Functions - Permutation Functions and Counting

K. Subramani[1]

[1] Lane Department of Computer Science and Electrical Engineering
West Virginia University

26 April 2015

Outline

Outline

Permutation Functions

Permutation Functions

Definition

Permutation Functions

Definition

A bijection f from a set A to itself is called a permutation function.

Permutation Functions

Definition

A bijection f from a set A to itself is called a permutation function.

Note that f has A as both its domain and its range.

Permutation Functions

Definition

A bijection f from a set A to itself is called a permutation function.

Note that f has A as both its domain and its range.

We use S_A to denote the set of all permutation functions from A onto itself.

Permutation Functions

Definition

A bijection f from a set A to itself is called a permutation function.

Note that f has A as both its domain and its range.

We use S_A to denote the set of all permutation functions from A onto itself.

Observation

Permutation Functions

Definition

A bijection f from a set A to itself is called a permutation function.

Note that f has A as both its domain and its range.

We use S_A to denote the set of all permutation functions from A onto itself.

Observation

A permutation function represents a reordering of the set.

Permutation Functions

Definition

A bijection f from a set A to itself is called a permutation function.

Note that f has A as both its domain and its range.

We use S_A to denote the set of all permutation functions from A onto itself.

Observation

A permutation function represents a reordering of the set. e.g.,

Permutation Functions

Definition

A bijection f from a set A to itself is called a permutation function.

Note that f has A as both its domain and its range.

We use S_A to denote the set of all permutation functions from A onto itself.

Observation

A permutation function represents a reordering of the set. e.g.,

$$A = \{1, 2, 3, 4\}$$

Permutation Functions

Definition

A bijection f from a set A to itself is called a permutation function.

Note that f has A as both its domain and its range.

We use S_A to denote the set of all permutation functions from A onto itself.

Observation

A permutation function represents a reordering of the set. e.g.,

$$A = \{1, 2, 3, 4\}$$
$$f = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,1\,4 \end{pmatrix}$$

Cycles

Cycles

Cycles

Definition

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2,

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2, a_2 is mapped to a_3,

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2, a_2 is mapped to a_3, $\ldots$,

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2, a_2 is mapped to a_3, ..., a_{k-1} is mapped a_k,

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2, a_2 is mapped to a_3, ..., a_{k-1} is mapped a_k, and a_k is mapped to a_1.

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2, a_2 is mapped to a_3, ..., a_{k-1} is mapped a_k, and a_k is mapped to a_1.

A cycle does not have to move all elements.

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2, a_2 is mapped to a_3, $\ldots$, a_{k-1} is mapped a_k, and a_k is mapped to a_1.

A cycle does not have to move all elements.

Consider the permutation

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2, a_2 is mapped to a_3, $\ldots$, a_{k-1} is mapped a_k, and a_k is mapped to a_1.

A cycle does not have to move all elements.

Consider the permutation

$$A = \{1, 2, 3, 4\}$$

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2, a_2 is mapped to a_3, ..., a_{k-1} is mapped a_k, and a_k is mapped to a_1.

A cycle does not have to move all elements.

Consider the permutation

$$\begin{aligned} A &= \{1, 2, 3, 4\} \\ f &= \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,1\,4 \end{pmatrix} \end{aligned}$$

Cycles

Definition

A cycle is a permutation of the form $(a_1, a_2, \ldots, a_k)$.

The cycle notation represents the fact that element a_1 is mapped to a_2, a_2 is mapped to a_3, $\ldots$, a_{k-1} is mapped a_k, and a_k is mapped to a_1.

A cycle does not have to move all elements.

Consider the permutation

$$\begin{aligned} A &= \{1, 2, 3, 4\} \\ f &= \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,1\,4 \end{pmatrix} \end{aligned}$$

It can be represented as: $(1, 2, 3)$.

Observations on Cycles

Observations on Cycles

Observations

Observations on Cycles

Observations

Observations on Cycles

Observations

1. When dealing with permutation functions, we assume that the set is

Observations on Cycles

Observations

1. When dealing with permutation functions, we assume that the set is $A = \{1, 2, 3, \ldots, n\}$,

Observations on Cycles

Observations

1. When dealing with permutation functions, we assume that the set is $A = \{1, 2, 3, \ldots, n\}$, although any set can be permuted.

