PACIFIC JOURNAL OF MATHEMATICS
Vol. 58, No. 2, 1975

THE UNIVERSAL FLIP MATRIX AND THE GENERALIZED FARO-SHUFFLE

ROBERT E. HARTWIG AND S. BRENT MORRIS

The permutation matrix P which flips a left direct product of two matrices into a right direct product is investigated on the basis of the generalized out faro-shuffle. Expressions are derived for the characteristic and minimal polynomials as well as the determinant and trace of P.

1. Introduction. One of the most interesting and lesser known matrices in the theory of left direct products, [7] p. 81, is the permutation matrix P, whose (i, j) block entry is the $m \times n$ unit matrix $E_{ji} = [\delta_{si}\delta_{rj}]$, $i = 1, \cdots, n$ $j = 1, \cdots, m$ namely

$$P = P_{m,n} = \begin{bmatrix} E_{11}E_{21} \cdots E_{m1} \\ E_{12} \qquad\quad \vdots \\ \vdots \qquad\quad \vdots \\ E_{1n} \cdots E_{mn} \end{bmatrix} = P_{n,m}^{T}.$$

The reason being, that for *any* pair of matrices $A_{m\times m}$, $B_{n\times n}$

$$P(A \otimes B)P^{-1} = B \otimes A, \tag{1}$$

i.e. P flips the order in any left direct product or equivalently converts a left direct product into a right direct product. If A and B are finite group representations then P represents the isomorphism relating the direct products of the two groups. In this note we give a short matrix proof of this result, which is valid over any commutative ring R with identity 1, and derive some further properties of the matrix P, after identifying the permutation Π associated with P with the generalized out faro-shuffle for a 1-dimensional deck of mn cards [9] [2]. In particular we shall give expressions for the characteristic and minimal polynomials of P in terms of m and n.

Throughout this paper we assume that all our matrices are over a commutative ring R with unity and char $R \neq 2$. Whenever necessary we shall first prove the result for real matrices, then specialize to integer matrices and employ Theorem 11 of [8], p. 49, to obtain the corresponding result for commutative rings with unity. In fact when working with matrices whose entries are integer multiples of $1 \in R$, we

may, if char R is zero or prime, just as well work with integer matrices. It is a well known fact that for *any* permutation matrix $P = [\mathbf{e}_{i_1}, \cdots, \mathbf{e}_{i_n}]$, where $\mathbf{e}_i$ is the ith unit vector, $P^T = P^{-1}$. For a real matrix P this says that P is real orthogonal and hence normal and simple.

The all important observation is now that if Π is the permutation associated with P, then the reduction of Π to a product of cycles, corresponds to a permutation similarity transformation on the matrix P, which reduces P to its weak cyclic canonical form, i.e.

$$\Pi \to \mathscr{C}_1 \mathscr{C}_2 \cdots \mathscr{C}_k \tag{2}$$

$$P \cong \operatorname{diag}[C_{k_1}, C_{k_2}, \cdots, C_{k_t}],\ k_1 \geqq k_2 \geqq \cdots \geqq k_t \geqq 1,$$

where

$$C_k = \begin{bmatrix} 0 & \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & \ddots & & & & 0 \\ \cdot & \cdot & \cdot & & & \vdots \\ \cdot & & \cdot & \cdot & & \vdots \\ 0 & \cdot & \cdot & & 1 & 0 \end{bmatrix}_{k \times k}$$

is the $k \times k$ cyclic matrix, which is also the lower companion matrix $L(\lambda^k - 1)$, for $\lambda^k - 1$. We remark that this canonical form is in general *not* equal to the Frobenius (rational) canonical form since $k_i \nmid k_{i-1}$ is general. Also since each C_k is *irreducible*, [3] Vol. 2, p. 62, (as its graph is strongly connected), the canonical form of (2) coincides with the canonical decomposition of a non-negative reducible matrix into a direct sum of nonnegative irreducible matrices.

