PERMANENTS OF CYCLIC MATRICES

M. F. TINSLEY

1. Introduction. Let $A=[a_{ij}]$ be an $n\times n$ matrix with non-negative real entries. The *permanent* of A, written $P(A)$, is defined by

$$P(A) = \sum a_{1i_1}a_{2i_2}\cdots a_{ni_n}\,, \tag{1.1}$$

where the summation extends over the $n!$ permutations of the integers $i_1, i_2, \cdots, i_n$. Thus the permanent and determinant are alike in definition except for sign changes. However unlike the determinant, the properties of the permanent function are little understood. The object of this paper is to determine for a certain class of matrices those matrices A for which the permanent and determinant are equal in absolute value. This property we write $P(A) = |D(A)|$. For such matrices the permanent may then be evaluated by the determinant.

Let $A = [a_{ij}]$ be an $n \times n$ matrix composed of 0's and 1's with row and column sums equal to s. Let $\Sigma = [\sigma_{ij}]$ be a permutation submatrix of A. This means that Σ is a permutation matrix of order n such that $\sigma_{kl} = 1$ implies $a_{kl} = 1$. With Σ we associate a permutation Σ' of the letters $1, 2, \cdots, n$

$$\Sigma'(i) = j \text{ if and only if } \sigma_{ij} = 1\,. \tag{1.2}$$

It follows by definition then that $P(A) = |D(A)|$ if and only if every Σ' is even or else every Σ' is odd.

By a theorem due to König (1), the matrix A may be written as a sum of s permutation matrices,

$$A = \pi_1 + \pi_2 + \cdots + \pi_s\,. \tag{1.3}$$

For convenience we will say that A is *defined* by the s permutations $\pi_1', \pi_2', \cdots, \pi_s'$. If $\pi_k'\pi_j' = \pi_j'\pi_k'$ for each j and k, then A will be called *abelian*. If for $i = 1, 2, \cdots, s$, $\pi_i' = (1, 2, \cdots, n)^{a_i}$ where $0 \leqq d_i < n$, then A is cyclic and will be said to be defined by the difference $d_1, d_2, \cdots, d_s$ mod n.

Now let C be the 7×7 cyclic matrix defined by the differences $0, 1, 3$, mod 7. The main result of the paper may be stated as follows:

Let A be an $n \times n$ abelian matrix with $s \geqq 3$ ones in each row and column. Then $P(A) = |D(A)|$ if and only if $s = 3$, $n = 7e$ and upon permutations of rows and columns A is transformed into the direct sum of C taken e times.

Received September 6, 1958, and in revised form, August 24, 1959. This research was supported in part by the Office of Ordnance Research.

Most of the results of this paper are taken from the author's doctoral thesis written at the Ohio State University under the supervision of Prof. H. J. Ryser. Theorem 1, 2, 3 and 6 are from that source, the proof of Theorem 6 being essentially altered here.

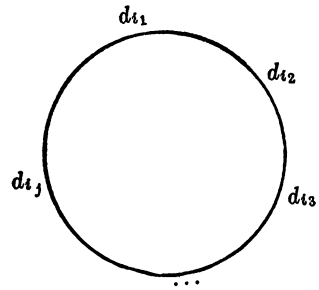
2. Representation of Cycles. Let A be a 0, 1 matrix of order n with s ones in each row and column. By (1.3) we may write $A = \pi_1 + \pi_2 + \cdots + \pi_s$. The matrix $B = \pi_s^{-1} A$ has ones on the main diagonal and possesses the same permanent and, apart from sign, the same determinant as A. Thus there is no loss in supposing A has ones on the main diagonal. If now Σ is a permutation submatrix of A any cycle of Σ' also corresponds to a permutation submatrix of A. Hence $P(A) = |D(A)|$ if and only if all such cycles are even. We shall refer to these cycles as the cycles of A.

If $P(A) = |D(A)|$ and $B = A - \pi_s$ then B has the same property since any term in the expansion of $D(B)$ also contributes to $D(A)$. Thus any results for matrices A with $P(A) = |D(A)|$ and $s = 3$ will also apply to matrices with $t \geqq 3$ ones in each row and column. It develops, at east for the class of abelian matrices, that the analysis for $s = 3$ is all lthat is necessary.

For the remainder of §§ 2, 3 and 4 only cyclic matrices will be considered. Let A be cyclic of order n and defined by the differences $0, d_1$ and $d_2 \bmod n$. Reading $\bmod n$, a cycle of A must have the form

$$a \longrightarrow a + d_{i_1} \longrightarrow a + d_{i_1} + d_{i_2} \longrightarrow \cdots \longrightarrow a + d_{i_1} + d_{i_2} + \cdots + d_{i_j}.$$

Here the d_{i_k}'s are d_1 or d_2 and $d_{i_1} + d_{i_2} + \cdots + d_{i_j} \equiv 0 \pmod n$. Now arrange the d_{i_k}'s in a circle as follows:



Then no consecutive selection of t of the d_{i_k}'s, $0 < t < j$, has a sum divisible by n. Otherwise there would be a cycle within a cycle.

Conversely, let $d_{i_1}, d_{i_2}, \cdots, d_{i_j}$ be a sequence formed from d_1 and d_2 such that $d_{i_1} + d_{i_2} + \cdots + d_{i_j} \equiv 0 \pmod n$ and, when arranged in a circle, no proper consecutive selection of the d_{i_k}'s has a sum divisible by n. Then for each $b = 1, 2, \cdots, n$,

$$b \longrightarrow b + d_{i_1} \longrightarrow b + d_{i_1} + d_{i_2} \longrightarrow \cdots \longrightarrow b + d_{i_1} + d_{i_2} + \cdots + d_{i_j}$$

is a cycle of A.

Now for a cycle $a \to a + d_{i_1} \to a + d_{i_i} + d_{i_j} \to \cdots \to a + d_{i_1} + \cdots + d_{i_j}$, let x_k denote the number of times that d_k occurs among $d_{i_1}, d_{i_2}, \cdots, d_{i_j}$. Then $j = x_1 + x_2$ and

$$d_1x_1 + d_2x_2 \equiv 0 \pmod{n} . \tag{2.1}$$

DEFINITION. We say that the solution (x_1, x_2) of the congruence $d_1x + d_2y \equiv 0 \pmod{n}$ *represents* a cycle of the matrix A. More precisely, let $d_1x' + d_2y' \equiv 0 \pmod{n}$, where $0 \leqq x', y'$ and $0 < x' + y'$. Suppose there exists some arrangement of x' α's and y' β's in a circle with the following property; For all other solutions x^*, y^* of (2.1) such that $0 \leqq x^* \leqq x', 0 \leqq y^* \leqq y'$ and $0 < x^* + y^*$, no consecutive selection of $x^* + y^*$ α's and β's totals exactly x^* α's. Then the solution (x', y') represents a cycle. If no such arrangement exists (x', y') does not represent a cycle.

