ISRAEL JOURNAL OF MATHEMATICS **143** (2004), 141–156

# THE COMBINATORICS OF A THREE-LINE CIRCULANT DETERMINANT

BY

NICHOLAS A. LOEHR*, GREGORY S. WARRINGTON* AND HERBERT S. WILF

*Department of Mathematics, University of Pennsylvania*
*Philadelphia, PA 19104-6395, USA*
*e-mail: nloehr@math.upenn.edu, gwar@math.upenn.edu, wilf@math.upenn.edu*

ABSTRACT

We study the polynomial $\Phi(x,y) = \prod_{j=0}^{p-1}(1 - x\omega^j - y\omega^{qj})$, where $\omega$ is a primitive $p$th root of unity. This polynomial arises in CR geometry [1]. We show that it is the determinant of the $p \times p$ circulant matrix whose first row is $(1, -x, 0, \ldots, 0, -y, 0, \ldots, 0)$, the $-y$ being in position $q+1$. Therefore, the coefficients of this polynomial $\Phi$ are integers that count certain classes of permutations. We show that all of the permutations that contribute to a fixed monomial $x^r y^s$ in $\Phi$ have the same sign, and we determine that sign. We prove that a monomial $x^r y^s$ appears in $\Phi$ if and only if $p$ divides $r + sq$. Finally, we show that the size of the largest coefficient of the monomials in $\Phi$ grows exponentially with $p$, by proving that the permanent of the circulant whose first row is $(1, 1, 0, \ldots, 0, 1, 0, \ldots, 0)$ is the sum of the absolute values of the monomials in the polynomial $\Phi$.

## 1. Introduction and statement of results

The stimulus for this work lies in the study [1] by John D'Angelo of invariant holomorphic mappings on hypersurfaces. In that work a construction is given of a certain real-analytic function $\Phi$ from which one can define the desired invariant mappings. As a source of examples the author used the familiar lens spaces $\mathcal{L}(p,q)$, and he showed that the invariant function in [1] determines a polynomial in two real variables we call $\Phi$. Specifically,

$$\Phi(x,y) = \Phi_{p,q}(x,y) = \prod_{j=0}^{p-1}(1 - x\omega^j - y\omega^{qj}), \tag{1}$$

* Supported by NSF Postdoctoral research grants.
Received December 24, 2003

where $\omega$ is a primitive $p$th root of unity. For example,

$$\Phi_{8,3}(x,y) = 1 - x^8 - 8x^5y - 12x^2y^2 + 2x^4y^4 - 8xy^5 - y^8.$$

Hence in the case of lens spaces, $\Phi$ is a polynomial in $x, y$ that has certain interesting extremal properties. For further investigation it is desirable to know more about these polynomials. In particular,

1. Are their coefficients always integers?
2. If so, what integers are they?
3. Precisely which monomials in $x, y$ appear in $\Phi_{p,q}(x,y)$?
4. Which of the coefficients of the monomials that appear are positive and which are negative?

Question 1 was already answered in the affirmative in [1]. In Section 2 we will give a particularly simple proof (and a combinatorial interpretation to the coefficients), by exhibiting $\Phi_{p,q}$ as the determinant of a certain $p \times p$ matrix that has integer entries.

Question 2 is harder. As a partial answer, in Section 3 as a corollary of Lemma 11, we will prove the following:

THEOREM 1: *In the expansion of the polynomial*

$$\Phi_{p,q}(x,y) = \sum_{r,s} a_{p,q}(r,s) x^r y^s,$$

*the coefficient $a_{p,q}(r,s)$ is equal, aside from its sign, to the number of permutations $\sigma$ of $p$ letters such that the differences*

$$\{(\sigma(j) - j) \mod p\}_{j=1}^{p}$$

*take the values 0, 1, and $q$ with respective multiplicities $p - r - s$, $r$, and $s$. Furthermore, these permutations all have the same signs, and in fact, all have the same cycle type.*

Regarding Question 3, we obtain the following from Lemma 6 of Section 2 and Theorem 15 of Section 4:

THEOREM 2: *The monomials $x^r y^s$ that appear in $\Phi_{p,q}(x,y)$ (i.e., that have nonzero coefficients) are precisely those for which $p$ divides $r + sq$.*

That $p$ must divide $r + sq$ for $x^r y^s$ to appear with nonzero coefficient is by far the easier implication to prove. This necessity follows from the underlying geometry (see [1]) or, as we will show, from a simple counting argument.

Finally, Question 4 about the signs of the terms is settled by the following result which follows from Lemma 11 in Section 3.

THEOREM 3: *Let $a_{p,q}(r,s)x^r y^s$ be a monomial that appears in $\Phi_{p,q}(x,y)$. Then the sign of this monomial is positive (resp. negative) if the integer*

$$\gcd\Big(r, s, \frac{r+sq}{p}\Big)$$

*is even (resp. odd).*

In Section 5 we show that, for fixed $q$, the coefficients in $\Phi_{p,q}$ grow exponentially with $p$.

*Remark 4:* D'Angelo [2] shows that the polynomial $f(x,y) = 1 - \Phi(x,y)$ is congruent to $(x+y)^p \pmod p$ if and only if $p$ is prime.

