Properties Sparse of Circulant Matrices

Brendan Whitaker

Ohio State University

whitaker.213@osu.edu

March 20, 2019

Overview

1. Preliminaries
2. Two Insights
3. The Main Proof

Objective

We wish to study the coefficients and signs of the terms of the following polynomial:

$$\Theta_{p,q_1,q_2}(x,y) = \prod_{j=0}^{p-1} (1 - x\omega^{q_1 j} - y\omega^{q_2 j}). \tag{1}$$

where ω is a primitive p-th root of unity, i.e. $\omega = e^{\frac{2k\pi i}{p}}$ where $k \nmid p$, and $1 \leqslant q_1, q_2 \leqslant p-1$.

Motivation

- These polynomials arise in the study of CR maps from balls in $\mathbb{C}^n$ to balls in $\mathbb{C}^N$.
- The polynomial Θ generates an associated group-invariant CR map given a finite subgroup, but this is beyond the scope of this work.
- For Θ, we wish to study when the coefficients are nonzero, positive or negative, and determine their magnitude.

Previous Work

- The case where $q_1 = 1$ has already been treated in [1].
- The cases where (p, q_1) or (p, q_2) are coprime are equivalent to the $q_1 = 1$ case under

$$(x, y) \mapsto (x\omega^{q_1}, y\omega^{q_2}). \tag{2}$$

- Let $\gamma(x, y) = (x\omega^{q_1}, y\omega^{q_2})$. Note

$$(\Theta_{p,q_1,q_2} \circ \gamma)(x, y) = \Theta_{p,q_1,q_2}, \tag{3}$$

which is proven in [2]. So the polynomial is **invariant under** γ.

Example Polynomial

Previous work proves we always have integer coefficients.

$$\Theta_{9,4,6}(x,y) = 1 - x^9 - 9x^3y + 9x^6y^2 - 3y^3 - 18x^3y^4 + 3y^6 - y^9. \tag{4}$$

Definitions

Definition

We define $l = \frac{rq_1 + sq_2}{p}$ as the **weight** of the monomial $a_{p,q_1,q_2}(r, s)x^r y^s$.

L.W.W.'s Result (previous work)

Theorem

In the polynomial

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

the monomials $x^r y^s$ *which appear are exactly those for which* $p | (r + sq)$*, and the coefficients* $a(r, s)$ *of these monomials are positive if and only if* $\gcd\left(r, s, \frac{r+sq}{p}\right)$ *is even.*

Context

- Loehr, Warrington, and Wilf prove the above for $\Theta_{p,1,q}$, i.e. in the case where $q_1 = 1$.
- We know the generalization of their theorem does not hold in general (for all values of p, q_1, q_2).

Question

So for which values of p, q_1, q_2 does their result generalize?

Generalizing [1]

Answer

We claim that the set of all parameters p, q_1, q_2 for which the generalization holds is exactly

$$\{ (p, q_1, q_2) : \gcd(p, q_1, q_2) = 1 \} . \tag{5}$$

Main Result

Theorem

Suppose $\gcd(p, q_1, q_2) = 1$. *In the polynomial*

$$\Theta_{p,q_1,q_2}(x, y) = \prod_{j=0}^{p-1} (1 - x\omega^{q_1 j} - y\omega^{q_2 j}), \tag{6}$$

the monomials $x^r y^s$ *which appear are exactly those for which* $p | (rq_1 + sq_2)$, *and the coefficients* $a(r, s)$ *of these monomials are positive if and only if* $\gcd(r, s, l)$ *is even.*

- We can't completely prove the first bit (this will take far too long).
- Instead, in this presentation, we give a formula for computing the coefficients.
- We also prove the second bit of the above theorem about the signs.

Two Insights from [1]

1. We can write Θ as the determinant of a sparse square circulant matrix.
2. Computing this determinant via a sum over the permutations of the rows (Leibniz's Formula) allows us to use combinatorial techniques to determine the coefficients.

Circulant Matrix?

Definition

An $n \times n$ **circulant matrix** is a matrix of the form

$$\begin{bmatrix} c_0 & c_1 & c_2 & \dots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \dots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \dots & c_{n-3} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ c_1 & c_2 & c_3 & \dots & c_0 \end{bmatrix}. \tag{7}$$

- So along each diagonal, all the values are identical.

Circulant Matrix

We can uniquely specify any $n \times n$ circulant matrix C by the n-tuple given by its first row, denoted $C = \mathrm{circ}(c_0, c_1, ..., c_{n-2}, c_{n-1})$.

Proposition

The following equality holds:

$$\Theta_{p,q_1,q_2}(x, y) = \prod_{j=0}^{p-1} (1 - x\omega^{q_1 j} - y\omega^{q_2 j}) = \det(C_\Theta) \tag{8}$$

where $C_\Theta = \mathrm{circ}(1, 0, \ldots, -x, 0, \ldots, -y, 0, \ldots)$, $-x$ *is in the* $(q_1 + 1)$*-th position, and* $-y$ *is in the* $(q_2 + 1)$*-th position.*

- We state without proof for brevity. The proof is available in the accompanying paper.

Computing the Determinant

Leibniz's Formula for the Determinant

Let C be an $n \times n$ matrix with entries $c_{i,j}$. Then we have

$$\det(C) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\, c_{1,\sigma(1)}\, c_{2,\sigma(2)} \cdots c_{n,\sigma(n)}. \tag{9}$$

Example Matrix

Note

$$C_{\Theta_{6,2,3}} = \begin{bmatrix} 1 & 0 & -x & -y & 0 & 0 \\ 0 & 1 & 0 & -x & -y & 0 \\ 0 & 0 & 1 & 0 & -x & -y \\ -y & 0 & 0 & 1 & 0 & -x \\ -x & -y & 0 & 0 & 1 & 0 \\ 0 & -x & -y & 0 & 0 & 1 \end{bmatrix}. \tag{10}$$

- In computing the determinant via Leibniz's Formula, we move down the rows and "pick" one element from each row, multiplying them together as we go.

