FIXED POINTS OF POWERS OF PERMUTATIONS

MELVYN B. NATHANSON

Abstract. Let $\sigma$ be a permutation of a finite or infinite set $X$, and let $F_X(\sigma^k)$ be the number of fixed points of the $k$th power of $\sigma$. This paper describes how the sequence $(F_X(\sigma^k))_{k=1}^\infty$ determines the permutation $\sigma$.

1. Fixed points of permutations

Let $X$ be a nonempty finite or infinite set and let $\vert X \vert$ denote the cardinality of $X$. An infinite set $X$ is not necessarily countably infinite. Let $\mathbb{Z}$ denote the set of integers and $\mathbb{N} = \{1, 2, 3, \ldots\}$ denote the set of positive integers.

Let $\text{Perm}(X)$ be the group of permutations of the set $X$. Let $\text{id}_X$ denote the identity permutation in $\text{Perm}(X)$. We write $S_n = \text{Perm}(X)$ if $X = \{1, 2, 3, \ldots, n\}$.

An element $x \in X$ is a fixed point of a permutation $\sigma \in \text{Perm}(X)$ if $\sigma(x) = x$.

For every integer $k$, let $F_X(\sigma^k)$ denote the number of fixed points of the $k$th power of the permutation $\sigma$. The number $F_X(\sigma^k)$ can be finite or infinite. The fixed point counting sequence of $\sigma$ is the infinite sequence $F_X(\sigma) = (F_X(\sigma^k))_{k=1}^\infty$.

For every positive integer $m$, we also have the finite sequence $F_X^{(m)}(\sigma) = (F_X(\sigma^k))_{k=1}^m$.

Note that $F_X(\sigma^0) = F_X(\text{id}_X) = \vert X \vert$ for all nonempty sets $X$.

Every permutation $\sigma$ has a unique decomposition as a product of pairwise disjoint cycles of finite or countably infinite length $\ell$. This decomposition is called the cyclic representation of $\sigma$. Permutations $\sigma$ and $\tau$ are equivalent if, in their representations as products of pairwise disjoint cycles, the number of cycles of length $\ell$ in $\sigma$ equals the number of cycles of length $\ell$ in $\tau$ for all $\ell$.

A permutation $\sigma \in \text{Perm}(X)$ will be called of finite type if it is the product of finitely many or infinitely many pairwise disjoint cycles of finite length. Equivalently, a permutation is of finite type if its cyclic representation contains no infinite cycle. A permutation $\sigma \in \text{Perm}(X)$ will be called of bounded type if there is a number $\ell^*$ such that the length of every finite cycle in the representation of $\sigma$ is at most $\ell^*$. A permutation with no cycle of finite length is of bounded type. The cyclic representation of a permutation of bounded type may also include infinite cycles. A permutation is of finite and bounded type if it is a product of finitely or infinitely many cycles of finite length with lengths bounded above by some number $\ell^*$. Of course, if $X$ is finite, then every $\sigma \in \text{Perm}(X)$ is of finite and bounded type.

Date: June 10, 2022.

2010 Mathematics Subject Classification. 20B05, 20B07, 20B10, 20F69.

Key words and phrases. Permutations, fixed points, cycle structure.
In this paper we prove that the fixed point counting sequence $F_X(\sigma)$ of a permutation $\sigma \in \text{Perm}(X)$ uniquely determines the equivalence class of $\sigma$ if and only if $\sigma$ is of finite and bounded type. In this case, we describe an algorithm that computes $\sigma$ from its fixed point counting sequence. We also classify the sequences that are fixed point counting sequences of permutations.

2. Periodic fixed point counting sequences

We have the following addition formula for fixed point counting sequences.

**Lemma 1.** Let $(X_i)_{i \in I}$ be a family of pairwise disjoint nonempty sets, and let $\sigma_i \in \text{Perm}(X_i)$ for all $i \in I$. Let $X = \bigcup_{i \in I} X_i$. The function $\sigma : X \to X$ defined by $\sigma(x) = \sigma_i(x)$ for all $x \in X_i$ is a permutation of $X$. Moreover, $F_X(\sigma_k) = \sum_{i \in I} F_{X_i}(\sigma_i^k)$ for all $k \in \mathbb{N}$ and $F_X(\sigma) = \sum_{i \in I} F_{X_i}(\sigma_i)$.

