DM549/DS820/MM537/DM547

Lecture 12: Partial Orders, Modular Arithmetic

Kevin Aguyar Brix
Email: kabrix@imada.sdu.dk

University of Southern Denmark

23 October, 2024

Last Time: Transitive Closure

Definition

For a relation R on a set A,

$$R^\star = \underbrace{\bigcup_{i=1}^{\infty}}_{R \cup R^2 \cup R^3 \cup \cdots} R^i \ .$$

Theorem (only proof sketch, Theorem 9.4.2)

The transitive closure of a relation R is

$$t(R) = R^\star.$$

Last Time: Equivalence Relations

Definitions:

- Equivalence relation: reflexive, symmetric, and transitive relation.
- Equivalence class of a with respect to equivalence relation R: $[a]_R$, the set of elements related to a.

Theorem (Theorem 9.5.2)

Let A be a set. There is a one-to-one correspondence between equivalence relations on A and partitions of A:

(1) For any equivalence relation R on A, $P = \{[a]_R \mid a \in A\}$ is a partition of A.

(2) For any partition $P = \{A_i \mid i \in I\}$ of A, there exists an equivalence relation R on A such that $\{[a]_R \mid a \in A\} = \{A_i \mid i \in I\}$.

Partial Orders

Definition (Definition 9.6.1)

A relation R on a set A is called a *partial order* (partiel ordning) if it is

- reflexive,
- antisymmetric, and
- transitive.

If this is the case, (A, R) is called a *partially ordered set* (partielt ordnet mængde) or *poset*.

Remarks:

- Instead of R, one often uses $\leq$ or $\preceq$ for partial orders.
- When using these notations, $a < b$ ($a \prec b$) can be used to indicate that $a \leq b$ ($a \preceq b$) and $a \neq b$.

Hasse Diagrams

Idea: Special representation of a partially ordered set $(A, \preceq)$.

Specifically: Like graph representation of relation but

- leave out edges implied by the relation being reflexive and transitive, and
- if $a \preceq b$ and edge not implied, leave out arrow head but draw a under b.
  - Since partial orders are transitive and antisymmetric, there are no cycles, and this is possible!

Special Elements of Partially Ordered Sets

Definition (cf. Section 9.6.4)

Let $(A, \preceq)$ be a poset. For $a \in A$, a is called

- a *minimal* element if $\neg \exists b \in A : b \prec a$.
- the *least* element if $\forall b \in A : a \preceq b$.
- a *maximal* element if $\neg \exists b \in A : a \prec b$.
- the *greatest* element if $\forall b \in A : b \preceq a$.

Remarks:

- Every least (greatest) element, is also a minimal (maximal) element, but not necessarily the other way around.
- If A is non-empty and finite, there always exists a minimal (maximal) element, but not necessarily least (greatest).

Total Orders

Definition (Definition 9.6.2)

Let $(A, \preceq)$ be a poset. We call $a, b \in A$ *comparable* (sammenlignelige) if $a \preceq b$ or $b \preceq a$.

Definition (Definition 9.6.3)

Let $(A, \preceq)$ be a poset. If all $a, b \in A$ are comparable, we call $\preceq$ a *total order* (total ordning).

Different view: Partial orders can be obtained from total order by removing edges.

The Lexicographic Order

Definition (cf. Section 9.6.2)

Let $(A_1, \preceq_1), (A_2, \preceq_2), \ldots, (A_n, \preceq_n)$ be partial orders. Then we can define a *lexicographic order*, a partial order, $\preceq$ on $A_1 \times A_2 \times \cdots \times A_n$ as follows.

For two different elements $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n)$ of $A_1 \times A_2 \times \cdots \times A_n$ that are not equal, $(a_1, a_2, \ldots, a_n) \preceq (b_1, b_2, \ldots, b_n)$ holds if and only if

- $a_1 \prec_i b_1$, or
- there exists an $i > 0$ such that $a_1 = b_1, a_2 = b_2, \ldots, a_i = b_i$ and $a_{i+1} \prec_i b_{i+1}$.

How to think about this:

- Think of how words are ordered in a dictionary.
- For instance, consider $n = 4$ and all four partial (in fact, total) orders are $(\{a, b, c, \ldots, z\}, \leq)$ where $\ell_1 \leq \ell_2$ iff ℓ_1 is no later than ℓ_2 in the alphabet.
- Then the corresponding lexicographic order can be viewed as the total order in which the corresponding four-letter words would appear in a dictionary.

A Quiz

Go to `pollev.com/kevs`

On the Exam

Date: 8 January, 2025.

Duration:

- DM547, MM537: 3 hours
- DM549, DS820: 4 hours

Allowed resources: Must not require the internet.

Tips:

- Start by getting an overview of the exam.
- Use paper and pen while taking the exam.
- Justify each answer to yourself (it may help to even *write* down reason).
- Use old exams to practice.

Q&A session:

The End of MM537 and DM547!

Number Theory

Definition: A branch of Mathematics devoted to the study of integers and their relations (such as divisibility).

Applications:

- Cryptology
- Hasing
- Pseudorandom numbers
- many more!

Beware: This topic may seem easy at first sight, but it is really one of the harder ones!

Divisibility

Definition (Definition 4.1.1)

For $a, b \in \mathbb{Z}$ with $a \neq 0$, we say that a *divides* b (a går op i b) if there exists $c \in \mathbb{Z}$ such that $ac = b$. Then we write $a \mid b$ (and otherwise $a \nmid b$).

We call a a *factor* (faktor) or *divisor* of b, and we call b a *multiple* (multiplum) of a.

Theorem (Theorem 4.1.1)

Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Then:

(i) If $a \mid b$ and $a \mid c$ for some $c \in \mathbb{Z}$, then $a \mid (b + c)$.

(ii) If $a \mid b$, then $a \mid bc$ for all $c \in \mathbb{Z}$.

(iii) If $a \mid b$ and $b \mid c$ for some $c \in \mathbb{Z}$, then $a \mid c$.

Corollary (Corollary 4.1.1)

Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Then, if $a \mid b$ and $a \mid c$, then $a \mid (kb + \ell c)$ for all $k, \ell \in \mathbb{Z}$.

Quotient and Remainder

Theorem (no proof, Theorem 4.1.3)

Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there exist precisely one pair $q \in \mathbb{Z}$, $r \in \{0, \dots, d-1\}$ such that

$$a = dq + r.$$

Definition (Definition 4.1.2)

In the theorem above, we call d the *divisor* (divisor), a the *dividend* (dividend), q the *quotient* (kvotient), and r the *remainder* (rest).

We also write

$$a \operatorname{div} d = q \quad \text{and} \quad a \bmod d = r,$$

where we say "modulo" for "mod".

Modular Arithmetic

Definition (Definition 4.1.3)

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then we have the *congruence* (kongruens)

$$a \equiv b \pmod{m}$$

if and only if m divides $a - b$. We also say that *a and b are congruent (kongruente) modulo m*.

Theorem (only proof sketch, Theorems 4.1.3 and 4.1.4)

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then the following statements are equivalent:

(i) $a \equiv b \pmod{m}$

(ii) $a \bmod m = b \bmod m$

(iii) There exists $k \in \mathbb{Z}$ with $a = b + km$.

Adding and Multiplying Congruences

Theorem (Theorem 4.5.1)

Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad a \cdot c \equiv b \cdot d \pmod{m}.$$

Remark:

- In particular, that means that we can add the same number to both sides of a congruence or multiply them with the same number.
- Question to think about until next lecture: Does the same work for subtraction and (assuming $c \mid a$ and $d \mid b$) division?