Chapter 6. Cycles in Permutations

A permutation of \([n]\) can be viewed as a bijection from \([n]\) to \([n]\). We can represent a permutation \(p\) as
\[
\begin{pmatrix}
  1 & 2 & 3 & \ldots & n \\
  p(1) & p(2) & p(3) & \ldots & p(n)
\end{pmatrix}
\]
(two-row notation)

or simply \(p = p_1 \ p_2 \ p_3 \ldots \ p_n\) (\(p_i \equiv p(c(i))\)).
(one-row notation)

For example, the permutation 4 2 3 1 can be viewed as a bijection \(f: [4] \rightarrow [4]\) defined by
\(f(1) = 4, \ f(2) = 2, \ f(3) = 3, \ f(4) = 1\).

**Defn.** The product of two permutations on \([n]\) is simply taking their composition,
\[p = f \cdot g \quad \Rightarrow \quad p(c(i)) = g(f(c(i))).\]

**Example:** \(f = 3\ 4\ 1\ 2, \ g = 4\ 1\ 3\ 2\)

Then
\[
\begin{align*}
(f \cdot g)(1) &= g(f(1)) = g(3) = 3 \\
(f \cdot g)(2) &= g(f(2)) = g(4) = 2 \\
(f \cdot g)(3) &= g(f(3)) = g(1) = 4 \\
(f \cdot g)(4) &= g(f(4)) = g(2) = 1
\end{align*}
\]

\(\therefore \ (f \cdot g) = 3\ 2\ 4\ 1\)

Now calculate \((g \cdot f)\).
\[(g \cdot f)(1) = f(g(1)) = f(4) = 2, \]
\[(g \cdot f)(2) = f(g(2)) = f(1) = 3, \]
\[(g \cdot f)(3) = f(g(3)) = f(3) = 1, \]
\[(g \cdot f)(4) = f(g(4)) = f(2) = 4. \]

\[\Rightarrow g \cdot f = 2314.\]

Thus, \(g \cdot f \neq f \cdot g\) in general.

1. **Cycles in Permutations.**

Consider the permutation \(g = 321564\).

+ \(g(2) = 2 \leq 2\) is a fixed point of \(g\).

+ \(g(1) = 3, g(3) = 1 \Rightarrow g^2(1) = 1, g^2(3) = 3.\)

\[\Rightarrow 1, 3 \text{ are fixed points of } g^2.\]

\[\Rightarrow (1, 3) \text{ is called a 2-cycle in } g.\]

+ \(g(4) = 5, g(5) = 6, g(6) = 4.\)

\[\Rightarrow g^3(4) = 4, g^3(5) = 5, g^3(6) = 6.\]

We say \((4, 5, 6)\) is a 3-cycle in \(g\).

\[\begin{array}{c}
g: \\
(1 \rightarrow 3 \rightarrow 0, 2 \rightarrow 4, 5 \rightarrow 6)
\end{array}\]

**Lemma:** For any permutation \(p: [n] \rightarrow [n]\) and any \(x \in [n]\), there exist \(1 \leq i \leq n\) s.t.
\[ p^i(x) = x. \]

**Proof.** Consider entries of \( p(x), p^2(x), \ldots, p^n(x) \). If none of them equal to \( x \), then by P.H.P. there exist two entries equal. Assume that

\[ p^j(x) = p^k(x) \quad (1 \leq j < k \leq n) \]

\[ \Rightarrow \quad p^{-j}(p^j(x)) = p^{-j}(p^k(x)) \]

\[ \Rightarrow \quad x = p^{k-j}(x). \quad \square \]

**Defn.** Let \( p : [n] \to [n] \) be a permutation. Let \( x \in [n] \) and let \( i \) be the smallest positive integer \( s.t. \)

\( p^i(x) = x \). Then we say that the entries \( (x), p(x), \ldots, p^{i-1}(x) \) form an \( i \)-cycle in \( p \).

