(m)k+\Psi_n(q)+1-r(m)\tau \leq r(m)k+\Psi_n(q)+1-r(m) \left\lceil \frac{r(m)k+\Psi_n(q)+1}{r(m)+1} \right\rceil < \mu < \tau$ by Lemma 5.6, so $\tau \notin \{t : t \leq \Psi_n(m^{k-t}q) + 1\}$. Hence by Theorem 5.7, $L(A) = \max\{t : t \leq \Psi_n(m^{k-t}q) + 1\} = \mu$. □

5.3 Rank One Matrices Generated by a Set of Vectors

For $n > 1$, let $T \subseteq \mathbb{Z}^n$ and let S be the semigroup of rank 1 matrices generated by T. That is, $S = \{au^T : a \in \mathbb{Z}^n \text{ and } u \in T\}$. Observe that by the matrix transpose the properties of any such S also hold for $S' = \{ua^T : a \in \mathbb{Z}^n$ and $u \in T\}$. Let A be an arbitrary element of S. Note that S has no identity and no units. Define $\gcd(u)$ to be the greatest common divisor of the entries of u. Let $G = \{\gcd(u) : u \in T^\bullet\}$.

Theorem 5.10. *If* $1 \in G$*, then* S *has no atoms.*

Proof. Since $\gcd(u) = 1$ for some $u \in T$, there exists an $x \in \mathbb{Z}^n$ such that $u^T x = 1$. Factor $A = au^T = (u^T x)au^T = a(u^T x)u^T = (au^T)(xu^T)$. □

Because of Theorem 5.10, we shall assume $1 \notin G$. Notice that if $(au^T)^2 = au^T$, then we must have $u^T a = 1$. Hence $\gcd(u) = 1$. Thus our assumption that $1 \notin G$ implies that S has no idempotents.

Lemma 5.11. *Let* $a, b, u, v \in \mathbb{Z}^n$*. If* $au^T = bv^T \neq 0$*, then* $u = rv$ *and* $b = ra$ *for some rational number* r*.*

Proof. Since $au^T = bv^T$, $a_i u_j = b_i v_j$ for all i, j. Since $au^T = bv^T \neq 0$, there exist s and t such that $a_s, b_s, u_t, v_t \neq 0$. Hence $\frac{a_s}{b_s} = \frac{v_t}{u_t}$. If $u_k, v_k \neq 0$, then $\frac{v_k}{u_k} = \frac{a_s}{b_s}$, hence $u_k = \frac{b_s}{a_s} v_k$. Suppose $u_k = 0$. If $v_k \neq 0$, then $a_s u_k \neq b_s v_k$. Hence $v_k = 0$. Thus $u_k = \frac{b_s}{a_s} v_k$. Letting $r = \frac{b_s}{a_s}$, we obtain $u = rv$. Hence $bv^T = au^T = a(rv)^T = (ra)v^T$. Thus we have $(b - ra)v^T = 0$. Since $v \neq 0$, we must have $b = ra$. □

Corollary 5.12. *For nonzero* $a, u \in \mathbb{Z}^n$ *there exist only finitely many* $b, v \in \mathbb{Z}^n$ *such that* $au^T = bv^T$*.*

Proof. Let $a, u \in \mathbb{Z}^n$. By Lemma 5.11, if $au^T = bv^T$, then $b = ra$ and $v = \frac{1}{r}u$ for some rational r. Hence the number of such b and v is equal to the number of r such that $ra, \frac{1}{r}u \in \mathbb{Z}^n$. Let $r = \frac{m}{n}$, where $(m, n) = 1$. If $\frac{m}{n}a \in \mathbb{Z}^n$, then we must have $n \mid \gcd(a)$. Hence $|n| \leq \gcd(a)$. Similarly, we have that $|m| \leq \gcd(u)$. Thus there exist only finitely many such r. $\square$

For $A \in S^\bullet$, define $R(A) = \{(a, u) \in \mathbb{Z}^n \times T : A = au^T\}$. Note that by Corollary 5.12, $|R(A)|$ is finite.

For any $H \subseteq \mathbb{Z} \setminus \{-1, 0, 1\}$ and $q \in \mathbb{Z} \setminus \{0\}$ define $\Theta_H(q)$ to be the maximum t such that there exist $h_1, \ldots, h_t \in H$ and $r \in \mathbb{Z} \setminus H$ such that $q = rh_1 \cdots h_t$. Observe that $\Theta_H(q)$ is finite for each H and q. Also notice that if $H = \{x : x \geq n\}$, then $\Theta_H(q) = \Psi_n(q)$.