**Proof.** It suffices to observe that if $\sigma_k(x) = x$, then there is a unique $i \in I$ such that $x \in X_i$ and $\sigma_i^k(x) = x$. Conversely, if $x \in X_i$ and $\sigma_i^k(x) = x$, then $\sigma^k(x) = x$. This completes the proof. $\blacksquare$

**Lemma 2.** Let $\sigma \in \text{Perm}(X)$. If $X$ is a nonempty finite set and $\sigma$ is a cycle of length $|X|$, then

$F_X(\sigma^k) = \begin{cases} |X| & \text{if } k \equiv 0 \pmod{|X|} \\ 0 & \text{if } k \not\equiv 0 \pmod{|X|} \end{cases}$

If $X = \{x_i : i \in \mathbb{Z}\}$ is a countably infinite set with $x_i \neq x_j$ for $i \neq j$ and if $\sigma$ is the cycle of infinite length defined by $\sigma(x_i) = x_{i+1}$ for all $i \in \mathbb{Z}$, then

$F_X(\sigma^k) = \begin{cases} |X| & \text{if } k = 0 \\ 0 & \text{if } k \neq 0. \end{cases}$

In both the finite and infinite cases, the sequence $F_X(\sigma^k)$ is periodic.

**Proof.** Klar. $\blacksquare$

**Lemma 3.** Let $X$ be a nonempty set and let $\sigma \in \text{Perm}(X)$ be a permutation of finite type. The sequence $F_X(\sigma)$ is periodic if and only if $\sigma$ is of bounded type.

**Proof.** Let $\sigma = \prod_{i \in I} \sigma_i$, where

$\sigma_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,\ell_i})$

is a cycle of length $\ell_i$ and the cycles $\sigma_i$ are pairwise disjoint. Let

$X_i = \{x_{i,r} : r \in \{1, 2, \ldots, \ell_i\}\}.$

Let $L = \{\ell_i : i \in I\}$ be the set of lengths of the cycles in $\sigma$.

The lengths of the cycles in $\sigma$ are bounded if and only if the set $L = \{\ell_i : i \in I\}$ is a finite set of positive integers. If $L$ is finite, then the least common multiple of the integers in $L$ is a positive integer $m$. For each $i \in I$ there is a positive integer
Lemma 3, the sequence $F$ for all $k$ and $q_i$ such that $m = \ell_i q_i$ and so $\sigma^{\ell_i q_i} = \sigma^{\ell_i} \sigma^{q_i} = \text{id}_X$. It follows that $\sigma^m = \text{id}_X$ and $\sigma$ is a permutation of finite order. For all $k \in \mathbb{N}$ we have $\sigma^{k+m} = \sigma^k$ and so

$$\sigma^{k+m}(x) = x \text{ if and only if } = \sigma^k(x) = x.$$  

Therefore, $F_X (\sigma^{k+m}) = F_X (\sigma^k)$ for all $k \in \mathbb{Z}$ and the fixed point counting sequence $F_X (\sigma) = (F_X (\sigma^k))_{k=1}^{\infty}$ is periodic with period $m$.

If the set $L = \{\ell_i : i \in I\}$ of lengths of cycles in $\sigma$ is unbounded, then $L$ is an infinite set of positive integers. Let $J = (\ell_i)_{i=1}^{\infty}$ be a strictly increasing infinite sequence of elements of $L$ and let $m_k = \text{lcm}(\ell_{i_1}, \ldots, \ell_{i_k})$ be the least common multiple of the first $k$ integers in the sequence $J$. Then

$$\sigma^{m_k}_{i_j} = \sigma^{\ell_{i_j}} = \text{id}_X$$

for all $j \in \{1, 2, \ldots, k\}$ and so

$$\sigma^{m_k}(x) = x$$

for all

$$x \in \bigcup_{j=1}^{k} X_{i_j}.$$  

It follows that

$$F_X (\sigma^{m_k}) \geq \sum_{j=1}^{k} |X_{i_j}| = \sum_{j=1}^{k} \ell_{i_j}$$

and

$$\lim_{k \to \infty} F_X (\sigma^{m_k}) = \infty.$$  

The sequence $F_X (\sigma)$ is unbounded and, therefore, not periodic. This completes the proof.