Observations on Cycles

Observations

1. When dealing with permutation functions, we assume that the set is $A = \{1, 2, 3, \ldots, n\}$, although any set can be permuted.
2. A permutation which maps each element to itself is called the identity permutation,

Observations on Cycles

Observations

1. When dealing with permutation functions, we assume that the set is $A = \{1, 2, 3, \ldots, n\}$, although any set can be permuted.
2. A permutation which maps each element to itself is called the identity permutation, e.g.,

Observations on Cycles

Observations

1. When dealing with permutation functions, we assume that the set is $A = \{1, 2, 3, \ldots, n\}$, although any set can be permuted.
2. A permutation which maps each element to itself is called the identity permutation, e.g.,

$$A = \{1, 2, 3, 4\}$$

Observations on Cycles

Observations

1. When dealing with permutation functions, we assume that the set is $A = \{1, 2, 3, \ldots, n\}$, although any set can be permuted.
2. A permutation which maps each element to itself is called the identity permutation, e.g.,

$$\begin{aligned} A &= \{1, 2, 3, 4\} \\ f &= \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix} \end{aligned}$$

Cycles (contd.)

Observations

Cycles (contd.)

Observations

1. Not all permutations are cycles,

Cycles (contd.)

Observations

1. Not all permutations are cycles, e.g.,

Cycles (contd.)

Observations

1. Not all permutations are cycles, e.g.,

$$A = \{1, 2, 3, 4, 5\}$$

Cycles (contd.)

Observations

1. Not all permutations are cycles, e.g.,

$$\begin{aligned} A &= \{1, 2, 3, 4, 5\} \\ f &= \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 4\ 5\ 2\ 1 \end{pmatrix} \end{aligned}$$

Cycles (contd.)

Observations

1. Not all permutations are cycles, e.g.,

$$\begin{aligned} A &= \{1, 2, 3, 4, 5\} \\ f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \end{aligned}$$

2. The length of a cycle is the number of elements in the cycle.

Cycles (contd.)

Observations

1. Not all permutations are cycles, e.g.,

$$\begin{aligned} A &= \{1,2,3,4,5\} \\ f &= \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{array} \right) \end{aligned}$$

2. The length of a cycle is the number of elements in the cycle.
3. A cycle of length 2 is called a transposition.

Cycles (contd.)

Observations

1. Not all permutations are cycles, e.g.,

$$\begin{aligned} A &= \{1, 2, 3, 4, 5\} \\ f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \end{aligned}$$

2. The length of a cycle is the number of elements in the cycle.
3. A cycle of length 2 is called a transposition.

   A transposition swaps two elements and leaves all other elements fixed.

Cycles (contd.)

Observations

1. Not all permutations are cycles, e.g.,

$$\begin{aligned} A &= \{1, 2, 3, 4, 5\} \\ f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \end{aligned}$$

2. The length of a cycle is the number of elements in the cycle.
3. A cycle of length 2 is called a transposition.

   A transposition swaps two elements and leaves all other elements fixed.
4. Two cycles are disjoint if they do not move the same element.

Cycles (contd.)

Cycles (contd.)

Properties of cycles

Cycles (contd.)

Properties of cycles

1. Permutation functions can be composed

Cycles (contd.)

Properties of cycles

1. Permutation functions can be composed (sometimes called a product of permutations);

Cycles (contd.)

Properties of cycles

1. Permutation functions can be composed (sometimes called a product of permutations); e.g.,

Cycles (contd.)

Properties of cycles

1. Permutation functions can be composed (sometimes called a product of permutations); e.g., Let

$$A = \{1, 2, 3, 4\}$$

Cycles (contd.)

Properties of cycles

1. Permutation functions can be composed (sometimes called a product of permutations); e.g., Let

$$A = \{1, 2, 3, 4\}$$
$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Cycles (contd.)

Properties of cycles

1. Permutation functions can be composed (sometimes called a product of permutations); e.g., Let

$$\begin{aligned} A &= \{1, 2, 3, 4\} \\ f &= \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix} \\ g &= \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,4\,2 \end{pmatrix} \end{aligned}$$

Cycles (contd.)

Properties of cycles

1. Permutation functions can be composed (sometimes called a product of permutations); e.g., Let

$$
\begin{aligned}
A &= \{1, 2, 3, 4\} \\
f &= \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix} \\
g &= \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,4\,2 \end{pmatrix} \\
g \circ f &= \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,2\,1 \end{pmatrix}
\end{aligned}
$$

Cycles (contd.)

