

Chapter 7: Modular arithmetic and partial orders

CS1231S Discrete Structures

Wong Tin Lok

National University of Singapore

2021/22 Semester 1

We have concluded that the trivial mathematics is, on the whole, useful, and that the real mathematics, on the whole, is not.
G.H. Hardy 1940

G. H. Hardy would have been surprised and probably displeased with the increasing interest in number theory for application to “ordinary human activities” such as information transmission (error-correcting codes) and cryptography (secret codes).

N. Koblitz 1987

What we saw

Let A be a set.

Definition 6.1.1. A **partition** of A is a set \mathcal{C} of *nonempty* subsets of A such that

$$\forall x \in A \exists ! S \in \mathcal{C} (x \in S).$$

Definitions 6.1.5 and 6.2.1. A **relation on A** is a subset of A^2 .

Definition 6.1.5. If R is a relation on A , then we write $x R y$ for $(x, y) \in R$.

Definitions 6.2.4 and 6.2.13. A relation R on A is an **equivalence relation** if

- ▶ (reflexivity) $\forall x \in A (x R x)$;
- ▶ (symmetry) $\forall x, y \in A (x R y \Rightarrow y R x)$; and
- ▶ (transitivity) $\forall x, y, z \in A (x R y \wedge y R z \Rightarrow x R z)$.

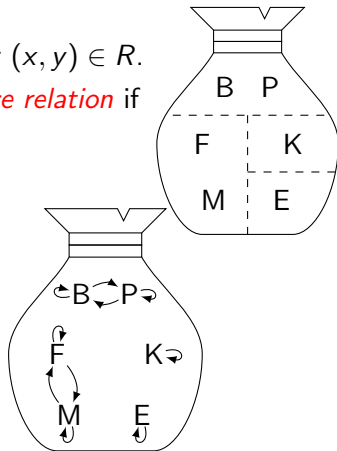
Proposition 6.2.16. The same-component relation with respect to a partition is an equivalence relation.

Definition 6.4.1. Let \sim be an equivalence relation on A . Then

$$A/\sim = \{[x]_{\sim} : x \in A\},$$

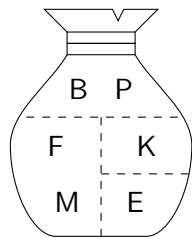
where $[x]_{\sim} = \{y \in A : x \sim y\}$.

Theorem 6.4.9. If \sim is an equivalence relation on A , then A/\sim is a partition of A .

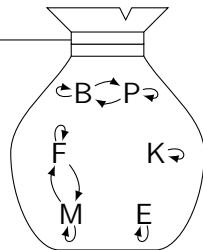


Informal descriptions of the terms

1. underlying set	A	the set to be "partitioned"
2. components	S	subsets of A , mutually disjoint, together union to A
3. partition	\mathcal{C}	the set of all components
4. same-component relation	\sim	equivalence relation



1. underlying set	A	the set of all vertices
2. relation	R	the set of all arrows
3. equivalence relation	\sim	If ignoring directions of arrows one can walk from x to y , then there is an arrow from x to y .
4. equivalence classes	$[x]$, where $x \in A$	connected components
5. quotient	A/\sim	the set of all connect components



Why partitions and equivalence relations

There are numerous situations when we want to treat different individuals as the same.

Example (take with a pinch of salt)

When should two programs be considered the same?

- ▶ To the file system: they are the same copy of a file.
- ▶ To the programmer: they have the same code.
- ▶ To the theoretical computer scientist: the underlying algorithms are the same.
- ▶ To the complexity theorist: they require the same (time or memory) resources.
- ▶ To the recursion theorist: on the same input, they give the same output.



Each view is represented by an equivalence relation on the set of all programs.

The formal mathematical language, together with the *univalence axiom*, fulfills the mathematicians' dream: a language for mathematics invariant under equivalence and thus freed from irrelevant details and able to merge the results of mathematicians taking different but equivalent approaches.

