BULLETIN OF THE
INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
Volume 14, Number 1, March 1986

FACTORABILITY OF POSITIVE-INTEGRAL MATRICES OF PRIME DETERMINANTS

BY

JEN-CHUNG CHUAN (全任重)
AND
WAI-FONG CHUAN (郭蕙芳)

1. **Introduction.** The main purpose of this paper is to investigate the factorability of the elements in the multiplicative semigroup $\tilde{\mathcal{S}}$ of all two-by-two matrices with positive integral entries and of positive determinants. If one thinks of positive integers as one-by-one matrices, the semigroup $\tilde{\mathcal{S}}$ under consideration would be a noncommutative analogue of the positive integers.

Let $\mathcal{S}_n$ denote the set of those elements of $\tilde{\mathcal{S}}$ which have determinant n. $\mathcal{S}_1$, also denoted by $\mathcal{S}$, is a subsemigroup of $\tilde{\mathcal{S}}$ which we have studied in [1]. It has been shown that an element of $\mathcal{S}$ is prime if and only if its minimum entry is equal to one (see also Theorem 2.3 of this paper). We shall show in Theorem 2.3 that for any prime in $\tilde{\mathcal{S}}$, its minimum entry must not exceed its determinant. Those primes in $\tilde{\mathcal{S}}$ whose minimum entries are equal to their determinants will be listed in Theorem 3.1. For a prime number n, the combination of Theorems 2.4, 3.1 and 3.6 will yield all the primes of determinant n.

All the results mentioned above depend upon Theorem 2.5 and Corollary 2.6 which provide a simple criterion for an element of $\tilde{\mathcal{S}}$ to possess a left or right divisor of determinant one. However, we should also note that in order to solve the whole problem of identifying the primes of $\tilde{\mathcal{S}}$, these theorems are apparantly not enough because there are composites which do not have any divisor

Received by the editors April 4, 1985 and in revised form September 3, 1985.

of determinant one. Example: $\begin{bmatrix}7 & 4\\ 6 & 7\end{bmatrix}=\begin{bmatrix}2 & 1\\ 1 & 3\end{bmatrix}\begin{bmatrix}3 & 1\\ 1 & 2\end{bmatrix}$.

As in [1], an element of $\tilde{\mathcal{S}}$ is said to be *composite* if it is the product of two elements of $\tilde{\mathcal{S}}$, it is *prime* if otherwise. An element B is said to be a *left* (respectively, *right*) *divisor* of an element A if there is an element C such that $A=BC$ (respectively, $A=CB$). Let ρ and τ denote the mapping of $\tilde{\mathcal{S}}$ onto itself given by

$$\rho(A)=\begin{bmatrix}a_{22} & a_{21}\\ a_{12} & a_{11}\end{bmatrix}$$

$$\tau(A)=\begin{bmatrix}a_{11} & a_{21}\\ a_{12} & a_{22}\end{bmatrix}$$

for $A=(a_{ij})$ in $\tilde{\mathcal{S}}$. For every real number x, let $[x]$ denote the largest integer which does not exceed the number x.

2. **Divisors of determinant one.** In this section we shall characterize those elements of $\tilde{\mathcal{S}}$ which possess left or right divisors of determinant one (Theorem 2.5). This result will be used, in the next section, to locate all the primes of $\tilde{\mathcal{S}}$ which have prime determinants.

We begin with the following theorem whose proof is almost identical with that of Theorem 2.1 of [1]. We include a proof for completeness.

THEOREM 2.1. *Let $A=(a_{ij})$ be in $\tilde{\mathcal{S}}$. Then A is composite if and only if there exist positive integers b_{ij}, $i, j=1, 2$, such that $b_{11}b_{22}-b_{12}b_{21}>0$ and the integers*

$$b_{22}a_{11}-b_{12}a_{21}, \qquad b_{22}a_{12}-b_{12}a_{22}$$

$$b_{11}a_{21}-b_{21}a_{11}, \qquad b_{11}a_{22}-b_{21}a_{12}$$

are all positive and are divisible by $b_{11}b_{22}-b_{12}b_{21}$.

Proof. Suppose that $A=BC$ where B and C are in $\tilde{\mathcal{S}}$. Let b_{ij}, $i, j=1, 2$, be the entries of B. Then these integers have the required properties because the entries of C are positive integers.