Theorem 5.13. *For $A \in S^\bullet$, $L(A) = \max_{(a,u) \in R(A)} \{\Theta_G(\gcd(a))\} + 1$.*

Proof. Suppose $A = A_1 A_2 \cdots A_t$. Then $A = A_1 A_2 \cdots A_t =$
$a_1 u_1^T a_2 u_2^T \cdots a_t u_t^T = (\prod_{i=1}^{t-1} u_i^T a_{i+1}) a_1 u_t^T$. Let $b = (\prod_{i=1}^{t-1} u_i^T a_{i+1}) a_1$. Since
$\prod_{i=1}^{t-1} gcd(u_i) \mid gcd(b)$, we have $t - 1 \leq \Theta_G(\gcd(b))$. Hence
$L(A) \leq \max_{(a,u) \in R(A)} \{\Theta_G(\gcd(a))\} + 1$.
Let $\theta = \max_{(a,u) \in R(A)} \{\Theta_G(\gcd(a))\}$. Then there exist $g_1, g_2 \ldots, g_\theta \in G$ and $s \in \mathbb{N} \setminus G$ such that $g_1 g_2 \cdots g_\theta s = \gcd(a)$. Let $a = g_1 g_2 \cdots g_\theta a'$. There exist $u_i \in T$ and $x_i \in \mathbb{Z}^n$ such that $u_i^T x_i = g_i$ for $1 \leq i \leq \theta$. Then $a = (\prod_{i=1}^{\theta} u_i^T x_i) a' u^T =$
$a' (\prod_{i=2}^{\theta} u_i^T x_i) u^T = (a' u_2^T)(\prod_{i=2}^{\theta-1} x_i u_{i+1}^T)(x_\theta u^T)$. Hence $L(A) \geq \theta + 1$. $\square$

Notice that Theorem 5.13 provides a classification of the atoms of S. Suppose $A = au^T$ with $\Theta_G(\gcd(a)) = 0$. If for each r such that $ra \in \mathbb{Z}^n$ and $\frac{1}{r}u \in T$ $\Theta_G(\gcd(ra)) = 0$, then A is an atom. In particular, this is satisfied when $|r| = 1$ for each such r.

Lemma 5.14. *Let s be a nonzero integer and let $a \in \mathbb{Z}^n$. If $\gcd(a) \mid s$, then there exists some $x \in \mathbb{Z}^n$ such that $a^T x = s$ and $\gcd(x) = 1$.*

Proof. Let $a^T x = s$. If $|s| = 1$, then $\gcd(x) = 1$. Suppose $|s| > 1$. Let $p_1, p_2, \ldots, p_t$ be the distinct prime factors of s. Let $P = \prod p_i$. Suppose $p_i \mid \gcd(x)$. By the maximality of $\gcd(a)$ there is some a_j such that $p_i \nmid \frac{a_j}{\gcd(a)}$. Let $k \neq j$. Replace x_j with $x_j + \frac{a_k}{\gcd(a)} \frac{P}{p_i}$ and replace x_k with $x_k - \frac{a_j}{\gcd(a)} \frac{P}{p_i}$. Hence we can obtain some x such that $p_i \nmid \gcd(x)$. Suppose there exists some nonunit q such that $q \mid \gcd(x)$. If p is some rational prime that divides q, then $p \mid \gcd(a)$. Hence $p \mid p_l$ for some l. Thus $p_l \mid \gcd(x)$, a contradiction. Hence $\gcd(x) = 1$. $\square$

Theorem 5.15. *S is bifurcus.*

Proof. Suppose $A = a_0 u_0^T$ is reducible. Let $\{\frac{m_i}{n_i}\}$ be the set of rational numbers such that $\frac{m_i}{n_i} a_0 \in \mathbb{Z}^n$ and $\frac{n_i}{m_i} u_0 \in T$ with $(m_i, n_i) = 1$. Let m_t be the integer of greatest magnitude of such $\frac{m_i}{n_i}$ that satisfy $\Theta_G(\frac{m_i}{n_i} \gcd(a_0)) > 0$. Suppose there are multiple j for which $|m_j| = |m_t|$. Choose the j that minimizes $|n_j|$. Let $a = \frac{m_t}{n_t} a_0$ and $u = \frac{n_t}{m_t} u_0$. Let $a = \gcd(a)a'$. We claim that there exist $v \in T$ and $x \in \mathbb{Z}^n$ such that $a'v^T$ and xu^T are atoms and $v^T x = \gcd(a)$.
Existence of v: There must be some $w \in T$ such that $\gcd(w) \mid \gcd(a)$. Let q be the integer of greatest magnitude such that $\frac{1}{q} w \in T$. If q and $-q$ both satisfy this, choose the positive of the two. Let $v = \frac{1}{q} w$. We claim that $a'v$ is an atom. If $\frac{m}{n} a' \in \mathbb{Z}^n$ and $\frac{n}{m} v \in T$ where $(m,n) = 1$, then $|n| = 1$. If $|m| \neq 1$, since $\frac{1}{m} v \in T$ we have that $\frac{1}{mq} w \in T$, which contradicts the maximality of $|q|$. Thus we have that $|\frac{m}{n}| = 1$. Hence $a'v$ is an atom.
Existence of x: By Lemma 5.14, there exists some $x \in \mathbb{Z}^n$ such that $\gcd(x) = 1$ and $v^T x = \gcd(a)$. We claim that xu^T is an atom. If $\frac{m}{n} x \in \mathbb{Z}^n$ and $\frac{n}{m} u \in T$ where $(m,n) = 1$, then $|n| = 1$. If $|m| \neq 1$, since $\frac{1}{m} u \in T$ we have that $\frac{n_t}{m m_t} u_0 \in T$, which contradicts the maximality of $|m_t|$ unless $m \mid n_t$. In this case, we have that $\frac{\frac{n_t}{m}}{m_t} u_0 \in T$. But this contradicts the minimality of $|n_t|$. Thus we have that $|\frac{m}{n}| = 1$. Hence xu^T is an atom. □