Example Determinant

Claim

The coefficient of $(-1)^{r+s}x^r y^s$ in Θ is the sum of the signs of those permutations in S_p that "hit" r of the $-x$'s in the matrix and s of the $-y$'s, the remaining values being fixed points.

- To see this, ask when is a term in Leibniz's formula of the form $ax^r y^s$?
- If $c_{i,\sigma(i)}$ in the formula is 0, the whole term is zero. So all factors must be $1, -x$, or $-y$.
- In particular, we must have r instances of $-x$, and s instances of $-y$ to get something of the form $ax^r y^s$.

Example Determinant

Let's compute the term in the sum for the permutation $(2\;4\;6\;3\;5) \in S_6$ in the case where $(p, q_1, q_2) = (6, 2, 3)$.

Note

$$\sigma(1) = 1, \sigma(2) = 4, \sigma(3) = 5, \sigma(4) = 6, \sigma(5) = 2, \sigma(6) = 3. \tag{11}$$

So we wish to compute

$$\mathrm{sgn}((2\;4\;6\;3\;5))\, c_{1,1}\, c_{2,4}\, c_{3,5}\, c_{4,6}\, c_{5,2}\, c_{6,3} \tag{12}$$

by multiplying the circled terms in

$$\begin{bmatrix} 1 & 0 & -x & -y & 0 & 0 \\ 0 & 1 & 0 & \text{-x} & -y & 0 \\ 0 & 0 & 1 & 0 & \text{-x} & -y \\ -y & 0 & 0 & 1 & 0 & \text{-x} \\ -x & \text{-y} & 0 & 0 & 1 & 0 \\ 0 & -x & \text{-y} & 0 & 0 & 1 \end{bmatrix}. \tag{13}$$

Example Determinant

Since each factor (apart from the 1's) contributes a (-1) to the product, we have

$$\begin{aligned} c_{1,1}c_{2,4}c_{3,5}c_{4,6}c_{5,2}c_{6,3} &= 1(-x)(-x)(-x)(-y)(-y) \\ &= (-1)^{3+2}x^3y^2 \\ &= (-1)^{r+s}x^ry^s. \end{aligned} \tag{14}$$

The sign of $(2\ 4\ 6\ 3\ 5)$ is 1, so the term is $(-1)^{3+2}x^3y^2$.

- Every term in the sum which contributes to ax^ry^s in Θ is of the form $\operatorname{sgn}(\sigma)(-1)^{r+s}x^ry^s$.
- When we sum them all, we get that the sum of the signs of the relevant permutations is the coefficient of $(-1)^{r+s}x^ry^s$, just as claimed.

Examining the Permutations

- We wish to characterize all permutations $\sigma \in S_p$ which contribute to $ax^r y^s$.
- Recall we needed to "hit" r of the $-x$'s, s of the $-y$'s, and all remaining factors had to be 1's.
- The 1's are fixed points of the permutation, and since we have p rows, we need $p - r - s$ of them.

Question

What do the locations of the $-x$'s and $-y$'s tell us about the permutation?

Examining the Permutations

- Recall $-x$ is in the $(q_1 + 1)$-th position in the first row, and $-y$ is in the $(q_2 + 1)$-th position in the first row.
- Observe:

$$\begin{bmatrix} 1 & 0 & -x & -y & 0 & 0 \\ 0 & 1 & 0 & \text{-x} & -y & 0 \\ 0 & 0 & 1 & 0 & \text{-x} & -y \\ -y & 0 & 0 & 1 & 0 & \text{-x} \\ -x & \text{-y} & 0 & 0 & 1 & 0 \\ 0 & -x & \text{-y} & 0 & 0 & 1 \end{bmatrix}. \tag{15}$$

- Note that in the i-th row, $-x$ is always in the $(i + q_1 \mod p)$-th position, and $-y$ is in the $(i + q_2 \mod p)$-th position.
- **NOTE:** Our $\mod p$ operation in this work is taken on $\{1, 2, \ldots, p\}$ instead of on $\{0, 1, \ldots, p - 1\}$.

Characterizing the Permutations

Definition

Let $\sigma \in S_p$. Call $k \in \{1, 2, \dots, p\}$ a q_1-**step** of σ if

$$\sigma(k) = k + q_1 \mod p. \tag{16}$$

- We define q_2-steps analogously. So 5 is a q_2-step (3-step) of $(2\ 4\ 6\ 3\ 5)$, since $5 \mapsto 2$ and $2 = 5 + 3 \mod 6$.
- So we want exactly those permutations which have r q_1-steps, s q_2-steps, and $p - r - s$ fixed points (0-steps).

Characterizing the Permutations

Definition

We define $T_{p,q_1,q_2}(r,s) \subseteq S_p$ to be the set of all permutations with

- r q_1-steps;
- s q_2-steps;
- $p - r - s$ fixed points (0-steps).

Example Permutation Set

Example

As an example, the set $T_{6,2,3}(3,2)$ contains

(2 4 6 3 5)
(1 3 5 2 4)
(1 3 6 2 4)
(1 3 6 2 5)
(1 4 6 3 5)
(1 4 6 2 5).