Note that if (y_1, y_2) represents a cycle then the cycle has length $y_1 + y_2$ and hence is even or odd according as $y_1 + y_2$ is odd or even. Thus to determine if $P(A) = |D(A)|$ it suffices to study the solutions of (2.1).

EXAMPLE 1. The 7×7 matrix C defined by the differences $0, 1, 3 \bmod 7$ has permanent equal to determinant. For consider the solutions of $x + 3y \equiv 0 \pmod 7$: (4, 1), (1, 2), (5, 3), (2, 4), (6, 5), (3, 6), (0, 7), (7, 0). One readily shows that (2, 4) can not represent a cycle and that only (4, 1), (1, 2), (0, 7) and (7, 0) may. Since the sums $4 + 1$, $1 + 2$, $0 + 7$ are odd it follows that $P(C) = |D(C)|$. Similarly one shows that the 7×7 matrix defined by the differences $0, 1, 5 \bmod 7$ has permanent equal to determinant.

3. Primitive Solutions. In this section we study a general congruence

$$ax + by \equiv 0 \pmod{n} , \tag{3.1}$$

where a and b are positive integers not necessarily distinct and x, y are non-negative integers.

Let (x_1, y_1) and (x_2, y_2) be solutions of (3.1). We write $(x_1, y_1) \geqq (x_2, y_2)$ provided $x_1 \geqq x_2, y_1 \geqq y_2$ and $(x_1, y_1) = (x_2, y_2)$ if $x_1 = x_2$ and $y_1 = y_2$. Furthermore, we write $(x_1, y_1) > (x_2, y_2)$ provided $x_1 > x_2, y_1 \geqq y_2$ or $x_1 \geqq x_2, y_1 > y_2$.

Now let (x_0, y_0) be a solution of (3.1) such that both x_0 and y_0 are positive.

DEFINITION. (x_0, y_0) will be called *primitive* if for every solution

(x_0', y_0') such that $(0, 0) \leqq (x_0', y_0') \leqq (x_0, y_0)$ either $(x_0', y_0') = (0, 0)$ or $(x_0', y_0') = (x_0, y_0)$.

Suppose now that the $n \times n$ matrix A is defined by the three differences $0, d_1, d_2 \bmod n$. From the definition and the discussion of § 2 it follows that primitive solutions of the congruence $d_1x + d_2y \equiv 0 \pmod n$ must represent cycles of A. Thus the study of primitive solutions is suggested as a starting point in our investigations. The first theorem concerns the determination of the primitive solutions of (3.1).

Let $n \equiv n_1 \pmod d$ and $d \equiv d_1 \pmod{n_1}$, where $0 \leqq d_1 < n_1 < d < n$. To simplify the notation we shall set $F = n/d$ and $G = d/n_1$.

THEOREM 1. *If the primitive solutions of* $x' + d_1y' \equiv 0 \pmod{n_1}$ *are those solutions for which* $y' = i, j, k, \cdots$, *then the primitive solutions of* $x + dy \equiv 0 \pmod n$ *are those solutions for which*

$$y = 1, 2, \cdots, [F], [([iG] + 1)F], [([jG] + 1)F], [([kG] + 1)F], \cdots .$$

If $n \equiv 0 \pmod d$, *then the primitive solutions of* $x + dy \equiv 0 \pmod n$ *are those solutions with* $y = 1, 2, \cdots, [F] - 1$.

Proof. Clearly the solutions of $x + dy \equiv 0 \pmod n$ with $y = 1, 2, \cdots, [F] - 1$ are primitive, since as y increases the corresponding x decreases. If n is divisible by d then these are all the primitive solutions. If $n \not\equiv 0 \pmod d$ then the solution with $y = [F]$ is also primitive. If, in addition, $d_1 = 0$ then n_1 is the greatest common divisor of n and d, and $(n_1, [F])$ is a primitive solution of $x + dy \equiv 0 \pmod n$. Moreover, if (x_0, y_0) is another solution and $y_0 > [F]$, then (x_0, y_0) is not primitive since x_0 must be a multiple of n_1. Thus in proving the theorem, both n_1 and d_1 may be supposed not zero.

Assume now that $[F] < v \neq [iF]$, $i = 1, 2, \cdots, d - 1$. Let (x_1, y_1) be the solution of $x + dy \equiv 0 \pmod n$ with $y_1 = v$. Then there is a solution (x', y') where $(0, 0) < (x', y') < (x_1, y_1)$ and $y' = [jF]$ for some $j, 1 \leqq j \leqq d - 1$. To show this let j be such that $[jF] < v < [(j + 1)F]$. Since $[F] \leqq [(j + 1)F] - [jF] \leqq [F] + 1$, we have $v = [jF] + r$, $r \leqq [F]$. Then $x_1 = (j + 1)n - ([jF] + r)d$. Now the x' corresponding to $y' = [jF]$ is $jn - [jF]d$. Thus if we set $x' = jn - [jF]d$ and $y' = [jF]$, then

$$x_1 - x' = \{(j + 1)n - ([jF] + r)d\} - \{jn - [jF]\} = n - rd \geqq n - [F]d > 0$$

and $(x', y') < (x_1, y_1)$. As a consequence, to determine the primitive solutions of the congruence $x + dy \equiv 0 \pmod n$ it suffices to consider those solutions with $y = [iF]$, $i = 1, 2, \cdots, d - 1$.

LEMMA 1. *If* $0 \leqq a_i < d < n$ $(i = 1, 2, \cdots, d - 1)$ *then*
(1) $in \equiv a_i \pmod d$ *if and only if* $a_i + d[iF] \equiv 0 \pmod n$. *For*

$0 \leqq a_i < d < n$ *and* $in \equiv a_i \pmod{d}$ $\qquad (i = 1, 2, \cdots, d-1)$,

(2) $x_0 = a_g$, $y_0 = [gF]$ *is a primitive solution of* $x + dy \equiv 0 \pmod{n}$ *if and only if* $a_1, a_2, \cdots, a_{g-1}$ *are all* $> a_g > 0$.

