Permutations

An overview of algebra and combinatorics through the concrete approach of permutations

Sirawit Pongnakintr

October 15, 2023

Table of contents

Main objectives of this journey!

- To get a “feeling” of invariants and quotients through concrete examples on permutations.

Main objectives of this journey!

- To get a “feeling” of invariants and quotients through concrete examples on permutations.
- To be able to practice competitive programming problems involving variants, invariants, duality, and permutations.

Main objectives of this journey!

- To get a “feeling” of invariants and quotients through concrete examples on permutations.
- To be able to practice competitive programming problems involving variants, invariants, duality, and permutations.

Expected duration: 2.5 hours

Motivation (Competitive Programming)

- *lingling* (2021-2022)
- *o58_mar_c2_permutepermute* (2014-2015)
- *https://szkopul.edu.pl/problemset/problem/_cVmDXXn2TjF0dF1rW6eazA0/site/?key=statement*
- *findpermutation* (2021-2022)
- *o61_may03_muscle* (2017-2018)
- $(\star)$ *abc* (2022-2023)
- *https://www.codechef.com/problems/CHRL3*
- $(\star)$ *sortingtapes* (2022-2023)
- $(\star)$ CEOI2016 trick (*https://cses.fi/193/list/*)
- $(\star)$ *https://oj.uz/problem/view/JOI18_bubblesort2*
- $(\star)$ *https://oj.uz/problem/view/JOI18_asceticism*
- $(\star)$ *https://codeforces.com/contest/1193/problem/C*

Permutations

Permutation

For any $n \in \mathbb{N}_+$, we define $\mathfrak{S}_n$ to be the set of all bijections from $\{1, \dots, n\}$ to $\{1, \dots, n\}$.

Remark

We may write the symbol $\mathfrak{S}_n$ simply as S_n.

Notation

Notation

For a bijection $\sigma \in \mathfrak{S}_n$, we write σ as $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

Example

Let $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$, then $\sigma_1 \in \mathfrak{S}_4$

Let $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 1 & 4 & 2 \end{pmatrix}$.

Remark

We denote $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ by Id_n.

Support

Definition 1

For any permutation $\sigma \in \mathfrak{S}_n$, we define its support $\mathsf{supp}(\sigma)$ as the set of integers from 1 to n where the permutation has effect on it. Formally,

$$\mathsf{supp}(\sigma) = \{x \in \{1, \ldots, n\} \colon \sigma(x) \neq x\}$$

Example

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 1 & 4 & 2 \end{pmatrix}$ What is $\mathsf{supp}(\sigma)$?

k-cycles

Definition 2

A permutation $\sigma \in \mathfrak{S}_n$ is said to be a k-cycle if there exists $x_1, x_2, \dots, x_k \in \{1, \dots, n\}$ all different such that $\sigma(x_i) = x_{i+1}$ for all $i \in \{1, \dots, k-1\}$ and $\sigma(x_k) = x_1$.

Example

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$ is a 4-cycle.

Cycle Notation

Products of permutations

Let σ_1 and σ_2 be some permutations of $\mathfrak{S}_n$, then the product of the permutations is $\sigma_1 \circ \sigma_2$.

Warning

In general $\sigma_1 \circ \sigma_2$ may not be $\sigma_2 \circ \sigma_1$. (Try to find an example.)

Remark

Product of cycles with disjoint support is commutative.

Exercises

Exercise 1

List all 3-cycles of $\mathfrak{S}_4$. Now, fix $2 \leq k \leq n$, how many k-cycles are there in $\mathfrak{S}_n$?

Exercise 2

Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 8 & 7 & 6 & 2 & 1 \end{pmatrix}$.

1. *Compute σ^{-1}.*
2. *Write σ as product of disjoint supports.*
3. *Write σ^2 in table notation and cycle notation.*
4. *Compute σ^{2019}.*

Factorization Theorem

Theorem 3 (Factorization Theorem)

Every permutation can be decomposed as a product of cycles with disjoint supports. This decomposition is unique up to order in which the cycles appear.

Proof

Transpositions

Definition 4

A transposition is a 2-cycle. Suppose $\sigma \in \mathfrak{S}_n$ is defined by $\sigma(i) = j$ and $\sigma(j) = i$ for $1 \leq i < j \leq n$ and $\sigma(k) = k$ for all $1 \leq k \leq n$ where $k \notin \{i, j\}$, then we may write σ as $\tau_{i,j}$.

Transpositions

Definition 4

A transposition is a 2-cycle. Suppose $\sigma \in \mathfrak{S}_n$ is defined by $\sigma(i) = j$ and $\sigma(j) = i$ for $1 \leq i < j \leq n$ and $\sigma(k) = k$ for all $1 \leq k \leq n$ where $k \notin \{i, j\}$, then we may write σ as $\tau_{i,j}$.

Proposition 5

For any transposition $\tau \in \mathfrak{S}_n$, $\tau^2 = \mathrm{Id}_n$.

Proof.

□

Decomposition into transpositions

Theorem 6

Every permutation can be decomposed as a product of transpositions (in a not necessarily unique way).