D.R. Grayson 2018

Congruence

Fix $n \in \mathbb{Z}^+$.

Definition 6.3.1

Let $a, b \in \mathbb{Z}$. Then *a is congruent to b modulo n* if $a - b = nk$ for some $k \in \mathbb{Z}$. In this case, we write $a \equiv b \pmod{n}$.

Proposition 6.3.4

Congruence-mod- n is an equivalence relation on \mathbb{Z} .

Examples 6.4.3 and 6.4.8

The equivalence classes with respect to the congruence-mod- n relation \sim_n on \mathbb{Z} are of the form

$$[x] = \{y \in \mathbb{Z} : x \equiv y \pmod{n}\} = \{nk + x : k \in \mathbb{Z}\},$$

where $x \in \mathbb{Z}$. So

$$\begin{aligned}\mathbb{Z}/\sim_n &= \{[x] : x \in \mathbb{Z}\} \\ &= \{\{nk : k \in \mathbb{Z}\}, \{nk + 1 : k \in \mathbb{Z}\}, \dots, \{nk + (n - 1) : k \in \mathbb{Z}\}\}.\end{aligned}$$

$$\text{Hence } \mathbb{Z}/\sim_2 = \{\{2k : k \in \mathbb{Z}\}, \{2k + 1 : k \in \mathbb{Z}\}\}.$$

\mathbb{Z}

\vdots	\vdots	\vdots	\vdots
-8	-7	-6	-5
-4	-3	-2	-1
0	1	2	3
4	5	6	7
8	9	10	11
\vdots	\vdots	\vdots	\vdots

\mathbb{Z}

\vdots	\vdots
-4	-3
-2	-1
0	1
2	3
4	5
\vdots	\vdots

Generalizing the arithmetic on even/odd from mod-2 to mod- n

We can do arithmetic on the equivalence classes with respect to the congruence-mod-2 relation.

	+	even	odd
even		even	odd
odd		odd	even

	×	even	odd
even		even	even
odd		even	odd

How to come up with these tables

Denote by \sim_2 the congruence-mod-2 relation on \mathbb{Z} , so that

$$\mathbb{Z}/\sim_2 = \{\{m \in \mathbb{Z} : m \text{ is even}\}, \{m \in \mathbb{Z} : m \text{ is odd}\}\}.$$

$$[x] + [y] = [x + y]$$

1. Let $S_1, S_2 \in \mathbb{Z}/\sim_2$, say $S_1 = \{m \in \mathbb{Z} : m \text{ is odd}\}$ and $S_2 = \{m \in \mathbb{Z} : m \text{ is even}\}$.
2. We want to define $S_1 + S_2$ and $S_1 \times S_2$, which will again be elements of \mathbb{Z}/\sim_2 .
3. Pick a representative $x \in S_1$ and a representative $y \in S_2$, say $x = 3$ and $y = -2$.
4. Sum the representatives; here $x + y = 3 + (-2) = 1$. ($[x] = S_1$ and $[y] = S_2$.)
5. There is a unique equivalence class S containing $x + y$ as \mathbb{Z}/\sim_2 is a partition of \mathbb{Z} .
6. Define $S_1 + S_2$ to be this S ; since $x + y = 1 \in \{m \in \mathbb{Z} : m \text{ is odd}\}$, we define $S_1 + S_2 = \{m \in \mathbb{Z} : m \text{ is odd}\}$ here. ($[x + y] = S$.)

Exercise 7.1.2. An element $x \in \mathbb{Z}$ is in an equivalence class S if and only if $[x] = S$.

Defining arithmetic modulo n in terms of representatives

Let $n \in \mathbb{Z}^+$.

Definition 7.1.1

A *representative* of an equivalence class is an element of the equivalence class.