An example of such semigroups is the semigroup of $n \times n$ matrices with $n-1$ rows of zeros and a row of entries divisible by k. This would be generated by $T\mathbb{Z}^n$ where $T = \{ke_1, ke_2, \ldots, ke_n\}$. Matrices with rows of zeros have been studied in different contexts. [26], [19] and [5] are examples of such contexts.

Next, we study a semigroup of matrices with $n-1$ rows of zeros that is not generated by any subset of $\mathbb{Z}^n$.

5.4 Rows of Zero

Let S be the semigroup of $n \times n$ matrices with $n-1$ rows of zeros and a row of entries in $\mathbb{Z}^*$. Let $S^\bullet$ be S without the zero matrix. Let $A \in S^\bullet$. Notice that $S^\bullet$ does not have the identity matrix. Thus $S^\bullet$ does not have units.

Theorem 5.16. *A is an atom of $S^\bullet$ if and only if* $\gcd(A) = 1$ *or A has a prime entry. Furthermore, $S^\bullet$ is bifurcus.*

Proof. Let $a_1, a_2, \ldots, a_n$ be the nonzero entries of A. If $A = BC$, where $B, C \in S^\bullet$, then there exists $b \in B$ such that $a_1, a_2, \ldots, a_n = bpk$ where $pk \in C$, p is prime and $k \in \mathbb{Z}$. Thus $a_1, a_2, \ldots, a_n$ are composite and $\gcd(A) \geq b > 1$. For the converse, assume $\gcd(A) \geq 1$ and A does not have a prime entry.
Case 1: $\gcd(A)$ is an entry of A.
Let $a_1, a_2, \ldots, a_n$ be the nonzero entries of A. WLOG, assume that $a_1 = \gcd(A)$. So $a_1 = p_1 p_2 \ldots p_n$. Then

$$A = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ p_1p_2\cdots p_n & a_2 & \cdots & a_n \\ 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ \frac{a_1}{p_1} & 2 & \cdots & 2 \\ 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \begin{pmatrix} p_1 & \frac{p_1a_2}{a_1} & \cdots & \frac{p_1a_n}{a_1} \\ 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}.$$

Case 2: $\gcd(A)$ is not an entry of A.
Let $g = \gcd(A)$. Then

$$A = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ gx_1 & \cdots & gx_n \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ g & 2 & \cdots & 2 \\ 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 & \cdots & x_n \\ 0 & \cdots & 0 \\ \vdots & \vdots & \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}. \qquad \square$$

Theorem 5.17. $L(A) = \begin{cases} r(\gcd(A)), & \textit{if } gcd(A) \textit{ is an entry of } A; \\ r(\gcd(A)) + 1, & \textit{if } gcd(A) \textit{ is not an entry of } A. \end{cases}$

Proof. Case 1: $\gcd(A)$ is an entry of A.
Let $a_1, a_2, \ldots, a_n$ be the nonzero entries of A. WLOG, assume that $a_1 = \gcd(A)$. So $a_1 = p_1p_2 \ldots p_r$ where p_i is prime; $a_1|a_2, a_3 \ldots a_n$. Then A can be factored into $r(a_1) = r$ atoms:

$$A = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ p_1p_2\cdots p_r & a_2 & \cdots & a_n \\ 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} =$$

$$\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ p_1 & \cdots & p_1 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} p_2 & \cdots & p_2 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \cdots \begin{pmatrix} p_r & \frac{p_r a_2}{a_1} & \cdots & \frac{p_r a_n}{a_1} \\ 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}.$$

Assume to the contrary that $L(A) = t > r$. Then a_1 is the product of t entries. But the maximum factorization length of a_1 is $r(a_1) = r$. Contradiction. Since the maximum factorization length of a_1 is its factorization into primes, $L(A) = r(\gcd(A))$.

Case 2: $\gcd(A)$ is not an entry of A.

Let $\gcd(A) = p_1 p_2 \cdots p_r$ where p_i is prime. Then A can be factored into $r+1$ atoms:

$$A = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ p_1 p_2 \cdots p_r x_1 & p_1 p_2 \cdots p_r x_2 & \cdots & p_1 p_2 \cdots p_r x_n \\ 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ p_1 & \cdots & p_1 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} p_2 & \cdots & p_2 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \cdots \begin{pmatrix} p_r & \cdots & p_r \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 & \cdots & x_n \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

where $x_1, x_2, \ldots, x_n > 1$ and $\gcd(x_1, x_2, \ldots, x_n) = 1$.