Since this reduction only involves 0 and 1, it is valid over any ring with 1, in particular it is valid over any commutative ring R with 1, for which we may define the concept of the characteristic polynomial $\Delta(\lambda)$ of P, [8] p. 163. The characteristic polynomial may indeed be written as

$$\Delta(\lambda) = \prod_{i=1}^{t} (\lambda^{k_i} - 1) = \prod_{p=1}^{N} [\lambda^{\theta(p)} - 1]^{1/\theta(p)} = |P|\, \lambda^N \Delta\left(\frac{1}{\lambda}\right), \tag{3}$$

where $\theta(p)$ is the order of the element p in the permutation Π, i.e.

$$\Pi^{\theta(p)}(p) = 1, \quad \Pi^k(p) \neq 1 \quad \text{for} \quad k < p. \tag{4}$$

Even though in general the minimal polynomial ψ may not exist, i.e. the null ideal is not principal, [8] p. 166, it will exist for special matrices such

as permutation and cyclic matrices. It is easily seen that $\lambda^k - 1$ is an annihilating polynomial for C_k, and that in fact it is minimal, for if $q(\lambda) = q_0 + q_1\lambda + \cdots + q_s\lambda^s$ is any annihilating polynomial of lower degree, i.e. $s < k$, then

$$q(C_k) = \begin{bmatrix} q_0 & 0 & \cdots & q_s & \cdots & q_1 \\ q_1 & & & & & q_s \\ \vdots & & & & & \\ q_s & & & & & 0 \\ 0 & q_s & & \cdots & & q_0 \end{bmatrix} = 0 \text{ implies that}$$

$q_i = 0$, $i = 0, \cdots, s$. Since $\lambda^k - 1$ is therefore a *monic* minimal polynomial the division algorithm for $R[\lambda]$ shows that $\psi = \lambda^k - 1$ divides every other annihilating polynomial and is hence unique.

Similarly we may define the minimal annihilating polynomial $\psi_x(\lambda)$ for a vector $\mathbf{x}$ with respect to the matrix P, [3] vol. 1, p. 176, in particular (4) becomes in matrix language $\psi_{e_p}(\lambda) = \lambda^{\theta(p)} - 1$.

The minimal polynomial may now be written from (2) as

$$\psi(\lambda) = \operatorname*{LCM}_{i=1,\cdots,t} (\lambda^{k_i} - 1) = \operatorname*{LCM}_{p=1,\cdots,n} (\lambda^{\theta(p)} - 1), \tag{5}$$

in which the latter may be interpreted in matrix notation as $\psi(\lambda) = \mathrm{LCM}(\psi_{e_i}(\lambda))$, where the $\{\mathbf{e}_i\}$ form a spanning set for R^n, [3] p. 176. Incidentally (3) and (5) are related as usual by $\psi \mid \Delta \mid \psi^n$, even for our ring R. Moreover we shall see that we may even talk about the number of linearly independent eigenvectors associated with the eigenvalues $\lambda = \pm 1$.

We note that if $r = \theta(\Pi)$ is the order of the permutation Π, then in general $\psi(\lambda) \neq \lambda^r - 1$, as may be seen from the example $\Pi = (1, 2)(3, 4, 5)$,

$$P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

for which $\theta(\Pi) = 6$, but $\psi(\lambda) = (\lambda + 1)(\lambda^3 - 1)$.

We shall see, however, that for our particular permuation matrix this cannot happen. We base this claim on the following result.

THEOREM 1. *If P is a permutation matrix over ring R, associated with permutation Π, which has cycles of order $k_1 \geqq k_2 \geqq \cdots \geqq k_t \geqq 1$, and*

elements of order $\theta(p_{i_1}) \geqq \theta(p_{i_2}) \geqq \cdots \geqq \theta(p_{i_N}) \geqq 1$, *and if* $r = \theta(\Pi) = \mathrm{LCM}(k_i) = \mathrm{LCM}(\theta(p_{i_j}))$ *then*

(i) $\psi(\lambda) = \lambda^r - 1$

(ii) $k_1 = r$

(iii) $\theta(p_{i_1}) = r$

are equivalent.