*Remark 5:* One can also consider expressions of the form

$$\Theta_{p,q,t} = \prod_{j=0}^{p-1}(1 - x\omega^{tj} - y\omega^{qj}). \tag{2}$$

If $\omega^t$ is a primitive root of unity (i.e., $\gcd(t,p) = 1$), then $\omega^q = \omega^{tq'}$ for some $q'$. This implies that $\Theta_{p,q,t}$ equals $\Phi_{p,q'}$. (A similar statement can be made when $\gcd(q,p) = 1$.) This extends somewhat the set of $(p,q,t)$ to which our results apply, but the general case remains open. The permanents of certain matrices associated to the $\Theta_{p,q,t}$ are investigated in [4] (see, in particular, Lemma 12).

## 2. Circulant matrices

A $p \times p$ **circulant matrix** is a matrix of the form

$$C = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{p-1} \\ a_{p-1} & a_0 & a_1 & \dots & a_{p-2} \\ a_{p-2} & a_{p-1} & a_0 & \dots & a_{p-3} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix}.$$

Since such a matrix is completely specified by, for example, its first row, we will sometimes refer to it as $\mathrm{circ}(a_0, a_1, \dots, a_{p-1})$. A circulant matrix can be written as $C = g(C_0)$ where $C_0 = \mathrm{circ}(0,1,0,\dots,0)$ and $g(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_{p-1}t^{p-1}$. Since the eigenvalues of $C_0$ are the $p$th roots of unity, the eigenvalues of the general circulant matrix $C$ are $g(\omega)$, where $\omega$ runs through the $p$th roots of unity. Consequently, the determinant of any circulant matrix is the product of these eigenvalues, namely

$$\det C = \prod_{\omega^p=1} g(\omega).$$

The above observations are well known from the classical theory of circulant matrices. See, for example, [6].

If we take $g(t) = 1 - xt - yt^q$ we see that the polynomial $\Phi(x, y)$, whose study is the main object of this paper, is the determinant of $g(C_0)$, as stated above. From the form of $g$ we see at once that the polynomial $\Phi$ has integer coefficients, thus answering Question 1 by inspection.

If we write $\Phi(x, y) = \sum_{r,s} a(r, s)x^r y^s$, then we can give a combinatorial interpretation to the coefficients $a(r, s)$. Indeed, by expanding the circulant determinant

$$\Phi(x, y) = \det(I - xC_0 - yC_0^q)$$
$$= \begin{vmatrix} 1 & -x & 0 & \dots & 0 & -y & 0 & 0 \\ 0 & 1 & -x & \dots & 0 & 0 & -y & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 & -y \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ -x & 0 & 0 & \dots & -y & 0 & 0 & 1 \end{vmatrix},$$

we see that the coefficient of $(-1)^{r+s}x^r y^s$ is the sum of the signs of those permutations of $p$ letters that "hit" $r$ of the $x$'s in the matrix and $s$ of the $y$'s, the remaining values being fixed points. Thus, let $T_{p,q}(r, s)$ denote the set of all permutations $\sigma$ of $1, 2, \dots, p$ such that

1. $\sigma$ has exactly $p - r - s$ fixed points, and
2. for exactly $r$ values of $j$ we have $\sigma(j) - j$ congruent to 1 modulo $p$, and
3. for exactly $s$ values of $j$ we have $\sigma(j) - j$ congruent to $q$ modulo $p$.

Then $(-1)^{r+s}a(r, s)$ is the excess of the number of even permutations in $T_{p,q}(r, s)$ over the number of odd permutations in $T_{p,q}(r, s)$.

As an example, take $p = 5$ and $q = 3$. Then

$$\Phi(x, y) = 1 - x^5 - 5x^2y - 5xy^3 - y^5.$$

Let us check the coefficient of $x^2y$. The set $T_{5,3}(2, 1)$ consists of the following permutations of 5 letters:

$$\{1, 2, 4, 5, 3\}, \{1, 3, 4, 2, 5\}, \{2, 3, 1, 4, 5\}, \{2, 5, 3, 4, 1\}, \{4, 2, 3, 5, 1\}.$$

These are all even permutations, hence $-a(2, 1)$ is 5, as we also see by inspection of $\Phi$. Note that all of the permutations in $T_{5,3}(2, 1)$ have the same cycle structure, viz. a 3-cycle and two fixed points.

Our goal is to show the following:

- (Uniqueness) If $T_{p,q}(r, s)$ is nonempty, then every $\sigma \in T_{p,q}(r, s)$ has the same cycle structure. We will explicitly describe this cycle structure.

- (Existence) $T_{p,q}(r,s)$ is nonempty if and only if $p$ divides $r+sq$.

We first consider two special cases. If $r=s=0$, then $T_{p,q}(0,0)$ consists of the identity permutation. If $s=0$ and $r>0$, it is easy to see from the definitions that $T_{p,q}(r,0)$ is nonempty iff $r=p$, in which case the only element of this set is the cycle $(1,2,\ldots,p)$. In what follows, therefore, we assume $s>0$.

## 3. Uniqueness of cycle structure

It is convenient to introduce the following notation for a permutation $\sigma \in T_{p,q}(r,s)$. Write $\sigma$ uniquely (up to order) as a product of $k \geq 0$ disjoint cycles $C_1,\ldots,C_k$ of lengths greater than 1. If $k=0$, then $\sigma$ is the identity. This happens only in the trivial case $r=s=0$, so we assume $k>0$ from now on.