Assume to the contrary that $L(A) = t > r+1$. Then each entry of A is the product of $t+1$ entries. As shown in case 1, $L(\gcd(A)) = r$. Then the last matrix is reducible. Contradiction. $\square$

5.5 The Semiring of Single-Valued $n \times n$ Matrices

A single-valued matrix is a matrix with all entries equal. We will consider semirings of single-valued matrices with entries from $\mathbb{N}$, $\mathbb{N}_0$, and $\mathbb{Z}$; regardless of which of these rings is chosen, the factorization properties are identical. Unlike most others within this paper, these semirings were inspired by the previous work of Bernard Jacobson in his paper *Matrix Number Theory: An Example of Nonunique Factorization*[14]. Jacobson focused on the specific case of 2×2 matrices. As the title suggests, his motivation was the nonuniqueness of factorization in the 2×2 single-valued matrices. As such, Jacobson discovered the atoms of the semiring but did not investigate the invariants that we are concerned with. Also, Jacobson produced motivation to extend the single-valued semiring to the $n \times n$ case, but did not complete this extension.

Taking Jacobson's paper as a starting point, this section completes the analysis and extends his idea to the $n \times n$ case. Throughout this section, define the semiring S_n to be the commutative semiring of single-valued $n \times n$ matrices with entries from either $\mathbb{N}$, $\mathbb{N}_0$, or $\mathbb{Z}$, where $n > 1$. S_n possesses a useful multiplicative property. Recall the notation $[a]$ for the $n \times n$ matrix with all entries equal to a (notation adopted from Jacobson) [14]. For $[a], [b] \in S_n$, $[a][b] = [nab]$. Although appearing a bit obscure, it is a fairly simple computation. Each entry of $[a][b]$ is the sum of n terms all equal to ab, resulting in $n(ab)$. This property of the product furnishes the factorization properties that follow.

Note that S_n has no identity and no units.

Lemma 5.18. *$[a] \in S_n^\bullet$ is an atom if and only if a is not divisible by n.*

Proof. Since any reducible $[s][t] = [nst]$ must have entries divisible by n, any element [a] where a is not divisible by n must be an atom. Conversely, if a is divisible by n, it is easily factored as $[a] = [nst] = [s][t]$. $\square$

Recall that the notation $\eta_n(a) = w$ denotes w as the greatest power of n that divides a.

Theorem 5.19. *If $[a] \in S_n^\bullet$ with $\eta_n(a) = w$, then the maximum factorization length $L([a]) = w + 1$. If $n = p^k$ for some prime $p \in \mathbb{P}$ with $\eta_p(a) = m$, then $\ell([a]) = \left\lceil \frac{m+k}{2k-1} \right\rceil$ and $\rho(S_{p^k}) = \frac{2k-1}{k}$. Otherwise, $S_n^\bullet$ is bifurcus. Further, if $n \in \mathbb{P}$, then $\Delta(S_n^\bullet) = \emptyset$; otherwise, $\Delta(S_n^\bullet) = \{1\}$.*

Proof. Let $w = \eta_n(a)$. Let $[a] = [a_1][a_2] \cdots [a_t]$ where $[a_i] \in S_n^\bullet$. Then $[a] = [a_1][a_2] \cdots [a_t] = [n^{t-1} a_1 a_2 \cdots a_t]$, so $\eta_n(a) \geq t - 1$. Hence $L([a]) \leq \eta_n(a) + 1$. Meanwhile, factor $[a] = [1]^w [\frac{a}{n^w}]$. Hence $L([a]) \geq w + 1 = \eta_n(a) + 1$.

Assume $n = p^k$. For any $[a] \in S_n$, $a = p^m y$ where y is not divisible by p. Assume [a] has atomic factorization length d. Then $[p^m y] = [p^{m_1} y_1][p^{m_2} y_2] \cdots [p^{m_d} y_d]$ where $y = \prod_{i=1}^{d} y_i$ and $m = \sum_{i=1}^{d} m_i + k(d-1)$. Each $[p^{m_i} y_i]$ is an atom, thus by Lemma 5.18, $m_i \in [0, k-1]$. Note that depending on the values of the m_i, $\sum_{i=1}^{d} m_i$ can take any integer value between 0 and $d(k-1)$. Introduce integer c, such that $\frac{\sum_{i=1}^{d} m_i}{k} = \frac{d(k-1)-c}{k}$ is an integer. Then $d = \frac{m-d(k-1)+c}{k} + 1$, so $d = \frac{m+c+k}{2k-1} \geq \left\lceil \frac{m+k}{2k-1} \right\rceil$. Hence $\ell([a]) = \left\lceil \frac{m+k}{2k-1} \right\rceil$. Observe that for any $[p^m y] \in S_{p^k}$, $\rho([(p^m y]) = \left(\left\lfloor \frac{m}{k} \right\rfloor + 1\right) / \left(\left\lceil \frac{m+k}{2k-1} \right\rceil\right) \leq \left(\frac{m}{k} + 1\right) / \left(\frac{m+k}{2k-1}\right) = \frac{2k-1}{k}$ This elasticity is achieved, since $[p^{k(2k-2)}] = [1]^{2k-1} = [p^{k-1}]^k$. That $\Delta(S_{p^k}) = \{1\}$ follows from the fact that $\sum_{i=1}^{d} m_i$ can take any integer value between 0 and $n(k-1)$, when $k \geq 2$. However, when $k = 1$, then $[a] = [p^m r] \in S_p$, $l([a]) = m + 1 = L([a])$ and $\Delta(S_p) = \emptyset$.