Proof. (ii) $\Rightarrow$ (i) This follows from (2) since $k_i \mid r$ implies that $\lambda^{k_i} - 1 \mid \lambda^r - 1$. (i) $\Rightarrow$ (ii) If $k_i < r$ then $k_i \mid r$ implies that $\lambda^r - 1 = (\lambda^{k_i} - 1)\phi_r(\lambda) f_i(\lambda)$, where $\phi_r(\lambda)$ is the rth cyclotomic polynomial, [5] p. 321. On the other hand

$$\lambda^r - 1 = \operatorname*{LCM}_{i=1,\cdots,t} (\lambda^{k_i} - 1) = \mathrm{LCM}(\phi_r(\lambda) \cdot (\lambda^{k_i} - 1) \cdot f_i)$$
$$= \phi_r \, \mathrm{LCM}((\lambda^{k_i} - 1) f_i),$$

which is clearly impossible. Hence $k_1 = r$. The last result follows in a similar fashion.

For the case $t = 2$, Theorem 1 is a special case of the following result.

THEOREM 2. *Let* R *be a commutative ring with unity, let* $f, g \in R(\lambda)$ *be monic polynomials over* R *and let* $\partial f \leqq \partial g$, *where* ∂ *denotes degree.*

(a) *If one of the following holds:*

(i) $f \mid g$

(ii) $\partial f \nmid \partial g$

then

$$(*) \qquad r = \partial \mathrm{LCM}(f, g) \leqq \mathrm{LCM}(\partial f, \partial g) = s.$$

(b) *Equality in* $(*)$ *implies that* $\partial f \mid \partial g$,

(c) *If* $f = \lambda^k - 1$, $g = \lambda^l - 1$ *then* $f \mid g$ *if and only if* $\partial f \mid \partial g$ *if and only if* $r = s$.

Proof. (a)(i) $f \mid g$ implies that $r = \partial g \leqq s$. (ii) $\partial f \nmid \partial g$ then $s \neq \partial g$ and so $s \geqq 2\partial g$. Whence $s \geqq 2\partial g \geqq \partial f + \partial g \geqq r$.

(b) Let $r = \partial \mathrm{LCM}(f, g) = \mathrm{LCM}(\partial f, \partial g) = s$, and assume $\partial f \nmid \partial g$ so that $\partial f < \partial g$. Now $\partial f \leqq \partial g \leqq r \leqq \partial f + \partial g$, but $\partial f \nmid \partial g$ implies that $s \geqq 2\partial g$ or $2\partial g \leqq s = r \leqq \partial f + \partial g$, i.e. $\partial g \leqq \partial f$ which is a contradiction.

(c) Clear, as $(\lambda^k - 1) \mid (\lambda^l - 1)$ if and only if $k \mid l$.

2. The universal flip matrix. The flip property (1) of the matrix P is based on the following column Lemma, which may be generalized to commutative rings with 1, **[12] [11] [4].**

COLUMN LEMMA. *If* $X = [\mathbf{x}_1, \cdots, \mathbf{x}_n]$ *and* $\operatorname{col}(X) = [\mathbf{x}_1^T, \cdots, \mathbf{x}_n^T]^T$, *then*

$$\operatorname{col}(AXB) = (B^T \otimes A)\operatorname{col}(X). \tag{6}$$

In particular $\operatorname{col}(\mathbf{ab}^T) = \mathbf{b} \otimes \mathbf{a}$.

Note also that $\operatorname{col}(\cdot)$ is a module isomorphism from $R_{m\times n}$ onto $R_{mn\times 1}$.

It is easily verified that for *any* $m \times n$ matrix M,

$$P_{m,n}^T \operatorname{col}(M) = \operatorname{col}(M^T) = P_{n,m} \operatorname{col}(M), \tag{7}$$

which is in fact the basis to our card shuffling interpretation for Π. Combining (6) and (7) we have for all $A \in R_{m\times k}$, $B \in R_{n\times 1}$, $X \in R_{l\times k}$,

$$(A \otimes B)\operatorname{col}(X) = \operatorname{col}(BXA^T) = P_{n,m} \operatorname{col}(A X^T B^T)$$
$$= P_{n,m}(B \otimes A)\operatorname{col}(X^T) = P_{n,m}(B \otimes A)P_{l,k}^T \operatorname{col}(X).$$

Since this holds for all $\operatorname{col}(X)$, equation (1) follows when $k = m$ and $l = n$.