Proof

Exercises

Exercise 3

Let $n \in \mathbb{N}_+$ and $\sigma \in \mathfrak{S}_n$ be a permutation.

1. *Let $\sigma_1, \sigma_2 \in \mathfrak{S}_6$ where $\sigma_1 = (2, 4, 5)$ and $\sigma_2 = (1, 3)$. Compute $ord(\sigma_1), ord(\sigma_2)$ and $ord(\sigma_1 \circ \sigma_2)$.*
2. *Assume $n, p \in \mathbb{N}_+$ and $2 \leq p \leq n$. Prove that for any p-cycle σ in $\mathfrak{S}_n$, $\sigma^p = \mathrm{Id}_n$ and for any $1 \leq k < p$, $\sigma^k \neq \mathrm{Id}_n$. Deduce $ord(\sigma)$.*
3. *Assume $n \in \mathbb{N}_+$ and let σ be any permutation in $\mathfrak{S}_n$. Show that $ord(\sigma) \leq n!$*

Exercises

Exercise 4

Fix an integer $n \geq 2$, a permutation $\sigma \in \mathfrak{S}_n$ and consider a p-cycle $c = (a_1, a_2, \ldots, a_p)$. Show that $\sigma \circ c \circ \sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_p))$

Exercise 5

Fix an integer $n \geq 2$ and consider the circular permutation $c = (1, 2, \ldots, n-1, n)$. Find all the permutations $\sigma \in \mathfrak{S}_n$ that commute with c (that is $\sigma \circ c = c \circ \sigma$).

Exercise 6

Let n be an odd integer and $\sigma \in \mathfrak{S}_n$. Show that 4 divides

$$\prod_{i=1}^{n} (\sigma(i)^2 - i^2)$$

Inversions

Definition 7

For a permutation $\sigma \in \mathfrak{S}_n$, we denote by $I(\sigma)$ the number of inversions of σ, which is defined by the number of ordered pairs (i, j) where $1 \leq i < j \leq n$ such that $\sigma(i) > \sigma(j)$.

Signature

Definition 8

For a permutation $\sigma \in \mathfrak{S}_n$, we denote by $\varepsilon(\sigma)$ the signature of σ, which is defined by $\varepsilon(\sigma) := (-1)^{l(\sigma)}$.

Remark

If $\varepsilon(\sigma) = 1$, we say that σ is an even permutation. Otherwise $\varepsilon(\sigma) = -1$ and we say that σ is an odd permutation.

An important lemma

Lemma 9

Let n be a positive integer and $\sigma \in \mathfrak{S}_n$. Then

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Proof

Exercises

Exercise 7

Let σ be a permutation, show that σ^2 is an even permutation.

Exercise 8

In $\mathfrak{S}_n$, consider $\tau = (1\,2)$ and $\sigma = (1\,2 \cdots n)$.

1. *Let k be an integer such that $0 \leq k \leq n-2$. Compute $\sigma^k \circ \tau \circ \sigma^{-k}$.*
2. *Deduce that every permutation in $\mathfrak{S}_n$ can be written as a product of a sequence of τ and σ.*

Bubble sort (`lingling`) (2021-2022)

What is the number of swaps during a bubble sort? In other words, for any permutation $\sigma \in \mathfrak{S}_n$, what is the minimum number of k such that $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$ where for any $1 \leq i \leq k$, there exists $1 \leq a < n$ such that $\tau_i = \tau_{a,a+1}$?

Proposition 10

Given a permutation $\sigma \in \mathfrak{S}_n$, the number of swaps in the bubble sort of σ is $I(\sigma)$.

Inversion Table

Recall the following definition.

Definition 11

For a permutation $\sigma \in \mathfrak{S}_n$, we denote by $I(\sigma)$ the number of inversions of σ, which is defined by the number of ordered pairs (i, j) where $1 \leq i < j \leq n$ such that $\sigma(i) > \sigma(j)$.

Inversion Table

Recall the following definition.

Definition 11

For a permutation $\sigma \in \mathfrak{S}_n$, we denote by $I(\sigma)$ the number of inversions of σ, which is defined by the number of ordered pairs (i, j) where $1 \leq i < j \leq n$ such that $\sigma(i) > \sigma(j)$.

If, instead of computing the total number of inversions, we define $I_j(\sigma)$ for each $1 \leq j \leq n$ to be the number of indices i where $1 \leq i < j$ such that $\sigma(i) > \sigma(j)$, we obtain the inversion table.

Example

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 1 & 4 & 2 \end{pmatrix}$.

Then the inversion table is

$I_1(\sigma)$	$I_2(\sigma)$	$I_3(\sigma)$	$I_4(\sigma)$	$I_5(\sigma)$	$I_6(\sigma)$
0	1	2	3	3	4

Exercises

Exercise 9

Write a program which receives a permutation and compute its invariant table. What is the best complexity you can get?

Exercise 10

Write a program which receives an invariant table and reconstruct a permutation. What is the best complexity you can get? (Try: `o61_may03_muscle`*)*

Asceticism (JOI Spring Camp 2017-2018)

Problem from *https://oj.uz/problem/view/JOI18_asceticism*.