**Theorem 1.** Let $X$ be a nonempty set and let $\sigma \in \text{Perm}(X)$. The fixed point counting sequence $F_X (\sigma)$ is periodic if and only if the permutation $\sigma$ is bounded type.

**Proof.** For $\sigma \in \text{Perm}(X)$, define the sets

$$\hat{X}_0 = \{x \in X : x \text{ is an element in a cycle of } \sigma \text{ of finite length}\}$$

and

$$\hat{X}_\infty = \{x \in X : x \text{ is an element in a cycle of } \sigma \text{ of infinite length}\}.$$  

If $\hat{X}_0 = \emptyset$, then $X = \hat{X}_\infty \neq \emptyset$ and $\sigma$ is a product of disjoint infinite cycles, and so $\sigma$ is of bounded type. It follows from Lemmas **1** and **2** that $F_X (\sigma^k) = 0$ for all $k \in \mathbb{N}$ and so $F_X (\sigma)$ is periodic with period 1.

If $\hat{X}_\infty = \emptyset$, then $X = \hat{X}_0 \neq \emptyset$ and $\sigma$ is a product of cycles of finite length. By Lemma **3** the sequence $F_X (\sigma)$ is periodic if and only if $\sigma$ is of bounded type.

Suppose that both $\hat{X}_0 \neq \emptyset$ and $\hat{X}_\infty \neq \emptyset$. Let $\hat{\sigma}_0$ be the restriction of $\sigma$ to $\hat{X}_0$ and let $\hat{\sigma}_\infty$ be the restriction of $\sigma$ to $\hat{X}_\infty$. We have $\hat{\sigma}_0 \in \text{Perm}(\hat{X}_0)$ and $\hat{\sigma}_\infty \in \text{Perm}(\hat{X}_\infty)$. Lemmas **1** and **2** imply

$$F_X (\sigma^k) = F_{\hat{X}_0} (\hat{\sigma}_0^k) + F_{\hat{X}_\infty} (\hat{\sigma}_\infty^k) = F_{\hat{X}_0} (\hat{\sigma}_0^k)$$

for all $k \in \mathbb{N}$. Applying Lemma **3** completes the proof.  

\(\square\)
Theorem 2. Let $X$ be a nonempty set and let $\sigma \in \text{Perm}(X)$. Let

$$\hat{X}_0 = \{ x \in X : x \text{ is an element in a cycle of } \sigma \text{ of finite length} \}$$

and

$$\hat{X}_\infty = \{ x \in X : x \text{ is an element in a cycle of } \sigma \text{ of infinite length} \}.$$

Let $\hat{\sigma}_0 \in \text{Perm}(\hat{X}_0)$ be the restriction of $\sigma$ to $\hat{X}_0$ and let $\hat{\sigma}_\infty \in \text{Perm}(\hat{X}_\infty)$ be the restriction of $\sigma$ to $\hat{X}_\infty$. Then

$$F_X(\sigma^k) = F_{\hat{X}_0}(\hat{\sigma}_0^k)$$

and so the fixed point counting sequence of a permutation $\sigma$ is determined by the restriction of $\sigma$ to the cycles of finite length in the cyclic decomposition of $\sigma$.

Proof. This is equation (3) in the proof of Theorem 1. \(\square\)

3. Examples of periodic fixed point counting functions

Here are examples of permutations $\sigma \in \text{Perm}(X)$ for which the sequence $F_X(\sigma)$ is periodic.