Proof. (1) *Necessity* If $in \equiv a_i \pmod{d}$ then $in = a_i + u_i d$ for some u_i, and $u_i = (in - a_i)/d = [iF]$. Substituting $[iF]$ for u_i, $a_i + d[iF] = in \equiv 0 \pmod{n}$.

Sufficiency. If $a_i + d[iF] \equiv 0 \pmod{n}$ then since $in \geqq d[iF] > (i-1)n$, we have $a_i + d[iF] = in$. Thus $in \equiv a_i \pmod{d}$.

(2) *Necessity.* Let $x_0 = a_g$, $y_0 = [gF]$ be a primitive solution of $x + dy \equiv 0 \pmod{n}$ and x', y' another solution. If $0 < y' < y_0$, then we must have $x' > x_0$. Thus for $y' = [jF] (j = 1, 2, \cdots, g-1)$, $a_j = x' > x_0 = a_g$.

Sufficiency. If (x_0, y_0) is not primitive then there is a solution (x_1, y_1) such that $(0, 0) < (x_1, y_1) < (x_0, y_0)$. If now $y_1 \geqq [F]$, then by the earlier remarks of this section there is a solution (x', y') such that $(0, 0) < (x', y') \leqq (x_1, y_1)$ and $y' = [jF]$ for some j, $1 \leqq j \leqq d - 1$. Since $y' < y_0$ we have $j < g$. But also since $x' \leqq x_0$, we have $a_j \leqq a_g$. If $y_1 < [F]$, then $a_1 < x_1$ so $a_1 < x_0 = a_g$ and $1 < g$. In either case we contradict $a_1, a_2, \cdots, a_{g-1} > a_g$.

Now consider the following table of values defined for each $k = 0, 1, 2, \cdots, n_1 - 1$.

(4.1)

b_i	i
$([kG] + 1)n_1 - kd$	$[kG] + 1$
$([kG] + 2)n_1 - kd$	$[kG] + 2$
$\vdots$	$\vdots$
$[(k+1)G]n_1 - kd$	$[(k+1)G]$

It follows readily that for the a_i of Lemma 1, $a_i \equiv in \equiv in_1 \equiv b_i \pmod{d}$, that $0 < b_i \leqq d$ and that b_i increases with i. Here i is understood as limited to those values in the table. Now $(k+1)d \geqq [(k+1)G]n_1$ implies $[(k+1)G]n_1 - kd \leqq d$ where equality holds only if $(k+1)d \equiv 0 \pmod{n_1}$. Thus $b_i = a_i$ unless $i = [(k+1)G]$ and $(k+1)d \equiv 0 \pmod{n_1}$. In this case $a_i = 0$ and $b_i = d$.

Now let $(a_j, [jF])$ be a primitive solution of the congruence $x + dy \equiv 0 \pmod{n}$. The integer j must occur as some i in table (4.1). Since b_i increses with i, we must have $j = [kG] + 1$, for some k, $0 \leqq k \leqq n_1 - 1$.

Finally, $kd \equiv 0 \pmod{n}$ implies k is divisible by $u = n_1/(d, n)$. Thus since $(0, [uGF])$ is a solution, those solutions $(a_i, [iF])$, where $i = [kG] + 1$ and $kd \equiv 0 \pmod{n_1}$, are not primitive.

Next consider the solution of $x' + d_1 y' \equiv 0 \pmod{n_1}$. For $k =$

$1, 2, \cdots, n_1 - 1$ define $\alpha_k \equiv -kd \equiv -kd_1 \pmod{n_1}$ where $0 \leqq \alpha_k < n_1$. Then the nontrivial solutions are $(\alpha_1, 1), (\alpha_2, 2), \cdots, (\alpha_{n_1-1}, n_1 - 1)$.

LEMMA 2. *Let $1 \leqq k, l < n$ where kd and ld are not divisible by n_1. If $e = [kG] + 1$ and $f = [lG] + 1$, then*

$$a_e - a_f = \alpha_k - \alpha_l .$$

Proof. $a_e = b_e = en_1 - kd$ and $a_f = b_f = fn_1 - ld$ while

$$\alpha_k = n_1 - \{kd - [kG]n_1\}$$

and

$$\alpha_l = n_1 - \{ld - [lG]n_1\} .$$

Thus $a_e - a_f = ([kG] - [lG])n_1 + (l - k)d = \alpha_k - \alpha_l$.

Now we may prove the theorem. List the primitive solutions of $x + dy \equiv 0 \pmod{n}$ as $(n - d, 1), (n - 2d, 2), \cdots, (n_1, [F']) = (a_1, [F']), (a_{j_1}, [j_1F']), (a_{j_2}, [j_2F']), \cdots, (a_{j_v}, [j_vF'])$, where by primitivity $a_1 > a_{j_1} > a_{j_2} > \cdots > a_{j_v} > 0$ and $1 < j_1 < j_2 < \cdots < j_v$. We have seen that each j_t must have the form $[kG] + 1$ where $kd \not\equiv 0 \pmod{n_1}$. For $1 \leqq p \leqq v$ define k_p by setting $j_p = [k_pG] + 1$ and consider the following solutions of $x' + d_1y' \equiv 0 \pmod{n_1}$:

$$(\alpha_{k_1}, k_1), (\alpha_{k_2}, k_2), \cdots, (\alpha_{k_v}, k_v) .$$

By Lemma 2, $\alpha_{k1} > \alpha_{k_2} > \cdots > \alpha_{k_v}$. We cannot have $\alpha_{k_v} = 0$ for then $k_vd \equiv 0 \pmod{n_1}$.

If for some $u, 1 \leqq u \leqq v, (\alpha_{k_u}, k_u)$ is not a primitive solution of $x' + d_1y' \equiv 0 \pmod{n_1}$, then there is a solution (α_r, r) such that $(0, 0) < (\alpha_r, r) < (\alpha_{k_u}, k_u)$. Set $H = 1/(d, n) = 1/(d_1, n_1)$. If $\alpha_r = 0$ then $rd_1 \equiv 0 \pmod{n_1}$ and $k_u > n_1H$.

But then $j_u \geqq [n_1HG] + 1 = dH + 1$ and $(0, [dHF']) < (a_{j_u}, [j_uF'])$, contradicting the primitivity of $(a_{j_u}, [j_uF'])$.

