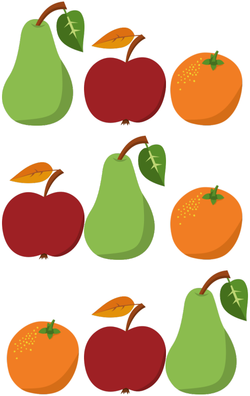
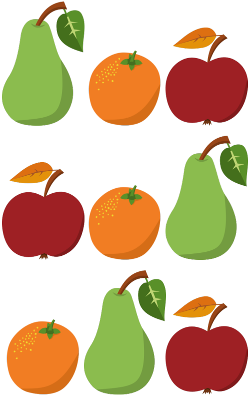
Discrete Mathematics in Computer Science

Permutations

Malte Helmert, Gabriele Röger

University of Basel





Permutations as Functions

- A permutation rearranges objects.

Permutations as Functions

- A permutation rearranges objects.
- Consider for example sequence o_2, o_1, o_3, o_4

Permutations as Functions

- A permutation rearranges objects.
- Consider for example sequence o_2, o_1, o_3, o_4
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.

Permutations as Functions

- A permutation rearranges objects.
- Consider for example sequence o_2, o_1, o_3, o_4
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,

Permutations as Functions

- A permutation rearranges objects.
- Consider for example sequence o_2, o_1, o_3, o_4
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,
  - the one from position 3 to position 1,

Permutations as Functions

- A permutation rearranges objects.
- Consider for example sequence o_2, o_1, o_3, o_4
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,
  - the one from position 3 to position 1,
  - the one from position 4 to position 3 and

Permutations as Functions

- A permutation rearranges objects.
- Consider for example sequence o_2, o_1, o_3, o_4
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,
  - the one from position 3 to position 1,
  - the one from position 4 to position 3 and
  - the one at position 2 stayed where it was.

Permutations as Functions

- A permutation rearranges objects.
- Consider for example sequence o_2, o_1, o_3, o_4
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,
  - the one from position 3 to position 1,
  - the one from position 4 to position 3 and
  - the one at position 2 stayed where it was.
- This corresponds to a bijection $\sigma : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ with $\sigma(1) = 4$, $\sigma(2) = 2$, $\sigma(3) = 1$, $\sigma(4) = 3$

Permutations as Functions

- A permutation rearranges objects.
- Consider for example sequence o_2, o_1, o_3, o_4
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,
  - the one from position 3 to position 1,
  - the one from position 4 to position 3 and
  - the one at position 2 stayed where it was.
- This corresponds to a bijection $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ with $\sigma(1) = 4$, $\sigma(2) = 2$, $\sigma(3) = 1$, $\sigma(4) = 3$
- We call such a bijection a permutation.

Permutation – Definition

Definition (Permutation)

Let S be a set. A bijection $\pi : S \to S$ is called a permutation of S.

Permutation – Definition

Definition (Permutation)

Let S be a set. A bijection $\pi : S \to S$ is called a permutation of S.

We will focus on permutations of finite sets.

The actual objects in S don't matter,
so we mostly work with $\{1, \ldots, |S|\}$.

Permutation – Definition

Definition (Permutation)

Let S be a set. A bijection $\pi : S \to S$ is called a permutation of S.

We will focus on permutations of finite sets.

The actual objects in S don't matter,
so we mostly work with $\{1, \ldots, |S|\}$.

How many permutations are there for a finite set S?

Two-line and One-line Notation (for Finite Sets)

Consider π with
$\pi(1) = 2, \pi(2) = 5, \pi(3) = 4, \pi(4) = 3, \pi(5) = 1, \pi(6) = 6.$

Two-line notation lists the elements of S in the first row and the image of each element in the second row:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 1 & 6 & 4 & 2 \\ 4 & 1 & 2 & 6 & 3 & 5 \end{pmatrix}$$

Two-line and One-line Notation (for Finite Sets)

Consider π with
$\pi(1) = 2, \pi(2) = 5, \pi(3) = 4, \pi(4) = 3, \pi(5) = 1, \pi(6) = 6.$

Two-line notation lists the elements of S in the first row and the image of each element in the second row:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 1 & 6 & 4 & 2 \\ 4 & 1 & 2 & 6 & 3 & 5 \end{pmatrix}$$

One-line notation only lists the second row for the natural order of the first row:

$$\pi = \begin{pmatrix} 2 & 5 & 4 & 3 & 1 & 6 \end{pmatrix}$$

Composition

- Permutations of the same set can be composed with function composition.