Example 1. Let $X = \{1, 2, 3, 4\}$ and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4.$$

We write the powers of $\sigma$ as products of disjoint cycles:

$$\sigma = (1, 2, 3, 4) \quad F_X(\sigma) = 0$$
$$\sigma^2 = (1, 3)(2, 4) \quad F_X(\sigma^2) = 0$$
$$\sigma^3 = (1, 4, 3, 2) \quad F_X(\sigma^3) = 0$$
$$\sigma^4 = (1)(2)(3)(4) = \text{id}_X \quad F_X(\sigma^4) = 4$$

The permutation $\sigma$ has order 4 and so $F_X(\sigma^{k_1}) = F_X(\sigma^{k_2})$ if $k_1 \equiv k_2 \pmod{4}$. The sequence $F_X(\sigma)$ has period 4 and

$$F_X^{(4)}(\sigma) = (0, 0, 0, 4).$$

Example 2. Let $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 2 & 5 & 4 & 7 & 8 & 6 \end{pmatrix} \in S_8.$$

We write powers of $\sigma$ as products of disjoint cycles:

$$\sigma = (1)(2, 3)(4, 5)(6, 7, 8) \quad F_X(\sigma) = 1$$
$$\sigma^2 = (1)(2)(3)(4)(5)(6, 8, 7) \quad F_X(\sigma^2) = 5$$
$$\sigma^3 = (1)(2, 3)(4, 5)(6)(7, 8) \quad F_X(\sigma^3) = 4$$
$$\sigma^4 = (1)(2)(3)(4)(5)(6, 7, 8) \quad F_X(\sigma^4) = 5$$
$$\sigma^5 = (1)(2, 3)(4, 5)(6, 8, 7) \quad F_X(\sigma^5) = 1$$
$$\sigma^6 = (1)(2)(3)(4)(5)(6)(7, 8) = \text{id}_X \quad F_X(\sigma^6) = 8.$$
The permutation $\sigma$ has order 6, and so $F_X(\sigma^{k_1}) = F_X(\sigma^{k_2})$ if $k_1 \equiv k_2 \pmod{6}$.

The sequence $F_X(\sigma)$ has period 6 and

$$F_X^6(\sigma) = (1, 5, 4, 5, 1, 8).$$

**Example 3.** Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 8 & 4 \end{pmatrix} = (1, 2, 3)(4, 5, 6, 7, 8) \in S_8.$$

The permutation $\sigma$ has order 15, the sequence $F_X(\sigma)$ has period 15, and

$$F_X^{15}(\sigma) = (0, 0, 3, 0, 5, 3, 0, 3, 0, 3, 0, 0, 8).$$

**Example 4.** Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ be the set of positive integers. Define $\sigma \in \text{Perm}(\mathbb{N})$ by

$$\sigma(x) = \begin{cases} x + 1 & \text{if } x \text{ is odd} \\ x - 1 & \text{if } x \text{ is even.} \end{cases}$$

Thus, $\sigma$ is an infinite product of 2-cycles:

$$\sigma = (1, 2)(3, 4)(5, 6)(7, 8) \cdots.$$

The permutation $\sigma$ has order 2, the sequence $F_X(\sigma)$ has period 2, and

$$F_X^{(2)}(\sigma) = (0, \aleph_0).$$

**Example 5.** Let $X = \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$. Define $\sigma \in \text{Perm}(\mathbb{Z})$ by

$$\sigma(x) = x + 2 \quad \text{for all } x \in \mathbb{Z}.$$

The permutation $\sigma$ is a product of two disjoint infinite cycles

$$\sigma = (\ldots, -4, -2, 0, 2, 4, 6, \ldots)(\ldots, -5, -3, -1, 1, 3, 5, \ldots),$$

and has infinite order. For every positive integer $k$, the permutation $\sigma^k$, defined by $\sigma^k(x) = x + 2k$, is a product of $2k$ pairwise disjoint infinite cycles and has no fixed point. The permutation $\sigma$ has infinite order, the sequence $F_X(\sigma)$ has period 1, and

