

# SEMIGROUPS OF NON-NEGATIVE INTEGRAL MATRICES

by CRAIG M. CORDES

(Received 18 October, 1972; revised 7 May, 1973)

In [1], Pall proved an interesting result on a certain class of  $2 \times 2$  integral matrices. He showed that the semigroup of  $2 \times 2$  matrices of determinant 1 and non-negative entries contains exactly 2 primes  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ , and every other non-unit is expressible uniquely as products of these primes. Before formally stating this result, we need some notation. Let  $G_n$  denote the semigroup of  $n \times n$  matrices with determinant 1 and nonnegative integral entries,  $I_n$  the  $n \times n$  identity matrix,  $E_{ij}^{(n)}$  the  $n \times n$  matrix with a 1 as its  $(i, j)$  element and zeros elsewhere, and let  $F_{ij}^{(n)} = I_n + E_{ij}^{(n)}$ . When the dimension is clear, we shall drop the superscripts.

**THEOREM 1.** (Pall)  $G_2$  is a free semigroup with generators  $F_{12}, F_{21}$ .

The question now is what can be said about  $G_n, n \geq 3$ . The first major change we encounter is that, for  $n \geq 3$ , units must be considered.

**THEOREM 2.** The units of  $G_n$ , i.e., all  $A \in G_n$  such that  $A^{-1} \in G_n$ , consist of  $I$  and all matrices obtained from  $I$  by permuting columns (rows) an even number of times.

*Proof.* Let  $A = (a_{ij}) \in G_n$  be a unit. Denote the cofactors of  $A$  by  $C_{ij}$  so that  $A^{-1} = (C_{ij})^T$  and

$$\sum_{i=1}^n a_{ij} C_{ik} = \delta_{jk} = \sum_{i=1}^n a_{ji} C_{ki},$$

where  $\delta_{jk}$  is the Kronecker  $\delta$ . Since  $A^{-1} \in G_n, C_{ij} \geq 0$  for all  $i, j$ . Hence, for each  $j$ , there is an  $i_j$  such that  $a_{i_j j} = C_{i_j j} = 1$  but for all  $i \neq i_j, a_{ij} = 0$ . The  $j$ th column has one element equal to 1 and its other elements zero. The  $n$  columns must be different, for  $\det A \neq 0$ . Furthermore this permutation of the columns of  $I$  must be even since  $\det A \neq -1$ .

So, in particular, the only unit for  $G_2$  is  $I_2$  and the units for  $G_3$  are  $I_3$ ,

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

It would be nice if every element of  $G_n$  was the product of units and the  $F_{ij}$ 's. For  $n \geq 3$ , this is not the case. In fact just finding all of the "primes" other than the  $F_{ij}$  appears formidable even for  $n = 3$ . The remainder of this paper deals with this problem.

Let  $A \in G_3$ . If  $A \neq I, F_{ij}$ , then, if  $A$  is prime (i.e., does not factor into two non-units), no row (column) can be greater than or equal component-wise to another row (column). This is true, since any matrix  $A$  that does not satisfy this condition has an  $F_{ij}$  factor. We abbreviate the above row condition to r.c. (c.c. for columns and r.c.c. when both hold) and call any

matrix satisfying the condition an r.c. (c.c., r.c.c.) matrix. It is easily seen that, if  $A = BC$  satisfies the r.c.c., then  $B$  and  $C$  satisfy the r.c. and c.c. respectively.