Definition 7.1.4

The quotient \mathbb{Z}/\sim_n , where \sim_n is the congruence-mod- n relation on \mathbb{Z} , is denoted \mathbb{Z}_n or $\mathbb{Z}/n\mathbb{Z}$. Define addition and multiplication on \mathbb{Z}_n as follows: whenever $[x], [y] \in \mathbb{Z}_n$,

$$[x] + [y] = [x + y] \quad \text{and} \quad [x] \cdot [y] = [x \cdot y].$$

What can go wrong?

Say $n = 2$.

- ▶ We have $[0] + [1] = [1]$ as *some* even number plus *some* odd number is odd.
- ▶ What if *some* even number plus *some* odd number is even, so that $[0] + [1] = [0]$ too? Then what is $[0] + [1]$?
- ▶ ... Fortunately, *any* even number plus *any* odd number is odd.



<https://tex.stackexchange.com/a/413506>

Exercise 7.1.2. An element $x \in \mathbb{Z}$ is in an equivalence class S if and only if $[x] = S$.

Example 7.1.3: same distance from 0

Define an equivalence relation \sim on \mathbb{Z} by setting, for all $x, y \in \mathbb{Z}$,

$$x \sim y \iff x = y \text{ or } x = -y.$$

Hence $x \sim y$ means $|x| = |y|$. Note

$$[0] = \{0\}, \quad [1] = \{1, -1\} = [-1], \quad [2] = \{2, -2\} = [-2], \quad \dots$$

So $\mathbb{Z}/\sim = \{\{0\}, \{1, -1\}, \{2, -2\}, \dots\}$. Define addition and multiplication on \mathbb{Z}/\sim as follows: whenever $[x], [y] \in \mathbb{Z}/\sim$,

$$[x] + [y] = [x + y] \quad \text{and} \quad [x] \cdot [y] = [x \cdot y].$$

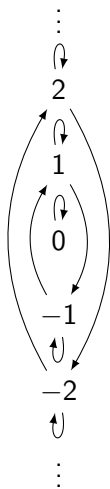
Then $+$ is not well defined because $[1] = [1]$ and $[2] = [-2]$, but

$$[1] + [2] = [1 + 2] = [3] \neq [-1] = [1 + (-2)] = [1] + [-2].$$

Note \cdot is well defined because whenever $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}/\sim$,

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \implies [x_1] \cdot [y_1] = [x_2] \cdot [y_2]. \quad \text{✎}$$

Definitions 6.4.1 and 6.4.6. Let \sim be an equivalence relation on a set A . Then $A/\sim = \{[x] : x \in A\}$, where $[x] = \{y \in A : x \sim y\}$.



Addition on \mathbb{Z}_n is well defined

Definitions 6.3.1 and 7.1.4. $\mathbb{Z}_n = \mathbb{Z}/\sim_n$, where
 $x \sim_n y \iff \exists k \in \mathbb{Z} (x - y = kn).$

Proposition 7.1.5

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \Rightarrow [x_1] + [y_1] = [x_2] + [y_2] \text{ and } [x_1] \cdot [y_1] = [x_2] \cdot [y_2].$$

Proof

1. Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
2. Then Lemma 6.4.4 implies $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$.
3. Use the definition of congruence to find $k, \ell \in \mathbb{Z}$ such that

$$x_1 - x_2 = nk \quad \text{and} \quad y_1 - y_2 = n\ell.$$

4. 4.1. Note $(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = nk + n\ell = n(k + \ell)$,
where $k + \ell \in \mathbb{Z}$.
- 4.2. So the definition of congruence tells us $x_1 + y_1 \equiv x_2 + y_2 \pmod{n}$.
- 4.3. Hence $[x_1] + [y_1] = [x_1 + y_1] = [x_2 + y_2] = [x_2] + [y_2]$ by Lemma 6.4.4.
5. We show that $[x_1] \cdot [y_1] = [x_2] \cdot [y_2]$

$$\begin{aligned} [x] + [y] &= [x + y]. \\ [x] \cdot [y] &= [x \cdot y]. \end{aligned}$$

Lemma 6.4.4. TFAE: (i) $x \sim y$; (ii) $[x] = [y]$; (iii) $[x] \cap [y] \neq \emptyset$.