$$F_X^{(1)}(\sigma) = (0).$$

**Example 6.** The permutation $\sigma \in \text{Perm}(\mathbb{N})$ defined by

$$\sigma = (1)(2, 3)(4, 5, 6)(7, 8, 9, 10) \cdots \left(\frac{n^2 - n}{2} + 1, \frac{n^2 - n}{2} + 1, \frac{n^2 - n}{2} + 1, \ldots, \frac{n^2 - n}{2} + n\right) \cdots$$

is an infinite product of disjoint cycles of lengths $1, 2, 3, 4, \ldots, n, \ldots$. We have $\sigma^k(x) = x$ if and only if the integer $x$ is in a cycle whose length is a divisor of $k$, and so

$$F_N(\sigma^k) = \sum_{d|k} d = \sigma(k)$$

where the arithmetic function $\sigma(k)$ is the sum of the positive divisors of $k$. For example, $\sigma^4(x) = x$ if and only if $x \in \{1, 2, 3, 7, 8, 9, 10\}$. Note that $\sigma(k) \geq k$ for all $k \in \mathbb{N}$. The permutation $\sigma$ has infinite order, but

$$\limsup_{x \to \infty} F_N(\sigma^k) = \infty$$

and the infinite sequence $F_N(\sigma)$ is not periodic.
4. An algorithm for permutations of finite type

Let \( \sigma \in \text{Perm}(X) \). By Theorem 2, the fixed point counting sequence \( F_X(\sigma) = (F_X(\sigma^k))_{k=1}^\infty \) does not “see” elements of \( X \) that belong to cycles of infinite length. Therefore, only if the permutation \( \sigma \) is of finite type, that is, a product of finitely many or infinitely many cycles of finite length, might it be possible to reconstruct \( \sigma \) from \( F_X(\sigma) \).

Let \( F_X(\sigma) \) be the fixed point counting sequence of a permutation \( \sigma \in \text{Perm}(X) \) of finite type. Let \( \ell_1 \) be the smallest positive integer such that \( F_X(\sigma^{\ell_1}) > 0 \). It follows that

(i) \( F_X(\sigma^k) = 0 \) for \( 1 \leq k \leq \ell_1 - 1 \),
(ii) \( \ell_1 \) is the length of the shortest cycle in \( \sigma \),
(iii) \( \sigma \) contains \( q_1 \) cycles of length \( \ell_1 \) for some nonzero, possibly infinite number \( q_1 \) if and only if

\[ F_X(\sigma^{\ell_1}) = \ell_1q_1. \]

Let \( Y_1 \) be the subset of \( X \) consisting of the \( \ell_1q_1 \) elements of \( X \) that belong to the \( q_1 \) cycles of length \( \ell_1 \), and let \( \tau_1 \) be the restriction of \( \sigma \) to the set \( Y_1 \). We have \( \tau_1 \in \text{Perm}(Y_1) \) and

\[ F_{Y_1}(\tau_1^k) = \begin{cases} \ell_1q_1 & \text{if } k \equiv 0 \pmod{\ell_1} \\ 0 & \text{if } k \not\equiv 0 \pmod{\ell_1}. \end{cases} \]

If \( X = Y_1 \), then \( \sigma = \tau_1 \) is the product of \( q_1 \) cycles of length \( \ell_1 \), and \( F_X(\sigma^k) = F_{Y_1}(\tau_1^k) \) for all \( k \in \mathbb{N} \).

If \( X \neq Y_1 \), then the set \( X_1 = X \setminus Y_1 \) is nonempty and the restriction of \( \sigma \) to \( X_1 \) is a permutation \( \sigma_1 \in \text{Perm}(X_1) \). By the addition formula of Lemma 1 for all \( k \in \mathbb{N} \) we have

\[ F_X(\sigma^k) = F_{Y_1}(\tau_1^k) + F_{X_1}(\sigma_1^k) \]

and so

\[ F_{X_1}(\sigma_1^k) = F_X(\sigma^k) - F_{Y_1}(\tau_1^k) = \begin{cases} F_X(\sigma^k) - \ell_1q_1 & \text{if } k \equiv 0 \pmod{\ell_1} \\ F_X(\sigma^k) & \text{if } k \not\equiv 0 \pmod{\ell_1}. \end{cases} \]