**THEOREM 3.** *Let  $A = (a_{ij}) \in G_3$  satisfy the r.c.c. If some  $a_{ij} = 0$ , then  $A$  is prime.*

*Proof.* Suppose that  $A$  is not a prime. Then  $A = BC$ , where  $B, C$  are non-units. Since  $a_{ij} = 0$ , the  $i$ th row of  $B$  or the  $j$ th column of  $C$  contains two zeros (and hence a 1 also). If the two zeros occur in a  $B$  row we may assume that the row number is the same as the column number of the 1. This is because we can adjust the rows of  $B$  and columns of  $C$  by  $BC = BUU^{-1}C$ , where  $U$  is a unit. Consider the case when

$$B = \begin{bmatrix} 1 & 0 & 0 \\ a & c & d \\ b & e & f \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ b & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & c & d \\ 0 & e & f \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ b & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & c & d \\ 0 & e & f \end{bmatrix}.$$

If either  $a$  or  $b$  is not 0,  $B$  has a left factor that does not satisfy r.c. and hence neither does  $A$ . So  $a = b = 0$ . But then  $\begin{bmatrix} c & d \\ e & f \end{bmatrix}$  does not satisfy r.c. unless it is  $I$ . This all shows that  $B$  is not of the form

$$\begin{bmatrix} 1 & 0 & 0 \\ a & c & d \\ b & e & f \end{bmatrix}.$$

In exactly the same manner we see that  $B$  is not of either of the forms

$$\begin{bmatrix} * & * & * \\ 0 & 1 & 0 \\ * & * & * \end{bmatrix}, \begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{bmatrix}.$$

The use of a similar column argument for  $C$  shows that  $C$  cannot contain a column with two zeros. Therefore, it is impossible to factor the r.c.c. matrix  $A$ .

The following theorem gives another class of primes.

**THEOREM 4.** *Any r.c.c. matrix in  $G_3$  with 1 and 2 in the same row or column is prime.*

*Proof.* First consider  $A = \begin{bmatrix} 1 & * & * \\ 2 & * & * \\ * & * & * \end{bmatrix}$  and suppose that  $A = BC$ . By the proof of

Theorem 3, we can assume that  $B$  is r.c.,  $C$  is c.c. and no row of  $B$  or column of  $C$  contains two zeros. Also, by using the units as before, we can assume the smallest nonzero element in the first row of  $B$  is in the first column.

If  $c_{11} = 0$ , where  $C = (c_{ij})$ , then, by the above assumptions,  $b_{11} = 1$ ,  $\{b_{12}, b_{13}\} = \{1, 0\}$ , where  $B = (b_{ij})$ . But it is easy to check that  $B$  cannot have determinant 1 now. So  $c_{11} = 1$ . Just as a row of  $B$  cannot contain two ones and a zero, neither can a column of  $C$ . However,  $a_{11} = 1$  implies there is at least one zero in the first row of  $B$  and first column of  $C$ . Suppose that  $b_{13} = c_{21} = 0$ . Then  $b_{23} \neq 0$ , because otherwise  $B = I$  or would not be r.c. Hence

$b_{21} = c_{21} = 0$  and  $c_{31} = 2, b_{23} = 1$ . Now  $B = \begin{bmatrix} 1 & a & 0 \\ 0 & b & 1 \\ c & d & e \end{bmatrix}$  and  $\det B = 1 = be - d + ac$ . For  $B$  to be r.c.,  $c, e \geq 1$  and  $a, b > d$ . But these inequalities contradict  $d + 1 = be + ac$ . The case  $b_{12} = c_{31} = 0$  is similar. The proof for  $A$  when  $a_{11} = 1, a_{21} = 2$  is now completed.

When  $a_{11} = 2, a_{21} = 1$ , the same argument can be applied to  $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} A = BC$ , where now  $\det B = -1$ . Any other combination of 1, 2 in the same row or column can be transformed to one of the above cases by using the units or by matrix transposes.

It is interesting to note that, if 2 is replaced by  $m \geq 3$  in Theorem 4, the result is not true in general. Counterexamples are supplied by the products

$$A_m \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 2 & 1 & 0 \end{bmatrix}, \text{ where } A_m = \begin{bmatrix} 1 & 3 & 0 \\ 1 & 2 & k \\ 2 & 1 & 5k-1 \end{bmatrix}, \begin{bmatrix} 1 & 2k-2 & 0 \\ 2 & 1 & k-1 \\ 1 & 2k-6 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 3 & 0 \\ 2 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 0 \\ 2 & 1 & 2 \\ 4 & 0 & 5 \end{bmatrix}$$

and  $m = 2k + 1, 2k (k \geq 4), 4, 6$ , respectively. These also show the existence of nonprime r.c.c. matrices.