- Kukai reads the sutra with N sentences. These sentences are ordered, and he has to read in order.
- Each sentence has one integer between 1 and N, inclusive. No two different sentences have the same number.
- He has to read the sentence with the integer i $(1 \leq i \leq N)$ in the i-th period among the N equally divided time periods in a day. Each sentence is so short that it is always possible for him to read a sentence in a period.

Kukai wants to read the whole sutra as fast as possible. However, how many days it takes for him to finish depends on the integers on the sentences in the sutra. JOI-kun was asked by Kukai to count the number of possible ways of integers on the sentences that takes Kukai exactly K days to finish reading, if he reads optimally.

Equivalent reformulation: Eulerian number

Given N and K. Count the number of permutations of length N such that there are K “ascents”. An index $2 \leq i \leq N$ is said to be an ascent of $\sigma \in \mathfrak{S}_N$ if $\sigma(i-1) < \sigma(i)$.

Invariants

Equivalence Relations

Definition 12

Let A be a set. We call a set $R \subseteq A \times A$ an equivalence relation if it satisfies three following properties:

- (Reflexivity) For all $x \in A$, $(x, x) \in R$.
- (Symmetry) For all $x, y \in A$ if $(x, y) \in R$ then $(y, x) \in R$ also.
- (Transitivity) For all $x, y, z \in A$ if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$ also.

Example: Congruence

Let $n \in \mathbb{N}_+$. We introduce a relation $R \subseteq \mathbb{Z} \times \mathbb{Z}$ defined by

$$R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \colon n \text{ divides } (x - y)\}$$

and write $x \equiv y \pmod{n}$ whenever $(x, y) \in R$ (and $x \not\equiv y \pmod{n}$ whenever $(x, y) \notin R$).

Example: The last digit

Define $f\colon \mathbb{Z} \to \{0, 1, \ldots, 9\}$ by

$$f(x) = \text{the last digit of } x.$$

Then the relation

$$R := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \colon f(x) = f(y)\}$$

is an equivalence relation.

Generalization: Partitions

In general, if $f\colon A \to B$, then one can define an equivalence relation $R_f \subseteq A \times A$ as

$$R := \{(x, y) \in A \times A\colon f(x) = f(y)\}.$$

In other words, one try to “color” each element of A with colors in B, and the relation essentially means $(x, y) \in R$ if and only if x has the same color as y.

Another perspective: from equivalence to partitions

For a given set A. Suppose R is an equivalence relation on A. For each element x of A one can define an equivalence class of x, denoted by $[x]_R$, by

$$[x]_R := \{y \in A \colon (x, y) \in R\}.$$

Observe that the set $\{[x]_R \colon x \in A\}$ defines a partition in A, i.e. the function

$$f \colon \begin{cases} A & \to \mathcal{P}(A) \\ x & \to [x]_R \end{cases}$$

is a coloring of each element x by the color $[x]_R$.

Identifying things

Definition 13 (Quotient of a set by an equivalence relation)

From an equivalence relation R on A, the set of partitions

$$\{[x]_R : x \in A\}$$

is called “the quotient of A by R” and is denoted by A/R.

Example: The set of integers

If one has $\mathbb{N} = \{0, 1, \dots\}$ but not $\mathbb{Z}$, how would one define $\mathbb{Z}$?

Example: The set of integers

If one has $\mathbb{N} = \{0, 1, \dots\}$ but not $\mathbb{Z}$, how would one define $\mathbb{Z}$?

People came up with a way to define $\mathbb{Z}$ as $(\mathbb{N} \times \mathbb{N})/\sim$ where

$$\sim := \{((x_1, x_2), (y_1, y_2)) \in (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \colon x_1 + y_2 = x_2 + y_1\}.$$

Extras: The rationals and the reals

We may do similar things to construct the rationals. That is, on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ one defines the equivalence relation $\sim_{\mathbb{Q}}$ as

$$\sim_{\mathbb{Q}} := \{((x_1, x_2), (y_1, y_2)) \in (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) \times (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) \colon x_1 y_2 = x_2 y_1\}.$$

Extras: The rationals and the reals

We may do similar things to construct the rationals. That is, on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ one defines the equivalence relation $\sim_{\mathbb{Q}}$ as

$$\sim_{\mathbb{Q}} := \{((x_1, x_2), (y_1, y_2)) \in (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) \times (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) \colon x_1 y_2 = x_2 y_1\}.$$

The reals are a bit complicated. It can be defined (in one way, among a few other definitions) as the quotient of the set of Cauchy sequences which is identified when the difference (term-wise) tends to zero. That is, consider the set of functions on $\mathbb{N} \to \mathbb{Q}$. We say f is (rational) Cauchy if for all $\varepsilon \in \mathbb{Q}_{>0}$ there exists $N \in \mathbb{N}$ such that for all $n, m \in \mathbb{N}$ if $n, m \geq N$ then $|f(n) - f(m)| < \varepsilon$. Let S be the set of all these functions. Then we define $\sim_{\mathbb{R}}$ as

$$\sim_{\mathbb{R}} := \{(f, g) \in S \times S \colon \forall \varepsilon \in \mathbb{Q}_{>0}, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq N \Rightarrow |f(n) - g(n)| < \varepsilon\}.$$

Then we define $\mathbb{R}$ to be $S/ \sim_{\mathbb{R}}$.

abc (2022-2023)

We call the string composed of letters “a”, “b”, or “c” as abc-string. Define the norm of an abc-string as

$$N(S) = (N_a(S) - N_b(S))^2 + (N_b(S) - N_c(S))^2 + (N_c(S) - N_a(S))^2$$

where $N_a(S), N_b(S), N_c(S)$ denotes the number of “a”s, “b”s, and “c”s inside S respectively.