If $\alpha_r > 0$ then by Lemma 2, if $f = [rG] + 1$, $(0, 0) < (a_f, [fF']) < (a_{j_u}, [j_uF'])$ again contradicting the primitivity of $(a_{j_u}, [j_uF'])$. Thus for $1 \leqq p \leqq v$, (α_{k_p}, k_p) is a primitive solution of $x' + d_1y' \equiv 0 \pmod{n_1}$. To complete the proof of the theorem we must show that there are no others.

Suppose (α_q, q) is a primitive solution of $x' + d_1y' \equiv 0 \pmod{n_1}$. Since $\alpha_1, \alpha_2, \cdots, \alpha_{q-1}$ are $> \alpha_q > 0$, Lemma 2 implies that $a_{[G]+1}, a_{[2G]+1}, \cdots, a_{[(q-1)G]+1}$ are $> a_{[qG]+1}$. Also $a_{[qG]+1} = ([qG] + 1)n_1 - qd$ and so is > 0. Now for each $t, 1 \leqq t \leqq q, a_{[tG]} > 0$ for otherwise td would be divisible by n_1 and α_t would be 0. Morever,

$$a_1 = n_1 > [G]n_1 + (n_1 - d) = a_{[G]+1} .$$

Hence by the discussion of the tables of (4.1) with $k = 0, 1, \cdots, q - 1$ we may conclude that

$$a_1, a_2, \cdots, a_{[qG]} \text{ are } > a_{[qG]+1} > 0 .$$

In Lemma 1 set $g = [qG] + 1$. This means that $(a_g, [gF])$ is primitive. Thus q was one of the k_p's and the theorem is proved.

As a collollary we give a more convenient computational form of the primitive solutions.

COROLLARY. *Let* (x, y) *be a solution of* $x + dy \equiv 0 \pmod{n}$ *such that* $y=[([iG]+1)F]$. *Then* $y=[F]([iG]+1)+i$ *and* $x=n_1-(id-[iG]n_1)$.

Proof. Let $n = q_1d + n_1$, $0 < n_1 < d$. Then $q_1 = [F]$.

$$([iG] + 1)n = q_1d([iG] + 1) + n_1([iG] + 1) ,$$

and

$$y = q_1([iG] + 1) + [G^{-1}([iG] + 1)] .$$

Since $id < n_1([iG] + 1) \leqq id + n_1 < (i + 1)d$, we have $y = q_1([iG] + 1) + i$.

Now write $x = ([iG] + 1)\, n - yd$. By substituting $[F]([iG] + 1) + i$ for y we obtain $x = n[iG] + n - d[F][iG] - d[F] - id$. Then substituting $[F]d + n_1$ for n and clearing gives $x = n_1 - (id - [iG]n_1)$.

In the notation of Theorem 1, let $n > d > n_1 > d_1 > 0$. Again let $F = n/d$ and $G = d/n_1$. Let

$$(x_1, y_1) = (n - [F]d, [F]) = (n_1, [F])$$

and

$$(x_2, y_2) = (n_1 - d + [G]n_1, [F]([G] + 1) + 1) = (n_1 - d_1, [F]([G] + 1) + 1) .$$

By Theorem 1 and Corollary, (x_1, y_1) and (x_2, y_2) are primitive solutions of $x + dy \equiv 0 \pmod{n}$. Concerning them we shall now prove the following useful theorem:

THEOREM 2. *If* (x', y') *is a solution of* $x + dy \equiv 0 \pmod{n}$ *and* $(0, 0) < (x', y') < (x_1 + x_2, y_1 + y_2)$, *where* (x_1, y_1) *and* (x_2, y_2) *are the above mentioned primitive solutions, then either* $(x', y') = (x_1, y_1)$ *or* $(x', y') = (x_2, y_2)$.

Proof. To prove the theorem we need the following lemma.

LEMMA. *Suppose there exist primitive solutions* (x_1, y_1) *and* (x_2, y_2) *of* $x + dy \equiv 0 \pmod{n}$ *such that* $x_1 + x_2 \leqq n$, $y_1 + y_2 \leqq n$ *and there is no other primitive solution* (x', y') *for which* $(x', y') < (x_1 + x_2, y_1 + y_2)$. *Then there is no other solution* (x^*, y^*) *such that* $(0, 0) < (x^*, y^*) < (x_1 + x_2, y_1 + y_2)$.

Proof of lemma. Let $(0, 0) < (x^*, y^*) < (x_1 + x_2, y_1 + y_2)$ where (x^*, y^*) is a solution of $x + dy \equiv 0 \pmod{n}$. Clearly $y^* \neq 0$ since x^* must be less than n. If there are solutions (x^*, y^*) with $x^* = 0$ and $(0, 0) < (x^*, y^*) < (x_1 + x_2, y_1 + y_2)$ then select the one with y^* minimal. Then $(x_1 + x_2, y_1 + y_2 - y^*)$ is a solution and by primitivity $y^* > y_1, y_2$. This implies $y_1 + y_2 - y^* < y^*, y_1, y_2$. But now the choice of y^* implies that there must be a primitive solution $(x', y') \leqq (x_1 + x_2, y_1 + y_2 - y^*)$. Such a primitive solution cannot be (x_1, y_1) or (x_2, y_2), and this contradicts the hypothesis. Hence we have shown that an arbitrary solution (x^*, y^*) which satisfies $(0, 0) < (x^*, y^*) < (x_1 + x_2, y_1 + y_2)$ can have neither $x^* = 0$ nor $y^* = 0$.

Thus the solution (x^*, y^*) must contain a primitive solution. This means for $i = 1$ or 2, $x_1 \leqq x^*$ and $y_i \leqq y^*$. For this i, $(x^* - x_i, y^* - y_i)$ is a solution. Either both $x^* - x_i$ and $y^* - y_i$ are zero or neither is zero. If $x^* \neq x_i$ and $y^* \neq y_i$ then for $j = 1$ or 2, $x^* - x_i \geqq x_j$ and $y^* - y_i \geqq y_j$. Again, either both $x^* - x_i - x_j$ and $y^* - y_i - y_j$ are zero or neither is zero. Continuing, we obtain

$$x^* = c_1x_1 + c_2x_2 \text{ and } y^* = c_1y_1 + c_2y_2 ,$$

where c_1 and c_2 are non-negative integers. If $(x_1, y_1) = (x_2, y_2)$ then $x^* = cx_1$, $y^* = cy_1$ where $c = c_1 + c_2$. In this case c would be 1 or 2 and the lemma follows. If $(x_1, y_1) \neq (x_2, y_2)$ we may let $x_1 > x_2$, $y_1 < y_2$. Then $x_1 > x_2$ and $x^* \leqq x_1 + x_2$ imply $c_1 \leqq 1$ while $y_1 < y_2$ and $y^* \leqq y_1 + y_2$ imply $c_2 \leqq 1$. This proves the lemma.