Composition

- Permutations of the same set can be composed with function composition.
- Instead of $\sigma \circ \pi$, we write $\sigma\pi$.

Composition

- Permutations of the same set can be composed with function composition.
- Instead of $\sigma \circ \pi$, we write $\sigma\pi$.
- We call $\sigma\pi$ the product of π and σ.

Composition

- Permutations of the same set can be composed with function composition.
- Instead of $\sigma \circ \pi$, we write $\sigma\pi$.
- We call $\sigma\pi$ the product of π and σ.
- The product of permutations is a permutation. Why?

Composition

- Permutations of the same set can be composed with function composition.
- Instead of $\sigma \circ \pi$, we write $\sigma\pi$.
- We call $\sigma\pi$ the product of π and σ.
- The product of permutations is a permutation. Why?
- Example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \qquad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$$

$\sigma\pi =$

$\pi\sigma =$

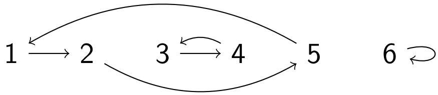
Cycle Notation – Idea

One-line notation still needs one entry per element and the effect of repeated application is hard to see.

Cycle Notation – Idea

One-line notation still needs one entry per element and the effect of repeated application is hard to see.

Consider again π with
$\pi(1) = 2, \pi(2) = 5, \pi(3) = 4, \pi(4) = 3, \pi(5) = 1, \pi(6) = 6.$

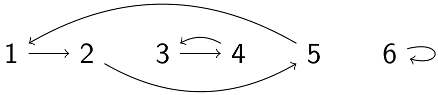


There is a cycle $(1 \quad 2 \quad 5) = (2 \quad 5 \quad 1) = (5 \quad 1 \quad 2)$
and a cycle $(3 \quad 4) = (4 \quad 3)$.

Cycle Notation – Idea

One-line notation still needs one entry per element and the effect of repeated application is hard to see.

Consider again π with
$\pi(1) = 2, \pi(2) = 5, \pi(3) = 4, \pi(4) = 3, \pi(5) = 1, \pi(6) = 6.$



There is a cycle $(1 \quad 2 \quad 5) = (2 \quad 5 \quad 1) = (5 \quad 1 \quad 2)$
and a cycle $(3 \quad 4) = (4 \quad 3)$.

Idea: Write π as product of such cycles.

Cycles

Definition (Cycle)

A permutation σ of finite set S has a *k-cycle* $(e_1 \quad e_2 \quad \dots \quad e_k)$ if

- $e_i \in S$ for $i \in \{1, \dots, k\}$
- $e_i \neq e_j$ for $i \neq j$
- $\sigma(e_i) = e_{i+1}$ for $i \in \{1, \dots, k-1\}$
- $\sigma(e_k) = e_1$

- Don't confuse cycles with permutations in one-line notation.
- A 2-cycle is called a transposition
- A 1-cycle is called a fixed-point of σ.

Cyclic Permutation

Definition (Cyclic Permutation)

A permutation is cyclic if it has a single k-cycle with $k > 1$.

In cycle notation, we represent a cyclic permutation by this cycle.

Cyclic Permutation

Definition (Cyclic Permutation)

A permutation is cyclic if it has a single k-cycle with $k > 1$.

In cycle notation, we represent a cyclic permutation by this cycle.

For example:

Permutation σ of $\{1, \ldots, 5\}$ with $\sigma = (1 \quad 3 \quad 4)$ in cycle representation corresponds to

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$$

in two-line notation.

Cyclic Permutation

Definition (Cyclic Permutation)

A permutation is cyclic if it has a single k-cycle with $k > 1$.