Multiplication on \mathbb{Z}_n is well defined

Definitions 6.3.1 and 7.1.4. $\mathbb{Z}_n = \mathbb{Z}/\sim_n$, where
 $x \sim_n y \iff \exists k \in \mathbb{Z} (x - y = kn)$.

Proposition 7.1.5

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \Rightarrow [x_1] + [y_1] = [x_2] + [y_2] \text{ and } [x_1] \cdot [y_1] = [x_2] \cdot [y_2].$$

Proof

1. Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
2. Then Lemma 6.4.4 implies $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$.
3. Use the definition of congruence to find $k, \ell \in \mathbb{Z}$ such that

$$x_1 - x_2 = nk \quad \text{and} \quad y_1 - y_2 = n\ell.$$

4. (It is shown that $[x_1] + [y_1] = [x_2] + [y_2]$.)
5. 5.1. Note $(x_1 \cdot y_1) - (x_2 \cdot y_2) = (nk + x_2)(n\ell + y_2) - x_2 y_2 =$
 $n^2 k\ell + nky_2 + n\ell x_2 = n(nk\ell + ky_2 + \ell x_2)$, where $nk\ell + ky_2 + \ell x_2 \in \mathbb{Z}$.
- 5.2. So the definition of congruence tells us $x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod{n}$.
- 5.3. Hence $[x_1] \cdot [y_1] = [x_1 \cdot y_1] = [x_2 \cdot y_2] = [x_2] \cdot [y_2]$ by Lemma 6.4.4. □

$$\begin{aligned} [x] + [y] &= [x + y]. \\ [x] \cdot [y] &= [x \cdot y]. \end{aligned}$$

Lemma 6.4.4. TFAE: (i) $x \sim y$; (ii) $[x] = [y]$; (iii) $[x] \cap [y] \neq \emptyset$.

“Well-defined function”

Definition 7.2.1

Let A, B be sets. A *function* or a *map* from A to B is an assignment to each element of A exactly one element of B . We write $f: A \rightarrow B$ for “ f is a function from A to B ”. Suppose $f: A \rightarrow B$.

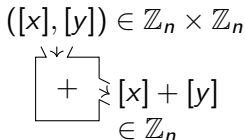
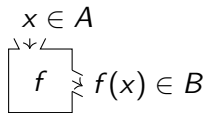
- (1) Let $x \in A$. Then $f(x)$ denotes the element of B that f assigns x to. We call $f(x)$ the *image* of x under f . If $y = f(x)$, then we say that *f maps x to y* , and we may write $f: x \mapsto y$.
- (2) Here A is called the *domain* of f , and B is called the *codomain* of f .

Convention 7.2.2

Instead of $+(x, y)$ and $\cdot(x, y)$, people usually write $x + y$ and $x \cdot y$ respectively.

Convention 7.2.3

In mathematics, one can read “Define $f: A \rightarrow B$ by Then f is well defined.” as “The condition ‘...’ defines a function $f: A \rightarrow B$. We use “...” to define f .”



$$[x] + [y] = [x + y] \quad \text{and} \quad [x_1] = [x_2] \text{ and } [y_1] = [y_2] \Rightarrow [x_1] + [y_1] = [x_2] + [y_2]$$

A polynomial function

Definition 7.2.1

Let A, B be sets. A **function** or a **map** from A to B is an assignment to each element of A exactly one element of B . We write $f: A \rightarrow B$ for “ f is a function from A to B ”. Suppose $f: A \rightarrow B$.

- (1) Let $x \in A$. Then $f(x)$ denotes the element of B that f assigns x to. We call $f(x)$ the **image** of x under f . If $y = f(x)$, then we say that **f maps x to y** , and we may write **$f: x \mapsto y$** .
- (2) Here A is called the **domain** of f , and B is called the **codomain** of f .