Properties of cycles

1. Permutation functions can be composed (sometimes called a product of permutations); e.g., Let

$$
\begin{aligned}
A &= \{1, 2, 3, 4\} \\
f &= \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix} \\
g &= \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,4\,2 \end{pmatrix} \\
g \circ f &= \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,2\,1 \end{pmatrix}
\end{aligned}
$$

2. The composition of disjoint cycles is commutative,

Cycles (contd.)

Properties of cycles

1. Permutation functions can be composed (sometimes called a product of permutations); e.g., Let

$$
\begin{aligned}
A &= \{1, 2, 3, 4\} \\
f &= \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix} \\
g &= \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,4\,2 \end{pmatrix} \\
g \circ f &= \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,2\,1 \end{pmatrix}
\end{aligned}
$$

2. The composition of disjoint cycles is commutative, i.e., if f and g are two disjoint cycles, then $f \circ g = g \circ f$.

Derangements

Derangements

Definition

Derangements

Definition

A permutation function in which no element is mapped to itself is called a derangement.

Derangements

Definition

A permutation function in which no element is mapped to itself is called a derangement.

Example

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

Cycle theorem

Cycle theorem

Theorem

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz.,

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1),

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Assume that the theorem is true for all sets with size at most $(n-1)$.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Assume that the theorem is true for all sets with size at most $(n - 1)$.

Let A be a set having n elements.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Assume that the theorem is true for all sets with size at most $(n - 1)$.

Let A be a set having n elements. Pick an element $a \in A$.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Assume that the theorem is true for all sets with size at most $(n-1)$.

Let A be a set having n elements. Pick an element $a \in A$.

Let f be some arbitrary permutation function defined on A.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Assume that the theorem is true for all sets with size at most $(n-1)$.

Let A be a set having n elements. Pick an element $a \in A$.

Let f be some arbitrary permutation function defined on A.

Let $f^{(i)}$ denote the result of applying f on a, i times.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Assume that the theorem is true for all sets with size at most $(n-1)$.

Let A be a set having n elements. Pick an element $a \in A$.

Let f be some arbitrary permutation function defined on A.

Let $f^{(i)}$ denote the result of applying f on a, i times. For instance, $f^{(1)}(a) = f(a)$,

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Assume that the theorem is true for all sets with size at most $(n-1)$.

Let A be a set having n elements. Pick an element $a \in A$.

Let f be some arbitrary permutation function defined on A.

Let $f^{(i)}$ denote the result of applying f on a, i times. For instance, $f^{(1)}(a) = f(a)$, $f^{(2)}(a) = f(f(a))$ and so on.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Assume that the theorem is true for all sets with size at most $(n-1)$.

Let A be a set having n elements. Pick an element $a \in A$.

Let f be some arbitrary permutation function defined on A.

Let $f^{(i)}$ denote the result of applying f on a, i times. For instance, $f^{(1)}(a) = f(a)$, $f^{(2)}(a) = f(f(a))$ and so on.

Without loss of generality, we can assume that f is a derangement.

Cycle theorem

Theorem

Every permutation on a finite set can be represented as a composition of disjoint cycles. This decomposition is unique up to a cyclic reordering.

Proof.

We use induction on the number of elements in the ground set A.

Assume that A has only one element. There is only one permutation, viz., (1), i.e., the identity permutation.

Assume that the theorem is true for all sets with size at most $(n-1)$.

Let A be a set having n elements. Pick an element $a \in A$.

Let f be some arbitrary permutation function defined on A.

Let $f^{(i)}$ denote the result of applying f on a, i times. For instance, $f^{(1)}(a) = f(a)$, $f^{(2)}(a) = f(f(a))$ and so on.

Without loss of generality, we can assume that f is a derangement. (Why?)

□

Proof of Cycle theorem

Proof of Cycle theorem

Proof.

Proof of Cycle theorem

Proof.

Consider the sequence

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a),$

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a),$

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat.

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that,

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$.

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$. (Why?)

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$. (Why?)

Let r be the smallest positive integer such that $f^{(r)}(a) = a$.

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$. (Why?)

Let r be the smallest positive integer such that $f^{(r)}(a) = a$. We must have $r \geq$

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$. (Why?)

Let r be the smallest positive integer such that $f^{(r)}(a) = a$. We must have $r \geq 2$.

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$. (Why?)

Let r be the smallest positive integer such that $f^{(r)}(a) = a$. We must have $r \geq 2$.

Then, we have a cycle: $C = (a, f(a), f(f(a)), \ldots, f^{(r-1)}(a))$.

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$. (Why?)

Let r be the smallest positive integer such that $f^{(r)}(a) = a$. We must have $r \geq 2$.