In cycle notation, we represent a cyclic permutation by this cycle.

For example:
Permutation σ of $\{1, \ldots, 5\}$ with $\sigma = (1 \quad 3 \quad 4)$ in cycle representation corresponds to

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$$

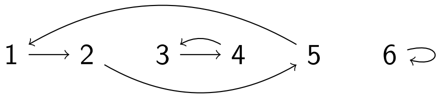
in two-line notation.

Question: Is this representation unique (canonical)?

Cycle Notation – Example

We can write every permutation as a product of disjoint cycles.

Consider again π with
$\pi(1) = 2, \pi(2) = 5, \pi(3) = 4, \pi(4) = 3, \pi(5) = 1, \pi(6) = 6.$



There is a cycle $(1 \quad 2 \quad 5) = (2 \quad 5 \quad 1) = (5 \quad 1 \quad 2)$
and a cycle $(3 \quad 4) = (4 \quad 3)$.

In cycle representation:
$\pi = (1 \quad 2 \quad 5)(3 \quad 4)(6) = (1 \quad 2 \quad 5)(3 \quad 4)$

Cycle Notation – Algorithm

Let π be a permutation of finite set S.

```
function ComputeCycleRepresentation(π, S)
    remaining = S
    cycles = ∅
    while remaining is not empty do
        Remove any element e from remaining.
        Start a new cycle c with e.
        while π(e) ∈ remaining do
            remaining = remaining \ {π(e)}
            Extend c with π(e).
            e = π(e)
        cycles = cycles ∪ {c}
    return cycles
```

The elements of *cycles* can be arranged in any order.

Cycle Notation – Algorithm

Let π be a permutation of finite set S.

```
function ComputeCycleRepresentation(π, S)
    remaining = S
    cycles = ∅
    while remaining is not empty do
        Remove any element e from remaining.
        Start a new cycle c with e.
        while π(e) ∈ remaining do
            remaining = remaining \ {π(e)}
            Extend c with π(e).
            e = π(e)
        cycles = cycles ∪ {c}
    return cycles
```

The elements of *cycles* can be arranged in any order. ⇝ Why?

Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \ldots \quad e_n)$ *and* $\pi' = (e'_1 \quad \ldots \quad e'_m)$ *be permutations of set* S *in cycle notation and let* π *and* π' *be disjoint, i. e.* $e_i \neq e'_j$ *for* $i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \dots \quad e_n)$ *and* $\pi' = (e'_1 \quad \dots \quad e'_m)$ *be permutations of set* S *in cycle notation and let* π *and* π' *be disjoint,*
i. e. $e_i \neq e'_j$ *for* $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Proof.

Consider an arbitrary element $e \in S$. We distinguish three cases:

□

Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \ldots \quad e_n)$ and $\pi' = (e'_1 \quad \ldots \quad e'_m)$ be permutations of set S in cycle notation and let π and π' be disjoint, i. e. $e_i \neq e'_j$ for $i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Proof.

Consider an arbitrary element $e \in S$. We distinguish three cases:

If $e = e_i$ for some $i \in \{1, \ldots, n\}$ then $\pi(e) = e_j$ for some $j \in \{1, \ldots, n\}$. Since the cycles are disjoint, $\pi'(e) = e$ and $\pi'(\pi(e)) = \pi(e)$. Together, this gives $\pi'(\pi(e)) = \pi(\pi'(e))$.

□

Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \dots \quad e_n)$ and $\pi' = (e'_1 \quad \dots \quad e'_m)$ be permutations of set S in cycle notation and let π and π' be disjoint, i. e. $e_i \neq e'_j$ for $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Proof.

Consider an arbitrary element $e \in S$. We distinguish three cases:

If $e = e_i$ for some $i \in \{1, \dots, n\}$ then $\pi(e) = e_j$ for some $j \in \{1, \dots, n\}$. Since the cycles are disjoint, $\pi'(e) = e$ and $\pi'(\pi(e)) = \pi(e)$. Together, this gives $\pi'(\pi(e)) = \pi(\pi'(e))$.