Table 4: Notation for Bistochastic Matrices

Symbol	Definition
$\min(A)$	the minimum entry of the matrix A
$\varsigma(A)$	the row sum and column sum of the bistochastic matrix A
$c(A)$	the column difference of the 2×2 bistochastic matrix A
$\bar{(}u, v\bar{)}$	the 2×2 bistochastic matrix A with $\varsigma(A) = u$ and $c(A) = v$

Now assume $n = st$ where $\gcd(s,t) = 1$. For an arbitrary $[a] \in S^\bullet$, let $w = \eta_n(a)$. Then $[a] = [n^w y]$ where $st = n \nmid y$, so at least one of $s, t \nmid y$. Without loss of generality, $s \nmid y$. Write $[a] = [n^w y] = [s^w t^w y] = [s^{w-1}][t^{w-1} y]$. Thus $\ell([a]) = 2$, so $S^\bullet$ is bifurcus. $\square$

6 Bistochastic Matrices

The familiar definition of a doubly stochastic matrix is a square matrix of non-negative real numbers, each of whose rows and columns sum to 1. For the purposes of this section, we will consider a bistochastic matrix to be a matrix with integral entries and a characteristic row and column sum. Note that any matrix with rational entries and row and column sum 1 may be converted into this form by multiplying by an integer to clear all denominators; the multiplier is then the row and column sum of the matrix.

Bistochastic matrices are important in probability and combinatorics. The most well-known result concerning doubly stochastic matrices is the Birkhoff-von Neumann Theorem, which states that the set of doubly stochastic matrices is the convex closure of the set of permutation matrices, and we will show that this result also holds for integral bistochastics. The problem of finding multiplicative atoms among the bistochastics has been previously studied[20][27]; we offer some results for the semigroup of such matrices with positive entries. The problem of approximating an arbitrary matrix as a bistochastic matrix has also been studied[25].

6.1 Semigroup of Bistochastic Matrices with the Operation of $+$

6.1.1 Entries from $\mathbb{N}$

Let S be the semigroup of bistochastic $n \times n$ matrices with entries from $\mathbb{N}$ and the operation of $+$. Let A be an arbitrary element of S. Note that S has no identity and no units.

Theorem 6.1. $L(A) = \min(A)$

Proof. Let $A = A_1 + A_2 + \cdots + A_t$. Since each A_i must contribute at least 1 to each entry of A, $t \leq \min(A)$. Thus $L(A) \leq \min(A)$.

Let $m = \min(A) - 1$. Then $A = m[1] + (A - [m])$. Hence $L(A) \geq m + 1 = \min(A)$. $\square$

Corollary 6.2. *A is an atom if and only if* $\min(A) = 1$.

Theorem 6.3. *S is bifurcus.*

Proof. Suppose that $A \in S$ is reducible. Then by Corollary 6.2 $\min(A) \geq 2$. Pick i, j such that $A_{ij} = \min(A)$. Let P be some permutation matrix such that $P_{ij} = 1$. Let $B = [1] + (\min(A) - 2)P$. Then $A = B + (A - B)$. Since $\min(B) = \min(A - B) = 1$, by Corollary 6.2 $\ell(A) = 2$. $\square$

6.1.2 Entries from $\mathbb{N}_0$

Let S be the semigroup of bistochastic $n \times n$ matrices with entries from $\mathbb{N}_0$ and the operation of $+$. Let A be an arbitrary element of S. Define $\varsigma(A)$ to be the row sum and column sum of A.

Lemma 6.4. *The only unit in S is the zero matrix.*

Proof. Let U be a unit in S. Then $U + (-U) = [0]$ for some $-U \in S$. Thus $\varsigma(U) + \varsigma(-U) = \varsigma([0]) = 0$, so $\varsigma(U) = -\varsigma(-U)$. Since all entries are nonnegative, $\varsigma(U) \geq 0$ and $\varsigma(-U) \geq 0$, so $\varsigma(U) = \varsigma(-U) = 0$, and therefore $U = [0]$. $\square$

Lemma 6.5. *For any $A \in S$, $A = A' + P$ where $A' \in S$ and P is a permutation matrix.*