Cycle Structure

Intuition

We wish to show that all the permutations in $T_{p,q_1,q_2}(r,s)$, i.e. all the permutations corresponding to a monomial $x^r y^s$, have identical cycle structure, and thus the same sign, so that we can say

$$|a(r,s)| = |T_{p,q_1,q_2}(r,s)|. \tag{17}$$

Cycle Structure

Cycle Decomposition

We decompose $\sigma \in T_{p,q_1,q_2}(r, s)$ into k disjoint cycles of length greater than 1 (to exclude fixed points):

$$\sigma = C_1 C_2 \cdots C_k. \tag{18}$$

Definition

Permutations in S_p permute the set $\{1, 2, \ldots, p\}$.

Cycle Example

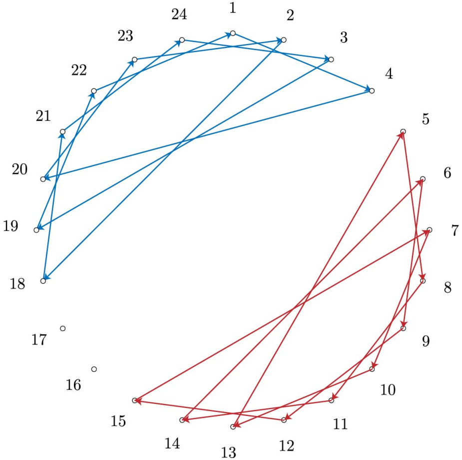


Figure: Nontrivial cycles for a permutation in $T_{24,3,16}(16,6)$.

Cycle Notation

Definition

We define

- r_i to be the number of q_1 steps in cycle C_i;
- s_i to be the number of q_2 steps in cycle C_i;
- l_i to be the weight of cycle C_i, given by

$$l_i = \frac{r_i q_1 + s_i q_2}{p}. \tag{19}$$

Cycle Notation

- We represent each cycle C_i by a **starting point** x_i and a word w_i (an $(r_i + s_i)$-tuple) specifying the **cycle steps** from the starting point which define the cycle.
- We write $C_i = (x_i; w_i)$.

Example

Consider the blue cycle in the figure. It is

$$C_1 = (20\ 23\ 2\ 18\ 21\ 24\ 3\ 19\ 22\ 1\ 4). \tag{20}$$

We write

$$\begin{aligned} C_1 &= (20; q_1, q_1, q_2, q_1, q_1, q_1, q_2, q_1, q_1, q_1, q_2) \\ &= (20; 3, 3, 16, 3, 3, 3, 16, 3, 3, 3, 16). \end{aligned} \tag{21}$$

Cycle Example

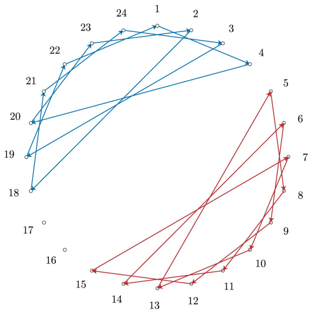


Figure: Nontrivial cycles for a permutation in $T_{24,3,16}(16,6)$.

$$\begin{aligned} C_1 &= (20\ 23\ 2\ 18\ 21\ 24\ 3\ 19\ 22\ 1\ 4) \\ &= (20; 3, 3, 16, 3, 3, 3, 16, 3, 3, 3, 16). \end{aligned} \tag{22}$$

Permutation/Cycle Image Notation

Definition

We write $\sigma^t(i)$ to denote the t-th image of $i \in \{ 1, 2, \ldots, p \}$ under the permutation σ.
Similarly, we write $C_i^t(i)$ to denote the t-th image of i under the cycle C_i.

Two Lemmas

Lemma

If $T_{p,q_1,q_2}(r,s)$ *is nonempty, and* C_i *is a cycle in* $\sigma \in T_{p,q_1,q_2}(r,s)$ *then* $p \mid (r_i q_1 + s_i q_2)$. *and* $p \mid (rq_1 + sq_2)$.

Lemma

If $T_{p,q_1,q_2}(r,s)$ *is nonempty, then* $\gcd(r_i, s_i, l_i) = 1$ *for all* $1 \leqslant i \leqslant k$, *for all* $\sigma \in T_{p,q_1,q_2}(r,s)$.

- We state these without proof for brevity.
- They will be used later on.

Definition of m-ordered sequence

- Recall we are considering everything $\mod p$, since all our permutations live in S_p.
- We can consider our permutations as acting on elements of the set $\{1, 2, \ldots, p\}$.

Definition of m-ordered sequence

Definition

Let $x_1, x_2, \dots, x_n \in \{1, 2, \dots, p\}$, and let $m \in \mathbb{N}$ such that $1 \leqslant m \leqslant p - 1$. We say the sequence $(x_1, x_2, \dots, x_n)$ is m-ordered on $\{1, 2, \dots, p\}$ if

1. $3 \leqslant n \leqslant \frac{\operatorname{lcm}(p,m)}{m}$;
2. $x_i \equiv x_j (\mod \gcd(p, m))$ for all i, j;
3. In the clockwise traversal of $\{1, 2, \dots, p\}$ by m-steps, starting with x_1, we hit x_i before x_j if and only if $i < j$.

Definition of m-ordered sequence

This is an opaque definition. Let's break it down.

Condition 1

$$3 \leqslant n \leqslant \frac{\operatorname{lcm}(p, m)}{m} \tag{23}$$

- We require that $n \geqslant 3$ since our definition is not meaningful with less than 3 points.
- Otherwise, any two point sequence which satisfies condition $\#2$ would be m-ordered.

Definition of m-ordered sequence

Condition 1

$$3 \leqslant n \leqslant \frac{\operatorname{lcm}(p, m)}{m} \tag{24}$$

- Note that $\operatorname{lcm}(p, m)$ is the maximum "distance" you can move around the circle when traversing by m-steps before coming back to the same point.

Definition of m-ordered sequence

- Note that $\operatorname{lcm}(p, m)$ is the maximum "distance" you can move around the circle when traversing by m-steps before coming back to the same point.
- If p and m are coprime, then $\operatorname{lcm}(p, m) = pm$.