Conversely, suppose that the positive integers b_{ij}, $i, j = 1, 2$, have the given properties and let $B = (b_{ij})$ and let C be defined in the obvious way. Then clearly B and C are in $\tilde{\mathcal{S}}$ and $A = BC$.

COROLLARY 2.2. *Let $A = (a_{ij})$ be in $\tilde{\mathcal{S}}$ and let $B = (b_{ij})$ be in $\mathcal{S}$. Then B is a left divisor of A if and only if*

$$\frac{b_{21}}{b_{11}} < \frac{a_{21}}{a_{11}} < \frac{a_{22}}{a_{12}} < \frac{b_{22}}{b_{12}} .$$

The following theorem is a generalization of Theorem 2.2 of [1] which implies that the primes of $\mathcal{S}$ are precisely those which have at least one entry equal to one.

THEOREM 2.3. *Let us suppose that n is a positive integer, that A is in $\mathcal{S}_n$, and that each entry of A is greater than n. Then A has a left divisor of the form $\begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}$ or $\begin{bmatrix} k+1 & k \\ 1 & 1 \end{bmatrix}$, where k is a positive integer; hence A is composite.*

To prove this theorem we need the following lemma which will also be employed in the proof of Theorem 3.1.

LEMMA 2.4. *Let n be a positive integer and let $A = (a_{ij})$ be in $\mathcal{S}_n$. Suppose that $a_{12} > n$ and that a_{11} is less than but does not divide a_{21}. Then A has a left divisor of the form $\begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}$, where k is a positive integer.*

Proof. Let $k = [a_{21}/a_{11}]$. Then

$$(k+1)\, a_{11} \geq a_{21} + 1 = a_{11}\, a_{22}/a_{12} + (1 - n/a_{12}) > a_{11}\, a_{22}/a_{12}$$

so that $a_{22}/a_{12} < k + 1$ and the result follows from Corollary 2.2.

Proof of Theorem 2.3. From the assumption it is clear that neither a_{21}/a_{11} nor a_{22}/a_{12} is an integer. We look at the cases (i) $a_{21} > a_{11}$ and (ii) $a_{21} < a_{11}$ separately.

If (i) holds, then the result follows immediately from Lemma 2.4. Now suppose (ii) holds. Multiplying the left side of the equality $a_{11}\, a_{22} = a_{12}\, a_{21} + n$ by a_{21} and the right side by a_{11}, we have

$$a_{11}a_{21}a_{22} < a_{11}a_{21}a_{12} + a_{11}n$$

and therefore $a_{21}(a_{22} - a_{12}) < n$. Since $a_{21} > n$ and $a_{22} \neq a_{12}$, we see that $a_{22} < a_{12}$. It then follows from Lemma 2.4 that ρA, and hence A, has a left divisor of the desired form. This completes the proof.

From the identities

$$\begin{bmatrix} 1 & m \\ k & km+1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}\begin{bmatrix} 1 & m-1 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} m & 1 \\ km-1 & k \end{bmatrix} = \begin{cases} \begin{bmatrix} 1 & 1 \\ k-1 & k \end{bmatrix}\begin{bmatrix} 1 & 0 \\ m-1 & 1 \end{bmatrix} & \text{if } k > 1, \\ \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ m-2 & 1 \end{bmatrix} & \text{if } k = 1, \end{cases}$$

we can write each prime A of $\mathfrak{S}$ as a product BC, where B is of the form $\begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}$ or $\begin{bmatrix} k+1 & k \\ 1 & 1 \end{bmatrix}$ and C is of the form $\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix}$ with some nonnegative integer m and positive integer k. Therefore, if an element of $\tilde{\mathfrak{S}}$ has a left divisor in $\mathfrak{S}$ then it has a left divisor of the form $\begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}$ or $\begin{bmatrix} k+1 & k \\ 1 & 1 \end{bmatrix}$. Similarly one can show that if an element of $\tilde{\mathfrak{S}}$ has a right divisor of determinant one, then it has a right divisor of the form $\begin{bmatrix} 1 & k \\ 1 & k+1 \end{bmatrix}$ or $\begin{bmatrix} k+1 & 1 \\ k & 1 \end{bmatrix}$.

This observation together with Corollary 2.2 give the following simple criterion for an element of $\tilde{\mathfrak{S}}$ to have left or right divisors of determinant one.