We must show that the solutions (x_1, y_1) and (x_2, y_2) of the theorem satisfy the hypothesis of the lemma. One readily verifies that $x_1 + x_2$ and $y_1 + y_2$ are less than n. Let (x^*, y^*) be a primitive solution such that $(0, 0) < (x^*, y^*) < (x_1 + x_2, y_1 + y_2)$. To prove the theorem it suffices to show that $x^* \leqq x_1$ and $y^* \leqq y_2$. Now consider the solution (x_3, y_3) where

$$y = [F]([2G] + 1) + 2 .$$

By Theorem 1 and its corollary there is no primitive solution (x', y') such that $y_2 < y' < y_3$. We have

$$y_3 - y_1 - y_2 = [F]([2G] - [G] - 1) + 1 \geqq [F]([G] - 1) + 1 \geqq 1 .$$

From this it follows that $y^* \leqq y_2$.

Now if $[F] = 1$, then $x^* \leqq x_1$. If $[F] > 1$, consider the solution $(x_0, y_0) = (n - [F]d) + d, [F] - 1$. There is no primitive solution (x'', y'') such that $x_0 > x'' > x_1$.
Furthermore

$$\begin{aligned} x_0 - x_1 - x_2 &= n - [F]d + d - (n - [F]d) - (n_1 - d + [G]n_1) \\ &= 2d - n_1 - n_1[G] > 0. \end{aligned}$$

Hence $x^* \leqq x_1$. Thus $x^* \leqq x_1$ and $y^* \leqq y_2$ so that (x^*, y^*) equals (x_1, y_1) or (x_2, y_2). The theorem follows from the lemma.

4. Application. Let A be a cyclic 0, 1 matrix of order n defined by differences 0, 1 and $d \bmod n$.

As covered in § 2, to show $P(A) > |D(A)|$ it is necessary and sufficient to show the existence of a solution (x', y') of $x + dy \equiv 0 \pmod n$ such that (x', y') represents a cycle and $x' + y'$ is even. The problem of determining when a solution (x', y'), $0 < x' + y'$, represents a cycle may be described as follows. Suppose there exists some arrangement of x' α's and y' β's in a circle with the following property: For each solution $(x^*, y^*) < (x', y')$, no selection of $x^* + y^*$ consecutive α's and β's totals exactly x^* α's (or y^* β's). Then (x', y') represents a cycle. If no such arrangement is possible then (x', y') does not represent a cycle.

For the purposes of this section it is not necessary to solve completely this problem in arrangements. In an important class of d and n Theorem 2 yields two primitive solutions (x_1, y_1) and (x_2, y_2) having the property that there is no other solution (x', y') such that $(0, 0) < (x', y') < (x_1 + x_2, y_1 + y_2)$. Thus if there is an arrangement of $x_1 + x_2$ α's and $y_1 + y_2$ β's in a circle such that no selection of $x_1 + y_1$ consecutive α's and β's totals exactly x_1 α's (or y_1 β's) then $(x_1 + x_2, y_1 + y_2)$ represents a cycle. Under these circumstances we have $P(A) > |D(A)|$. For (x_1, y_1) and (x_2, y_2) represent cycles, and if $x_1 + y_1$ and $x_2 + y_2$ are both odd then $x_1 + x_2 + y_1 + y_2$ is even. The proof of Theorem 3 is based upon this device.

THEOREM 3. *Let A be a cyclic 0, 1 matrix of order n defined by the differences 0, 1, $d \bmod n$. Then $P(A) = |D(A)|$ if and only if $n = 7$ and $d = 3$ or 5.*

Proof. If $n = 7$ and $d = 3$ or 5 then $P(A) = |D(A)|$ by Example 1. We assume $P(A) = |D(A)|$ and will show $n = 7$ and $d = 3$ or 5. If n or d is even then $P(A) > |D(A)|$. For if n is even the permutation $(1, 2, \cdots, n)$ is odd. The solution $(x', y') = (n - d, 1)$ is primitive so if n is odd and d is even then $x' + y' = n - d + 1$ is even. Thus we may assume that both n and d are odd. As before we set $F = n/d$ and $G = d/n_1$.

We may also assume that $[F] = 1$.

For if $[F] \geqq 2$ then $d < n/2$ and $n - d + 1 > n/2 + 1$. Thus $[n(n - d + 1)^{-1}] = 1$. Now

$$A = I + P + P^d$$

where P is a permutation matrix and $P^n = I$. Since $A^T = I + P^{-1} + P^{-d}$ and $B = PA^T = I + P + P^{n+1-d}$, it follows that $P(A) = |D(A)|$ if and

only if $P(B) = |D(B)|$. Thus if $[F] \geqq 2$, we may study the matrix B with $[n(n-d+1)^{-1}] = 1$. Hence we may assume $[F] = 1$. Note that if $n = 7, d = 3$ then $n - d + 1 = 5$.

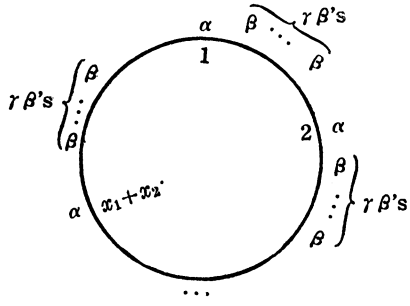
We may assume further that in the notation of Theorem 1, $n > d > n_1 > d_1 \geqq 1$. For if $d_1 = 0$ then n_1 is the greatest common divisor of n and d. Since $n_1 = n - d$ and since n, d are odd, n_1 would have to be both even and odd.

Finally, we may assume $[G] > 1$. For if $[G] = 1$, consider the primitive solution $(x', y') = (n_1 - d_1, [F]([G] + 1) + 1)$. Since d is odd and $d = n_1 + d_1$, $x' + y' \equiv n_1 + d_1 + 1 \equiv 0 \pmod 2$.

In the remainder of the proof let (x_1, y_1) and (x_2, y_2) denote the primitive solutions $(n_1, 1)$ and $(n_1 - d_1, [G] + 2)$ respectively, as in Theorem 2.