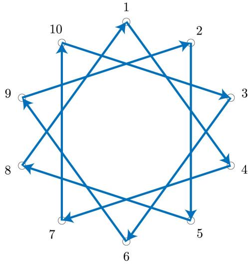


Figure: Note 10 and 3 are coprime, so we cover $\operatorname{lcm}(10, 3) = 30$ points, or three full rotations before coming back to the starting point.

Definition of m-ordered sequence

- Note that $\mathrm{lcm}(p, m)$ is the maximum "distance" you can move around the circle when traversing by m-steps before coming back to the same point.

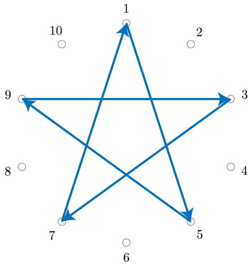


Figure: When $p = 10$, and $m = 4$, we pass $\mathrm{lcm}(10, 4) = 20$ points before coming back to the starting point.

Definition of m-ordered sequence

- If we want to know the maximum number of m-steps we can take before coming back to the starting point (i.e. the longest possible sequence which makes sense), we just divide the number of points we pass $\operatorname{lcm}(p, m)$ by the size of each step m.

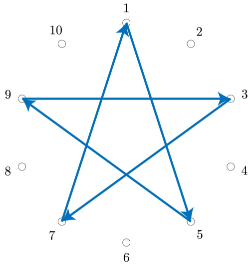


Figure: Note $\operatorname{lcm}(10, 4) = 20$. So we pass 20 points taking size 4 steps, so we can take at most $20/4 = 5$ steps before coming back to the same spot.

Definition of m-ordered sequence

Hence:

Condition 1

$$3 \leqslant n \leqslant \frac{\operatorname{lcm}(p, m)}{m} \tag{25}$$

Definition of m-ordered sequence

Condition 2

$$x_i \equiv x_j \mod \gcd(p, m) \text{ for all } i, j \tag{26}$$

- Condition 2 tells us nothing if $\gcd(p, m) = 1$.
- When the $\gcd$ is greater than 1, Condition 2 simply tells us that all elements in the sequence are in the same equivalence class $\mod p$ generated by m-steps.

Definition of m-ordered sequence

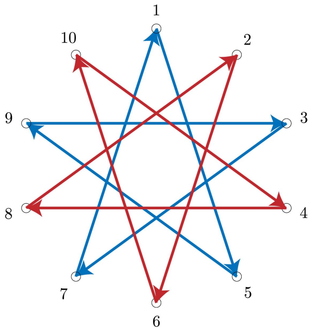


Figure: The two equivalence classes $\mod 10$ generated by taking 4-steps in $\{1, 2, \ldots, 10\}$.

Definition of m-ordered sequence

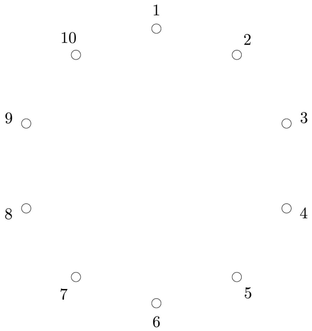
Condition 3

In the clockwise traversal of $\{1, 2, \ldots, p\}$ by m-steps, starting with x_1, we hit x_i before x_j if and only if $i < j$.

- We give some intuition for this notion with a few examples.

Definition of m-ordered sequence

Consider sequences of elements in $\{1, 2, \ldots, 10\}$.

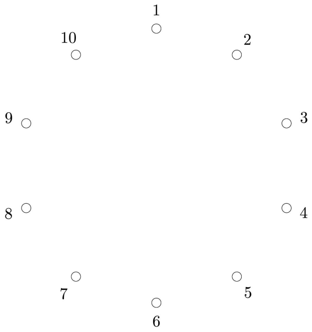


Question

Is $(1, 2, 3, 4)$ 1*-ordered?*

Definition of m-ordered sequence

Consider sequences of elements in $\{1, 2, \ldots, 10\}$.

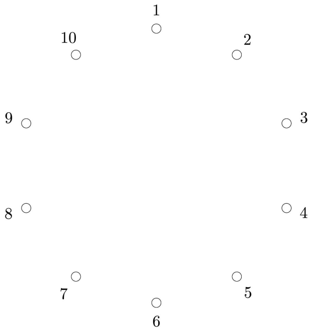


Question

Is $(1, 2, 3, 5)$ 1*-ordered?*

Definition of m-ordered sequence

Consider sequences of elements in $\{1, 2, \ldots, 10\}$.

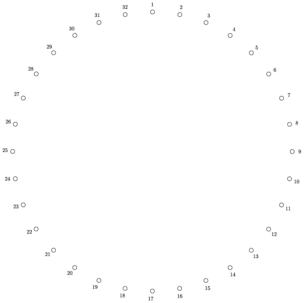


Question

Is $(1, 2, 4, 3)$ 1*-ordered?*

Definition of m-ordered sequence

Consider sequences of elements in $\{ 1, 2, \ldots, 32 \}$.

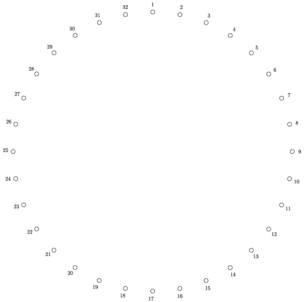


Question

Is $(3, 8, 13)$ 5*-ordered?*

Definition of m-ordered sequence

Consider sequences of elements in $\{1, 2, \ldots, 32\}$.