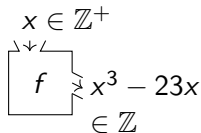
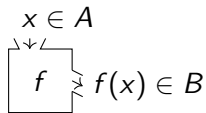
Example 7.2.4

Define $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}$ by setting, for each $x \in \mathbb{Z}$,

$$f(x) = x^3 - 23x.$$

Then the domain of f is \mathbb{Z}^+ and codomain of f is \mathbb{Z} . We know

$$f(1) = 1^3 - 23 \times 1 = -22 \quad \text{and} \quad f(2) = 2^3 - 23 \times 2 = -38.$$



Identity functions

Definition 7.2.1

Let A, B be sets. A *function* or a *map* from A to B is an assignment to each element of A exactly one element of B . We write $f: A \rightarrow B$ for “ f is a function from A to B ”. Suppose $f: A \rightarrow B$.

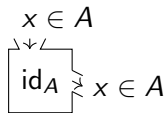
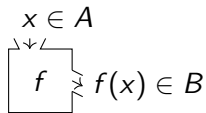
- (1) Let $x \in A$. Then $f(x)$ denotes the element of B that f assigns x to. We call $f(x)$ the *image* of x under f . If $y = f(x)$, then we say that *f maps x to y* , and we may write $f: x \mapsto y$.
- (2) Here A is called the *domain* of f , and B is called the *codomain* of f .

Definition 7.2.5 and Remark 7.2.6

Let A be a set. Then the *identity function* on A , denoted id_A , is the function $A \rightarrow A$ which satisfies, for all $x \in A$,

$$\text{id}_A(x) = x.$$

The domain and the codomain of id_A are both A .



Bad definitions

Definition 7.2.1

A *function* $A \rightarrow B$ is an assignment to each element of A exactly one element of B .

Question 7.2.7

Define $f: \mathbb{Q} \rightarrow \mathbb{Q}$ by setting $f(x) = 2^x$ for all $x \in \mathbb{Q}$. Why is f not well defined?

Define $g: \mathbb{Q} \rightarrow \mathbb{Q}$ by setting

$$g(x) = \frac{x^2 + 1}{x^2 + 2x + 1}$$

for all $x \in \mathbb{Q}$.

Define $h: \mathbb{Q} \rightarrow \mathbb{Z}$ by setting
 $h(m/n) = m$ for all $m, n \in \mathbb{Z}$
where $n \neq 0$.

Checkpoint

We have $+$ and \cdot on \mathbb{Z}_n for any $n \in \mathbb{Z}^+$.

We can then...

- ▶ try to do subtraction and division;
- ▶ solve equations and systems of equations;
- ▶ develop the RSA cryptosystem;
- ▶ build combinatorial designs;
- ▶ etc.

4	9	2
3	5	7
8	1	6

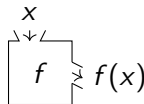
We also saw a precise definition of functions.

We will return to the study of functions later.

Next

Partial orders

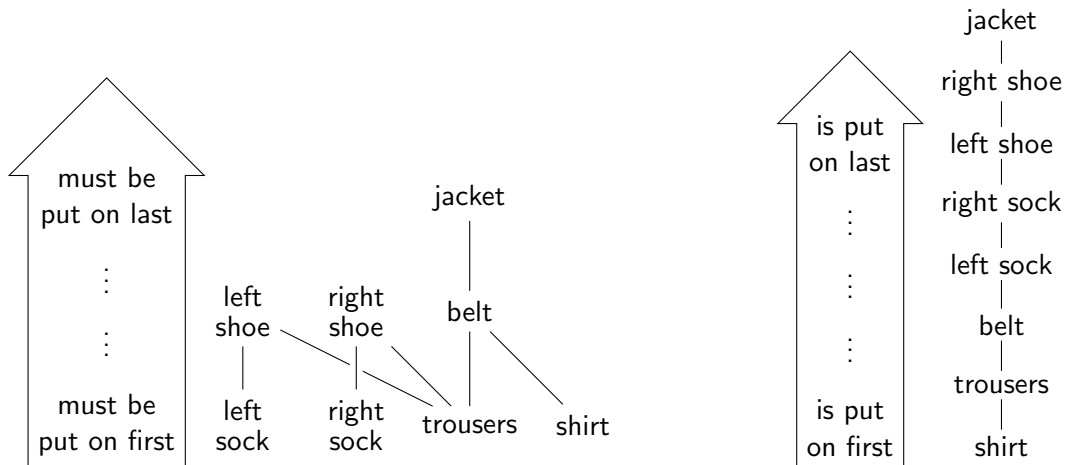
$+$	even	odd	\times	even	odd
even	even	odd	even	even	even
odd	odd	even	odd	even	odd