THEOREM 2.5. *Let $A = (a_{ij})$ be in $\tilde{\mathfrak{S}}$. Then*

(i) *A has a left divisor of determinant one if and only if one of the following conditions hold.*

(a) *There exists a positive integer k such that*

$$k < \frac{a_{21}}{a_{11}} < \frac{a_{22}}{a_{12}} < k+1.$$

(b) *There exists a positive integer k such that*

$$k < \frac{a_{12}}{a_{22}} < \frac{a_{11}}{a_{21}} < k+1.$$

(ii) *A has a right divisor of determinant one if and only if one of the following conditions holds.*

(c) *There exists a positive integer k such that*

$$k < \frac{a_{12}}{a_{11}} < \frac{a_{22}}{a_{21}} < k+1.$$

(d) *There exists a positive integer k such that*

$$k < \frac{a_{21}}{a_{22}} < \frac{a_{11}}{a_{12}} < k+1.$$

An immediate consequence of Theorem 2.5 is the following corollary which enables us to tell whether a given element of prime determinant is prime or not.

COROLLARY 2.6. *Suppose that $A = (a_{ij})$ has prime determinant. Then A is composite if and only if at least one of the conditions* (a)–(d) *of Theorem* 2.5 *holds.*

3. **Primes of $\tilde{\mathcal{S}}$.** From Theorem 2.3, we know explicitly all the primes of $\tilde{\mathcal{S}}$ of determinant one. In this section we attempt to determine the primes of $\tilde{\mathcal{S}}$ of determinant n. We have already shown in Theorem 2.3 that each such prime has at least one entry less than or equal to n. Those primes which have minimum entries n will be given explicitly in Theorem 3.1. In the case n is a prime number, we shall also be able to write down, using Theorem 3.6, all the primes of determinant n.

For each positive integer k, let $\mathcal{N}_k$ denote the set of all elements in $\tilde{\mathcal{S}}$ having minimum entry k.

For the rest of this section, we fix a positive integer n and let $A = (a_{ij})$ be of determinant n.

THEOREM 3.1. *Suppose that A is in $\mathcal{N}_n$ and let*

$$\mathcal{W}_n = \left\{\begin{bmatrix} n & nk \\ nm & nkm+1 \end{bmatrix} : k \geq 1,\ m \geq 1\right\} \cup \left\{\begin{bmatrix} nk & n \\ nkm-1 & nm \end{bmatrix} : km > 1\right\}.$$

Then A is prime if and only if A is in $\mathcal{W}_n \cup \rho(\mathcal{W}_n)$.

Proof. We first show that $A=\begin{bmatrix} n & nk \\ nm & nkm+1 \end{bmatrix}$, where $k \geq 1$, $m \geq 1$, is prime by way of contradiction. Suppose that $A=BC$ where $B=(b_{ij})$ and $C=(c_{ij})$ are in $\tilde{\mathcal{S}}$. Then according to Theorem 2.1, the determinant d of B divides both $b_{11}(nkm+1)-b_{21}nk$ and $b_{11}nm-b_{21}n$. Thus d divides b_{11}. But then

$$b_{11}c_{11}=b_{11}(b_{22}n-b_{12}nm)/d=(b_{11}/d)\,n(b_{22}-b_{12}m)\geq n,$$

a contradiction. Consequently A is prime.

Similarly we prove that each $\begin{bmatrix} nk & n \\ nkm-1 & nm \end{bmatrix}$ where $km>1$ is prime. Hence $\mathcal{W}_n \cup \rho(\mathcal{W}_n)$ consists of primes.

Now suppose A does not belong to $\mathcal{W}_n \cup \rho(\mathcal{W}_n)$. We are to show that A is composite.

Case (i) $a_{11}=n$: Since A is not in $\mathcal{W}_n$, a_{11} does not divide both a_{12} and a_{21}.

If a_{11} does not divide a_{21} and $a_{12}>n$, then Lemma 2.4 implies that A is composite. If a_{11} does not divide a_{21} and $a_{12}=n$, then $a_{22}=a_{21}+1<n(k+1)+1$ where $k=[a_{21}/a_{11}]$. But since A is not in $\mathcal{W}_n$, $a_{22}<n(k+1)$ so that

$$k<\frac{a_{21}}{a_{11}}<\frac{a_{22}}{a_{12}}<k+1.$$

Hence A is composite, according to Theorem 2.5.

Now if a_{11} does not divide a_{12}, it follows from what we have just shown and the fact $\tau(\mathcal{W}_n \cup \rho(\mathcal{W}_n))=\mathcal{W}_n \cup \rho\mathcal{W}_n$ that $\tau(A)$, and hence A, is composite.