We represent each cycle $C_i$ by a pair $(x_i;w_i)$, where $x_i \in \{1,2,\ldots,p\}$ and $w_i$ is a word consisting of $r_i$ 1's and $s_i$ $q$'s. Here, $x_i$ is an arbitrary point appearing in the cycle $C_i$, $r_i+s_i$ is the number of points involved in the cycle, and the word $w_i$ gives the differences (mod $p$) between consecutive elements of the cycle starting at $x_i$. Formally, if $w_i = w_i(1)w_i(2)\cdots w_i(r_i+s_i)$, then

$$\sigma^t(x_i) \equiv x_i + \sum_{j=1}^{t} w_i(j) \pmod{p}, \quad \text{for } 0 \leq t \leq r_i+s_i. \tag{3}$$

(We take our residue system modulo $p$ to be the set $[p]=\{1,2,\ldots,p\}$.) For example, when $q=3$ and $p=10$, the pair $(4;3,1,1,3,1,1)$ represents the cycle $(4,7,8,9,2,3)$. The pair $(8;1,3,1,1,3,1)$ also represents this cycle.

LEMMA 6: *If $T_{p,q}(r,s)$ is nonempty, then $p$ divides $r+sq$.*

*Proof:* Take any $\sigma \in T_{p,q}(r,s)$, and describe $\sigma$ using the notation above. Each cycle $C_i$ has $r_i+s_i$ elements in it. Letting $t=r_i+s_i$ in (3) gives

$$x_i = \sigma^{r_i+s_i}(x_i) \equiv x_i + \sum_{j=1}^{r_i+s_i} w_i(j) \equiv x_i + r_i\cdot 1 + s_i\cdot q \pmod{p}.$$

Thus, $p$ divides $r_i+qs_i$ for each $i$. It is easy to see from the definitions that $r=r_1+\cdots+r_k$ and $s=s_1+\cdots+s_k$. Hence, $r+qs=\sum_{i=1}^{k}(r_i+qs_i)$ is also divisible by $p$. ∎

By the proof of the last lemma, $p$ divides all the quantities $r_i+qs_i$. So, given $\sigma \in T_{p,q}(r,s)$, we can define positive integers $\ell_i=(r_i+qs_i)/p$ and $\ell=(r+qs)/p=\sum_{i=1}^{k}\ell_i$.

LEMMA 7: *If $T_{p,q}(r,s)$ is nonempty, then $\gcd(r_i, s_i, \ell_i) = 1$ for $1 \leq i \leq k$.*

*Proof:* Fix $i$ between 1 and $k$. We assume that $\gcd(r_i, s_i, \ell_i) = d > 1$ and derive a contradiction. Set $r' = r_i/d$, $s' = s_i/d$, and $\ell' = \ell_i/d$. Since $r_i + qs_i = \ell_i p$, we have $r' + qs' = \ell' p$.

We claim that there exists a string of $r' + s'$ consecutive symbols in $w_i$ consisting of $r'$ 1's and $s'$ $q$'s.

To prove this, we start by factoring the word $w_i$ into $d$ subwords

$$w_i = v_1 v_2 \cdots v_d,$$

where each word $v_j$ has length $r' + s'$. For $1 \leq j \leq d$, let $v_j$ consist of $a_j$ 1's and $b_j$ $q$'s, where $a_j + b_j = r' + s'$. If $a_j = r'$ for any $j$, then the claim is true. If $a_j > r'$ for all $j$, then the total number of 1's in $w_i$ is greater than $r'd = r_i$, which is a contradiction. If $a_j < r'$ for all $j$, then the total number of 1's in $w_i$ is less than $r'd = r_i$, which is a contradiction. So we are reduced to the case where $a_{j_1} > r'$ for some $j_1$ and $a_{j_2} < r'$ for some $j_2$. Clearly, in this case we can choose $j_1$ and $j_2$ with $|j_2 - j_1| = 1$. We have (say)

$$v_{j_1} = x_1 x_2 \cdots x_{r'+s'},$$
$$v_{j_2} = v_{j_1+1} = x_{r'+s'+1} \cdots x_{2r'+2s'}.$$

Define a function $g$: $\{1, 2, \ldots, r' + s' + 1\} \to \mathbb{Z}$ by declaring $g(m)$ to be the number of 1's in the string $x_m x_{m+1} \cdots x_{m+r'+s'-1}$. Then $g(1) = a_{j_1} > r'$ and $g(r' + s' + 1) = a_{j_2} < r'$ and $|g(i+1) - g(i)| \leq 1$ for all $i$. Hence, there must exist some $m$ with $g(m) = r'$. The subword of $w_i$ of length $r' + s'$ beginning with $x_m$ must then contain $r'$ 1's and $s'$ $q$'s. This proves the claim.

By the claim, for some $j \geq 0$ there is a subword

$$w_i(j+1) w_i(j+2) \cdots w_i(j + r' + s')$$

consisting of $r'$ 1's and $s'$ $q$'s. Consider the elements

$$y = \sigma^j(x_i), \quad z = \sigma^{j+r'+s'}(x_i)$$

on the cycle $C_i$. On one hand, we have $y \neq z$ since $r' + s' = (r_i + s_i)/d$ is less than the length $r_i + s_i$ of $C_i$. On the other hand, (3) gives

$$z - y \equiv \sum_{m=j+1}^{j+r'+s'} w_i(m) \equiv r' + s'q = \ell' p \equiv 0 \pmod{p}.$$

Since $1 \leq y, z \leq p$, we get $y = z$, a contradiction. ∎

We will now precisely characterize the cycles in $C$. In order to avoid having to keep track of when $z + q \leq p$ in what follows, we introduce the following notation: For $z_1, \ldots, z_m \in [p]$ with $m \geq 3$, we write $\overrightarrow{z_1 \cdots z_m}$ if there exists a $j$ with $1 \leq j \leq m$ such that

$$z_j < \cdots < z_m < z_1 < \cdots < z_{j-1}. \tag{4}$$

If we think of $[p]$ being arranged in clockwise order around a circle, then $\overrightarrow{z_1 \cdots z_m}$ amounts to having the clockwise traversal from $z_1$ to $z_m$ encounter $z_i$ before $z_j$ if and only if $i < j$.