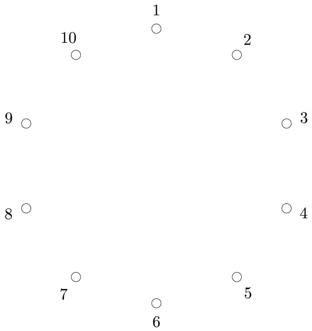


Question

Is $(3, 13, 18)$ 5*-ordered?*

Definition of m-ordered sequence

Consider sequences of elements in $\{1, 2, \dots, 10\}$.

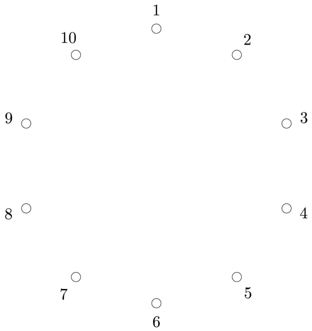


Question

Is $(1, 4, 2, 5)$ 3-ordered?

Definition of m-ordered sequence

Consider sequences of elements in $\{1, 2, \ldots, 10\}$.

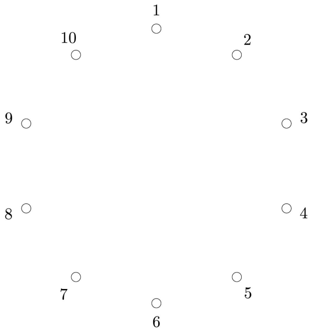


Question

Is $(2, 5, 6, 3)$ 3-ordered?

Definition of m-ordered sequence

Consider sequences of elements in $\{1, 2, \ldots, 10\}$.



Question

Is $(1, 5, 3)$ 4*-ordered? Is it* 2*-ordered?*

Definition of m-ordered sequence

Definition

Let $x_1, x_2, \dots, x_n \in \{1, 2, \dots, p\}$, and let $m \in \mathbb{N}$ such that $1 \leqslant m \leqslant p-1$. We say the sequence $(x_1, x_2, \dots, x_n)$ is m-ordered on $\{1, 2, \dots, p\}$ if

1. $3 \leqslant n \leqslant \frac{\operatorname{lcm}(p,m)}{m}$;
2. $x_i \equiv x_j \pmod{\gcd(p, m)}$ for all i, j;
3. In the clockwise traversal of $\{1, 2, \dots, p\}$ by m-steps, starting with x_1, we hit x_i before x_j if and only if $i < j$.

Proving Identical Cycle Structure

Lemma

If $\sigma \in T_{p,q_1,q_2}(r,s)$, *and* $\gcd(p, q_1, q_2) = 1$, *we must have* $r_1 = r_2 = \cdots = r_k$ *and* $s_1 = s_2 = \cdots = s_k$.

- "All cycles in a permutation from $T_{p,q_1,q_2}(r,s)$ have the same number of q_1-steps and the same number of q_2-steps."

Proving Identical Cycle Structure

- Let C_k, C_l be two distinct, nontrivial cycles in $\sigma \in T_{p,q_1,q_2}(r,s)$.
- We write $C_k = (x_k; w_k)$ using our **starting-point/step-vector** notation.
- And we group all q_1-steps together which precede each q_2-step, so we have

$$w_k = (q_1^{\rho_1}, q_2, \ldots, q_1^{\rho_{s_k}}, q_2) \tag{27}$$

where $\sum \rho_i = r_k$, the number of q_1 steps in the cycle.

Proving Identical Cycle Structure

Grouping q_1-steps example

Recall our example cycle from a permutation in $T_{24,3,16}(16,6)$:

$$C_1 = (20\ 23\ 2\ 18\ 21\ 24\ 3\ 19\ 22\ 1\ 4). \tag{28}$$

We write

$$\begin{aligned} C_1 &= (20; q_1, q_1, q_2, q_1, q_1, q_1, q_2, q_1, q_1, q_1, q_2) \\ &= (20; 3, 3, 16, 3, 3, 3, 16, 3, 3, 3, 16) \\ &= (20; 3^2, 16, 3^3, 16, 3^3, 16) \\ &= (x_i; q_1^{\rho_1}, q_2, q_1^{\rho_2} q_2, q_1^{\rho_3}, q_2). \end{aligned} \tag{29}$$

Proving Identical Cycle Structure

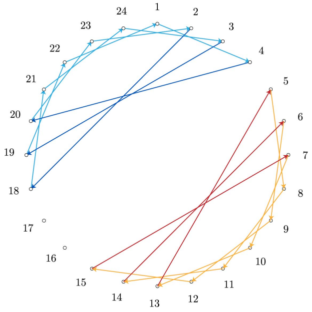


Figure: q_2-steps from C_1 are in dark blue, and q_2-steps from C_2 are in red.

Identical Number of q_2-steps

We proceed to show $s_k = s_l$, i.e. the number of q_2-steps in C_k is the same as the number of q_2-steps in C_l.

Proving Identical Cycle Structure

- We first argue that $s_l \geqslant s_k$.
- If $s_k = 0$, there is nothing to prove, so assume $s_k \geqslant 1$, i.e. we have at least one q_2-step in C_k.

Defining e_i points and d_i points

We enumerate the q_2-steps (we use the term q_2-step here to denote a point from which we jump q_2 points on the circle) as $\{ e_i \}$, and the images of the q_2-steps as $\{ d_i \}$, where $1 \leqslant i \leqslant s_k$.

Proving Identical Cycle Structure

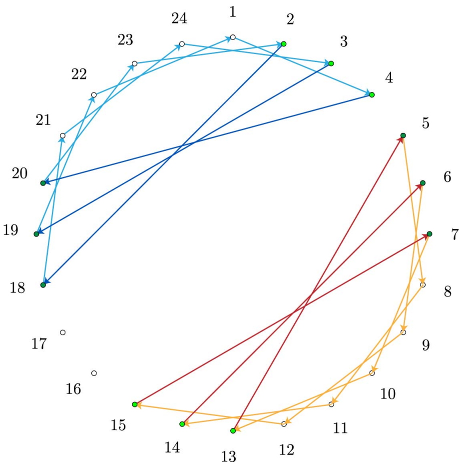


Figure: The $\{ e_i \}$ points (q_2-steps) are light-green, and the $\{ d_i \}$ points (images of q_2-steps) are in dark-green.