Case (ii) $a_{12}=n$: The proof is similar to that of case (i).

Case (iii) $a_{21}=n$ or $a_{22}=n$: The conclusion follows from (i) and (ii) by considering $\rho(A)$ or $\tau(A)$.

This completes the proof.

EXAMPLE 3.2. From Corollary 2.6 and Theorem 3.1 we are now able to list all the primes of $\tilde{\mathcal{S}}$ of determinant 2:

B is such a prime if and only if B or $\rho(B)$ is of one of the following forms:

$$\begin{bmatrix} 1 & k \\ m & km+2 \end{bmatrix}, \quad \text{where } k \geq 1, \ m \geq 1,$$

$$\begin{bmatrix} k & 1 \\ km-2 & m \end{bmatrix}, \quad \text{where } km > 2,$$

$$\begin{bmatrix} 2 & 2k \\ 2m & 2km+1 \end{bmatrix}, \quad \text{where } k \geq 1, \ m \geq 1,$$

$$\begin{bmatrix} 2k & 2 \\ 2km-1 & 2m \end{bmatrix}, \quad \text{where } km > 1.$$

From now on, we assume further that n is a prime number ≥ 3 and consider the following two cases:

(1) (i) $2 \leq a_{11} < n$ and each entry of A is greater than or equal to a_{11}.

(2) (ii) $2 \leq a_{12} < n$ and each entry of A is greater than or equal to a_{12}.

Note that if (1) holds, then neither a_{12} nor a_{21} is divisible by a_{11} so that we can write

$$a_{12} = s\,a_{11} + u \quad \text{and} \quad a_{21} = t\,a_{11} + v \tag{3}$$

where s, t, u, v are positive integers and u, v are less than a_{11}.

Similarly if (2) holds, we write

$$a_{11} = q\,a_{12} + w \quad \text{and} \quad a_{22} = r\,a_{12} + z \tag{4}$$

where q, r, w, z are positive integers and w, z are less than a_{12}.

THEOREM 3.3. *Suppose that* (1) *holds and* u, v *are given by* (3). *Then* A *is prime if and only if* $a_{12} \leq n/(a_{11} - v)$ *and* $a_{21} \leq n/(a_{11} - u)$.

Proof. We observe that condition (1) implies that $a_{12} > a_{11}$ and $a_{21} > a_{11}$. Thus, by virtue of Corollary 2.6,

A is composite

$\iff$ condition (a) or condition (c) of Theorem 2.5 holds

$\iff \dfrac{a_{22}}{a_{21}} < s+1$ or $\dfrac{a_{22}}{a_{12}} < t+1$.

The result now follows by noting that

$$\frac{a_{22}}{a_{21}} < s+1 \Longleftrightarrow \frac{n+a_{12}a_{21}}{a_{11}a_{21}} < s+1 \Longleftrightarrow \frac{n}{a_{11}-u} < a_{21},$$

and

$$\frac{a_{22}}{a_{12}} < t+1 \Longleftrightarrow \frac{n}{a_{11}-v} < a_{12}.$$

A similar result is true when (2) holds:

THEOREM 3.4. *Suppose that* (2) *holds and* w, z *are given by* (4). *Then* A *is prime if and only if* $a_{22} \leq n/w$ *and* $a_{11} \leq n/z$.

REMARK 3.5. Suppose that (1) holds. Then Theorem 3.3 implies, in particular, the following results which are sometimes useful.

(i) A is composite if $a_{12} > n$ or $a_{21} > n$.

(ii) A is prime if both a_{12} and a_{21} are less than or equal to n and a_{11} divides both $a_{12}+1$ and $a_{21}+1$.

Similar results are true when (2) holds.

Now, for any prime number $n \geq 3$ and for $2 \leq k < n$, let

$$\sum\nolimits_1^*(k) = \{(u, v) : u, v \text{ are positive integers less than } k \text{ and } k \text{ divides } n+uv\}$$

and for (u, v) in $\sum_1(k)$, let $s(k; u, v)$, $t(k; u, v)$ be the smallest positive integers such that

$$ks(k; u, v) + u > \frac{n}{k-v}$$

and

$$kt(k; u, v) + v > \frac{n}{k-u},$$

that is,

$$s(k; u, v) = \max\left\{\left[\frac{n-u(k-v)}{k(k-v)}\right]+1, 1\right\}$$

and

$$t(k; u, v) = \max\left\{\left[\frac{n-v(k-u)}{k(k-u)}\right]+1, 1\right\}.$$

Let $\mathcal{U}_k$ be the set of all elements of $\tilde{\mathcal{S}}$ that are of the form

$$\begin{bmatrix} k & ks+u \\ kt+v & kst+ut+sv+\dfrac{n+uv}{k} \end{bmatrix},$$

where (u, v) is in $\sum_1(k)$, $1 \le s < s(k; u, v)$ and $1 \le t < t(k; u, v)$.