LEMMA 8: *Let $z_1, \ldots, z_m \in [p]$ and set $\pi(z) = z + q \pmod{p}$. Then*

$$\overrightarrow{z_1 \cdots z_m} \iff \overrightarrow{\pi(z_1) \cdots \pi(z_m)}. \tag{5}$$

*Proof:* Assume $\overrightarrow{z_1 \cdots z_m}$ and pick $j$ as in (4). Certainly

$$z_j + q < \cdots < z_m + q < z_1 + q < \cdots < z_{j-1} + q. \tag{6}$$

If $z_j + q > p$ or $z_{j-1} + q \leq p$, then we immediately obtain $\overrightarrow{\pi(z_1) \cdots \pi(z_m)}$. Otherwise, there is a minimal $t$ (with respect to the order $j < \cdots < m < 1 < \cdots < j-1$), $t \neq j$, such that $z_t + q > p$. Then the only nontrivial inequality in

$$\pi(z_t) < \cdots < \pi(z_{j-1}) < \pi(z_j) < \cdots < \pi(z_{t-1}) \tag{7}$$

is $\pi(z_{j-1}) < \pi(z_j)$. But this must be true as $z_{j-1} - p \leq 0 < z_j$ implies $\pi(z_{j-1}) = z_{j-1} + q - p < z_j + q = \pi(z_j)$. The other implication of (5) results from the above arguments applied to $\pi^{-1}$, which is the map sending $z$ to $z+p-q \pmod{p}$. ∎

LEMMA 9: *For $\sigma \in T_{p,q}(r, s)$, we must have $r_1 = r_2 = \cdots = r_k$ and $s_1 = s_2 = \cdots = s_k$.*

*Proof:* Let $C_k$ and $C_l$ be two distinct cycles in $T_{p,q}(r, s)$. For simplicity, we substitute $C, C', a, b, a', b'$ for $C_k, C_l, r_k, s_k, r_l, s_l$, respectively. Write

$$C = (x; v) \quad \text{where } v = 1^{\alpha_1} q \cdots 1^{\alpha_b} q,\ x \in [p], \text{ and } \sum_i \alpha_i = a. \tag{8}$$

In traversing the orbit of $x$ under $C$, we will refer to those $z$ for which $C(z) \equiv z + q \pmod{p}$ as "$q$-steps"; "1-steps" are defined analogously.

If $b$ were to be 0, then $a$ would equal $p$ and $C = (1, 2, \ldots, p)$. In this scenario, there are no nontrivial cycles disjoint from $C$. This contradicts our hypothesis. Hence, $b > 0$. Similarly, $b' > 0$. We wish to show that $b' \geq b$. If $b = 1$, there is nothing to prove, so assume furthermore that $b > 1$.

Set $d_1 = x$ and $e_1 = C^{\alpha_1}(x)$. Then, for $2 \leq i \leq b$, we recursively define $d_i = C(e_{i-1})$ and $e_i = C^{\alpha_i}(d_i)$. Note that $d_i$ is the image of the $(i-1)$-st $q$-step, and $e_i$ is the $i$-th $q$-step.

There exists a unique permutation $\tau$ such that $\tau(1) = 1$ and

$$\overrightarrow{d_{\tau(1)}e_{\tau(1)} \cdots d_{\tau(b)}e_{\tau(b)}}. \tag{9}$$

Notice that each $e_{\tau(j)}$ is a $q$-step of $C$. For brevity in what follows, we interpret the indices of $e$ and $d$, and the arguments of $\tau$, modulo $b$. Set

$$\begin{aligned} V_{\tau(j)} &= \{y \in [p] \colon C(y) = y \text{ and } \overrightarrow{e_{\tau(j)}ye_{\tau(j+1)}}\} \\ &= \{y \in [p] \colon C(y) = y \text{ and } \overrightarrow{d_{\tau(j)}yd_{\tau(j+1)}}\}. \end{aligned}$$

The equality of these two sets is due to the fact that each of the cyclic intervals $\{z \colon \overrightarrow{d_{\tau(j)}ze_{\tau(j)}}\}$ consists only of points moved by $C$.

Now let $z$ be moved by $C'$ (hence fixed by $C$). By (9), $z \in V_{\tau(j)}$ for a unique $j$. If $z$ is a 1-step of $C'$, then $C'(z) \in V_{\tau(j)}$ also as $C$ and $C'$ are disjoint. If $z$ is a $q$-step of $C'$, then $\pi(z) = C'(z)$. So by Lemma 8, since $\overrightarrow{e_{\tau(j)}ze_{\tau(j+1)}}$, we find that $\overrightarrow{d_{\tau(j)+1}C'(z)d_{\tau(j+1)+1}}$. Or, equivalently, that $C'(z) \in V_{\tau(j)+1}$. Iterating this argument, we see that the orbit of $z$ visits $V_{\tau(j)}, V_{\tau(j)+1}, V_{\tau(j)+2}, \ldots$ in turn. We conclude that $C'$ has at least $b$ $q$-steps. Then, by definition, $b' \geq b$. Arguing with the roles of $C$ and $C'$ switched, we find that $b = b'$.