It also follows immediately that if $A_i \in R_{m\times m}$, $B_i \in R_{n\times n}$ then

$$P\left(\sum_{i=1}^{k} A_i \otimes B_i\right) P^{-1} = \sum_{i=1}^{k} B_i \otimes A_i. \tag{8}$$

Further note that

$$P^T(\mathbf{a} \otimes \mathbf{b}) = P^T \operatorname{col}(ba^T) = \operatorname{col}(ab^T) = \mathbf{b} \otimes \mathbf{a}. \tag{9}$$

Let us now turn to a more detailed analysis of the flip matrix P. We begin by considering the simplest case where $m = n$, in which case we only need (7) and no explicit expression for $\Pi(p)$ is needed.

Case 1. $m = n$. It is clear that $P^T = P = P^{-1}$ and hence $\psi(\lambda) = \lambda^2 - 1$, and $\Delta(\lambda) = (\lambda - 1)^p(\lambda + 1)^q$ where $p + q = N = mn$. To calculate Δ we can either evaluate $|\lambda I - P|$ directly, which is straightforward but tedious, or make us of the following important consequence of (7).

LEMMA 1. *Over any commutative ring R with unity, there exist a one-to-one correspondence between the numbers of linearly independent*

solutions to $P\mathbf{a} = \pm\mathbf{a}$ *and the number of linearly independent solutions to* $\operatorname{col}(A) = \pm\operatorname{col}(A^T)$, *in the sense that each side contains exactly the same number of independent parameters.*

Proof. If $P\mathbf{a} = \pm\mathbf{a}$, let $A_{m\times n} = \operatorname{col}^{-1}(\mathbf{a})$ and use (7). Conversely again use (7).

In the case $m = n$, the number of linearly independent solutions to $\operatorname{col}(A) = \operatorname{col}(A^T)$ is *exactly* the number of symmetric matrices over R, i.e. $\frac{1}{2}n(n+1)$, while the number of linearly independent solutions to $\operatorname{col}(A) = -\operatorname{col}(A^T)$ is exactly the number of skew-symmetric matrices over R, i.e. $\frac{1}{2}n(n-1)$. For our *real* permutation matrix this says that P has exactly $\frac{1}{2}n(n\pm 1)$ independent eigenvectors associated with $\lambda = \pm 1$, and since the geometric multiplicity ν_i of λ_i is bounded above by the algebraic multiplicity n_i of λ_i (with equality over the complex field), it follows that

$$\Delta(\lambda) = (\lambda+1)^{n(n-1)/2}(\lambda-1)^{n(n+1)/2} = (\lambda-1)^n(\lambda^2-1)^{n(n-1)/2}. \tag{10}$$

Again this holds also over R since (10) is really a consequence of the identities $\sigma_k = \Sigma\,|P_\alpha^\alpha|$, between the coefficients σ_k of Δ and the kth order principal minors $|P_\alpha^\alpha|$ of P, $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_k)$. These identities are also valid over the integers and hence by Theorem 11, [8] p. 49, remain valid over R.

It is further easily seen that the elementary divisors of P over $\mathbf{Z}$ are $\lambda \pm 1$, with multiplicities $n(n\pm 1)/2$ respectively. Let us now turn to the most general case $m \neq n$ and without loss of generality assume that $m < n$.

3. The case $m \neq n$. In this case there is no symmetry, i.e. $P^T \neq P$, and we have to examine the permutation explicitly. First we observe from the structure of P that $P = 1 \oplus Q \oplus 1$ so that $\Delta_p = (\lambda-1)^2\Delta_Q$ and $\psi_p = \psi_Q$. Hence $(\lambda-1)^2\psi_p \mid \Delta_p$. The determinant of P can also be obtained from the recurrence relation

$$|P_{m,n}| = (-1)^{(n-1)m(m-1)/2}\,|P_{m,n-1}|,$$

yielding

$$|P_{m,n}| = (-1)^{m(m-1)n(n-1)/4}. \tag{11}$$

The explicit form of the permutation Π is given by

$$\Pi = \begin{pmatrix} \overbrace{1,2,\quad n}^{k=0} & \overbrace{n+1, n+2 \cdots 2n}^{k=1} & \cdots & \underbrace{(m-1)n+1 \cdots mn}_{k=m-1} \\ 1, 1+m, 1+2m \cdots 1+(n-1)m & 2,2+2m \cdots 2+(n-1)m & \cdots & m \cdots \quad mn \end{pmatrix} \text{ i.e.} \tag{12}$$

$$\Pi(nk+l) = k+1+m(l-1) \quad k = 0, \cdots, m-1, \; l = 1, \cdots, n, \tag{13}$$

however in this form the 2 parameter permutation is almost intractable.