**Corollary.** All permutations can be decomposed into the disjoint unions of their cycles.

**Proof.** Each entries of \( [n] \) belongs to a cycle. By the definition of cycle, distinct cycle are disjoint. \( \square \)

By the above example, the permutation \( 321564 \) has 3 cycles \( (3,1), (2), (5,4,6) \).

Reversely, given a cycle decomposition \((3,1)(2)(5,6,4)\) of \( g \), we can reconstruct \( g \)
as follow: the image $g(c_i)$ is the entry right after $i$ in its circle.

To avoid confusion, we write our permutations in canonical cycle form. That is each cycle starts with its largest element, and the largest elements increasing.

Thus $g = 321564 = (23) (31) (645)$.

Note that: The set of all permutations of $[n]$ is also called the "Symmetric Group" in group theory.

**Theorem.** Let $a_1, a_2, \ldots, a_n$ be nonnegative integers s.t. $\sum i a_i = n$. Then the number of $n$-permutations with $a_i$ circles of length $i$ (i.e. $[n]$) is

$$\frac{n!}{a_1! a_2! \ldots a_n! 1^{a_1} 2^{a_2} \ldots n^{a_n}}.$$

**Proof:** We write all elements of $[n]$ in a row in some order (there are $n!$ ways to do so). Then we insert parenthesis as follows. First, we put $a_1$ pairs of parenthesis to make $a_1$ cycles of length 1, then $a_2$ pairs of parenthesis to make $a_2$ cycles of length 2, and so on. There is only one way to do so for any ordering of $[n]$.

This gives us a permutation with $a_i$ cycles of length $i$. 

However, there are several ways to write down n integers that will lead the same permutation. We need to figure out how many.

The elements in a i-cycle can be in i different orders and still yield the same cyclic permutation. Therefore, every permutation can be obtained from $(1 \alpha_1) (2 \alpha_2) \ldots (n \alpha_n)$ rows of n integers by cyclical moving elements in cycles. Moreover, $\alpha_i$ cycles of length i can be permuted, and still yield the same permutation. There are $\alpha_i!$ way to permute such cycles. Thus there are total

$$\alpha_1! \alpha_2! \ldots \alpha_n! (1 \alpha_1) (2 \alpha_2) \ldots (n \alpha_n)$$

rows of n integers corresponding to the same permutation.

If an n-permutation p has $\alpha_i$ cycles of length i, for $i = 1, 2, \ldots, n$, then we say that $(\alpha_1, \ldots, \alpha_n)$ is the type or cycle type of p.

**Defn.** The number of n-permutations with k cycles is called a **signless Stirling number of the first kind**, and is denoted by $c(n, k)$. The number $s(n, k) = (-1)^{n-k} c(n, k)$ is called a **Stirling number of the first kind**.

$c(0, 0) = 1$, $c(n, k) = 0$ if $n < k$
**Theorem:** Let \( n \) and \( k \) be positive integers satisfying \( n \geq k \). Then

\[
\binom{n}{k} = \binom{n-1}{k-1} + (n-1) \binom{n-1}{k}
\]

**Proof.** We need to show that the RRTS counts all \( n \)-permutations with \( k \) cycles.

There are 2 possibilities of the entry \( n \):

**Case 1:** \( n \) forms a 1-cycle. Then the \( n-1 \) remaining entries form an \( (n-1) \)-permutation with \( k-1 \) circles. There are \( \binom{n-1}{k-1} \) such \( n \)-permutations.

**Case 2:** \( n \) belongs to a cycle of length at least 2. To form such a permutation, we pick any \( n-1 \) permutation with \( k \) cycles, and insert \( n \) into any of these cycles, after each element. There are \( (n-1) \binom{n-1}{k} \) such ways.