Marcel Ern  (1985),
There must be order!

Motivating examples of partial orders

- (1) the “*must be* done before (or at the same time as)” relation on the set of all tasks
- (2) the “*is* done before (or at the same time as)” relation on the set of all tasks



Motivating examples of partial orders: a closer look

- (1) the “*must be* done before (or at the same time as)” relation on the set of all tasks
- (2) the “*is* done before (or at the same time as)” relation on the set of all tasks

- ▶ Each such relation has two versions: one with the parenthetical phrase, and one without. They have the same mathematical content. We focus on the former.
- ▶ So all such relations are reflexive and transitive.
- ▶ No multi-tasking is allowed, i.e., if R is one of the relations above, then

$$\forall x, y (x R y \wedge y R x \Rightarrow x = y). \quad (\text{antisymmetry})$$

- ▶ There may be x, y such that x need not be done before y , and y need not be done before x , i.e., maybe $\exists x, y (x \not R y \wedge y \not R x)$ if R is the relation in (1). (partiality)
- ▶ However, as time is linear and there is no multi-tasking, for all tasks x, y , either x is done before or at the same time as y , or y is done before or at the same time as x , i.e.,
$$\forall x, y (x R y \vee y R x) \quad \text{if } R \text{ is the relation in (2).} \quad (\text{totality})$$
- ▶ Here “partiality” means “possibly partial”, while “total” means “necessarily total”.

Partial orders

Definition 7.3.1

Let A be a set and R be a relation on A .

- (1) R is *antisymmetric* if $\forall x, y \in A (x R y \wedge y R x \Rightarrow x = y)$.
- (2) R is a *(non-strict) partial order* if R is reflexive, antisymmetric, and transitive.
- (4) R is a *(non-strict) total order* if R is a partial order and $\forall x, y \in A (x R y \vee y R x)$.
- (5) We say that the ordered pair (A, R) is a *partially ordered set*, or a *poset* for short, if R is a partial order on A .

Definition 6.2.4. (1) R is *reflexive* if $\forall x \in A x R x$.
(3) R is *transitive* if $\forall x, y, z \in A (x R y \wedge y R z \Rightarrow x R z)$.



linear order

x and y are *comparable*

any two elements are comparable

Note 7.3.2

A total order is always a partial order.


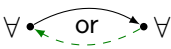
Plan

- ▶ examples and non-examples
- ▶ min and max
- ▶ linearization (aka topological sorting)

Inequalities

Definition 7.3.1

Let A be a set and R be a relation on A .

- (1) R is **antisymmetric** if $\forall x, y \in A (x R y \wedge y R x \Rightarrow x = y)$.  
- (2) R is a **(non-strict) partial order** if R is reflexive, antisymmetric, and transitive.
- (4) R is a **(non-strict) total order** if R is a partial order and $\forall x, y \in A \underbrace{(x R y \vee y R x)}_{x \text{ and } y \text{ are comparable}}$.

Example 7.3.3

Let R denote the non-strict less-than relation on \mathbb{Q} , i.e., for all $x, y \in \mathbb{Q}$,

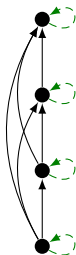
$$x R y \Leftrightarrow x \leq y.$$

Then R is antisymmetric. In fact, it is a total order.