Then, we have a cycle: $C = (a, f(a), f(f(a)), \ldots, f^{(r-1)}(a))$.

Moreover, any cycle containing a has to be of the above form (up to a cyclic re-ordering).

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$. (Why?)

Let r be the smallest positive integer such that $f^{(r)}(a) = a$. We must have $r \geq 2$.

Then, we have a cycle: $C = (a, f(a), f(f(a)), \ldots, f^{(r-1)}(a))$.

Moreover, any cycle containing a has to be of the above form (up to a cyclic re-ordering).

Remove C from A.

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$. (Why?)

Let r be the smallest positive integer such that $f^{(r)}(a) = a$. We must have $r \geq 2$.

Then, we have a cycle: $C = (a, f(a), f(f(a)), \ldots, f^{(r-1)}(a))$.

Moreover, any cycle containing a has to be of the above form (up to a cyclic re-ordering).

Remove C from A.

It is now easy to use the first principle of induction and establish that f can be represented as a composition of cycles.

Proof of Cycle theorem

Proof.

Consider the sequence $(f(a), f^{(2)}(a), f^{(3)}(a), \ldots)$.

The above sequence must eventually repeat. (Why?)

It follows that there exist k and l such that, $k < l$ and $f^{(k)}(a) = f^{(l)}(a)$.

Hence $f^{(l-k)}(a) = a$. (Why?)

Let r be the smallest positive integer such that $f^{(r)}(a) = a$. We must have $r \geq 2$.

Then, we have a cycle: $C = (a, f(a), f(f(a)), \ldots, f^{(r-1)}(a))$.

Moreover, any cycle containing a has to be of the above form (up to a cyclic re-ordering).

Remove C from A.

It is now easy to use the first principle of induction and establish that f can be represented as a composition of cycles.

□

Completing the proof

Completing the proof

Proof.

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Suppose $a, b \in A$.

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Suppose $a, b \in A$.

Then, if the cycles of a and b are not disjoint, there exist j, k such that

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Suppose $a, b \in A$.

Then, if the cycles of a and b are not disjoint, there exist j, k such that $f^{(j)}(b) = f^{(k)}(a)$,

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Suppose $a, b \in A$.

Then, if the cycles of a and b are not disjoint, there exist j, k such that $f^{(j)}(b) = f^{(k)}(a)$, where $k > j$, without loss of generality.

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Suppose $a, b \in A$.

Then, if the cycles of a and b are not disjoint, there exist j, k such that $f^{(j)}(b) = f^{(k)}(a)$, where $k > j$, without loss of generality. (Why?)

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Suppose $a, b \in A$.

Then, if the cycles of a and b are not disjoint, there exist j, k such that $f^{(j)}(b) = f^{(k)}(a)$, where $k > j$, without loss of generality. (Why?)

This forces $b = f^{(k-j)}(a)$, so b is in the cycle of a.

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Suppose $a, b \in A$.

Then, if the cycles of a and b are not disjoint, there exist j, k such that $f^{(j)}(b) = f^{(k)}(a)$, where $k > j$, without loss of generality. (Why?)

This forces $b = f^{(k-j)}(a)$, so b is in the cycle of a. (Why?)

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Suppose $a, b \in A$.

Then, if the cycles of a and b are not disjoint, there exist j, k such that $f^{(j)}(b) = f^{(k)}(a)$, where $k > j$, without loss of generality. (Why?)

This forces $b = f^{(k-j)}(a)$, so b is in the cycle of a. (Why?)

But then, starting the cycle at b, we see that the cycle of b is the same as the cycle of a.

Completing the proof

Proof.

It thus suffices to show that any two cycles obtained this way are either equal or disjoint.

Suppose $a, b \in A$.

Then, if the cycles of a and b are not disjoint, there exist j, k such that $f^{(j)}(b) = f^{(k)}(a)$, where $k > j$, without loss of generality. (Why?)

This forces $b = f^{(k-j)}(a)$, so b is in the cycle of a. (Why?)

But then, starting the cycle at b, we see that the cycle of b is the same as the cycle of a.

Thus, the cycles of a and b must be either identical or disjoint.

□

Counting Functions

Counting Functions

Counting mappings

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \rightarrow T$ denote a function from S to T.

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \rightarrow T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \to T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?
$n \cdot n \cdot \ldots n =$

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \rightarrow T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?
$n \cdot n \cdot \ldots n = n^m$.

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \rightarrow T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?
$n \cdot n \cdot \ldots n = n^m$.