To show that $a = a'$, it suffices to consider the equalities $a + bq = \ell p$ and $a' + bq = \ell' p$. Subtracting, $a - a' = (\ell - \ell')p$. Since $b = b' > 0$, we know that $0 \leq a, a' < p$. So $-p < a - a' < p$. It follows that $a = a'$. ∎

*Example 10:* Set $p = 32$ and $q = 17$. The cycle

$$(8, 9, 10, 11, 28, 13, 14, 15, 32, 1, 2, 3, 4, 21, 22, 23)$$

illustrated in Figure 1 can be written according to the conventions of (8) as

$$(8; 1^3 q q 1^2 q 1^4 q 1^2 q).$$

Notice that $a = 11$ and $b = 5$. The permutation $\tau$ obtained by reading the indices of the $V_j$ clockwise starting with $V_1$ is written in one-line notation as $\{1, 3, 5, 2, 4\}$. The values of the $d_j$ and $e_j$ are not illustrated in the figure, but

we mention, for example, that $d_{\tau(3)} = 21$ and $e_{\tau(3)} = 23$. We have also shown how, for some potential $C'$, that $C'(6) \in \{y\colon \overrightarrow{e_{\tau(5)}ye_{\tau(1)}}\}$ (as 6 is a 1-step for $C'$), but that $C'(7)$ is clearly forced to be in $V_{\tau(5)+1} = V_{4+1} = V_5$.

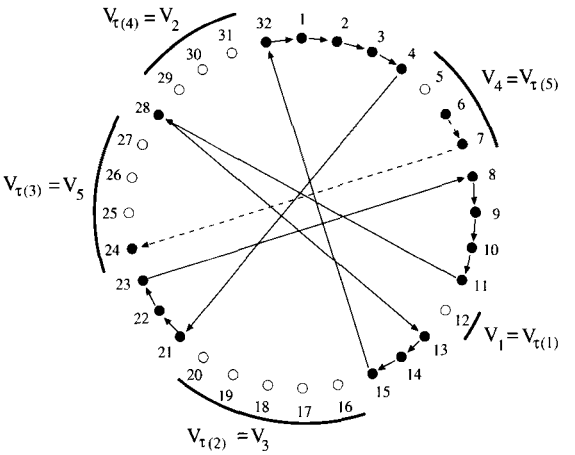


Figure 1. Illustration for Example 10.

LEMMA 11: *If $\sigma \in T_{p,q}(r,s)$, we must have $k = \gcd(r,s,\ell)$, $r_i = r/k$ for all $i$, and $s_i = s/k$ for all $i$. Thus, the cycle structure of all elements of $T_{p,q}(r,s)$ is uniquely determined by $p$, $q$, $r$, and $s$. Also, $\operatorname{sgn}(\sigma) = (-1)^{r+s+\gcd(r,s,\ell)}$.*

*Proof:* Take any $\sigma \in T_{p,q}(r,s)$. Since $\sum_{i=1}^{k} r_i = r$ and $\sum_{i=1}^{k} s_i = s$, Lemma 9 implies that we must have $r_i = r/k$ and $s_i = s/k$ for all $i$. Then, for each $i$,

$$\ell_i = (r_i + s_i q)/p = \frac{(r+sq)/p}{k} = \ell/k.$$

Note that $r_i$ and $s_i$ and (by Lemma 6) $\ell_i$ are all integers. By Lemma 7, $\gcd(r_i, s_i, \ell_i) = 1$. Therefore

$$k = k\gcd(r_i, s_i, \ell_i) = \gcd(kr_i, ks_i, k\ell_i) = \gcd(r,s,\ell).$$

The last statement of the lemma follows by noting that

$$\operatorname{sgn}(\sigma) = (-1)^{p-\operatorname{cyc}(\sigma)},$$

where $\operatorname{cyc}(\sigma)$ is the number of cycles in $\sigma$ (including 1-cycles). There are $p-r-s$ 1-cycles, so

$$\operatorname{sgn}(\sigma) = (-1)^{p-(k+p-r-s)} = (-1)^{r+s+\gcd(r,s,\ell)}. \qquad \blacksquare$$

We point out the fact that if $p$ is odd then the sign of $\sigma$ is $-1$ iff $r$ and $s$ are odd. (Note that Codenotti & Resta [5, Cor. 9] determined the fact that all $\sigma \in T_{p,q}(r,s)$ have the same sign when $p$ is prime.)

## 4. Construction of elements in $T_{p,q}(r,s)$

Assume $r + sq = \ell p$ and $\gcd(r, s, \ell) = 1$. Consider a lattice path

$$\nu = [\nu_0 = (0,0), \nu_1, \nu_2, \ldots, \nu_{r+s} = (r,s)]$$

from $(0,0)$ to $(r,s)$, where $\nu_i - \nu_{i-1}$ equals $(1,0)$ or $(0,1)$ for $i > 0$. Associate with $\nu$ a cycle $(z;v)$ in which $v$ is an $(r+s)$-tuple in $\{1,q\}^{r+s}$ (having $r$ 1's and $s$ $q$'s) as follows: If $\nu_i - \nu_{i-1} = (1,0)$, then let the $i$-th entry in $v$ be a 1; if $\nu_i - \nu_{i-1} = (0,1)$, then set the $i$-th entry in $v$ to be a $q$. We refer to these cases as "east" and "north" steps, respectively. We aim to show that if $\nu$ is chosen appropriately, then $(z;v)$ is a well-defined element of $T_{p,q}(r,s)$ for each $z \in [p]$. It is interesting to note that our construction of $\nu$ depends only on $r$ and $s$.