Proving Identical Cycle Structure

Labeling the e_i and d_i points

- Recall
$$C_k = \left(x_k; (q_1^{\rho_1}, q_2, \ldots, q_1^{\rho_{s_k}}, q_2)\right). \tag{30}$$
- Set $d_1 = x_k$.
- Set $e_1 = C_k^{\rho_1}(x_k)$.
- If $s_k > 1$, iteratively define
$$\begin{aligned} d_i &= C_k(e_{i-1}) \\ e_i &= C_k^{\rho_i}(d_i) \end{aligned} \tag{31}$$

for $1 \leqslant i \leqslant s_k$.

Proving Identical Cycle Structure

Example

Recall

$$\begin{aligned} C_1 &= (20\ 23\ 2\ 18\ 21\ 24\ 3\ 19\ 22\ 1\ 4) \\ &= (20; 3^2, 16, 3^3, 16, 3^3, 16) \\ &= (x_i; q_1^{\rho_1}, q_2, q_1^{\rho_2} q_2, q_1^{\rho_3}, q_2). \end{aligned} \tag{32}$$

So

$$\begin{aligned} d_1 &= 20; \quad e_1 = 2; \\ d_2 &= 18; \quad e_2 = 3; \\ d_3 &= 19; \quad e_3 = 4. \end{aligned} \tag{33}$$

Proving Identical Cycle Structure

Claim

We assert that there exists a unique permutation $U \in S_{s_k}$ such that

1. *If $e_j = d_j$, then $U(j) = j$.*
2. *If $e_j \neq d_j$, then for any $x \in \{1, 2, \ldots, p\}$ such that $(e_j, x, d_{U(j)})$ is q_1-ordered, $x \notin \{d_i\}$.*

Intuition

We assert that for each q_2-step (e point), we have a d point which is "hit" first when we traverse $\{1, 2, \ldots, p\}$ by q_1-steps starting from the e point, and these are distinct for each distinct e point. If the d point is also an e point, we let $U(j) = j$ and say that the e point itself is the first d point we hit.

Proving Identical Cycle Structure

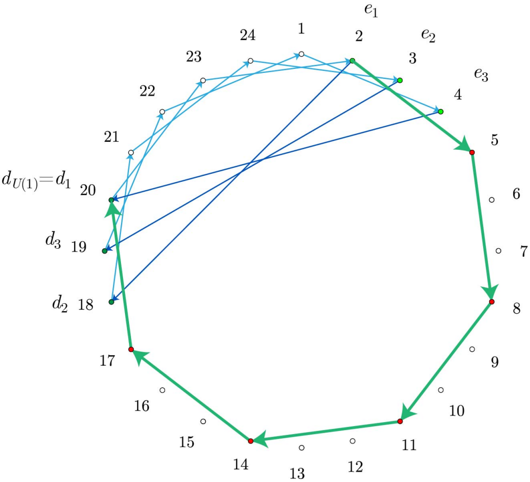


Figure: Finding $U(1)$ for cycle C_1 in a permutation in $T_{24,3,16}(16,6)$. The points in red are all $x \in \{1, 2, \ldots, 24\}$ for which (e_1, x, d_1) is q_1-ordered.

Proving Identical Cycle Structure

Question

When could the claim be false?

- It could be false if when traversing by q_1-steps from e_j, we never hit a d point.
- This could only be true if none of the d points are in the equivalence class $\mod \gcd(p, q_1)$ generated by traversing by q_1-steps from e_j.
- But we know $d_j \equiv e_j \mod \gcd(p, q_1)$ by taking q_1-steps **backwards** (counter-clockwise).
- Thus there is at least one d point in the same equivalence class as e_j, so this is impossible.

Proving Identical Cycle Structure

Question

When could the claim be false?

- So the only other way it could be false is if the first d point (call it d) we hit moving by q_1-steps from e_i is the same as the one we hit first moving from e_j.
- WLOG assume (e_i, e_j, d) is q_1-ordered.
- Then we cannot have d_j is between e_i and e_j, else we would hit that point before d traversing from e_i. So we must have that (d_j, e_i, e_j, d) is q_1-ordered, i.e. d_j comes "before" e_i in our traversal.
- Then we can traverse by q_1-steps **within our cycle** between d_j and e_j, so e_i must be the image of a q_1-step, but it is the image of a q_2-step by definition, and $q_1 \neq q_2$, so we have a contradiction.

Proving Identical Cycle Structure

Remark

Note we get uniqueness of the permutation of the images of the q_1-steps (d points) because we are looking for the **first** d point hit in our traversal.

Proving Identical Cycle Structure

Definition

We define our V-sets

$$V_j = \left\{ x : (e_j, x, d_{U(j)}) \text{ is } q_1\text{-ordered} \right\}. \tag{34}$$

Note we have one for each q_2-step e_j.

Remark

The points in V_j are the points we hit between e_j and the first d point we hit in our traversal from e_j by q_1-steps.

Proving Identical Cycle Structure

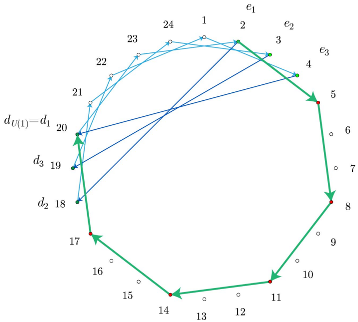


Figure: The points in red are the points in V_1.