(ii) How many functions are possible from S to T, assuming that f is injective?

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \to T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?
$n \cdot n \cdot \ldots n = n^m$.

(ii) How many functions are possible from S to T, assuming that f is injective?
$n \cdot (n-1) \cdot (n-1) \ldots [n-(m-1)] =$

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \rightarrow T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?
$n \cdot n \cdot \ldots n = n^m$.

(ii) How many functions are possible from S to T, assuming that f is injective?
$n \cdot (n-1) \cdot (n-1) \ldots [n-(m-1)] = \frac{n!}{(n-m)!} =$

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \rightarrow T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?
$n \cdot n \cdot \ldots n = n^m$.

(ii) How many functions are possible from S to T, assuming that f is injective?
$n \cdot (n-1) \cdot (n-1) \ldots [n-(m-1)] = \frac{n!}{(n-m)!} = P(n, m)$.

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \rightarrow T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?
$n \cdot n \cdot \ldots n = n^m$.

(ii) How many functions are possible from S to T, assuming that f is injective?
$n \cdot (n-1) \cdot (n-1) \ldots [n-(m-1)] = \frac{n!}{(n-m)!} = P(n, m)$.

(iii) How many functions are possible from S to T, assuming that f is surjective?

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \rightarrow T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?
$n \cdot n \cdot \ldots n = n^m$.

(ii) How many functions are possible from S to T, assuming that f is injective?
$n \cdot (n-1) \cdot (n-1) \ldots [n-(m-1)] = \frac{n!}{(n-m)!} = P(n, m)$.

(iii) How many functions are possible from S to T, assuming that f is surjective?

No nice formula or easy answer.

Counting Functions

Counting mappings

Let S and T be sets with cardinality m and n respectively.

Let $f : S \rightarrow T$ denote a function from S to T.

(i) How many functions are possible from S to T, assuming no restriction on f?
$n \cdot n \cdot \ldots n = n^m$.

(ii) How many functions are possible from S to T, assuming that f is injective?
$n \cdot (n-1) \cdot (n-1) \ldots [n-(m-1)] = \frac{n!}{(n-m)!} = P(n, m)$.

(iii) How many functions are possible from S to T, assuming that f is surjective?

No nice formula or easy answer.

We count the number of non-onto functions and subtract this quantity from the total number of functions!

Counting the non-onto functions

Counting the non-onto functions

Establishing the bound

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$.

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Let $t_1, t_2, \ldots, t_n$ denote the elements of T.

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Let $t_1, t_2, \ldots, t_n$ denote the elements of T.

Let A_i denote the set of functions from S to T that do not map any element of S to t_i.

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Let $t_1, t_2, \ldots, t_n$ denote the elements of T.

Let A_i denote the set of functions from S to T that do not map any element of S to t_i.

Every non-onto function belongs to at least one such set!

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Let $t_1, t_2, \ldots, t_n$ denote the elements of T.

Let A_i denote the set of functions from S to T that do not map any element of S to t_i.

Every non-onto function belongs to at least one such set!

Therefore, the total number of non-onto functions is $|A_1 \cup A_2 \ldots A_n|$.

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Let $t_1, t_2, \ldots, t_n$ denote the elements of T.

Let A_i denote the set of functions from S to T that do not map any element of S to t_i.

Every non-onto function belongs to at least one such set!

Therefore, the total number of non-onto functions is $|A_1 \cup A_2 \ldots A_n|$.

Observe that,

$$|A_1 \cup A_2 \ldots A_n| = \sum_{1 \leq i \leq n} |A_i|$$

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Let $t_1, t_2, \ldots, t_n$ denote the elements of T.

Let A_i denote the set of functions from S to T that do not map any element of S to t_i.

Every non-onto function belongs to at least one such set!

Therefore, the total number of non-onto functions is $|A_1 \cup A_2 \ldots A_n|$.

Observe that,

$$|A_1 \cup A_2 \ldots A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|$$

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Let $t_1, t_2, \ldots, t_n$ denote the elements of T.

Let A_i denote the set of functions from S to T that do not map any element of S to t_i.

Every non-onto function belongs to at least one such set!

Therefore, the total number of non-onto functions is $|A_1 \cup A_2 \ldots A_n|$.

Observe that,

$$\begin{aligned} |A_1 \cup A_2 \ldots A_n| &= \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \ldots \end{aligned}$$

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Let $t_1, t_2, \ldots, t_n$ denote the elements of T.