There are only two primes in  $G_2$ , but an infinite number in  $G_3$ , for every matrix of the form  $\begin{bmatrix} 1 & 0 & c+d \\ 1 & a+b & 0 \\ 1 & a & d \end{bmatrix}$ , where  $a, b, c, d \geq 1$  with  $ad - bc = 1$ , is prime by Theorem 3.

The uniqueness of prime factorization in  $G_2$  fails in  $G_3$  also. For instance,

$$\begin{bmatrix} 1 & 2 & 4 \\ 2 & 1 & 0 \\ 0 & 2 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 6 & 3 \\ 4 & 1 & 2 \\ 3 & 2 & 2 \end{bmatrix}$$

are primes by Theorem 4, but

$$\begin{bmatrix} 1 & 2 & 4 \\ 2 & 1 & 0 \\ 0 & 2 & 5 \end{bmatrix}^2 = F_{12} F_{31} \begin{bmatrix} 1 & 6 & 3 \\ 4 & 1 & 2 \\ 3 & 2 & 2 \end{bmatrix} F_{23} F_{12} F_{23}.$$

Finding all the primes in  $G_3$  seems to be an unlikely occurrence. The following is a complete list (up to units) of those provided by the above theorem, based on the largest element  $k (k \leq 4)$  in the matrix.

$k = 1 : F_{ij}$ .

$k = 2 : \text{none.}$

$$k = 3 : \begin{bmatrix} 1 & 1 & 1 \\ 2 & 0 & 1 \\ 0 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 2 \\ 2 & 1 & 0 \\ 0 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 2 \\ 2 & 0 & 1 \\ 0 & 3 & 2 \end{bmatrix}.$$

$k = 4$  :  $\begin{bmatrix} 0 & 4 & 3 \\ 2 & 3 & 3 \\ 3 & 0 & 2 \end{bmatrix}$  and the following matrices and their transposes

$$\begin{bmatrix} 0 & 4 & 1 \\ 1 & 1 & 1 \\ 3 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 3 \\ 1 & 4 & 0 \\ 1 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 4 \\ 1 & 1 & 2 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 1 \\ 1 & 4 & 0 \\ 2 & 1 & 4 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 4 \\ 2 & 2 & 1 \\ 3 & 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 4 \\ 2 & 2 & 3 \\ 3 & 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 4 & 1 \\ 2 & 3 & 2 \\ 3 & 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 4 & 3 \\ 1 & 2 & 2 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 4 & 3 \\ 2 & 3 & 3 \\ 3 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 4 \\ 2 & 4 & 1 \\ 2 & 3 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 4 & 0 \\ 2 & 3 & 3 \\ 2 & 1 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 3 & 0 \\ 3 & 2 & 3 \\ 3 & 1 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 3 & 1 \\ 3 & 2 & 3 \\ 3 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 1 & 3 \\ 0 & 4 & 3 \\ 3 & 3 & 4 \end{bmatrix}.$$

All of these matrices are prime by previous theorems. However,  $\begin{bmatrix} 2 & 5 & 11 \\ 6 & 5 & 6 \\ 7 & 4 & 2 \end{bmatrix}$  is prime,

but does not satisfy the conditions of any of the theorems. The fact that  $\begin{bmatrix} 2 & 5 & 11 \\ 6 & 5 & 6 \\ 7 & 4 & 2 \end{bmatrix}$  is prime was proved by laboriously checking all possibilities for factors.

#### REFERENCE

1. Gordon Pall, Binary quadratic and cubic forms and unipositive matrices; to appear in *J. Number Theory*.

LOUISIANA STATE UNIVERSITY  
BATON ROUGE, LOUISIANA 70803