- Also note that all points in V_j are fixed by the cycle C_k, since any points in C_k are in a sequence of q_1-steps starting from some d point.

Proving Identical Cycle Structure

Definition

Next we define functions to specify the previous element when traversing by q_1-steps, the next element when traversing by q_1-steps, and the image of a q_2-step from an arbitrary point:

$$\begin{aligned} \mathrm{Prev}_{q_1}(x) &= x - q_1 \mod p; \\ \mathrm{Next}_{q_1}(x) &= x + q_1 \mod p; \\ \mathrm{Jump}_{q_2}(x) &= x + q_2 \mod p. \end{aligned} \tag{35}$$

Proving Identical Cycle Structure

Definition

Then we define the W-sets

$$\begin{aligned} W_j &= \{\, y : (\mathrm{Prev}_{q_1}(\mathrm{Jump}_{q_2}(e_j)), y, \mathrm{Next}_{q_1}(e_{j+1}) \text{ is } q_1\text{-ordered} \,\} \\ &= \{\, y : (\mathrm{Prev}_{q_1}(d_{j+1}), y, \mathrm{Next}_{q_1}(e_{j+1}) \text{ is } q_1\text{-ordered} \,\}\,. \end{aligned} \tag{36}$$

- Intuitively, these are the points hit in a **string of q_1-steps within a cycle** C_k, starting with some d point.

Proving Identical Cycle Structure

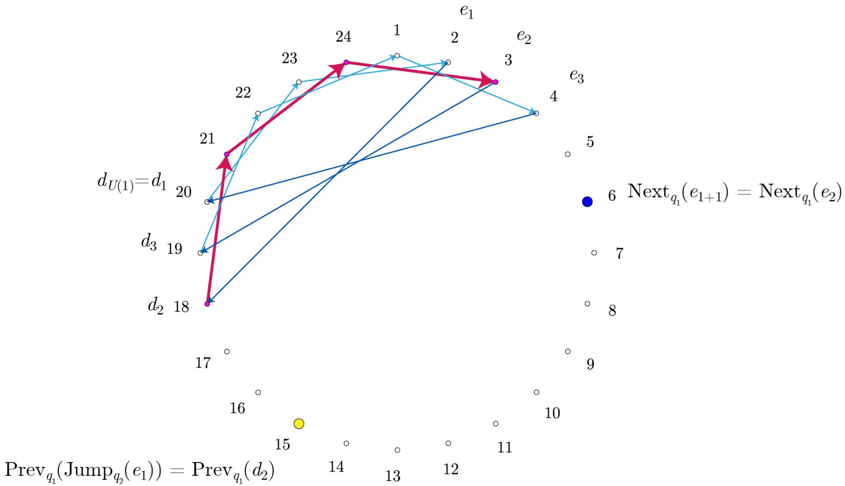


Figure: The points in W_1 are pink.

Proving Identical Cycle Structure

Proposition

We claim that for each $x \in V_j$*, if* $\mathrm{Jump}_{q_2}(x) \in C_k$*, then* $\mathrm{Jump}_{q_2}(x) \in W_j$*, and if* $\mathrm{Jump}_{q_2}(x) \notin C_k$*, then* $\mathrm{Jump}_{q_2}(x) \in V_{j+1}$*.*

- We state this without proof for brevity, and instead give visual intuition.

Proving Identical Cycle Structure

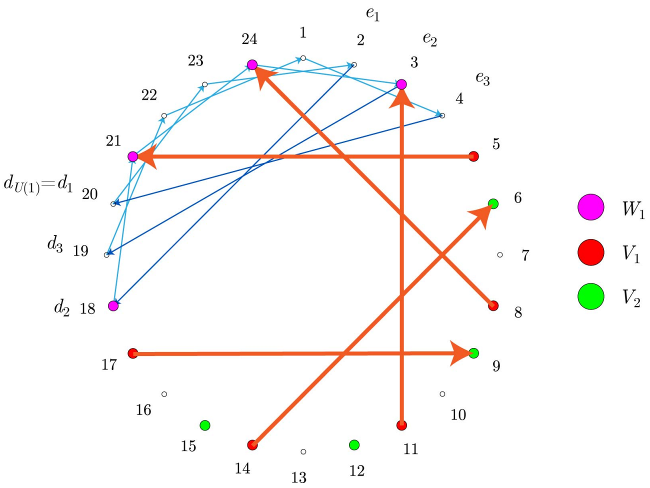


Figure: Illustration of $\mathrm{Jump}_{q_1}(x)$ (orange arrows) for each $x \in V_1$.

Proving Identical Cycle Structure

Claim

We also claim that each fixed point of C_k is contained in V_j for some j.

Proving Identical Cycle Structure

Claim

We also claim that each fixed point of C_k is contained in V_j for some j.

- We first prove that there is an e point in each equivalence class $\mod \gcd(p, q_1)$.
- **Case 1:** If $\gcd(q_1, q_2) = 1$, then we have a q_2-step (e point) in each equivalence class $\mod \gcd(p, q_1)$, since each q_2-step takes us to a new equivalence class.
- **Case 2:** If $\gcd(q_1, q_2) = \psi > 1$, then $\gcd(\psi, p) = \gcd(p, q_1, q_2) = 1$. So we must still visit every equivalence class to complete a cycle, and so we have an e point in each.

Claim

We also claim that each fixed point of C_k is contained in V_j for some j.

- So pick a fixed point x of C_k.
- Traverse backwards by q_1-steps.
- We have just proven you will hit a q_2-step $e_j$eventually, and before you hit any other point of C_k.
- So $x \in V_j$.