Instead we shall use the following representation.

$$\Pi(p) = mp - m + 1 \bmod(mn-1), \; p = 1, \cdots, mn, \tag{14}$$

which is *exactly* the generalized one-dimensional out faro-shuffle [10]. In this shuffle a deck of mn cards, labeled from top to bottom, is cut into m portions of n cards, and each portion is given in clockwise fashion to one of m players seated at a circular table, starting with the dealer. If, starting with the dealer, in clockwise fashion, each player plays his top card when it is his turn, until all cards have been played, we obtain the permutation Π, labeled from the bottom cards up.

When $m = 2$ this reduces to the classical out faro-shuffle (in which an even deck of cards is cut in halves and then ruffled such that the first and the last cards remain in fixed positions) which is the basis to serveral remarkable card tricks [1], [2], [9].

From (14) we see that

$$\Pi^k(p) = m^k p - m^k + 1 \bmod(mn-1) \tag{15}$$

and hence

$$\Pi^k(p) = p \Leftrightarrow (m^k - 1)(p-1) \equiv 0 \bmod(mn-1). \tag{16}$$

From this it follows that the order of the element 2, $\theta(2)$, is the *smallest* integer k such that

$$m^k \equiv 1 \bmod(mn-1) \tag{17}$$

and that if $k = \theta(2)$, (16) holds for *any* $p = 2, 3, \cdots, mn-1$, i.e.

$$\Pi^{\theta(2)}(p) = p \text{ or } \theta(p) \mid \theta(2). \tag{18}$$

In terms of annihilating polynomials this says that $\psi_{e_p}(\lambda) = \lambda^{\theta(p)} - 1 \mid \lambda^{\theta(2)} - 1$. Thus $r = \theta(\Pi) = \theta(2) \leqq mn - 1$, since the order of a group element divides the order of the group, and thus by Theorem 1,

$\psi(\lambda) = \lambda^r - 1$. We may simplify (16) by setting $d = gcd(p-1, mn-1)$, $p = 1, 2, \cdots, mn$, to obtain

$$(19) \qquad (m^k - 1)\left(\frac{p-1}{d}\right) \equiv 0 \bmod \left(\frac{mn-1}{d}\right) \text{ or}$$

$$m^k \equiv 1 \bmod \left(\frac{mn-1}{d}\right).$$

Thus $\theta(p)$ is the exponent to which m belongs modulo $(mn-1)/d$, which clearly depends on d only. Substituting this in (3) yields Δ. We note that even though the order of each cycle divides $\theta(2)$, they need *not* be *nested*, i.e. need not divide each other, as seen from the example $m = 2$, $n = 106$, $\theta(6) = 6$, $\theta(8) = 4$.

The question that remains is how many cycles of a given order are contained in Π? This we now examine on the basis of (19). We first state a result that holds for any permutation matrix P.

THEOREM 3. *If P is any $N \times N$ permutation matrix over R, with associated permuation Π, as given in (3), and if $\phi_i(\lambda)$ is the ith cyclotomic polynomial of degree $\partial\phi_i(\lambda) = \Phi_i(\lambda)$, the Euler function at i, then*

(i) $\Delta(\lambda) = \prod_{i=1}^{k_1} \phi_i^{n_i}(\lambda)$, *where n_i is the number of cycles in Π whose order is divisible by i.*

(ii) $\psi(\lambda) = \prod_{i=1}^{k_1} \phi_i^{m_i}(\lambda)$, *where $m_i = 1$ if Π has a cycle of order divisible by i, and $m_i = 0$ otherwise.*