Given an abc-string S. Find the substring that attains the maximum norm (if there are multiple such substrings, return any).

Observations

The order of characters in S is not important, one can just consider $(N_a(S), N_b(S), N_c(S))$ as a triple, and define

$$\widetilde{N}(a, b, c) := (a - b)^2 + (b - c)^2 + (c - a)^2$$

as a function from $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$.

Observations

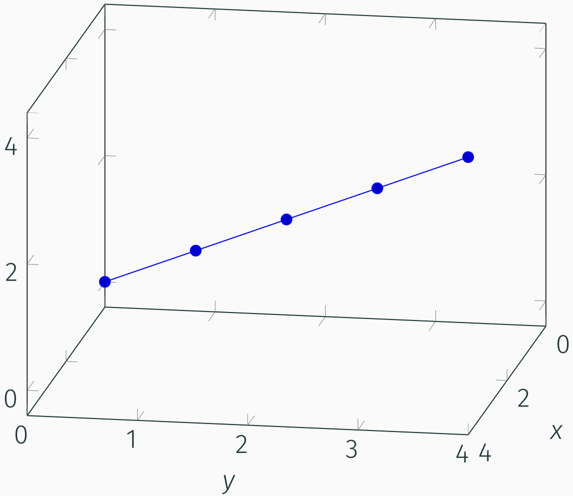
$$\widetilde{N}(a, b, c) = \widetilde{N}(a+1, b+1, c+1) = \dots$$

Observations

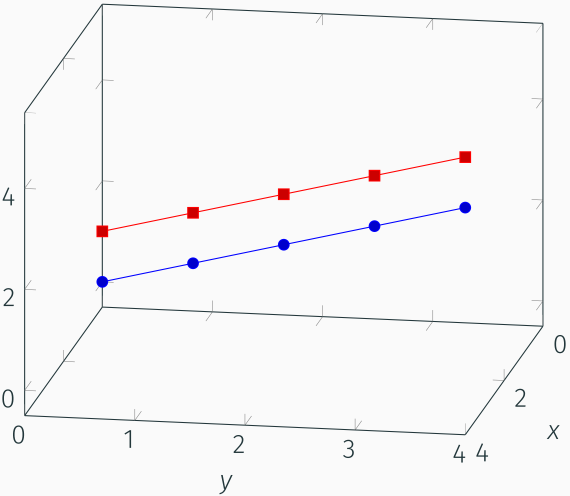
$$\widetilde{N}(a, b, c) = \widetilde{N}(a + 1, b + 1, c + 1) = \dots$$

How about we quotient the set $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ by this “coloring” of $\widetilde{N}$?