Proving Identical Cycle Structure

Remark

It is easily proven that the V_j sets do not overlap, so x lies within a unique V_j.

- So let $C_l(x) = x$, so x must be a fixed point of C_k, since the cycles are disjoint.
- We proved that x must be in a unique V_j.
- **Case 1:** x is a q_1-step of C_l. Then $C_l(x) \in V_j$ as well, since then $C_l(x) = x + q_1$ can only be in V_j or in C_k.
- **Case 2:** x is a q_2-step of C_l. Then $C_l(x) = x + q_2$ is a fixed point of C_k. So $C_l(x) = \mathrm{Jump}_{q_2}(x)$ for $x \in V_j$, so $C_l(x) \in V_{j+1}$.
- Taking $C_l^t(x)$ and iterating on t, i.e. following the orbit of x along the cycle C_l, we see it must visit each V_j set.
- So we have at least s_k q_2-steps in C_l.
- Arguing with roles switched, we have at least s_l q_2-steps in C_k, so $s_l = s_k$.

Proving Identical Cycle Structure

Lemma

If $T_{p,q_1,q_2}(r,s)$ is nonempty, and C_i is a cycle in $\sigma \in T_{p,q_1,q_2}(r,s)$ then $p \mid (r_i q_1 + s_i q_2)$. and $p \mid (rq_1 + sq_2)$.

- By the above Lemma stated earlier, we have $r_k q_1 + s_k q_2 = \lambda_k p$ and $r_l q_1 + s_k q_2 = \lambda_l p$ for integers λ_k, λ_l, since $s_k = s_l$.
- Then $r_k - r_l = (\lambda_k - \lambda_l)p$. Since $s_k = s_l > 0$, we have

$$\begin{gathered} 0 \leqslant r_k, r_l \leqslant p-1 \\ -(p-1) \leqslant r_k - r_l \leqslant p-1, \end{gathered} \tag{37}$$

  so since $p \mid (r_k - r_l)$, we must have $r_k = r_l$.
- ($q_1, q_2 > 1$, so at most $p/2$ q_1-steps.)

Proving Identical Cycle Structure

We just proved:

Lemma

If $\sigma \in T_{p,q_1,q_2}(r,s)$, *and* $\gcd(p,q_1,q_2) = 1$, *we must have* $r_1 = r_2 = \cdots = r_k$ *and* $s_1 = s_2 = \cdots = s_k$.

Theorem

If k *is the number of cycles in* σ, *then* $k = \gcd(r,s,l)$, $r_i = r/k$, $s_i = s/k$, *and all permutations in* $T_{p,q_1,q_2}(r,s)$ *have identical cycle structure. So* $\operatorname{sgn}(\sigma) = (-1)^{r+s+\gcd(r,s,l)}$.

- We already know $\sum s_i = s$ and $\sum r_i = r$. So by the Lemma we just proved, $s = s_i/k$, and $r = r_i/k$.
- Then

$$l_i = \frac{r_i q_1 + s_i q_2}{p} = \frac{\frac{rq_1+sq_2}{p}}{k} = \frac{l}{k}. \tag{38}$$

Proving Identical Cycle Structure

Recall we also stated:

Lemma

If $T_{p,q_1,q_2}(r,s)$ is nonempty, then $\gcd(r_i, s_i, l_i) = 1$ for all $1 \leqslant i \leqslant k$, for all $\sigma \in T_{p,q_1,q_2}(r,s)$.

- So
$$k = k\gcd(r_i, s_i, l_i) = \gcd(kr_i, ks_i, kl_i) = \gcd(r, s, l). \qquad (39)$$
- So we have determined the number of cycles **from only the parameters** of $T_{p,q_1,q_2}(r,s)$!
- Recall the sign of σ is defined as $p - c$ where c is the total number of cycles in σ, including 1-cycles (fixed points).
- So $c = k + (p - r - s)$.
- So
$$\operatorname{sgn}(\sigma) = (-1)^{p-(k+p-r-s)} = (-1)^{r+s+\gcd(r,s,l)}. \qquad (40)$$

Conclusions

- We have proved the sign of every permutation in $T_{p,q_1,q_2}(r,s)$ is the identical.
- So we know the magnitude of the coefficients:

$$|a_{p,q_1,q_2}(r,s)| = |T_{p,q_1,q_2}(r,s)|. \tag{41}$$

Recall we proved:

Claim

The coefficient of $(-1)^{r+s}x^r y^s$ in Θ is the sum of the signs all $\sigma \in T_{p,q_1,q_2}(r,s)$.

Conclusions

Recall we proved:

Claim

The coefficient of $(-1)^{r+s}x^r y^s$ in Θ is the sum of the signs of those permutations in S_p that "hit" r of the $-x$'s in the matrix and s of the $-y$'s, the remaining values being fixed points.

So we (finally) have

Formula for Coefficients

$$\begin{aligned} a_{p,q_1,q_2}(r,s) &= (-1)^{r+s}|T_{p,q_1,q_2}(r,s)|(-1)^{r+s+\gcd(r,s,l)} \\ &= (-1)^{\gcd(r,s,l)}|T_{p,q_1,q_2}(r,s)|. \end{aligned} \tag{42}$$

References

Nicholas A. Loehr, Gregory S. Warrington, and Herbert S. Wilf. "The combinatorics of a three-line circulant determinant". In: *Israel Journal of Mathematics* 143.1 (2004), pp. 141–156. ISSN: 1565-8511. DOI: 10.1007/BF02803496. URL: https://doi.org/10.1007/BF02803496.

John P. D'Angelo and Daniel Lichtblau. "Spherical space forms, CR mappings, and proper maps between balls". In: *Journal of Geometric Analysis* 2 (Sept. 1992), pp. 391–415. DOI: 10.1007/BF02921298.