Because \( \ell_1 \) is the smallest positive integer such that \( F_X(\sigma^{\ell_1}) > 0 \) and because \( F_X(\sigma^{\ell_1}) = \ell_1q_1 \), it follows that

\[ F_{X_1}(\sigma_1^k) = \ell_1q_1 - \ell_1q_1 = 0 \quad \text{for } k \leq \ell_1. \]

Let \( \ell_2 \) be the smallest positive integer such that \( F_{X_1}(\sigma_1^{\ell_2}) > 0 \). We have

\[ \ell_1 < \ell_2 \]

and \( \ell_2 \) is the length of the shortest cycle in \( \sigma_1 \). Then \( \sigma_1 \) contains \( q_2 \) cycles of length \( \ell_2 \) for some nonzero, possibly infinite number \( q_2 \) if and only if

\[ F_{X_1}(\sigma_1^{\ell_2}) = \ell_2q_2. \]

Let \( Y_2 \) be the subset of \( X_1 \) consisting of the \( \ell_2q_2 \) elements of \( X_1 \) that belong to the \( q_2 \) cycles of length \( \ell_2 \), and let \( \tau_2 \) be the restriction of \( \sigma \) to the set \( Y_1 \). Then \( \tau_2 \in \text{Perm}(Y_2) \) and

\[ F_{Y_2}(\tau_2^k) = \begin{cases} \ell_2q_2 & \text{if } k \equiv 0 \pmod{\ell_2} \\ 0 & \text{if } k \not\equiv 0 \pmod{\ell_2}. \end{cases} \]
If \( X_1 = Y_2 \), then \( \sigma_1 = \tau_2 \) is the product of \( q_2 \) cycles of length \( \ell_2 \) and \( \sigma \in \text{Perm}(X) \) is a product of \( q_1 \) cycles of length \( \ell_1 \) and \( q_2 \) cycles of length \( \ell_2 \). Equivalently,

\[
F_X(\sigma^k) = F_{Y_1}(\tau_1^k) + F_{Y_2}(\tau_2^k)
\]

for all \( k \in \mathbb{N} \).

If \( X_1 \neq Y_2 \), then the set

\[
X_2 = X_1 \setminus Y_1 = X \setminus (Y_1 \cup Y_2)
\]

is nonempty and the restriction of \( \sigma \) to \( X_2 \) is a permutation \( \sigma_2 \in \text{Perm}(X_2) \). Because \( \ell_2 \) is the smallest positive integer such that \( F_{X_1}(\sigma_2^{\ell_2}) > 0 \), it follows that

\[
F_{X_2}(\sigma_2^{\ell_2}) = 0 \quad \text{for} \quad k \leq \ell_2.
\]

If \( \ell_3 \) is the smallest positive integer such that \( F_{X_2}(\sigma_2^{\ell_3}) > 0 \), then

\[
\ell_1 < \ell_2 < \ell_3
\]

and \( \ell_3 \) is the length of the shortest cycle in the permutation \( \sigma_2 \in \text{Perm}(X_2) \). Continuing inductively, we obtain a strictly increasing sequence of positive integers

\[
\ell_1 < \ell_2 < \ell_3 < \ell_4 < \cdots
\]

that are the lengths of the cycles in \( \sigma \). This process terminates after finitely many iterations if and only if \( \sigma \) is a permutation of bounded type, that is, if and only if the set of lengths of cycles in \( \sigma \) is finite. If the algorithm terminates in \( r \) steps, then

\[
F_X(\sigma^k) = \sum_{i=1}^{r} F_{Y_i}(\tau_i^k)
\]

for all \( k \in \mathbb{N} \), and \( \sigma \) is the product of \( q_1 \) cycles of length \( \ell_1 \), \( q_2 \) cycles of length \( \ell_2 \), \( \ldots \), \( q_r \) cycles of length \( \ell_r \).

This algorithm deduces the structure of a permutation of finite and bounded type from its fixed point counting function.