**Lemma:**

\[
\sum_{k=0}^{n} \binom{n}{k} x^k = x(x+1) \cdots (x+n-1)
\]

**Proof:** We show that the coefficients of \( x^k \) on the RRTS also satisfy the recurrence in the previous theorem for the Stirling number of the first kind.
Let \( G_n(x) = x(x+1) \cdots (x+n-1) = \sum_{k=0}^{n} a_{n,k} x^k. \)

Then
\[
G_n(x) = (x+n-1) G_{n-1}(x) = (x+n-1) \sum_{k=0}^{n-1} a_{n-1,k} x^k
\]
\[
= \sum_{k=1}^{n} a_{n-1,k-1} x^k + (n-1) \sum_{k=0}^{n-1} a_{n-1,k} x^k
\]
\[
\Rightarrow \sum_{k=0}^{n} a_{n,k} x^k = \sum_{k=1}^{n} a_{n-1,k-1} x^k + (n-1) \sum_{k=0}^{n-1} a_{n-1,k} x^k
\]

Comparing the coefficients of \( x^k \) on both sides, we get
\[
a_{n,k} = a_{n-1,k-1} + (n-1) a_{n-1,k}.
\]

Moreover, \( a_{0,0} = 1 = C(0,0) \), \( a(n,0) = 0 = C(n,0) \) if \( n \geq 0 \). Thus
\[
a_{n,k} = C(n,k) \text{ (by induction on } n+k \text{).}
\]

Now we replace \( x \) by \(-x\) in the Lemma above, and multiply both sides by \((-1)^n\). We get
\[
\sum_{k=0}^{n} S(n,k) x^k = (x)_n.
\]

Comparing with the formula of Stirling number of the second kind
\[
x^n = \sum_{k=0}^{n} S(n,k) (x)_k.
\]
Consider the vector space \( P \) of all polynomials with the natural polynomial addition and scalar multiplication.

There are two bases of \( P \):

\[ B = \{ 1, x, x^2, x^3, \ldots \} \]

and

\[ B' = \{ 1, (x)_1, (x)_2, \ldots \} \]

Now let \( S \) be the infinite matrix with the \((n,k)\)-entry \( S(n,k) \) and \( s \) the matrix with \((n,k)\)-entry \( s(n,k) \). Then \( S \) and \( s \) are the transition matrices from \( B' \) to \( B \) and from \( B \) to \( B' \), respectively.

**Theorem**: \( SS = sS = I \).

2. **Permutations with Restricted Cycle Structure**

**Lemma (Transition Lemma)**

Let \( p: [n] \to [n] \) be a permutation written in canonical cycle notation. Let \( g(p) \) be a permutation obtained from \( p \) by removing the parentheses and read entries as a permutation in the one-line notation. Then \( g \) is a bijection from the set \( S_n \) of all \( n \)-permutations onto \( S_n \).
Example: $p = 321564 = (2)(31)(645)$
$\Rightarrow g(p) = 231645$.

**Proof:**

We will show that for each permutation $q = q_1...q_n$, there is exactly one permutation $p$ such that $g(p) = q$. In other words, there is exactly one way to insert parentheses into the string $q = q_1...q_n$ so that we get a permutation in canonical cycle form.

The entry $q_1$ starts a new circle, so the first parenthesis must be inserted in front of the string. The second parenthesis is where the first circle ends. Since we want to get a permutation in canonical cycle form, all other entries in the first cycle must be less than $q_1$. Assume that $q_i$ is the first entry such that $q_i < q_1$; then the second parenthesis must be inserted some where before $q_i$. On the other hand, if $j < i$, then the second circle cannot start with $q_j$ as we now that $q_j < q_1$, then our cycle form is not canonical anymore (the largest elements of circles are increasing). Thus, the second circle must start with $q_i$.

Then we can continue this procedure to find the starting entry of the third cycle (if exists), and so on.
Example:
\[ q = 6 \quad 2 \quad 4 \quad 7 \quad 10 \quad 8 \quad 35 \quad 1 \quad 9 \]
\[ p = (6 \quad 2 \quad 4) \quad (7) \quad (10 \quad 8 \quad 35 \quad 1 \quad 9). \]

**Definition.** The entries \( q \) that are larger than all entries on the left are called **left-to-right maxima**.

**Observation:** If \( q \) has \( t \) left-to-right maxima, then \( p = g^{-1}(q) \) has \( t \) cycles.

**Proposition.** Let \( i \) and \( j \) be two elements of \([n]\). Then \( i \) and \( j \) are in the same cycle in exactly half of all \( n \)-permutations.