The proof will be completed by showing that if n and d are not 7 and 5 respectively, then $(x_1 + x_2, y_1 + y_2)$ represents a cycle. Several cases will be considered.

Case 1*a* $y_1 + y_2 \equiv 0 \pmod{x_1 + x_2}$.
Consider the following circular arrangement of $x_1 + x_2$ α's and $y_1 + y_2$ β's, where r denotes the quotient $(y_1 + y_2)/(x_1 + x_2)$.

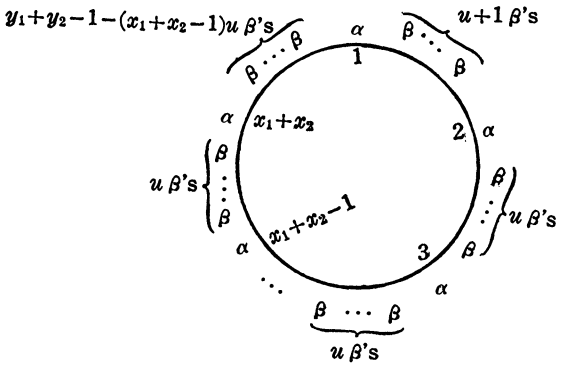


If a selection of $t = x_1 + y_1$ consecutive α's and β's totals x_1 α's then it totals at least $(x_1 - 1)r$ β's. Let s represent $(2n_1 - d_1)^{-1}$. Since $[G] \geqq 2$,

$$(x_1 - 1)r = (n_1 - 1)s([G] + 3) \geqq 5s(n_1 - 1) > 1 = y_1 .$$

Thus for case $P(A) > |D(A)|$.

Case 1*b* $y_1 + y_2 \not\equiv 0 \pmod{x_1 + x_2}$ and $x_1 + x_2 < y_1 + y_2$. Consider the following circular arrangement of $x_1 + x_2$ α's and $y_1 + y_2$ β's. To simplify the notation we set $u = [(y_1 + y_2)/(x_1 + x_2)]$.
Since $y_1 + y_2 - 1 \geqq (x_1 + x_2)u$, we have $y_1 + y_2 - 1 - (x_1 + x_2 - 1)u > u$. Thus if $1 \leqq t \leqq x_1 + x_2 - 1$, a selection of consecutive α's and β's which totals t α's will total at most $y_1 + y_2 - 1 - (x_1 + x_2 - 1)u + tu + 1 = y_1 + y_2 - (x_1 + x_2 - t - 1)u$ β's.

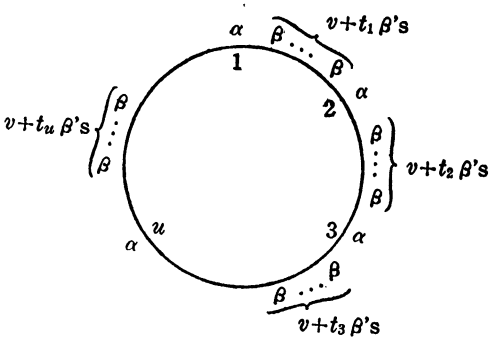


Let $t = x_2$ and set $s = (2n_1 - d_1)^{-1}$. It suffices to show that $y_2 > y_1 + y_2 - (x_1 + x_2 - x_2 - 1)u$ and thus to show $(n_1 - 1)[([G] + 3)s] > 1$. This will be true if $n_1 > 2$.

If $n_1 = 2$ then $d_1 = 1$ and $(n_1 - 1)[([G] + 3)s] = [1/3([G] + 3)]$. This is > 1 unless $[G] = 2$. But then $d_1 = 1, n_1 = 2 = [G]$, and $[F] = 1$ together imply $d = 5$ and $n = 7$.

Case 2 $x_1 + x_2 \geqq y_1 + y_2$.

Consider the following circular arrangement of α's and β's.



We are supposing throughout the proof that $(x_1, y_1) = (n_1, 1)$ and

$$(x_2, y_2) = (n_1 - d_1, [G] + 2).$$

Let

$$u = y_1 + y_2, v = \left[\frac{x_1 + x_2}{y_1 + y_2}\right]$$

and set $t_1 = t_3 = t_5 = \cdots = 0$. For each $i = 1, 2, \cdots, [u/2]$ we wish to select t_{2i} so that $0 \leqq t_{2i} \leqq n_1 - 2v - 1$ and $t_2 + t_4 + t_6 + \cdots = x_1 + x_2 - (y_1 + y_2)v$. For then any selection of consecutive α's and β's which totals $y_1 = 1\,\alpha$ will total less than $n_1 = x_1\,\beta$'s.

To show that the t's may be so selected it suffices to prove that

$$uv + \left[\frac{u}{2}\right](n_1 - 2v - 1) \geqq x_1 + x_2 .$$

Let $q = ([G] + 3)$. We must show that

$$q[(2n_1 - d_1)q^{-1}] + \left[\frac{1}{2}q\right](n_1 - 2[(2n_1 - d_1)q^{-1}] - 1) \geqq 2n_1 - d_1 .$$

The left side equals

$$\left[\frac{1}{2}q\right]n_1 + [(2n_1 - d_1)q^{-1}]\left(q - 2\left[\frac{1}{2}q\right]\right) - \left[\frac{1}{2}q\right], \tag{5.1}$$

and is $\geqq [(1/2)q](n_1 - 1)$. This is $\geqq 2n_1 - d_1$ unless $d_1 = 1$ and $[G] = 2$. If $d_1 = 1$ and $[G] = 2$, then (5.1) becomes

$$2n_1 + \left[\frac{2n_1 - 1}{5}\right] - 2 .$$

However,

$$2n_1 + \left[\frac{2n_1 - 1}{5}\right] - 2 < 2n_1 - 1$$

and $n_1 > 1$ together imply that $n_1 = 2$ and hence that $d = 5, n = 7$. Thus (5.1) $\geqq 2n_1 - d_1$ unless $d = 5$ and $n = 7$.

5. The Main Theorem. In this section we shall obtain a generalization of Theorem 3 by means of elementary group theory. Let a, b be elements of a multiplicative group G.