Example 7.3.4

Let R' denote the strict less-than relation on \mathbb{Q} , i.e., for all $x, y \in \mathbb{Q}$,


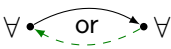
$$x R' y \Leftrightarrow x < y.$$



Equivalence relations

Definition 7.3.1

Let A be a set and R be a relation on A .

- (1) R is **antisymmetric** if $\forall x, y \in A (x R y \wedge y R x \Rightarrow x = y)$.  
- (2) R is a **(non-strict) partial order** if R is reflexive, antisymmetric, and transitive.
- (4) R is a **(non-strict) total order** if R is a partial order and $\forall x, y \in A \underbrace{(x R y \vee y R x)}_{x \text{ and } y \text{ are comparable}}$.

Example 7.3.5

Let R denote the equality relation on a set A , i.e., for all $x, y \in A$,

$$x R y \Leftrightarrow x = y.$$



Then R is antisymmetric. It is a partial order, but not a total order unless $|A| \leq 1$.

Example 7.3.6

Fix $n \in \mathbb{Z}^+$. Let R' denote the congruence-mod- n relation on \mathbb{Z} , i.e., for all $x, y \in \mathbb{Z}$,

$$x R' y \Leftrightarrow x \equiv y \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z} (x - y = nk).$$


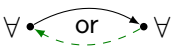
Then R' is not antisymmetric because $0 R' n$ and $n R' 0$ but $0 \neq n$.

\vdots	\vdots	\vdots	\vdots	\mathbb{Z}
-8	-7	-6	-5	
-4	-3	-2	-1	
0	1	2	3	
4	5	6	7	
8	9	10	11	
\vdots	\vdots	\vdots	\vdots	

Divisibility

Definition 7.3.1

Let A be a set and R be a relation on A .

- (1) R is **antisymmetric** if $\forall x, y \in A (x R y \wedge y R x \Rightarrow x = y)$.  
- (2) R is a **(non-strict) partial order** if R is reflexive, antisymmetric, and transitive.
- (4) R is a **(non-strict) total order** if R is a partial order and $\forall x, y \in A \underbrace{(x R y \vee y R x)}_{x \text{ and } y \text{ are comparable}}$.

Example 7.3.7

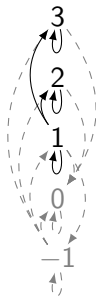
Let R denote the divisibility relation on \mathbb{Z} , i.e., for all $x, y \in \mathbb{Z}$,

$$x R y \Leftrightarrow x \mid y \Leftrightarrow \exists k \in \mathbb{Z} (y = xk).$$

Example 7.3.8

Let R' denote the divisibility relation on \mathbb{Z}^+ , i.e., for all $x, y \in \mathbb{Z}^+$,


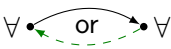
$$x R' y \Leftrightarrow x \mid y \Leftrightarrow \exists k \in \mathbb{Z} (y = xk).$$



Inclusion

Definition 7.3.1

Let A be a set and R be a relation on A .

- (1) R is **antisymmetric** if $\forall x, y \in A (x R y \wedge y R x \Rightarrow x = y)$.  
- (2) R is a **(non-strict) partial order** if R is reflexive, antisymmetric, and transitive.
- (4) R is a **(non-strict) total order** if R is a partial order and $\forall x, y \in A \underbrace{(x R y \vee y R x)}_{x \text{ and } y \text{ are comparable}}$.

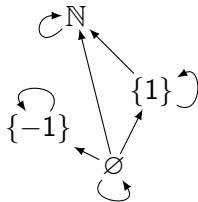
Example 7.3.9

Let R denote the subset relation on a set U of sets, i.e., for all $x, y \in U$,

$$x R y \Leftrightarrow x \subseteq y.$$

Then R is antisymmetric. It is always a partial order, but it may not be a total order.