To determine $\nu$, start by setting $\nu_0 = (0,0)$ as above. Suppose the point $\nu_i = (x_i, y_i)$ is determined. Then set

$$\nu_{i+1} = \begin{cases} \nu_i + (1,0), & \text{if } sx_i \le ry_i, \\ \nu_i + (0,1), & \text{if } sx_i > ry_i. \end{cases} \tag{10}$$

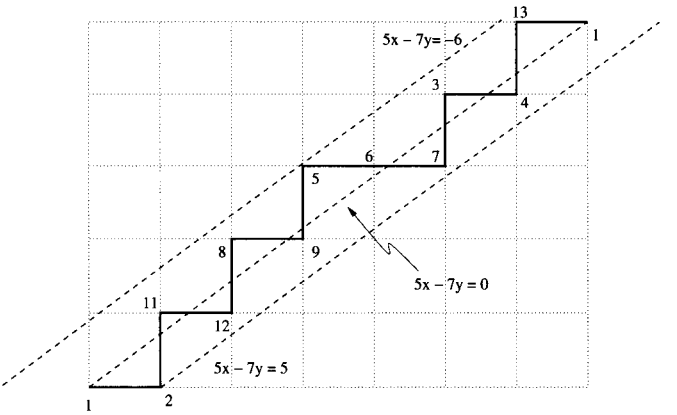


Figure 2. The path $\nu$ for $p = 13$, $q = 9$, $r = 7$ and $s = 5$.

In other words, go east if we are weakly above the line $sx - ry = 0$ and go north otherwise. (This is effectively the Freeman approximation used to draw

diagonal lines on a computer screen. As such, the word $v$ can also encode the continued fraction expansion for $r/s$; see [9].) Figure 2 gives an example of the construction. In the figure, $\nu_0 = (0,0)$ is labeled by $z = 1$. Each successive $\nu_i$ is labeled by the label of $\nu_{i-1}$ plus either 1 or $q$ according to whether an east or north step, respectively, separates the two vertices. Naturally, these labels are reduced modulo $p$. Then the label of $\nu_i$ is precisely $(z;v)^i(z)$. The pair $(z;v)$ is a well-defined cycle if and only if the only two vertices $\nu_i$ with equal labels are $\nu_0$ and $\nu_{r+s}$.

We first bound the number of 1-steps and $q$-steps that can appear between any two vertices $\nu_i$ and $\nu_j$.

LEMMA 12: *Determine $\nu$ as in (10). Let $0 \le i, j \le r+s$ and write $\nu_i = (x_i, y_i)$ and $\nu_j = (x_j, y_j)$. If $b = y_j - y_i$ and $a = x_j - x_i$, then $|as - br| \le r + s - 1$.*

*Proof:* We claim that $-r < sx_i - ry_i \le s$ for all points $(x_i, y_i)$ on the path $\nu$. This is true when $i = 0$, since $(x_i, y_i) = (0,0)$. Assume the claim is true for some $i$, and consider two cases. First, if $sx_i - ry_i \le 0$, then $(x_{i+1}, y_{i+1}) = (x_i + 1, y_i)$. In this case, $sx_{i+1} - ry_{i+1} = (sx_i - ry_i) + s$, so the claim is true for $i+1$. Second, if $sx_i - ry_i > 0$, then $(x_{i+1}, y_{i+1}) = (x_i, y_i + 1)$. In this case, $sx_{i+1} - ry_{i+1} = (sx_i - ry_i) - r$, so the claim is true for $i+1$.

Using the claim for the points $(x_i, y_i)$ and $(x_j, y_j) = (x_i + a, y_i + b)$, we get

$$-r + 1 \le s(x_i + a) - r(y_i + b) \le s,$$
$$-s \le -sx_i + ry_i \le r - 1.$$

Adding gives

$$-(r + s - 1) \le sa - rb \le r + s - 1,$$

or equivalently $|as - br| \le r + s - 1$. ∎

LEMMA 13: *If $a, b, r, s, p$, and $q$ are integers such that $p$ divides both $a + bq$ and $r + sq$, then $sa - rb = 0$ or $|sa - rb| \ge p$.*

*Proof:* Pick integers $\ell$ and $m$ such that $a + bq = pm$ and $r + sq = p\ell$. Then

$$|sa - rb| = |s(a + bq) - b(r + sq)| = |p(sm - b\ell)|.$$

The integer $|sm - b\ell|$ is either 0 or at least 1, which gives the desired result. ∎

THEOREM 14: *$(z;v)$ is a well-defined cycle with $r$ 1-steps and $s$ $q$-steps.*

*Proof:* $(z;v)$ has the requisite number of 1-steps and $q$-steps by construction. The elements of $[p]$ moved by $(z;v)$ are those of the form $z+x_i+qy_i \pmod p$ for $0 \le i < r+s$. We need only show that these $r+s$ elements are all distinct. If this were not so, choose $i<j$ in the stated range with $z+x_i+qy_i \equiv z+x_j+qy_j \pmod p$. Setting $a=x_j-x_i$ and $b=y_j-y_i$ as in Lemma 12, we would then have $p$ dividing $a+bq$; say, $a+bq=mp$. Also, by Lemma 13, either $|sa-rb|=0$ or $|sa-rb| \ge p$. On the other hand, Lemma 12 gives $|sa-rb| < r+s \le p$. Together, these force $sa-rb=0$. Now, $b \ne 0$; otherwise $a=0$ also, contradicting the fact that $(x_i,y_i) \ne (x_j,y_j)$. So we can write $r/s=a/b$ where $a+b<r+s$. Let $t=\alpha/\beta \in \mathbb{Q}$ such that $r=at$, $s=bt$. Pick $\alpha,\beta$ such that $\alpha,\beta \ge 1$ and $\gcd(\alpha,\beta)=1$. Then

$$\ell p = r+sq = (a+bq)t = mp\frac{\alpha}{\beta} \tag{11}$$

and hence, $\alpha m = \beta \ell$. Since $\alpha$ and $\beta$ are relatively prime, $\alpha$ divides $\ell$. Likewise, $\beta r = a\alpha$ and $\beta s = b\alpha$ imply that $\alpha$ divides both $r$ and $s$. As $a<r$, we must have $\alpha > \beta \ge 1$. This yields a contradiction with our requirement that $\gcd(r,s,\ell)=1$. ∎