**Proof:** As we can relabel our entries by switching \( n \) and \( j \) and switching \( n-1 \) and \( j \), it is sufficient to prove that the entry \( n-1 \) and \( n \) are in the same cycle in exactly half of all \( n \)-permutations.

Let \( q = q_1 \quad q_2 \quad \ldots \quad q_n \) be an \( n \)-permutation, and let \( g(p) = q \) (as \( g \) defined in the previous lemma).

The entries \( n \) is always the last left-to-right maximum of \( q \). Therefore, the last cycle starts with \( n \). Therefore, \( q \) contains \( n \) and \( n-1 \) in the same cycle if and only if \( n-1 \) is on the right of \( n \) in \( q \). As that happens in half of all \( n \)-permutations, the proof follows. \( \Box \)
Lemma. Let \( i \in [n] \). Then for all \( K \in [n] \), there are exactly \((n-1)! \) \( n \)-permutations in which \( i \) is in a \( K \)-cycle.

Proof. Again it is sufficient to prove for \( i = n \). (The map \( \Phi_p : q \rightarrow q \cdot p \) is a bijection in \( S_n \), for any \( p \)).

Let \( q = q_1q_2 \ldots q_n \) be an \( n \)-permutation, \( q(p) = q \), and \( q_n = n \). Then the cycle \( C \) containing \( n \) in \( q \) has length \((n-i+1)\) as \( n \) is the leading entry of the last cycle. So if we want \( C \) has length \( K \), we must have \( i = n+1-K \). However, there are \((n-1)!\) permutations of length \( n \) containing \( n \) in a given position, and the proof follows.

This Lemma shows that the probability that a given entry \( i \) is part of a \( K \)-cycle is \( \frac{1}{n} \), i.e. independent from \( K \).

Denote by \( \text{ODD}(m) \) an \( \text{EVEN}(m) \) the sets of permutations of length \( m \) with all cycles odd an even, respectively.

Lemma. \( |\text{ODD}(2m)| = |\text{EVEN}(2m)| \).

Proof. We construct a bijection \( \Phi \) between \( \text{ODD}(2m) \) and \( \text{EVEN}(2m) \).

Let \( p \in \text{ODD}(2m) \). Then \( p \) consists of even number \( 2K \) of odd cycles. Denote by \( C_1, C_2, \ldots, C_{2K} \) the cycles in \( p \) in canonical order. For all \( i \),
we take the last element of \( C_{2i-1} \) and put it to the end of \( C_{2i} \) to get \( \phi(p) \).

For example, 
\[
p = (3) (624)(71)(85)
\]
then 
\[
\phi(p) = (6243)(7)(851).
\]

It is easy to see that \( \phi(p) \) is also in canonical cycle order, and if \( C_{2i-1} \) is a singleton, then it disappears.

We claim that \( \phi \) is a bijection from \( \text{ODD}(2m) \) onto \( \text{EVEN}(2m) \). Let \( \sigma \in \text{EVEN}(2m) \), with even circles \( C_1, C_2, \ldots, C_n \). We will show that there is exactly one \( \tau \in \text{ODD}(2m) \) s.t. \( \phi(\tau) = \sigma \).

First, we consider the last entry of \( C_n \). If it is greater than the first entry of \( C_{n-1} \) we take the last entry of \( C_n \) to make a new singleton in front of \( C_{n-1} \).

If the last entry of \( C_n \) is less than the first entry of \( C_{n-1} \), we insert the last entry of \( C_n \) to the end of \( C_{n-1} \).