Let A_i denote the set of functions from S to T that do not map any element of S to t_i.

Every non-onto function belongs to at least one such set!

Therefore, the total number of non-onto functions is $|A_1 \cup A_2 \ldots A_n|$.

Observe that,

$$\begin{aligned}
|A_1 \cup A_2 \ldots A_n| &= \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\
&+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \ldots \\
&+ (-1)^{n+1} |A_1 \cap A_2 \ldots \cap A_n|
\end{aligned}$$

Counting the non-onto functions

Establishing the bound

Without loss of generality, assume that $m \geq n$. Why?

Let $t_1, t_2, \ldots, t_n$ denote the elements of T.

Let A_i denote the set of functions from S to T that do not map any element of S to t_i.

Every non-onto function belongs to at least one such set!

Therefore, the total number of non-onto functions is $|A_1 \cup A_2 \ldots A_n|$.

Observe that,

$$\begin{aligned} |A_1 \cup A_2 \ldots A_n| &= \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \ldots \\ &+ (-1)^{n+1} |A_1 \cap A_2 \ldots \cap A_n| \end{aligned}$$

(Principle of Inclusion and Exclusion)

Cardinality of set of onto functions

Cardinality of set of onto functions

Establishing the bound

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$.

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n, 1) \cdot (n-1)^m$.

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)^m$.

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)^m$.

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)^m$.

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)^m$. (Why?)

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)^m$.

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)^m$. (Why?)

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)^m$.

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)^m$.

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)^m$. (Why?)

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)^m$.

It follows that:

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)^m$.

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)^m$. (Why?)

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)^m$.

It follows that:

$$\begin{aligned} |A_1 \cup A_2 \ldots A_n| &= C(n,1) \cdot (n-1)^m - C(n,2) \cdot (n-2)^m \\ &\quad + \ldots + (-1)^{n+1} C(n,n) \cdot (n-n)^m \end{aligned}$$

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)^m$.

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)^m$. (Why?)

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)^m$.

It follows that:

$$\begin{aligned} |A_1 \cup A_2 \ldots A_n| &= C(n,1) \cdot (n-1)^m - C(n,2) \cdot (n-2)^m \\ &\quad + \ldots + (-1)^{n+1} C(n,n) \cdot (n-n)^m \end{aligned}$$

Therefore, the number of onto functions is:

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)^m$.

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)^m$. (Why?)

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)^m$.

It follows that:

$$\begin{aligned} |A_1 \cup A_2 \ldots A_n| &= C(n,1) \cdot (n-1)^m - C(n,2) \cdot (n-2)^m \\ &\quad + \ldots + (-1)^{n+1} C(n,n) \cdot (n-n)^m \end{aligned}$$

Therefore, the number of onto functions is:

n^m

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)^m$.

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)^m$. (Why?)

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)^m$.

It follows that:

$$\begin{aligned} |A_1 \cup A_2 \ldots A_n| &= C(n,1) \cdot (n-1)^m - C(n,2) \cdot (n-2)^m \\ &\quad + \ldots + (-1)^{n+1} C(n,n) \cdot (n-n)^m \end{aligned}$$

Therefore, the number of onto functions is:

$n^m - [C(n,1) \cdot (n-1)^m - C(n,2) \cdot (n-2)^m - \ldots$

Cardinality of set of onto functions

Establishing the bound

For any fixed A_i, $|A_i| = (n-1)^m$. (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)^m$.

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)^m$. (Why?)

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)^m$.

It follows that:

$$\begin{aligned} |A_1 \cup A_2 \ldots A_n| &= C(n,1) \cdot (n-1)^m - C(n,2) \cdot (n-2)^m \\ &\quad + \ldots + (-1)^{n+1} C(n,n) \cdot (n-n)^m \end{aligned}$$

Therefore, the number of onto functions is:

$n^m - [C(n,1) \cdot (n-1)^m - C(n,2) \cdot (n-2)^m - \ldots + (-1)^n C(n,n-1) \cdot (1)^m]$.

Counting derangements

Counting derangements

Establishing the bound

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

We want to count the number of possible derangements on a set with n elements.

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

We want to count the number of possible derangements on a set with n elements.

This is once again a difficult task, but we use the same approach as was used for counting the number of onto functions.

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

We want to count the number of possible derangements on a set with n elements.

This is once again a difficult task, but we use the same approach as was used for counting the number of onto functions.

Observe that the total number of derangements (d)

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

We want to count the number of possible derangements on a set with n elements.