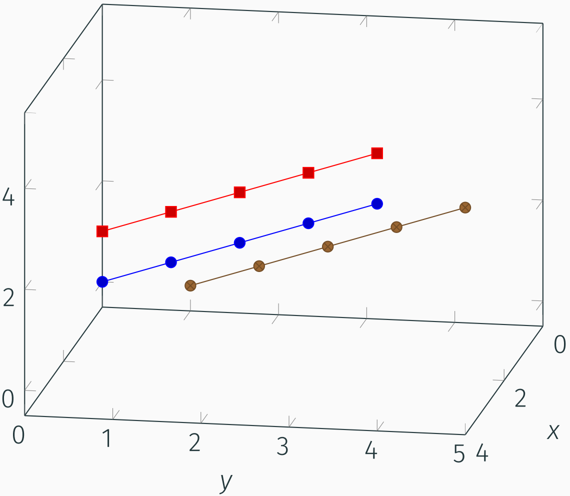
Geometric Intuition



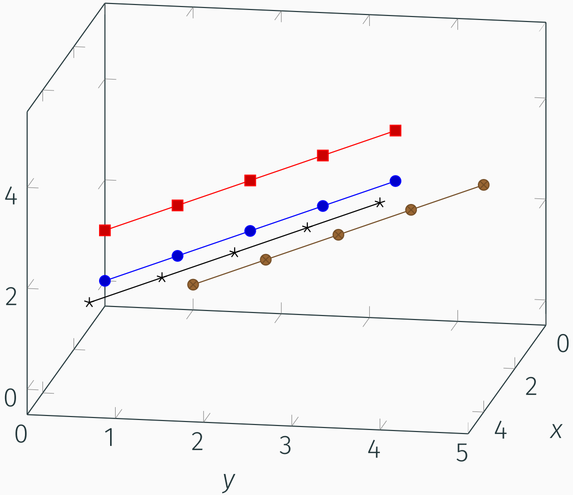
Geometric Intuition



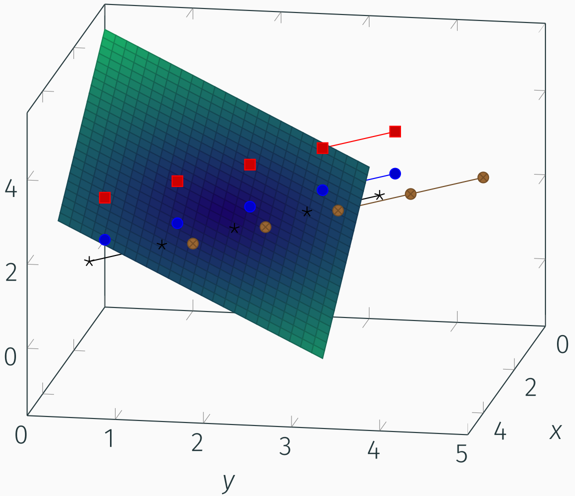
Geometric Intuition



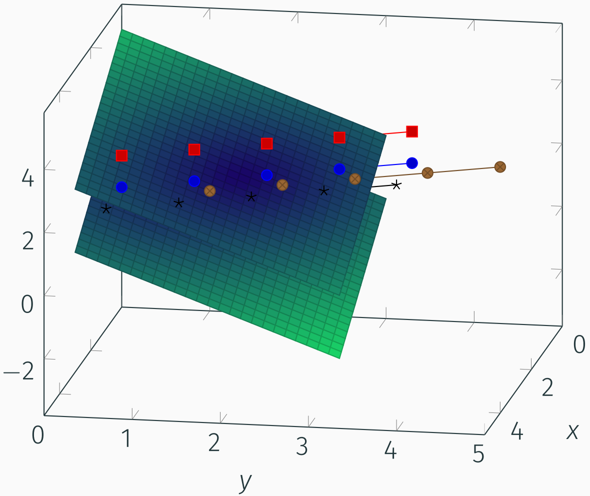
Geometric Intuition



Geometric Intuition



Geometric Intuition



Projection onto the plane $x + y + z = 0$

If (a, b, c) and (a', b', c') are two points, and let $\pi\colon \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ be the projection function into the plane $x + y + z = 0$, then $\widetilde{N}(a - a', b - b', c - c') = \widetilde{N}(\pi(a, b, c) - \pi(a', b', c'))$.

Projection onto the plane $x + y + z = 0$

If (a, b, c) and (a', b', c') are two points, and let $\pi\colon \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ be the projection function into the plane $x + y + z = 0$, then $\widetilde{N}(a - a', b - b', c - c') = \widetilde{N}(\pi(a, b, c) - \pi(a', b', c'))$.

Proof.

One may define $\pi(a, b, c)$ as $(a - \min(a, b, c), b - \min(a, b, c), c - \min(a, b, c))$ for all $a, b, c \in \mathbb{N}$. Then (let $m := \min(a, b, c)$ and $m' = \min(a', b', c')$),

$$\begin{aligned}
&\widetilde{N}(\pi(a, b, c) - \pi(a', b', c')) \\
&= \widetilde{N}((a - m, b - m, c - m) - (a' - m', b' - m', c' - m')) \\
&= \widetilde{N}(a - a' - m + m', b - b' - m + m', c - c' - m + m') \\
&= \widetilde{N}(a - a', b - b', c - c').
\end{aligned}$$

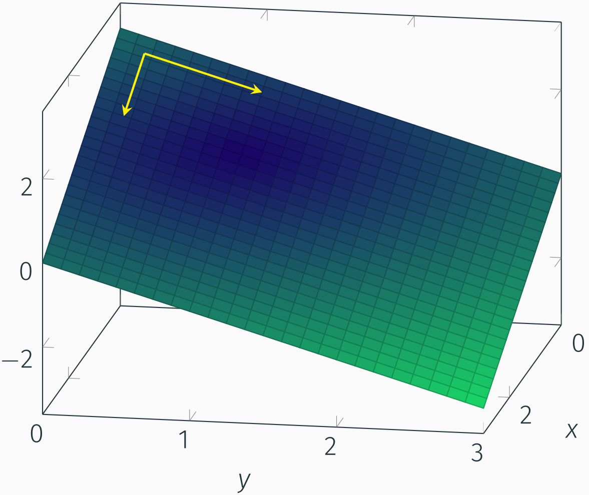
This completes the proof. □

Correspondence

$$\begin{tikzcd}
\textit{\texttt{abc-string}} \arrow[d, "\phi"] \\
(\mathbb{N} \times \mathbb{N} \times \mathbb{N})^{n} \arrow[d, "\text{quicksum}"] \\
(\mathbb{N} \times \mathbb{N} \times \mathbb{N})^{n+1} \arrow[d, "\pi"] \\
(\text{point on plane } x + y + z = 0)^{n+1}
\end{tikzcd}$$

Now, if we want to find a substring that maximizes N, it corresponds to finding the indices L and R $(0 \leq L < R \leq N)$ such that $\widetilde{N}(\mathrm{QS}_R - \mathrm{QS}_L)$ is maximized, which is actually: “find the farthest pair of points in the projected plane”.