We repeat the process for the left most unchanged cycles. If there is only one even circle remains, we create a singleton cycle in front of it using its last entry.
Theorem.

\[ |\text{ODD}(2m)| = |\text{EVEN}(2m)| = 1^2 3^2 \ldots (2m-1)^2 = (2m-1)!!^2. \]

Proof.

By the previous lemma, we only need to show
\[ |\text{EVEN}(2m)| = (2m-1)!!^2. \]  \(\star\)

Assume \( p \) is a permutation of \([2m]\) with even cycles only.

Clearly \( p(1) \neq 1 \), otherwise the first cycle has length 1.

\( \Rightarrow \) there are \((2m-1)\) choices for \( p(1) \). Then there are
\((2m-1)\) choices for \( p^2(1) = p(p(1)) \), as we choose every

entry but \( p(1) \) itself.

So for we choose \( p(1) \) and \( p^2(1) \). These two elements
will either form a 2-cycle, or they will not. In either
case we will have \((2m-3)\) choices for the image of the
next entry. That is, if \( p(1) \) and \( p^2(1) \) form a
2-cycle (i.e. \( p^2(1) = 1 \)), and \( i \) is an element outside
the cycle, then there are \((2m-3)\) choices for \( p(1) \).

In deed, we can choose anything except \( 1, p(1), i \).

If \( p(1) \) and \( p^2(1) \) do not form a 2-cycle, then
we choose \( p^3(1) \). We again can choose any thing
except \( p(1), p^2(1) \), that already chosen, and \( i \) as
that would create a 3-cycle (i.e. \( p(1), p^2(1), p^3(1) \)). Thus
we have \((2m-3)\) choices for the next element
in this case too.

Continuing this arguments, we get \( \star \) from
the Multiplication Principle. \( \Box \)
Theorem. \[ |\text{ODD}(2m+1)| = (2m+1) |\text{ODD}(2m)| \]
\[ = (2m+1)!! \frac{2}{(2m+1)} \]

Proof. We construct a bijection between \( \text{ODD}(2m+1) \) and \( \text{ODD}(2m) \times [2m+1] \).

Each \( n \)-permutation has \( n+1 \) gap positions, one after each entry in each cycle, and one in front of the first entry. For example, \( p = (4,3)(5,2,1) \) has six gap positions \( |(4,3) (5,2,1)| \).

Let \( \pi \in \text{ODD}(2m) \) and let \( k \leq 2m+1 \). We define \( \Psi(\pi, k) \) as follows.

First, take \( \phi(\pi) \), where \( \phi \) is defined in the previous lemma. (Thus \( \phi(\pi) \in \text{EVEN}(2m) \)).

We add 1 to each entry of \( \phi(\pi) \), then \( \phi(\pi) \) becomes a permutation of \( 1, 2, \ldots, 2m+1 \) with even cycles only. Insert entry 1 to the \( k \)th gap position of the resulting permutation. Thus only one cycle changing its length to odd, and the canonical form is preserved. Apply \( \phi^{-1} \) to the remaining cycles whose length are still even, to get a permutation \( \lambda \in \text{ODD}(2m+1) \). Take \( \lambda = \Psi(\pi, k) \).

We will show that \( \Psi \) is a bijection from \( \text{ODD}(2m) \times [2m+1] \) onto \( \text{ODD}(2m+1) \). To find the reverse of \( \Psi \), take \( \lambda \in \text{ODD}(2m+1) \), put the cycle of \( \lambda \) that contain 1 aside, and
run the remaining cycles through $\phi$ to get even cycles. Insert odd cycle back, read off the position $K$ of entry 1. Remove 1, reduce remaining entries by 1 each. Apply $\phi^{-1}$ to the resulting permutation. To obtain $\pi \in \text{ODD}(2m)$. Take $\psi^{-1}(\lambda) = (\pi, n)$. 