(iii) *If the characteristic of R is zero and i divides some cycle of order k_j, then*

$$(20) \qquad \dim \ker[\phi_i(P)] = \partial[\phi_i^{n_i}(\lambda)] = n_i \Phi(i).$$

Proof. (i) From (3) we have that $\Delta = \prod_{i=1}^{t}(\lambda^{k_i} - 1) = \prod_{i=1}^{t} \prod_{d|k} \phi_d(\lambda)$. Clearly $\phi_s(\lambda)$ will appear exactly *once* in each factor $\prod_{d|k_i} \phi_d$, for $s \mid k_i$. (ii) Now $\psi(\lambda) = \mathrm{LCM}_i(\lambda^{k_i} - 1) = \mathrm{LCM}\{\prod_{d|k_i} \phi_d, \cdots, \prod_{d|k_t} \phi_d\}$. It is easily seen that $\phi_1(\lambda) = \lambda - 1$ appears in each term, while $\phi_s(\lambda)$ will appear in the LCM if and only if $\exists k_i$ such that $s \mid k_i$. Hence

$$\psi = \prod_{i=1}^{k_1} \phi_i^{m_i}(\lambda), \quad \text{where} \quad m_i = \begin{cases} 1 & \text{if } i \mid k_j \text{ some } j \\ 0 & \text{otherwise} \end{cases}.$$

In particular $m_1 = 1 = m_{k_1}$. (iii) Since $\phi_i(\lambda)$ is monic with integer coefficients, $\phi_i(P)$ is an integer matrix with entries from $\langle 1 \rangle$, the subring generated by $1 \in R$. If char $R = 0$, then $\langle 1 \rangle$ is isomorphic to $\mathbf{Z}$, the ring of rational integers, and we may consider the left hand side of (20) as the

number of independent solutions to $\phi_i(P)\mathbf{x} = \mathbf{0}$ over $\mathbf{Z}$. But this number is equal to the number of independent solutions over Q, the field of rationals. Now since the ϕ_i are pairwise coprime and *irreducible* over Q, we may apply the Primary Decomposition Theorem, **[6]** p. 219, to yield the desired identity.

When char $R = p$, a prime, then $\langle 1 \rangle$ is isomorphic to $\mathbf{Z}_p$, which is a field, however in this case $\phi_i(\lambda)$ may be reducible over $\mathbf{Z}_p$, as seen from $\phi_2(\lambda) = \lambda^2 + \lambda + 1 = (\lambda + 2)^2$ over $\mathbf{Z}_3$. As a Corollary to Theorem 3, we see that the geometric and algebraic multiplicities of the eigenvalue $\lambda = 1$ are both equal to the number of cycles in Π. This is indeed valid over any R, as seen from (2), because $C_k\mathbf{x} = \mathbf{x}$ clearly has only one independent solution $[\alpha, \alpha, \cdots, \alpha]^T, \alpha$ *arbitrary. Hence the total number of independent parameters in the general solution to* $P\mathbf{a} = \mathbf{a}$ equals the number of cycles in Π. Similarly for the eigenvalue $\lambda = -1$, the algebraic multiplicity in Δ yields the number of even cycles, in Π, if any, while $C_k\mathbf{x} = -\mathbf{x}$ has only the zero solution when k is odd and char $R \neq 2$, and yields exactly one independent solution $[\alpha, \cdots, \alpha]^T, \alpha$ arbitrary, when k is even.

Returning to our flip matrix we conclude from Theorem 3 that the number of independent solutions to $\operatorname{col}(A) = \mp \operatorname{col}(A^T)$ is exactly the number of (even) cycles in Π.

The trace of the matrix P is exactly the number of cyles of order 1 in π i.e. $\#\{p \mid \Pi(p) = p, p = 1, \cdots, mn\}$. Using (14) this may be calculated from

$$(m-1)(p-1) \equiv 0 \bmod (mn-1) \text{ or}$$

$$m \equiv 1 \bmod \left(\frac{mn-1}{d}\right), \quad d = \text{g.c.d.}(p-1, mn-1).$$

Thus

$$\operatorname{Tr}(P) = \#\{p; (mn-1) \mid (p-1)(m-1), p = 1, \cdots, mn-1\},$$

which in the symmetric case reduces to n as then each $E_{ii}\, i = 1, \cdots, n$ has a 1 on the diagonal.