Proof. Suppose $A \in S$ is a nonzero matrix permutation equivalent to the following matrix

$$B = \left(\begin{array}{ccc|ccc|c}
a_{1,1} & \cdots & a_{1,k} & & & & r_1 \\
\vdots & D_{k\times k} & \vdots & & C & & \vdots \\
a_{k,1} & \cdots & a_{k,k} & & & & r_k \\
\hline
 & & & a_{k+1,k+1} & \cdots & a_{k+1,t} & r_{k+1} \\
 & & & \vdots & E_{t-k\times t-k} & \vdots & \vdots \\
 & & & a_{t,k+1} & \cdots & a_{t,t} & r_t \\
\hline
c_1 & \cdots & c_k & c_{k+1} & \cdots & c_t & [0]_{n-t\times n-t}
\end{array}\right)$$

where $a_{i,i} > 0$, $c_i \in M_{n-t,1}(\mathbb{N})$, $r_i \in M_{1,n-t}(\mathbb{N})$, k is the number of r_i which contain only zeros, and $t \leq n$ is maximal. Since k of the r_i are zero, without loss of generality $r_1 = r_2 = \cdots = r_k = [0]_{1\times n-t}$. Define $R_{x,y}$ to be the permutation matrix that exchanges row x with row y.

Toward a contradiction, suppose $t < n$.

If there exists some j such that c_j and r_j each contain a positive entry, pick s such that the sth row of c_j is positive; then $R_{j,t+s}B$ contains at least $t + 1$ positive entries along the main diagonal, which contradicts the maximality of t. Hence $c_{k+1} = c_{k+2} = \cdots c_t = [0]_{n-t\times 1}$.

Suppose that $C = [0]_{k\times t-k}$. Then $\sum A_{t-k\times t-k} = (t-k)\varsigma(A)$, so $r_{k+1} = \cdots = r_t = [0]_{1\times n-t}$. But this would imply B has a column of zeros, so C cannot be $[0]_{k\times t-k}$. That is, there exists some entry $C_{u,v} > 0$. Then $R_{u,n}R_{u,v+k}B$ has at least $t+1$ positive entries along the main diagonal, which contradicts the maximality of t. Hence $t = n$.

Consequently, A is permutation equivalent to some $B = I + B'$ where $B' \in S$. Hence, for some permutation matrices Q_1, Q_2, $A = Q_1BQ_2 = Q_1(I+B')Q_2 = Q_1Q_2 + Q_1B'Q_2$. Thus there exists some permutation matrix $P = Q_1Q_2$ such that $A = A' + P$ where $A' = Q_1B'Q_2 \in S$. $\square$

Theorem 6.6. *A is an atom in S if and only if A is a permutation matrix.*

Proof. Suppose A is reducible. Then $A = B + C$ where $\varsigma(B), \varsigma(C) \geq 1$, so $\varsigma(A) \geq 2$. Hence if A is a permutation matrix, then A is an atom.
Suppose $\varsigma(A) \geq 2$. By Lemma 6.5, $A = A' + P$ where $A' \in S$ and P is a permuation matrix. Since $\varsigma(A') = \varsigma(A) - 1 \geq 1$, A' is not a unit, so A is reducible. $\square$

Corollary 6.7. *S is half-factorial and $L(A) = \ell(A) = \varsigma(A)$.*

Proof. Since $\varsigma(A_1 + A_2) = \varsigma(A_1) + \varsigma(A_2)$ and $\varsigma(P) = 1$ for all atoms $P \in S$, by Theorem 2.1 $L(A) = \ell(A) = \varsigma(A)$. $\square$

6.2 Semigroup of Bistochastic Matrices with the Operation of $\times$ and Entries from $\mathbb{N}$ and Odd Determinant

Let S be the semigroup of bistochastic 2×2 matrices with entries from $\mathbb{N}$ and odd determinant. Let $A = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ be an arbitrary element of S. Define $c(A) = a - b$. Note that S has no identity and no units.

Set $u = \varsigma(A) = a + b$ and $v = c(A) = a - b$, so that $a = \frac{u+v}{2}$ and $b = \frac{u-v}{2}$. Thus we can represent A as the ordered pair $\overline{(u,v)}$. Since $a, b \in \mathbb{N}$, $u \geq |v|+2$ and $u \equiv v \pmod 2$. Since $\det A = a^2 - b^2 = (a+b)(a-b) = uv$ and $\det A$ is odd, u and v must be odd. Since $\begin{pmatrix} \frac{u+v}{2} & \frac{u-v}{2} \\ \frac{u-v}{2} & \frac{u+v}{2} \end{pmatrix} \begin{pmatrix} \frac{x+y}{2} & \frac{x-y}{2} \\ \frac{x-y}{2} & \frac{x+y}{2} \end{pmatrix} = \begin{pmatrix} \frac{ux+vy}{2} & \frac{ux-vy}{2} \\ \frac{ux-vy}{2} & \frac{ux+vy}{2} \end{pmatrix}$, $\overline{(u,v)}\overline{(x,y)} = \overline{(ux,vy)}$.