Computation in the plane



Or you could even project it to the plane $z = 0$. (Try to prove that this also works!)

Partially Ordered Set

Partial order

Definition 14

A binary relation R on A (i.e. a subset of $A \times A$) is said to be a partial order if

- (Reflexivity) For all $x \in A$, $(x, x) \in R$.
- (Antisymmetry) For all $x, y \in A$, if $(x, y) \in R$ and $(y, x) \in R$ then $x = y$.
- (Transitivity) For all $x, y, z \in A$ if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$ also.

Example

Let $\preceq$ be a relation on $\mathbb{N}$ defined by
$\preceq := \{(x, y) \in \mathbb{N} \times \mathbb{N} \colon \exists k \in \mathbb{N}, y = kx\}$.

Another example

Example

Let $S = \{a, b, c, d\}$, then consider the power set $\mathcal{P}(S)$ and the relation $\subseteq$ defined on the power set. $(\mathcal{P}(S), \subseteq)$ is a partially ordered set.

Hasse Diagrams

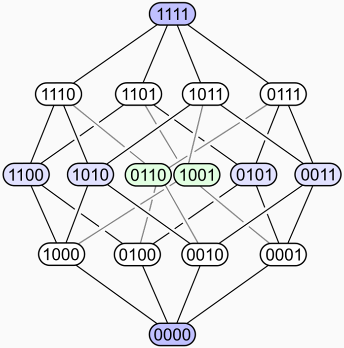


Figure 1: First diagram

Hasse Diagrams

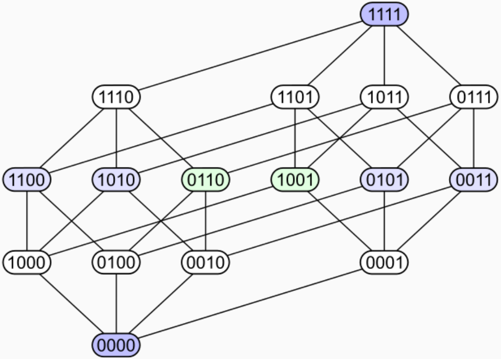


Figure 2: Second diagram

Hasse Diagrams

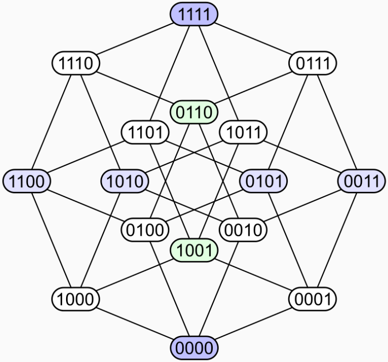


Figure 3: Third diagram

Hasse Diagrams

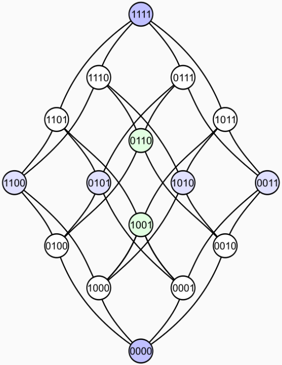


Figure 4: Fourth diagram

Figures credits: ”Watchduck”, Public domain, via Wikimedia Commons.
(see `https://en.wikipedia.org/wiki/Hasse_diagram`)

Total order

Definition 15

A partial order R on A is said to be total if and only if for all $x, y \in A$, $(x, y) \in R$ or $(y, x) \in R$.

Chains and antichains

Let R be a partial order on A.

Definition 16

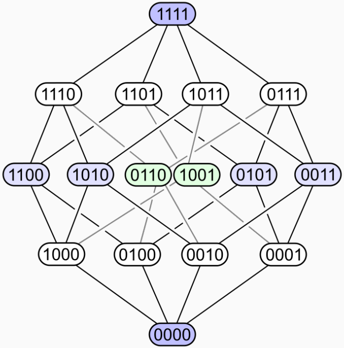
A set $S \subseteq A$ is a chain (with respect to the partial order R) if and only if R is a total order of S.

Definition 17

A set $S \subseteq A$ is an antichain (with respect to the partial order R) if and only if for all $x \neq y \in S$, both (x, y) and (y, x) are not in R. (i.e. no pair of elements in S is comparable)

Example (divisibility)

Another Example



An LIS Problem

Given an array A of N elements, find the length of longest increasing subsequence.

Another LIS Problem

Chef plays with the sequence of N numbers. During a single move Chef is able to choose a non-decreasing subsequence of the sequence and to remove it from the sequence. Help him to remove all the numbers in the minimal number of moves.

Problem source:
https://www.codechef.com/problems/CHRL3

Dilworth’s theorem

Theorem 18 (Dilworth’s theorem)

For a finite partially ordered set S with partial order $\preceq$ on S, the largest antichain has the same size as the smallest chain decomposition of S.

Dilworth's theorem

Theorem 18 (Dilworth's theorem)

For a finite partially ordered set S with partial order $\preceq$ on S, the largest antichain has the same size as the smallest chain decomposition of S.