5. Examples of the algorithm

These are the inverse constructions for some of the permutations in Section 3.

Example 1a. If \( F_X(\tau) \) is the periodic sequence \((0, 0, 0, 4)\), then \( |X| = 4 \), \( \ell_1 = 4 \) and \( q_1 = 1 \). For the set \( X = \{1, 2, 3, 4\} \), the permutation \( \tau \) is the 4-cycle \((1, 2, 3, 4)\).

Example 2a. If \( F_X(\tau) \) is the periodic sequence \((1, 5, 4, 5, 1, 8)\), then \( |X| = 8 \), \( \ell_1 = q_1 = 1 \). Let \( X = \{1, 2, 3, 4, 5, 6, 7, 8\} \) and \( Y_1 = \{1\} \). Then \( X_1 = \{2, 3, 4, 5, 6, 7, 8\} \). With \( \tau_1 = \text{id}_{Y_1} \), we have \( F_{Y_1}(\tau_1) = (1) \). We obtain the periodic sequence

\[
F_{X_1}(\tau_1) = F_X(\tau) - F_{Y_1}(\tau_1)
\]

\[
= (1, 5, 4, 5, 1, 8) - (1, 1, 1, 1, 1, 1)
\]

\[
= (0, 4, 3, 4, 0, 7)
\]

and so \( \ell_2 = q_2 = 2 \). Let \( Y_2 = \{2, 3, 4, 5\} \) and \( X_2 = \{6, 7, 8\} \). The permutation \( \tau_2 = (2)(3)(4, 5) \) is the product of two 2-cycles and \( F_{Y_2}(\tau_2) \) is the periodic sequence \((0, 4)\). Therefore,
\[ F_{X_2}(\sigma_2) = F_{X_1}(\sigma_1) - F_{Y_2}(\tau_2) = (0, 4, 3, 4, 0, 4) - (0, 4, 0, 4, 0, 4) = (0, 0, 3, 0, 0, 3) \]
and so \( \ell_3 = 3 \) and \( q_3 = 1 \). It follows that \( X_3 = Y_3 \). The permutation \( \tau_3 = (6, 7, 8) \) is a 3-cycle and \( F_{Y_3}(\tau_3) \) is the periodic sequence \( (0, 0, 3) \). We obtain
\[ F_{X_3}(\sigma_3) = F_{X_2}(\sigma_2) - F_{Y_3}(\tau_3) = (0, 0, 3) - (0, 0, 3) = (0, 0, 0) \]
and so \( \sigma = (1)(2, 3)(4, 5)(6, 7, 8) \).

Example 4a. If \( F_{X}(\sigma) \) is the periodic sequence \((0, \omega_0)\), then \( \ell_1 = 2 \) and \( q_1 = \omega_0 \). It follows that the permutation \( \sigma \) is a countably infinite product of 2-cycles, for example, \( \sigma = (1, 2)(3, 4)(5, 6)(7, 8) \cdots \).

Example 5a. If \( F_{X}(\sigma) \) is the periodic sequence \((0, 0)\), then \( \sigma \) has no fixed points and so \( \sigma \) must be a product of cycles of infinite length.

6. The structure of a fixed point counting sequence

For \( I = \{1, 2, \ldots, r\} \) or \( I = \mathbb{N} \), let \((\ell_i)_{i \in I}\) be a strictly increasing sequence of positive integers and let \((q_i)_{i \in I}\) be a sequence of nonzero cardinal numbers. Let
\[ A(\ell_i, q_i) = (a_{i,k})_{k=1}^{\infty} \]
where
\[ a_{i,k} = \begin{cases} \ell_i q_i & \text{if } k \equiv 0 \pmod{\ell_i} \\ 0 & \text{if } k \not\equiv 0 \pmod{\ell_i} \end{cases} \]
Consider the sum of sequences
\[ A = \sum_{i \in I} A(\ell_i, q_i) = (a_k)_{k=1}^{\infty}. \]
Note that \( a_{i,k} = 0 \) if \( k < \ell_i \) and so
\[ a_k = \sum_{i \in I} a_{i,k} \]
is a sum of only finitely many nonzero numbers, even if the set \( I \) is infinite.