**Example:**

$\pi = (2) (635) (741) (8), \quad k = 6$

$\in \text{ODD}(8)$ add 1

$\phi(\pi) = (6352) (74) (81) \rightarrow (7463) (85) (92)$

insert 1 $\rightarrow (7463) (815) (92)$

Apply $\phi^{-1}$ to $(7463)(92) \rightarrow (74632)(9)$

$\Rightarrow \psi(\pi, 6) = (74632) (815) (9) \in \text{ODD}(9)$.

**Reversely:** $\lambda = (74632)(815)(9)$

$\Rightarrow$ remove $(815) : (74632)(9)$

apply $\phi : (7463)(92)$

Insert $(815)$ back $(7463)(815)(92)$

Read 1 at position $K = 6$.

Remove 1, subtract 1 from each entry

$(6352)(74)(81)$

Apply $\phi^{-1}$:

$(2)(635) (741)(8)$. 
Stirling Number and Rook Theory

Defn. A "placement of K rooks" on a given Ferrer board (diagram) is a subset of K squares in the Ferrer board s.t. we can place K non-attacking rooks on these squares.

Example:

```
  R
R R
R
```

This is a placement of 4 rooks on the Ferrer board (corresponding to the partition) \((7,4,4,3,2)\).

Theorem. For \(n \geq 0\) and \(0 \leq K \leq n\), let \(S'(n, K)\) denote the number of placements of \(n-K\) rooks on the Ferrer board \(\Delta_n = (n-1, n-2, \ldots, 1)\). Assume by convention that \(S'(n, 0) = 0\), \(S'(n, n) = 1\).

Then \(S'(n, K) = S(n, K)\).

Proof. We prove that \(S'(n, K)\) satisfies the same recurrence as \(S(n, K)\):

\[
S'(n, K) = S'(n-1, K-1) + K S'(n-1, K)
\]

for \(n > 1\) and \(0 < K < n\).
Proof: Fix \( n \geq 1, 0 < k < n \). Let \( A, B, C \) be the set of rook placements counted by \( S^r(n, k) \), \( S^r(n-1, k-1) \) and \( S^r(n-1, k) \), respectively.

Divide \( A \) into two disjoint subsets:
- \( A_0 \) consisting of all placements with no rook on the top row of \( \Delta_k \)
- \( A_1 \) consisting of placements with one rook on the top row.

We have a bijection between \( B \) and \( A_0 \) by removing a first row in placements of \( A_0 \):

\[ |B| = |A_0| \]

On the other hand, we can construct rook placements in \( A_1 \) by follows. First pick any placements of \( n-k-1 \) rooks on the \( \Delta_{n-1} \) viewed as the union of rows 2, 3, ..., \( n-1 \) of \( \Delta_n \). Then these \( n-k-1 \) rook occupy \( n-k-1 \) columns on \( \Delta_n \). Therefore \( (n-1) - (n-k-1) = k \) columns remain that we can place the last rook on the first row:

\[ k |C| = |A_1| \]

Thus \( |A| = |A_0| + |A_1| = |B| + k |C| \)

Defn. Assume that “\( W \) rook” (or weak rook) is a new chess piece, that attack only squares on its row.
**Theorem:** Let $S'(n,k)$ denote the number of placements of $n-k$ wrooks on $\Delta_n$.

Then $S'(n,k) = \binom{n}{k}$.

**Proof.** We show that $S'(n,k)$ and $\binom{n}{k}$ satisfy the same recurrence:

$S'(n,k) = S'(n-1,k-1) + (n-1)S'(n-1,k)$.

Let $A_0, B, C$ be the set of wrook placements counted by $S(n,k)$, $S'(n-1,k-1)$, and $S'(n-1,k)$, respectively. We define $A_0$ and $A_1$ similarly to the one in the previous proof.

We still have the same bijection between $A_0$ and $B$.

To obtain a placement in $A_1$, we first put the first wrook on the top row in $(n-1)$ ways.

Then we place the remaining wrooks in $\Delta_{n-1}$ in $S'(n-1,k)$ ways.

$\Rightarrow |A_1| = (n-1)|C|$

Thus,

$|A| = |A_0| + |A_1| = |B| + (n-1)|C| \square$