Similarly, let

$$\sum\nolimits_2(k) = \{(w, z) : w, z \text{ are positive integers less than } k \text{ and } k \text{ divides } n - wz\},$$

and for (w, z) in $\sum_2(k)$, let $q(k; w, z)$, $r(k; w, z)$ be the smallest positive integers such that

$$kq(k; w, z) + w > n/z$$

and

$$kr(k; w, z) + z > n/w,$$

that is,

$$q(k; w, z) = \max\left\{\left[\frac{n-wz}{kz}\right] + 1, 1\right\}$$

$$r(k; w, z) = \max\left\{\left[\frac{n-wz}{kw}\right] + 1, 1\right\}.$$

Let $\mathcal{V}_k$ be the set of all elements of $\tilde{\mathcal{S}}$ that are of the form

$$\begin{bmatrix} kq+w & k \\ kqr+rw+qz-\dfrac{n-wz}{k} & kr+z \end{bmatrix},$$

where (w, z) in $\sum_2(k)$, $1 \le q < q(k; w, z)$, $1 \le r < r(k; w, z)$ and $kqr + rw + qz \ge (n - wz)/k + k$.

Theorems 3.3 and 3.4 now lead to the following theorem.

THEOREM 3.6. *Suppose $n \ge 3$ is a prime and $2 \le k < n$. Let $\mathcal{U}_k$ and $\mathcal{V}_k$ be defined as above. Then the set $(\mathcal{U}_k \cup \mathcal{V}_k) \cup \rho(\mathcal{U}_k \cup \mathcal{V}_k)$ consists of all the primes which have determinant n and minimum entry k.*

We conclude this section with the following two examples.

EXAMPLE 3.7. For any prime $n \ge 3$, the set of all primes which belong to $\mathcal{N}_2$ and have determinant n is given by $(\mathcal{U}_2 \cup \mathcal{V}_2) \cup \rho(\mathcal{U}_2 \cup \mathcal{V}_2)$ where

$$\mathcal{U}_2 = \left\{ \begin{bmatrix} 2 & k \\ m & \dfrac{km+n}{2} \end{bmatrix} : k \text{ and } m \text{ are odd integers greater than one and less than or equal to } n \right\},$$

and

$$\mathcal{V}_2 = \left\{ \begin{bmatrix} k & 2 \\ \dfrac{km-n}{2} & m \end{bmatrix} : k \text{ and } m \text{ are odd integers greater than one and less than or equal to } n, \text{ and } km \geq n+4 \right\}.$$

EXAMPLE 3.8. A is a prime of determinant 3 if and only if A or ρA is of one of the following forms:

$$\begin{bmatrix} 1 & k \\ m & km+3 \end{bmatrix}, \quad \text{where } k \geq 1, \ m \geq 1,$$

$$\begin{bmatrix} k & 1 \\ km-3 & m \end{bmatrix}, \quad \text{where } km > 3,$$

$$\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}, \quad \begin{bmatrix} 3 & 2 \\ 3 & 3 \end{bmatrix},$$

$$\begin{bmatrix} 3 & 3k \\ 3m & 3km+1 \end{bmatrix}, \quad \text{where } k \geq 1, \ m \geq 1,$$

$$\begin{bmatrix} 3k & 3 \\ 3km-1 & 3m \end{bmatrix}, \quad \text{where } km \geq 2.$$

REFERENCES

1. J. Chuan and W. Chuan, *Factorizations in a semigroup of integral matrices*, to appear in Linear and Multilinear Algebra.

2. J. M. Howie, *An introduction to semigroup theory*, Academic Press, 1976.

J. C. Chuan
Department of Mathematics
National Tsing Hua University
Hsinchu, Taiwan 300, R. O. C.

W. F. Chuan
Department of Mathematics
Chung Yuan Christian University
Chung Li, Taiwan 320, R. O. C.