Theorem 3. For every nonempty set \( X \) and every permutation \( \sigma \in \text{Perm}(X) \), the fixed point counting sequence \( F_X(\sigma) \) is a sequence \( A \) of the form (4). Conversely, for every sequence \( A \) of the form (4) there is a nonempty set \( X \) and a permutation \( \sigma \in \text{Perm}(X) \) such that \( A \) is the fixed point counting function of \( \sigma \).

Proof. The algorithm in Section 4 shows that every fixed point counting sequence is a sequence of the form \( A \).

Conversely, let \( A \) be the sequence constructed from the set \( I = \{1, 2, \ldots, r\} \) or \( I = \mathbb{N} \), from a strictly increasing sequence \((\ell_i)_{i \in I}\) of positive integers, and from a sequence \((q_i)_{i \in I}\) of nonzero cardinal numbers. Let \( X' \) be a set of cardinality \( \sum_{i \in I} \ell_i q_i \). There is a partition of \( X' \) into a union of \( \sum_{i \in I} q_i \) pairwise disjoint finite
sets with $q_i$ sets of size $\ell_i$ for all $i \in I$. Let $X''$ be the union of a family of pairwise disjoint countably infinite sets such that $X' \cap X'' = \emptyset$, and let $X = X' \cup X''$. We obtain a partition of $X$ into nonempty pairwise disjoint sets. Let $\sigma$ be the permutation of $X$ that is a cyclic permutation on each set in the partition. The sequence $A$ is the fixed point counting sequence of $\sigma$. This completes the proof. □

7. Notes

This paper arose from a talk by Ariane Masuda [3] at the 20th Annual Workshop on Combinatorial and Additive Number Theory (CANT 2022). In her talk, “Rényi permutations with the same cycle structure,” she mentioned a theorem of Deng [1] that a permutation of a finite set is uniquely determined by the number of fixed points of powers of the permutation. She subsequently sent me a copy of Deng’s article, which is written in a mathematical language that I do not understand. This paper is the result of my effort to understand the fixed point counting function.

In response to the initial posting of this paper on arXiv, Andrew Sutherland wrote, “Another possible reference is that one can view this as a very special case of the Grothendieck-Lefschetz trace formula (applied to an algebraic variety of dimension zero defined by an integer polynomial $f(x)$), see page 5 of [5]… This is of course using a sledgehammer to kill a mosquito.”

The period of the fixed point counting sequence of a permutation $\sigma$ of a finite set of cardinality $n$ is the order of the permutation. Let $g(n)$ denote the maximum order of a permutation of a set of size $n$. Using analytic number theory and the prime number theorem, Landau proved that $\log g(n) \sim \sqrt{n \log n}$. Nathanson [4] gave an elementary proof that $g(n)$ grows faster than any polynomial, that is, $\lim_{n \to \infty} g(n)/n^k = \infty$ for every positive integer $k$.

References

[1] G. Deng, Isomorphic digraphs from affine maps of finite cyclic groups, ISRN Combinatorics, Volume 2013, Article ID 398641, 5 pages, [http://dx.doi.org/10.1155/2013/398641](http://dx.doi.org/10.1155/2013/398641).
[2] E. Landau, Handbuch der Lehre von der Verteilung der Primzahlen, Chelsea Publishing Company, New York, 1953.
[3] A. Masuda, Réényi permutations with the same cycle structure, 20th Annual Workshop on Combinatorial and Additive Number Theory (CANT 2022), CUNY Graduate Center, 2022.
[4] M. B. Nathanson, On the greatest order of an element in the symmetric group, Amer. Math. Monthly 79 (1972), 500–501.
[5] A. Sutherland, Sato-Tate distributions, Contemp. Math. 740 (2019), 197–248.

Department of Mathematics, Lehman College (CUNY), Bronx, NY 10468

Email address: melvyn.nathanson@lehman.cuny.edu