What is a "chain decomposition"?

Dilworth's theorem

Theorem 18 (Dilworth's theorem)

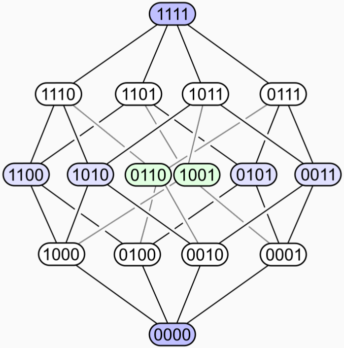
For a finite partially ordered set S with partial order $\preceq$ on S, the largest antichain has the same size as the smallest chain decomposition of S.

What is a "chain decomposition"?

Definition 19

A chain decomposition D is a partition of S such that for any $X \in D$, X is a chain.

The Same Old Example



Proof (given by Galvin, 1994)

By induction, remove a maximal element a of S and assume that $S - \{a\}$ has a smallest chain decomposition P with k chains (we write P as $P = \{P_1, P_2, \ldots, P_k\}$ where P_i is a chain, i.e., a totally-ordered subset of S) and that A_0 is a largest antichain with size k. Then for all $i \in \{1, \ldots, k\}$, $A_0 \cap P_i \neq \emptyset$. (Why?)

Proof (given by Galvin, 1994)

By induction, remove a maximal element a of S and assume that $S - \{a\}$ has a smallest chain decomposition P with k chains (we write P as $P = \{P_1, P_2, \ldots, P_k\}$ where P_i is a chain, i.e., a totally-ordered subset of S) and that A_0 is a largest antichain with size k. Then for all $i \in \{1, \ldots, k\}$, $A_0 \cap P_i \neq \emptyset$. (Why?)

Moreover, $A_0 \cap P_i$ has cardinality 1 (and they are all different).

Proof (given by Galvin, 1994)

By induction, remove a maximal element a of S and assume that $S - \{a\}$ has a smallest chain decomposition P with k chains (we write P as $P = \{P_1, P_2, \ldots, P_k\}$ where P_i is a chain, i.e., a totally-ordered subset of S) and that A_0 is a largest antichain with size k. Then for all $i \in \{1, \ldots, k\}$, $A_0 \cap P_i \neq \emptyset$. (Why?)

Moreover, $A_0 \cap P_i$ has cardinality 1 (and they are all different).

Before going to the main proof. Let us consider that proving that S has either an antichain of size $k + 1$ or a chain decomposition of size k is enough. Why?

Proof (given by Galvin, 1994)

By induction, remove a maximal element a of S and assume that $S - \{a\}$ has a smallest chain decomposition P with k chains (we write P as $P = \{P_1, P_2, \ldots, P_k\}$ where P_i is a chain, i.e., a totally-ordered subset of S) and that A_0 is a largest antichain with size k. Then for all $i \in \{1, \ldots, k\}$, $A_0 \cap P_i \neq \emptyset$. (Why?)

Moreover, $A_0 \cap P_i$ has cardinality 1 (and they are all different).

Before going to the main proof. Let us consider that proving that S has either an antichain of size $k + 1$ or a chain decomposition of size k is enough. Why?

Observe that S cannot have an antichain of size more than $k + 1$. (because we only add $\{a\}$ to $S - \{a\}$ which has the size of maximum antichain as k) Also observe that we cannot have a chain decomposition of size less than k. (because $S - \{a\}$ already has a smallest chain decomposition of size k)

Proof (cont.)

If S has an antichain of size $k + 1$, can the smallest chain decomposition have size k?

Proof (cont.)

If S has an antichain of size $k+1$, can the smallest chain decomposition have size k?

The answer is no, because if there is an antichain of size $k+1$ and a chain decomposition of size k, then by the pigeonhole principle, two elements of the antichain belong to the same chain, which is a contradiction.

Proof (cont.)

If S has an antichain of size $k + 1$, can the smallest chain decomposition have size k?

The answer is no, because if there is an antichain of size $k + 1$ and a chain decomposition of size k, then by the pigeonhole principle, two elements of the antichain belong to the same chain, which is a contradiction.

Now, if S has a chain decomposition of size k, can there be an antichain of size $k + 1$? (Surely there is an antichain of size k in S because A_0 is already an antichain of size k in $S - \{a\}$)

Proof (cont.)

If S has an antichain of size $k+1$, can the smallest chain decomposition have size k?

The answer is no, because if there is an antichain of size $k+1$ and a chain decomposition of size k, then by the pigeonhole principle, two elements of the antichain belong to the same chain, which is a contradiction.

Now, if S has a chain decomposition of size k, can there be an antichain of size $k+1$? (Surely there is an antichain of size k in S because A_0 is already an antichain of size k in $S - \{a\}$)

The same argument holds, if there is an antichain of size $k+1$ then two elements belong to the same chain (by the pigeonhole principle) and this is a contradiction.

Proof (cont.)

Now, consider each chain $P_i \in P$. Take the maximal element x_i from P_i such that there exists an antichain of size k in $S - \{a\}$ containing x_i. (Why is this always possible?)