This is once again a difficult task, but we use the same approach as was used for counting the number of onto functions.

Observe that the total number of derangements (d) is precisely the difference between

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

We want to count the number of possible derangements on a set with n elements.

This is once again a difficult task, but we use the same approach as was used for counting the number of onto functions.

Observe that the total number of derangements (d) is precisely the difference between the total number of permutation functions (f)

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

We want to count the number of possible derangements on a set with n elements.

This is once again a difficult task, but we use the same approach as was used for counting the number of onto functions.

Observe that the total number of derangements (d) is precisely the difference between the total number of permutation functions (f) and the total number of permutation functions that map at least one least one element to itself (g),

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

We want to count the number of possible derangements on a set with n elements.

This is once again a difficult task, but we use the same approach as was used for counting the number of onto functions.

Observe that the total number of derangements (d) is precisely the difference between the total number of permutation functions (f) and the total number of permutation functions that map at least one least one element to itself (g),
i.e., $d = f - g$.

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

We want to count the number of possible derangements on a set with n elements.

This is once again a difficult task, but we use the same approach as was used for counting the number of onto functions.

Observe that the total number of derangements (d) is precisely the difference between the total number of permutation functions (f) and the total number of permutation functions that map at least one least one element to itself (g),
i.e., $d = f - g$.

We know that $f =$

Counting derangements

Establishing the bound

Recall that a derangement is a permutation function in which no element is mapped to itself.

We want to count the number of possible derangements on a set with n elements.

This is once again a difficult task, but we use the same approach as was used for counting the number of onto functions.

Observe that the total number of derangements (d) is precisely the difference between the total number of permutation functions (f) and the total number of permutation functions that map at least one least one element to itself (g),
i.e., $d = f - g$.

We know that $f = n!$.

Counting derangements (contd.)

Counting derangements (contd.)

Establishing the bound

Counting derangements (contd.)

Establishing the bound

Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the ground set.

Counting derangements (contd.)

Establishing the bound

Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the ground set.

Let A_i denote the set of permutations that leave a_i fixed.

Counting derangements (contd.)

Establishing the bound

Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the ground set.

Let A_i denote the set of permutations that leave a_i fixed.

It follows that the total number of non-derangements is:

Counting derangements (contd.)

Establishing the bound

Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the ground set.

Let A_i denote the set of permutations that leave a_i fixed.

It follows that the total number of non-derangements is:

$$|A_1 \cup A_2 \ldots A_n|$$

Counting derangements (contd.)

Establishing the bound

Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the ground set.

Let A_i denote the set of permutations that leave a_i fixed.

It follows that the total number of non-derangements is:

$$|A_1 \cup A_2 \ldots A_n| = \sum_{1 \leq i \leq n} |A_i|$$

Counting derangements (contd.)

Establishing the bound

Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the ground set.

Let A_i denote the set of permutations that leave a_i fixed.

It follows that the total number of non-derangements is:

$$\begin{aligned} |A_1 \cup A_2 \ldots A_n| &= \sum_{1 \le i \le n} |A_i| \\ &- \sum_{1 \le i < j \le n} |A_i \cap A_j| \end{aligned}$$

Counting derangements (contd.)

Establishing the bound

Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the ground set.

Let A_i denote the set of permutations that leave a_i fixed.

It follows that the total number of non-derangements is:

$$
\begin{aligned}
|A_1 \cup A_2 \ldots A_n| \quad = \quad & \sum_{1 \leq i \leq n} |A_i| \\
& - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\
& + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \ldots
\end{aligned}
$$

Counting derangements (contd.)

Establishing the bound

Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the ground set.

Let A_i denote the set of permutations that leave a_i fixed.

It follows that the total number of non-derangements is:

$$
\begin{aligned}
|A_1 \cup A_2 \ldots A_n| \quad = \quad & \sum_{1 \le i \le n} |A_i| \\
& - \sum_{1 \le i < j \le n} |A_i \cap A_j| \\
& + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \ldots \\
& + (-1)^{n+1} |A_1 \cap A_2 \ldots \cap A_n|
\end{aligned}
$$

Counting derangements (contd.)

Establishing the bound

Let $A = \{a_1, a_2, \ldots, a_n\}$ denote the ground set.

Let A_i denote the set of permutations that leave a_i fixed.