A *word* is by definition either void and written 1 or a succession $c_1c_2 \cdots c_q$ where $c_i (i = 1, 2, \cdots, q)$ is a or b. Two words are equal provided they are identical termwise. If $W_1 = c_1c_2 \cdots c_r$ and $W_2 = c_{r+1}c_{r+2} \cdots c_{r+s}$ are words then the *product word* W_1W_2 is defined as $c_1c_2 \cdots c_rc_{r+1} \cdots c_{r+s}$. If W_0 is the void word and W is any word then by definition $W_0W = WW_0 = W$. A non-void word $W = c_1c_2 \cdots c_t$ will be called a relation between a and b if $c_1c_2 \cdots c_t$, considered as an element of G, is the identity 1. The relation will be said to have length t. Finally, W is a *minimal relation* provided W is a relation and any expression of W as a product $W = W_1W_2W_3$ with W_2 a relation implies that $W = W_2$.

THEOREM 4. *Let G be a finite group generated by two distinct elements a and b. Suppose H is a normal subgroup of G and in the homomorphism $G \to G/H$, $a \to \bar{a}$ and $b \to \bar{b}$. If there is a minimal relation between $\bar{a}$ and $\bar{b}$ in G/H having even length then there is a minimal relation between a and b in G having even length.*

Proof. Let $\overline{W}$ be a minimal relation between $\bar{a}$ and $\bar{b}$ in G/H having even length. Replace each $\bar{a}$ and $\bar{b}$ in $\overline{W}$ by a and b respectively, thus obtaining a word W on a and b. Then W regarded as a group element is in H. We may suppose that for some $u > 1$, the word W^{u+1} can be written in the form $W^{u+1} = W_1 W_2 W_3$, where W_2 is a minimal relation, but W^u cannot. The theorem will be proved by showing that either $W_1 = W_3 = W_0$, the void word, or $W = W_1 W_3$ and consequently that W_2 is a minimal relation of even length.

By the choice of u, there are words W_1', W_3' such that

$$W_2 = W_3' W^{u-1} W_1' \text{ and } W = W_1 W_3' = W_1' W_3 .$$

If $W_3' \neq W_3$ then either

(1) $W_3' = W_3^* W_3$ where W_3^* is a non-void word, or

(2) $W_1 = W_4 W_5$, $W_3 = W_5 W_6$, $W = W_4 W_5 W_6$ where W_4, W_5, W_6 are not void. Since the word W_2 is a relation, both the group elements W and $W_1 W_3$ are in H.

Thus if (1), $W = W_1 W_3^* W_3$ implies the group element W_3^* is in H. This contradicts the minimality of the relation $\overline{W}$ unless $W_1 = W_3 = W_0$, the void word.

If (2), the group element W_5 must be in H, contradicting the minimality of $\overline{W}$.

With the aid of Theorem 4 the following generalization of Theorem 3 will now be proved:

THEOREM 5. *Let I (the identity), P and Q be disjoint permutations on the letters $1, 2, \cdots, n$ such that $PQ = QP$ and let A be the $0, 1$ matrix of order n defined by them. Suppose the permutation group G generated by P and Q is transitive. Then $P(A) = |D(A)|$ if and only if upon simultaneous permutations of rows and columns A is transformed into the cyclic 7×7 matrix C defined by differences $0, 1, 3 \bmod 7$.*

Proof. The sufficiency is a consequence of Theorem 3. The necessity will be proved by induction on n. If $n = 3$ then $P(A) > |D(A)|$ and the theorem is true. Let B be of order N, $3 \leqq N < n$, and defined by the disjoint permutations $I, P' Q'$ where the group G' generated by P' and Q' is transitive and abelian. Moreover, let $P(B) = |D(B)|$. Then the induction hypothesis asserts that B is transformable into C by simultaneous permutations of rows and columns.

Since G is abelian, G is regular and of order n. Hence $i, i^P, i^{P^2}, \cdots, i^{P^{x_1}}, i^{P^{x_1}Q}, \cdots i^{P^{x_1}Q^{y_1}}, \cdots, i^{P^{x_1}Q^{y_1}P^{x_2}Q^{y_2}\cdots}$ is a cycle if and only if $P^{x_1}Q^{y_1}P^{x_2}Q^{y_2} \cdots$ is a minimal relation between P and Q. Thus $P(A) = |D(A)|$ if and only if every minimal relation between P and Q has odd length.

If G is not cyclic then G is homomorphic to an elementary p group

$\overline{G}$ of type (p, p). Under this homomorphism, denote the images of P and Q by $\overline{P}$ and $\overline{Q}$, respectively. Since $\overline{P}$ and $\overline{Q}$ must be independent generators of $\overline{G}$, the relation $(\overline{P}\overline{Q})^p$ is minimal. Thus by Theorem 4 there is a minimal relation between P and Q having even length. Hence $P(A) > |D(A)|$.

Now suppose G is cyclic, $P(A) = |D(A)|$ and consider two cases: (1) G is generated by P and (2) Neither P nor Q generate G.

Case 1. Since G is transitive P must be a cycle of length n. Thus there is a permutation R such that $R^{-1}PR = (1, 2, \cdots, n)$. Consider the $n \times n$ cyclic matrix A^* defined by $I, R^{-1}PR, R^{-1}QR$. A^* is obtained from A by simultaneous permutations of rows and columns so by Theorem 3, A^* and hence A is transformable into C. Note here that the cyclic 7×7 matrix defined by differences $0, 1, 5 \bmod 7$ is transformable into C.

Case 2. For this case n must be divisible by at least two distinct primes p_1, p_2. We show first that $n = p_1p_2$. Let H_1, H_2 be subgroups of G having orders p_1 and p_2 respectively. If H_1 does not contain any of P, Q, PQ^{-1} consider the homomorphism $G \to G'$ where G' is the regular representation of G/H_1 Let $P \to P', Q \to Q'$ and form the $n/p_1 \times n/p_1$ matrix A' defined by I, P' and Q'. The group G' is generated by P', Q' and is cyclic and transitive. Moreover, P', Q' and I are disjoint permutations. By Theorem 4 every minimal relation in G' between P' and Q' must have odd length. Thus $P(A') = |D(A')|$ and, by the induction hypothesis, A' is transformable into C. Hence $p_2 = 7$ and $n = p_1p_2$.

If both H_1 and H_2 contain one of the three elements P, Q, PQ^{-1} then since P and Q generate $G, G = H_1 \times H_2$. Hence again $n = p_1p_2$.

We may thus suppose that P has order p_1 and Q has order p_2. Now consider the $n \times n$ matrix A^* difined by I, Q^{-1}, PQ^{-1}.

Since $P(A) = |D(A)|$ we have $P(A^*) = |D(A^*)|$. However Q^{-1} and PQ^{-1} generate G and PQ^{-1} has order n. By Case 1 then n must be 7 so that Case 2 does not arise.