If $e = e'_i$ for some $i \in \{1, \dots, m\}$, we can use the analogous argument to show that $\pi(\pi'(e)) = \pi'(\pi(e))$.

□

Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \ldots \quad e_n)$ and $\pi' = (e'_1 \quad \ldots \quad e'_m)$ be permutations of set S in cycle notation and let π and π' be disjoint, i. e. $e_i \neq e'_j$ for $i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Proof.

Consider an arbitrary element $e \in S$. We distinguish three cases:

If $e = e_i$ for some $i \in \{1, \ldots, n\}$ then $\pi(e) = e_j$ for some $j \in \{1, \ldots, n\}$. Since the cycles are disjoint, $\pi'(e) = e$ and $\pi'(\pi(e)) = \pi(e)$. Together, this gives $\pi'(\pi(e)) = \pi(\pi'(e))$.

If $e = e'_i$ for some $i \in \{1, \ldots, m\}$, we can use the analogous argument to show that $\pi(\pi'(e)) = \pi'(\pi(e))$.

If e occurs in neither cycle then $\pi(e) = e$ and $\pi'(e) = e$, so $\pi'(\pi(e)) = e = \pi(\pi'(e))$. □

In General Cycles Do not Commute

Consider cycles $(1 \quad 2)$ and $(2 \quad 3)$ and set $S = \{1, 2, 3\}$.

$(1 \quad 2)(2 \quad 3) =$

$(2 \quad 3)(1 \quad 2) =$

Transpositions

Theorem

Every cycle can be expressed as a product of transpositions.

Proof idea.

Consider k-cycle $\sigma = (e_1 \quad \dots \quad e_k)$.
We can express σ as $(e_1 \quad e_k)(e_1 \quad e_{k-1})\dots(e_1 \quad e_2)$. □

Inverse

- Every permutation has an inverse, which is again a permuation.
  - If π is represented in two-line notation, we get π^{-1} by swapping the rows, e. g.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 2 & 4 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

  - If π is a cycle, we get π^{-1} by reversing the order of the elements, e. g. $(1 \quad 3 \quad 4 \quad 2)^{-1} = (2 \quad 4 \quad 3 \quad 1)$
  - $(\pi\sigma)^{-1} = \sigma^{-1}\pi^{-1}$

Example

$\sigma = (4 \quad 5)(2 \quad 3) \qquad \pi = (4 \quad 5)(2 \quad 1)$

$\sigma\pi^{-1} =$

Another Example

Determine the arrangement of some objects after applying a permutation that operates on the locations.

Another Example

Determine the arrangement of some objects after applying a permutation that operates on the locations.

 and π permutation of $\{1, 2, 3\}$.

Another Example

Determine the arrangement of some objects after applying a permutation that operates on the locations.

 and π permutation of $\{1, 2, 3\}$.

Define f with $f($$) = 1$, $f($$) = 2$, $f($$) = 3$
to describe the initial configuration.

Another Example

Determine the arrangement of some objects after applying a permutation that operates on the locations.

 and π permutation of $\{1, 2, 3\}$.

Define f with $f($$) = 1$, $f($$) = 2$, $f($$) = 3$
to describe the initial configuration.

Then $\pi \circ f$ describes the resulting configuration.

Last Example

Determine the permutation of locations that leads from one configuration to the other.

Last Example

Determine the permutation of locations that leads from one configuration to the other.

 $\Rightarrow$ .

Last Example

Determine the permutation of locations that leads from one configuration to the other.

Define f with $f($$) = 1$, $f($$) = 2$, $f($$) = 3$
to describe the initial configuration and

function g with $g($$) = 2$, $g($$) = 1$, $g($$) = 3$
for the final configuration.

Last Example

Determine the permutation of locations that leads from one configuration to the other.

 $\Rightarrow$ .

Define f with $f($$) = 1$, $f($$) = 2$, $f($$) = 3$
to describe the initial configuration and
function g with $g($$) = 2$, $g($$) = 1$, $g($$) = 3$
for the final configuration.

Then $g \circ f^{-1}$ describes the permutation.