We now relax the assumption that $\gcd(r,s,\ell)=1$. Indeed, suppose this gcd is $k>1$.

Consider $(z;v)$ where $v$ is determined by the lattice path $\nu$ from $(0,0)$ to $(r/k,s/k)$ constructed in (10). Theorem 14 assures us that $(z;v)$ is a valid cycle.

THEOREM 15: *Let $k=\gcd(r,s,\ell)$ and $\nu$ be as above and write $C_j$ for $(1+(j-1)(q-1);v)$. Then*

$$\sigma = C_1 C_2 \cdots C_k$$

*is a well-defined element of $T_{p,q}(r,s)$.*

*Proof:* We already know that each cycle $C_j$ is well-defined; it suffices to check that these cycles are disjoint. The set

$$\{1+(j-1)(q-1)+x_i+qy_i \pmod p : 0 \le i < r/k+s/k, 1 \le j \le k\}.$$

consists of those elements moved by $C_j$. Suppose two such elements are equal mod $p$, say

$$1+(j_1-1)(q-1)+x_{i_1}+qy_{i_1} = 1+(j_2-1)(q-1)+x_{i_2}+qy_{i_2}+pM.$$

We must show that $i_1 = i_2$ and $j_1 = j_2$. Choose labels so that $j_1 \geq j_2$. Set $a = x_{i_2} - x_{i_1}$, $b = y_{i_2} - y_{i_1}$, $r' = r/k$, $s' = s/k$, $\ell' = \ell/k$, and $j = j_1 - j_2$. We then have $0 \leq j \leq k-1$ and

$$j(q-1) = a + qb + pM.$$

Set $A = a + j$ and $B = b - j$. Then $p(-M) = A + qB$, so that $p$ divides $A + qB$. Since $p$ also divides $r' + s'q$, Lemma 13 says that $s'A - r'B = 0$ or $|s'A - r'B| \geq p$.

Assume the second alternative occurs. Then

$$|s'a - r'b + j(s' + r')| \geq p.$$

Now Lemma 12 gives

$$|s'a - r'b| < r' + s'.$$

Hence,

$$j(s' + r') \geq |s'a - r'b + j(s' + r')| - |s'a - r'b| > p - (r' + s').$$

This gives $j > p/(r' + s') - 1$. But $r + s \leq p$, so that $r' + s' = r/k + s/k \leq p/k$, which implies $k \leq p/(r' + s')$. We deduce that $j > k - 1$, contradicting the fact that $0 \leq j \leq k - 1$.

We must therefore have $s'A - r'B = 0$, or $s'a - r'b = -j(s' + r')$. It is still true that $|s'a - r'b| < r' + s'$, so we see that

$$|j(r' + s')| < r' + s'.$$

Since $j$ is an integer and $r' + s' > 0$, we must have $j = 0$ and $j_1 = j_2$. Then $s'a - r'b = 0$ as well. If $a = b = 0$, then $i_1 = i_2$ and we are done. Otherwise, both $a$ and $b$ are nonzero and we get $r'/s' = a/b$ with $a + b < r' + s'$. This contradicts $\gcd(r', s', \ell') = 1$, just as in the proof of Theorem 14. ∎

*Example 16:* We illustrate the case of $p = 17$, $q = 5$, $r = 6$ and $s = 9$. $r + sq = 6 + 9 \cdot 5 = 51 = 3 \cdot 17$, so $\ell = 3$ and $k = \gcd(r, s, \ell) = 3$. Shown in Figure 3 are $C_1 = (1; v)$ (solid), $C_2 = (1 + 4; v)$ (dashed) and $C_3 = (1 + 2 \cdot 4; v)$ (dotted).

THEOREM 17: *The coefficient $a(r, s)$ in $\Phi_{p,q}(x, y)$ is zero if $p$ does not divide $r + qs$. Otherwise, this coefficient is nonzero with sign*

$$(-1)^{\gcd(r,s,(r+qs)/p)}.$$

*Proof:* Immediate from all the preceding results. ∎

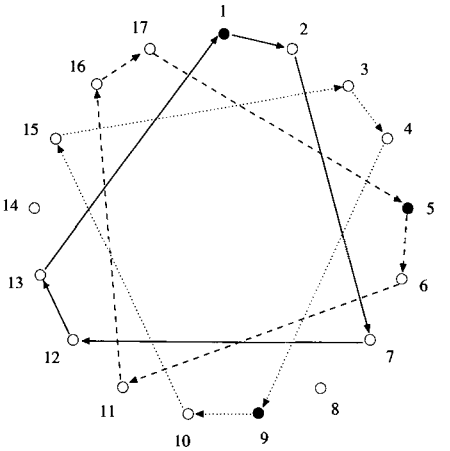


Figure 3. Illustration for Example 16.