Lemma 6.8. *$\overline{(u,v)}$ is reducible if and only if there exist $x, y \in \mathbb{Z}$ such that $xy = uv$ and $0 \leq x - y < u - v$.*

Proof. Suppose there exist such $x, y \in \mathbb{Z}$. Suppose that $x \geq u$; then $y = \frac{u}{x}v < v$, so $x - y \geq u - v$, $\rightarrow\leftarrow$. Hence $x < u$. Since $uv = xy$ and $x < u$, $g = \gcd(u, y) > 1$. Since $x < u$, there must be some $\alpha < g$ such that $x = \alpha\frac{u}{g}$. Then $y = \frac{uv}{x} = \frac{g}{\alpha}v$. Since $0 < \alpha < g$ and $x \geq y$, $\frac{x}{\alpha} > \frac{y}{g}$. Hence we can factor $\overline{(u,v)} = \overline{(\frac{x}{\alpha}, \frac{y}{g})}\overline{(g,\alpha)}$.

Now suppose that $\overline{(u,v)}$ is reducible. Then $\overline{(u,v)} = \overline{(\mu,\nu)}\overline{(\frac{u}{\mu}, \frac{v}{\nu})}$ where $\mu > \nu$ and $\frac{u}{\mu} > \frac{v}{\nu}$. Note that $v = \nu\frac{v}{\nu} < \nu\frac{u}{\mu} < \mu\frac{u}{\mu} = u$ and $v = \nu\frac{v}{\nu} < \mu\frac{v}{\nu} < \mu\frac{u}{\mu} = u$. $\square$

Lemma 6.9. *If* $\det A = k^2$ *for some* $k \in \mathbb{Z}$*, then* A *is reducible. If* $d \in \mathbb{Z}$ *is not a perfect square, then there exists exactly one atom* $P_d \in S$ *such that* $\det P_d = d$*.*

Proof. Let $A = \bar{(}u, v\bar{)}$ such that $uv = \det A = k^2$. Since $k \cdot k = uv$ and $v < k \leq k < u$, by Lemma 6.8 A is reducible.
Let $d \in \mathbb{Z}$ such that d is not a perfect square. Let $P_d = \bar{(}u, v\bar{)}$ such that $uv = d$ and $u - v$ is minimal. By the minimality of $u - v$, there are no $x, y \in \mathbb{Z}$ such that $xy = uv$ and $0 < x - y < u - v$, and since d is not a perfect square, there are no $x, y \in \mathbb{Z}$ such that $xy = uv$ and $0 \leq x - y < u - v$. Hence by Lemma 6.8 P_d is an atom. Meanwhile, for any $B = \bar{(}\varsigma(B), c(B)\bar{)} \in S$ such that $\det B = d$ and $B \neq P_d$, by the minimality of $u - v$, $0 < u - v < \varsigma(B) - c(B)$ and $uv = d = \varsigma(B)c(B)$, so by Lemma 6.8 B is reducible. □

Define $\Xi(u, v)$ to be the maximum t such that there exist $u_1, u_2, \ldots, u_t$, $v_1, v_2, \ldots, v_t$ such that $u = \prod_{i=1}^{t} u_i$ and $v = \prod_{i=1}^{t} v_i$ and $u_i > v_i$. Note that $\Xi(u, v) \leq \Psi_2(u)$.

Theorem 6.10. $L(A) = \Xi(\varsigma(A), c(A))$.

Proof. Suppose $A = A_1 A_2 \cdots A_t$. $\varsigma(A) = \varsigma(A_1)\varsigma(A_2)\cdots\varsigma(A_t)$ and $c(A) = c(A_1)c(A_2)\cdots c(A_t)$. Since all entries are positive, $c(A_i) < \varsigma(A_i)$. Hence $t \leq \Xi(\varsigma(A), c(A))$, so $L(A) \leq \Xi(\varsigma(A), c(A))$.
Let $k = \Xi(\varsigma(A), c(A))$. Then there exist $\varsigma_1, \varsigma_2, \ldots, \varsigma_k, c_1, c_2, \ldots, c_k$ where $\prod_{i=1}^{t} \varsigma_i = \varsigma(A)$ and $\prod_{i=1}^{t} c_i = c$ and $\varsigma_i > v_i$. Since $\varsigma(A)$ and $c(A)$ are odd, all ς_i and c_i must be odd, so $\varsigma_i + c_i$ and $\varsigma_i - c_i$ are even. Let $B_i = \begin{pmatrix} \frac{\varsigma_i + c_i}{2} & \frac{\varsigma_i - c_i}{2} \\ \frac{\varsigma_i - c_i}{2} & \frac{\varsigma_i + c_i}{2} \end{pmatrix}$. Then $A = B_1 B_2 \cdots B_k$, so $L(A) \geq k = \Xi(\varsigma(A), c(A))$. □

6.3 Semigroup of Bistochastic Matrices with the Operation of $\times$ and Entries from $\mathbb{N}$ and Any Determinant

Let S be the semigroup of bistochastic 2×2 matrices with entries from $\mathbb{N}$ and any determinant. Let $A = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ be an arbitrary element of S. Define $c(A) = a - b$. Note that S has no identity and no units.