Since the order of a cycle equals $r = \theta(\Pi)$ if and only if $d = 1$, it follows that we have $(mn-1)/r$ cycles of order r, where $\Phi(k)$ is Euler's function. Similarly if

$$\Phi\left(\frac{k}{d}\right) = \#\{s \mid s < k, \gcd(s,k) = d\},$$

and if $\{d_p\}$ are the possible values for $\gcd(p-1, mn-1)$, as p ranges from 2 to $mn-1$, we can associate through (19) with each d_p a *unique* order k_p, with $k_p = r$ corresponding to $d_p = 1$.

Consequently we have $\Phi((mn-1)/d_p)/k_p$ cycles of length k_p, so that Δ may be written as

$$\Delta = (\lambda^2 - 1) \prod_p (\lambda^{k_p} - 1)^{\Phi(mn-1/d_p)/k_p} \tag{21}$$

and the total number of cycles equals

$$\nu_1 = 2 + \sum_p \Phi\left(\frac{mn-1}{d_p}\right) \Big/ k_p, \tag{22}$$

while the number of even cycles equals

$$\nu_{-1} = \sum_{\substack{p \\ k_p \text{ even}}} \Phi\left(\frac{mn-1}{d_p}\right) \Big/ k_p.$$

A few of the characteristic and minimal polynomials for $P_{m,n}$ are given below

m	n	ψ	Δ	Π
2	3	λ^4-1	$(\lambda-1)^2(\lambda^4-1)$	(2345)
2	4	λ^3-1	$(\lambda-1)^2(\lambda^3-1)^2$	(235)(476)
3	3	λ^2-1	$(\lambda^2-1)(\lambda+1)(\lambda^2-1)^3$	(24)(37)(5)(6, 8)(9)
3	4	λ^5-1	$(\lambda^2-1)(\lambda^5-1)^2$	(2, 4, 10, 6, 5) $\times$ (3, 7, 8, 11, 9)

The first five cyclotomic polynomials are given by

$$\phi_1 = \lambda - 1, \quad \phi_2 = \lambda + 1, \quad \phi_3 = \lambda^2 + \lambda + 1, \quad \phi_4 = \lambda^2 + 1$$
$$\phi_5 = \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1.$$

ACKNOWLEDGEMENTS. We wish to thank Professors Carlitz and Luh for their encouragement and many stimulating and informative discussions.

REFERENCES

1. A. Elmsley, *Mathematics of the Weave shuffle*, The Pentagram, **11**, # 9, (1957), 70–71, **11**, # 10, (1957), 77–79, **11**, # 11 (1957), 85.
2. S. W. Golomb, *Permutations by cutting and shufflling*, SIAM Rev. #4 (1961), 293–297.
3. F. R. Grantmacher, *The theory of Matrices*, vol. 1,2 Chelsea, N. Y. 1960.

4. R. E. Hartwig, *The resultant and the matrix equation* $AX = XB$, SIAM J. Appl. Math., **22** (1972), 538–544.
5. I. N. Herstein, *Topics in Algebra*, Ginn and Co. Mass., 1964.
6. K. Hoffman and R. Kunze, *Linear Algebra*, Prentice Hall, N. J. 1971.
7. C. C. MacDuffee, *The Theory of Matrices*, Chelsea, N. Y.
8. N. H. McCoy, *Rings and Ideals*, Carus Monogrpahs # 8
9. S. B. Morris, ***The basic mathematics of the Faro-shuffle***, **to be published in Pi Mu Epsilon J.**
10. S. B. Morris, *The generalized Faro-shuffle*, to be published.
11. H. Neudecker, *A note on the Kronecker matrix products and matrix equation systems*, SIAM J. Appl. Math., **17** (1969), 603–606.
12. W. E. Roth, *On direct Product matrices*, Bull. Amer. Math. Soc., **40** (1934), 461–468.

Received February 11, 1974.

NORTH CAROLINA STATE UNIVERSITY AND DUKE UNIVERSITY