Proof (cont.)

Now, consider each chain $P_i \in P$. Take the maximal element x_i from P_i such that there exists an antichain of size k in $S - \{a\}$ containing x_i. (Why is this always possible?)

Is $A = \{x_1, x_2, \ldots, x_k\}$ an antichain of $S - \{a\}$? Why?

Proof (cont.)

Now if $x_i \preceq a$ for some $i \in \{1, \ldots, k\}$.

Proof (cont.)

Now if $x_i \preceq a$ for some $i \in \{1, \ldots, k\}$.

Consider the chain $K = \{a\} \cup \{z \in P_i : z \preceq x_i\}$.

Proof (cont.)

Now if $x_i \preceq a$ for some $i \in \{1, \ldots, k\}$.

Consider the chain $K = \{a\} \cup \{z \in P_i : z \preceq x_i\}$.

What is the size of the smallest chain decomposition of $S - K$? Well, by the induction hypothesis, it is equal to the maximum size of antichain in $S - K$, which, hmm... How much is it?

Proof (cont.)

Now if $x_i \preceq a$ for some $i \in \{1, \ldots, k\}$.

Consider the chain $K = \{a\} \cup \{z \in P_i : z \preceq x_i\}$.

What is the size of the smallest chain decomposition of $S - K$? Well, by the induction hypothesis, it is equal to the maximum size of antichain in $S - K$, which, hmm... How much is it?

Surely it is no more than k, and at least it is $k - 1$ (because $A - \{x_i\}$ is an antichain). The question is, can it be k?

Proof (cont.)

Now if $x_i \preceq a$ for some $i \in \{1, \ldots, k\}$.

Consider the chain $K = \{a\} \cup \{z \in P_i : z \preceq x_i\}$.

What is the size of the smallest chain decomposition of $S - K$? Well, by the induction hypothesis, it is equal to the maximum size of antichain in $S - K$, which, hmm... How much is it?

Surely it is no more than k, and at least it is $k - 1$ (because $A - \{x_i\}$ is an antichain). The question is, can it be k?

The answer is no. Basically, $S - K$ has all the chains P_j except P_i where K is removed from P_i. If $P_i - K$ has an element y such that $(A - \{x_i\}) \cup \{y\}$ is an antichain, then $x_i \preceq y$, which contradicts the condition that x_i is the maximal element such that there exists an antichain of size k in $S - \{a\}$ containing x_i.

Proof (cont.)

So the size of smallest chain decomposition of $S - K$ is $k - 1$, which is equal to the maximum size of antichain in $S - K$. Now when we consider $S = (S - K) \cup K$, we can think of adding the chain K to the existing chain decomposition of $S - K$. Now, the size of the new chain decomposition is $k - 1 + 1 = k$. Which completes the proof in this case (where there exists $i \in \{1, \ldots, k\}$ such that $x_i \preceq a$).

Proof (cont.)

Now if $x_i \npreceq a$ for all $i \in \{1, \ldots, k\}$. By our assumption that a is maximal, $a \npreceq x_i$ for all $i \in \{1, \ldots, k\}$ also. So $A \cup \{a\}$ is an antichain of size $k + 1$. This completes the proof in this case (where there is no $i \in \{1, \ldots, k\}$ such that $x_i \preceq a$)

Proof (cont.)

Now if $x_i \not\preceq a$ for all $i \in \{1, \ldots, k\}$. By our assumption that a is maximal, $a \not\preceq x_i$ for all $i \in \{1, \ldots, k\}$ also. So $A \cup \{a\}$ is an antichain of size $k + 1$. This completes the proof in this case (where there is no $i \in \{1, \ldots, k\}$ such that $x_i \preceq a$)

Hence, the two cases are now proved. □

Proof (see also)

(I read it from *`https://en.wikipedia.org/wiki/Dilworth%27s_theorem#Inductive_proof`*)

Problems

Let’s try

- *lingling* (2021-2022)
- *o58_mar_c2_permutepermute*
- *https://szkopul.edu.pl/problemset/problem/_cVmDXXn2TjF0dF1rW6eazA0/site/?key=statement*
- *findpermutation* (2021-2022)
- ($\star$) *abc* (2022-2023)
- *https://www.codechef.com/problems/CHRL3*
- ($\star$) *sortingtapes* (2022-2023)
- ($\star$) CEOI2016 trick (*https://cses.fi/193/list/*)
- ($\star$) *https://oj.uz/problem/view/JOI18_bubblesort2*
- ($\star$) *https://oj.uz/problem/view/JOI18_asceticism*
- ($\star$) *https://codeforces.com/contest/1193/problem/C*

Sources

- Discrete mathematics lectures provided by François Alouges (at École Polytechnique)
- Reduction of Endomorphisms lectures provided by David Burguet (at École Polytechnique) with notes provided by Javier Fresán.
- An Introduction to the Analysis of Algorithms (2nd edition) by Robert Sedgewick and Phillipe Flajolet.
- Elementary Set Theory lectures provided by Thanatkrit Kaewtem (at Mahidol Wittayanusorn School).

Thank you!

And good luck with the training camp!