Conjecture 6.11. *Let* $d \in \mathbb{Z}$*. If* d *is a perfect square and* $16 \nmid d$*, then* S *has no atoms with determinant* d*. If* d *is a perfect square and* $16 \mid d$*, then there exists exactly one atom* $P_d \in S$ *with determinant* $\det P_d$*. If* d *is not a perfect square and* $16 \nmid d$*, then there exists exactly one atom* $P_d \in S$ *with determinant* $\det P_d$*. Finally, if* d *is not a perfect square and* $16 \mid d$*, then there exist exactly two atoms* $P_d, Q_d \in S$ *with determinant* $\det P_d = \det Q_d = d$*.*

References

[1] Jeff Amos, S. T. Chapman, Natalie Hine, and João Paixão. Sets of lengths do not characterize numerical monoids. *Integers*, 7:A50, 8, 2007.

[2] Jên Chung Ch'uan and Wai Fong Chuan. Factorizations in a semigroup of integral matrices. *Linear and Multilinear Algebra*, 18(3):213–223, 1985.

[3] Jên Chung Ch'üan and Wai Fong Chuan. Factorability of positive-integral matrices of prime determinants. *Bull. Inst. Math. Acad. Sinica*, 14(1):11–20, 1986.

[4] P. M. Cohn. Noncommutative unique factorization domains. *Trans. Amer. Math. Soc.*, 109:313–331, 1963.

[5] Craig M. Cordes and D. P. Roselle. Generalized frieze patterns. *Duke Math. J.*, 39:637–648, 1972.

[6] Dennis R. Estes. Factorization in hereditary orders. *Linear Algebra Appl.*, 157:161–164, 1991.

[7] M. A. Frumkin. Fast computations with frobenius matrices. In *Computational processes and systems, No. 5 (Russian)*, pages 302–311. "Nauka", Moscow, 1987.

[8] Alfred Geroldinger and Franz Halter-Koch. *Non-unique factorizations*, volume 278 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.

[9] Gene H. Golub and Charles F. Van Loan. *Matrix computations*. Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, Baltimore, MD, third edition, 1996.

[10] Gracinda M. S. Gomes, Helena Sezinando, and Jean-Eric Pin. Presentations of the Schützenberger product of n groups. *Comm. Algebra*, 34(4):1213–1235, 2006.

[11] Gebhard Greiter. Nonunique factorization in subsemigroups of semigroups with unique prime factorization. *Amer. Math. Monthly*, 87(6):473–474, 1980.

[12] Vesa Halava and Tero Harju. On Markov's undecidability theorem for integer matrices. *Semigroup Forum*, 75(1):173–180, 2007.

[13] Glyn Harman. Approximation of real matrices by integral matrices. *J. Number Theory*, 34(1):63–81, 1990.

[14] Bernard Jacobson. Classroom Notes: Matrix Number Theory: An Example of Nonunique Factorization. *Amer. Math. Monthly*, 72(4):399–402, 1965.

[15] Bernard Jacobson and Robert J. Wisner. Matrix number theory. I. Factorization of 2×2 unimodular matrices. *Publ. Math. Debrecen*, 13:67–72, 1966.

[16] Mark Kambites. On the Krohn-Rhodes complexity of semigroups of upper triangular matrices. *Internat. J. Algebra Comput.*, 17(1):187–201, 2007.

[17] Melven Krom. An unsolvable problem with products of matrices. *Math. Systems Theory*, 14(4):335–337, 1981.

[18] Shao-wu Liu and Guo-dong Zhang. Maps preserving rank 1 matrices over fields. *Heilongjiang Daxue Ziran Kexue Xuebao*, 23(1):138–140, 2006.

[19] E. Ja. Melamud. Realization of positive matrix-valued functions according to Darlington. Polynomial realization in the case of degeneration. *Izv. Akad. Nauk Armyan. SSR Ser. Mat.*, 14(4):237–250, 314, 1979.

[20] G. Picci, J. M. van den Hof, and J. H. van Schuppen. Primes in several classes of the positive matrices. *Linear Algebra Appl.*, 277(1-3):149–185, 1998.

[21] Richard Shell and Ernest Hall. *Handbook of Industrial Automation.* CRC Press, 2000.

[22] 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):57–64, 2006.

[23] Seok-Zun Song. Separability of distinct boolean rank-1 matrices. *J. Appl. Math. Comput.*, 18(1-2):197–204, 2005.

[24] Seok-Zun Song and Kyung-Tae Kang. Rank and perimeter preserver of rank-1 matrices over max algebra. *Discuss. Math. Gen. Algebra Appl.*, 23(2):125–137, 2003.

[25] Pawoumodom L. Takouda. Un problème d'approximation matricielle: quelle est la matrice bistochastique la plus proche d'une matrice donnée? *RAIRO Oper. Res.*, 39(1):35–54, 2005.

[26] P. Vermes. Certain classes of series to series transformation matrices. *Amer. J. Math.*, 72:615–620, 1950.

[27] Ji Tuan Zhou and Lin Zhang Lu. Primes in the doubly stochastic circulant matrices of order 3 or 4. *Acta Math. Sinica (Chin. Ser.)*, 50(3):661–668, 2007.