COROLLARY 1. *Let I, P, Q be disjoint permutations on the letters $1, 2, \cdots, n$ such that $PQ = QP$ and let A be the $0, 1$ matrix of order n defined by them. Then $P(A) = |D(A)|$ if and only if $n = 7e$ and upon simultaneous permutations of rows and columns A is transformed into the direct sum of C taken e times.*

Proof. By the theorem it is sufficient to prove the necessity for the case that the group G generated by P and Q is intransitive.

Let the letters $1, 2, \cdots, n$ be divided into $t > 1$ transitivity sets containing $N_1, N_2, \cdots, N_t$ letters, respectively. Then upon simultaneous permutations of rows and columns A is transformed into the direct sum

of t matrices $A_1, A_2, \cdots, A_t$ such that for $1 \leqq j \leqq t$, A_j is of order N_j and defined by disjoint permutations I, P_j, Q_j. Moreover $P_jQ_j = Q_jP_j$. Applying the theorem to each $A_j (j = 1, 2, \cdots, t)$ proves the corollary.

COROLLARY 2. *Let A be an abelian matrix of order n with 4 ones in each row and column. Then $P(A) > |D(A)|$.*

Proof. Without loss we suppose A is defined by permutations I, P, Q, R where P, Q and R comute pairwise.

If $P(A) = |D(A)|$ then Corollary 1 implies that $n = 7e$ and there is a permutation X such that the $n \times n$ matrix defined by $I, X^{-1}PX, X^{-1}QX$ is the direct sum of C taken e times. Now on the letters $1, 2, \cdots, 7$, $X^{-1}PX$ and $X^{-1}QX$ must be the cycles $(1, 2, \cdots, 7)$ and $(1, 2, \cdots, 7)^3$ since these are the only cycles of C having length 7. Thus on the letters $1, 2, \cdots, 7$, $X^{-1}RX$ must equal $(1, 2, \cdots, 7)^d$ for some $d \not\equiv 0, 1, 3 \pmod 7$. The matrix formed from the first 7 rows and columns of the transformed A is then cyclic and defined by the differences $0, 1, 3, d \bmod 7$. Furthermore by Theorem 3, $d = 5$. However the 7×7 cyclic matrix B defined by differences $1, 3, 5 \bmod 7$ has $P(B) > |D(B)|$. Thus we cannot have $P(A) = |D(A)|$.

It seems to be a plausible conjecture that in Corollaries 1 and 2 the condition that A be abelian may be omitted. Little progress has been made in proving this but it is hoped that in time the full result will yield.

The final theorem will concern the determination of all cyclic matrices A for which $P(A) = |D(A)|$.

A *perfect difference set* mod n is by definition a set of integers $d_1, d_2, \cdots, d_\kappa$, $n - 1 = k(k - 1)$, such that every integer $1, 2, \cdots, n - 1$ is congruent mod n to exactly one of the numbers $d_i - d_j (1 \leqq i, j \leqq k)$. Difference sets have been studied extensively in connection with cyclic projective planes and designs (2.3) but for present purposes we are interested only in a unique role played by the perfect difference set mod 7.

It is readily verified that if A is a 7×7 cyclic matrix with $P(A) = |D(A)|$ then A is defined by a perfect difference set mod 7. Also if A_1 and A_2 are defined by perfect difference sets mod 7 then A_1 may be changed into A_2 by permutations of rows and columns.

THEOREM 6. *Let A by a cyclic 0, 1 matrix of order n defined by the differences $0, d_1, d_2 \bmod n$. Then $P(A) = |D(A)|$ if and only if $n = 7e$, $d_1 = ed_1'$, $d_2 = ed_2'$, where $0, d_1', d_2'$ is a perfect difference set* mod 7.

Proof. The sufficiency is a consequence of the following lemma.

LEMMA. *Let B be cyclic of order n and defined by the differences $d_1, d_2, \cdots, d_s \bmod n$. For $e \geqq 1$ a positive integer, let B_e be the cyclic matrix of order en defined by the differences $ed_1, ed_2 \cdots, ed_s \bmod en$. Then by simultaneous permutations of rows and columns B_e may be transformed into the direct sum of B taken e times.*

Proof. Let B_t denote the $n \times n$ matrix formed from the intersections of the rows $t, e+t, \cdots, (n-1)e+t$ and columns $t, e+t, \cdots, (n-1)e+t$ of B_e. Here t is a fixed integer on the interval $1 \leqq t \leqq e$, We prove $B_t = B$.

Suppose $1 \leqq i, j \leqq n$. There is a 1 in row $(i-1)e+t$, column $(j-1)e+t$ of B_e if and only if for some k, $1 \leqq k \leqq s$,

$$(j-1)e + t \equiv (i-1)e + t + ed_\kappa \pmod{en} .$$

This congruence holds if and only if $j \equiv i + d_\kappa \pmod n$. Thus for each t, $1 \leqq t \leqq e$, $B_t = B$. Thus the matrix B_e contains e principal minors B, and these minors are disjoint from one another. This means that by simultaneous permutations of rows and columns we may write B_e in the desired form.

The proof of the necessity is by induction. The theorem is true for $n = 3$. Let B be cyclic of order $N (3 \leqq N < n)$ and defined by differences $0, a, b \bmod N$ and suppose that $P(B) = |D(B)|$. Then the induction hypothesis asserts that $N = 7l$, $a = a'l$ and $b = b'l$ where $0, a', b'$ form a perfect difference set mod 7.

Now let $P(A) = |D(A)|$ and consider the permutation group G generated by $(1, 2, \cdots, n)^{d_1}$ and $(1, 2, \cdots, n)d^2$. If G is transitive then Theorem 6 follows by Theorem 5. If G is intransitive then $(d_1, d_2, n) = t > 1$ and we may define a cyclic matrix B of order n/t by the differences $0, d_1/t, d_2/t \bmod n/t$. By the lemma, $P(B) = |D(B)|$. The induction completes the proof.

BIBLIOGRAPHY

1. König, Dénes, *Theorie der Endlichen und Unendlichen Graphen*, Chelsea, New York, (1950), 170–178.

2. Hall, Jr. Marshall, *Cyclic projective planes*, Duke Math. J. **14** (1947), 1079–1090.

3. Hall Marshall and H. J. Ryser, *Cyclic incidence matrices*, Can. Jour. Math., **3** (1951), 495–502.

THE OHIO STATE UNIVERSITY,

FLORIDA STATE UNIVERSITY