## 5. The largest coefficient

We have identified the coefficients of the monomials in $\Phi_{p,q}$ as the numbers of permutations in certain classes. In this section we will obtain two-sided bounds on the size of the largest coefficient.

Consider the **permanent**

$$D_{p,q}(x,y) = \text{per}(\text{circ}(1,x,0,\ldots 0,y,0,\ldots,0)),$$

in which the $y$ is the $(q+1)$-st entry. Since all of the permutations that contribute to a given monomial in the determinant

$$\Phi_{p,q}(x,y) = \det(\text{circ}(1,-x,0,\ldots,0,-y,0,\ldots,0))$$

have the same sign, it follows that if

$$\Phi_{p,q}(x,y) = \sum_{r,s} a_{p,q}(r,s)x^r y^s,$$

then

$$D_{p,q}(x,y) = \sum_{r,s} |a_{p,q}(r,s)|x^r y^s.$$

Hence, $D_{p,q}(1,1)$ is the sum of the absolute values of the coefficients $a_{p,q}(r,s)$. Let $M(p,q) = \max_{r,s} |a_{p,q}(r,s)|$. Then we have

$$\frac{D_{p,q}(1,1)}{N(p,q)} \leq M(p,q) \leq D_{p,q}(1,1),$$

in which $N(p,q)$ is the number of distinct monomials that appear.

We now obtain two-sided estimates for $D_{p,q}(1,1)$. This is the permanent of a circulant matrix that has three cyclic diagonals of 1's and whose other entries are 0's.

For the upper bound we have the following theorem of Brègman–Minc [3, 10, 11].

THEOREM 18 (Brègman, Minc): *Let $A$ be an $n \times n$ 0-1 matrix with $r_i$ 1's in row $i$, for each $i = 1, 2, \ldots, n$. Then the permanent of $A$ satisfies*

$$\operatorname{per}(A) \leq \prod_{i=1}^{n} (r_i!)^{1/r_i}.$$

*Furthermore, equality holds iff the rows and columns of $A$ can be permuted to give a matrix with $r_i \times r_i$ blocks of 1's on the main diagonal, with all other entries being 0's.*

If we apply this theorem to $D_{p,q}(1,1)$ we find that

$$M(p,q) \leq 6^{p/3} = (1.817\ldots)^p.$$

For the lower bound, using results of Voorhoeve [13] or Schrijver [12], we have

$$\left(\frac{4}{3}\right)^p \leq D_{p,q}(1,1). \tag{12}$$

Since $N(p,q)$, the number of monomials that appear, is at most $p^2$, this implies that

$$p^{-2}\left(\frac{4}{3}\right)^p \leq M(p,q). \tag{13}$$

We have proved the following theorem.

THEOREM 19: *Fix $q$. Then the maximum absolute value of the coefficients in the polynomial $\Phi_{p,q}(x,y)$ satisfies*

$$\frac{4}{3} \leq \liminf_{p\to\infty} M(p,q)^{1/p} \leq \limsup_{p\to\infty} M(p,q)^{1/p} \leq 6^{1/3} = 1.817\ldots.$$

*In particular, the largest coefficient grows exponentially with $p$.*

ACKNOWLEDGEMENT: The authors thank John D'Angelo for useful discussions involving this problem, and Noga Alon for supplying useful references.

## References

[1] J. P. D'Angelo, *Invariant holomorphic mappings,* Journal of Geometric Analysis **6** (1996), 163–179.

[2] J. P. D'Angelo, *Number-theoretic properties of certain CR mappings,* Preprint, 2003.

[3] L. M. Brègman, *Certain properties of nonnegative matrices and their permanents,* (Russian) Doklady Akademii Nauk SSSR **211** (1973), 27–30.

[4] B. Codenotti, V. Crespi, and G. Resta, *On the permanent of certain* $(0,1)$ *Toeplitz matrices,* Linear Algebra and its Applications **267** (1997), 65–100.

[5] B. Codenotti and G. Resta, *Computation of sparse circulant permanents via determinants,* Linear Algebra and its Applications **355** (2002), 15–34.

[6] P. J. Davis, *Circulant Matrices,* Wiley-Interscience, New York–Chichester–Brisbane, 1979.

[7] G. P. Egorychev, *Reshenie problemy van-der-Wardena dlia permanentov,* Institute of Physics im. L. V. Kirenskogo, USSR Academy of Sciences, Siberian Branch, preprint IFSO-13M, Krasnoiarsk, 1980.

[8] D. I. Falikman, *A proof of van der Waerden's conjecture on the permanent of a doubly stochastic matrix,* Matematicheskie Zametki **29** (1981), 931–938.

[9] M. McIlroy, *Number theory in computer graphics,* in *The Unreasonable Effectiveness of Number Theory (Orono, ME)*, Proceedings of Symposia in Applied Mathematics **46** (1992), 105–121.

[10] H. Minc, *Upper bounds for permanents of* $(0,1)$*-matrices,* Bulletin of the American Mathematical Society **69** (1963), 789–791.

[11] A. Schrijver, *A short proof of Minc's conjecture,* Journal of Combinatorial Theory, Series A **25** (1978), 80–83.

[12] A. Schrijver, *Counting* 1*-factors in regular bipartite graphs,* Journal of Combinatorial Theory, Series B **72** (1998), 122–135.

[13] M. Voorhoeve, *A lower bound for the permanents of certain* $(0,1)$*-matrices,* Indagationes Mathematicae **41** (1979), 83–86.