It follows that the total number of non-derangements is:

$$
\begin{aligned}
|A_1 \cup A_2 \ldots A_n| &= \sum_{1 \le i \le n} |A_i| \\
&\quad - \sum_{1 \le i < j \le n} |A_i \cap A_j| \\
&\quad + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \ldots \\
&\quad + (-1)^{n+1} |A_1 \cap A_2 \ldots \cap A_n|
\end{aligned}
$$

(Principle of Inclusion and Exclusion)

Counting derangements (contd.)

Counting derangements (contd.)

Establishing the bound

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n, 1) \cdot (n-1)!$

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n, 1) \cdot (n-1)!$

For any fixed A_i and A_j, $|A_i \cap A_j| =$

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n, 1) \cdot (n-1)!$

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)!$

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n, 1) \cdot (n-1)!$

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)!$

Therefore, the total number of such terms is

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n, 1) \cdot (n-1)!$

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)!$

Therefore, the total number of such terms is $C(n, 2) \cdot (n-2)!$

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n, 1) \cdot (n-1)!$

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)!$

Therefore, the total number of such terms is $C(n, 2) \cdot (n-2)!$

It follows that the total number of non-derangements is

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)!$

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)!$

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)!$

It follows that the total number of non-derangements is

$$\begin{aligned} |A_1 \cup A_2 \ldots \cup A_n| &= C(n,1) \cdot (n-1)! \\ &\quad -C(n,2) \cdot (n-2)! + \ldots \\ &\quad +(-1)^{n+1} C(n,n) \cdot (n-n)! \end{aligned}$$

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)!$

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)!$

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)!$

It follows that the total number of non-derangements is

$$\begin{aligned} |A_1 \cup A_2 \ldots \cup A_n| &= C(n,1) \cdot (n-1)! \\ &\quad - C(n,2) \cdot (n-2)! + \ldots \\ &\quad + (-1)^{n+1} C(n,n) \cdot (n-n)! \end{aligned}$$

Therefore, the total number of derangements is:

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n, 1) \cdot (n-1)!$

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)!$

Therefore, the total number of such terms is $C(n, 2) \cdot (n-2)!$

It follows that the total number of non-derangements is

$$\begin{aligned} |A_1 \cup A_2 \ldots \cup A_n| &= C(n,1) \cdot (n-1)! \\ &\quad -C(n,2) \cdot (n-2)! + \ldots \\ &\quad +(-1)^{n+1} C(n,n) \cdot (n-n)! \end{aligned}$$

Therefore, the total number of derangements is:

$n!$

Counting derangements (contd.)

Establishing the bound

For any fixed A_i, $|A_i| = (1) \cdot (n-1) \cdot (n-2) \ldots (1) = (n-1)!$ (Why?)

Therefore, the total number of such terms is $C(n,1) \cdot (n-1)!$

For any fixed A_i and A_j, $|A_i \cap A_j| = (n-2)!$

Therefore, the total number of such terms is $C(n,2) \cdot (n-2)!$

It follows that the total number of non-derangements is

$$\begin{aligned} |A_1 \cup A_2 \ldots \cup A_n| &= C(n,1) \cdot (n-1)! \\ &\quad -C(n,2) \cdot (n-2)! + \ldots \\ &\quad +(-1)^{n+1} C(n,n) \cdot (n-n)! \end{aligned}$$

Therefore, the total number of derangements is:

$$n! - [C(n,1) \cdot (n-1)! - C(n,2) \cdot (n-2)! + \ldots + (-1)^{n+1} C(n,n) \cdot (n-n)!]$$

Examples

Example

Let $S = \{A, B, C\}$ and $T = \{a, b\}$.

Examples

Example

Let $S = \{A, B, C\}$ and $T = \{a, b\}$.

(i) How many onto functions exist from S to T?

Examples

Example

Let $S = \{A, B, C\}$ and $T = \{a, b\}$.

(i) How many onto functions exist from S to T? **Solution:**

Examples

Example

Let $S = \{A, B, C\}$ and $T = \{a, b\}$.

(i) How many onto functions exist from S to T? **Solution:** 6.

Examples

Example

Let $S = \{A, B, C\}$ and $T = \{a, b\}$.

(i) How many onto functions exist from S to T? **Solution:** 6.

(ii) How many derangements exist on S?

Examples

Example

Let $S = \{A, B, C\}$ and $T = \{a, b\}$.

(i) How many onto functions exist from S to T? **Solution:** 6.

(ii) How many derangements exist on S? **Solution:**

Examples

Example

Let $S = \{A, B, C\}$ and $T = \{a, b\}$.

(i) How many onto functions exist from S to T? **Solution:** 6.

(ii) How many derangements exist on S? **Solution:** 2.