Remark 5.1.22(2). For all sets A, B ,
 $A = B \Leftrightarrow A \subseteq B \text{ and } B \subseteq A.$



Hasse diagrams

Read \preccurlyeq as “(curly) less than or equal to”.

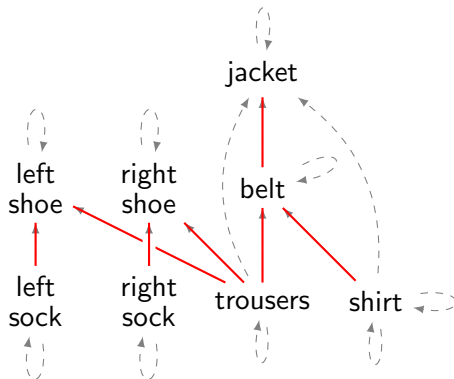
Notation 7.3.10

We often use \preccurlyeq to denote a partial order. This symbol is often defined and redefined to mean different partial orders in different situations. If \preccurlyeq denotes a partial order, then we write $x \prec y$ for $x \preccurlyeq y \wedge x \neq y$.

Definition 7.3.11

Let \preccurlyeq be a partial order on a set A . A *Hasse diagram* of \preccurlyeq satisfies the following condition for all $x, y \in A$:

If $x \prec y$ and no $z \in A$ is such that $x \prec z \prec y$, then x is placed below y and there is a line joining x to y , else no line joins x to y .



Positive divisors of 30

Notation 7.3.10

We often use \preccurlyeq to denote a partial order. This symbol is often defined and redefined to mean different partial orders in different situations. If \preccurlyeq denotes a partial order, then we write $x \prec y$ for $x \preccurlyeq y \wedge x \neq y$.

Definition 7.3.11

Let \preccurlyeq be a partial order on a set A . A *Hasse diagram* of \preccurlyeq satisfies the following condition for all $x, y \in A$:

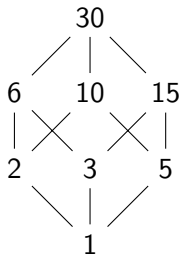
If $x \prec y$ and no $z \in A$ is such that $x \prec z \prec y$, then x is placed below y and there is a line joining x to y , else no line joins x to y .

Read \preccurlyeq as “(curly) less than or equal to”.

Example 7.3.12

Consider $\{d \in \mathbb{Z}^+ : d \mid 30\}$ partially ordered by the divisibility relation \mid .

A Hasse diagram is as follows:



Subsets of $\{1, 2, 3\}$

Notation 7.3.10

We often use \preceq to denote a partial order. This symbol is often defined and redefined to mean different partial orders in different situations. If \preceq denotes a partial order, then we write $x \prec y$ for $x \preceq y \wedge x \neq y$.

Definition 7.3.11

Let \preceq be a partial order on a set A . A *Hasse diagram* of \preceq satisfies the following condition for all $x, y \in A$:

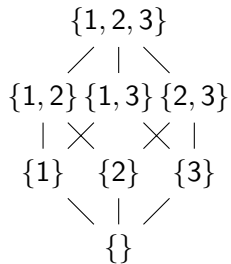
If $x \prec y$ and no $z \in A$ is such that $x \prec z \prec y$, then x is placed below y and there is a line joining x to y , else no line joins x to y .

Read \preceq as “(curly) less than or equal to”.

Example 7.3.13

Consider $\mathcal{P}(\{1, 2, 3\})$ partially ordered by the inclusion relation \subseteq .

A Hasse diagram is as follows:



The usual order on $\{1, 2, 3, 4\}$

Notation 7.3.10

We often use \preccurlyeq to denote a partial order. This symbol is often defined and redefined to mean different partial orders in different situations. If \preccurlyeq denotes a partial order, then we write $x \prec y$ for $x \preccurlyeq y \wedge x \neq y$.

Definition 7.3.11

Let \preccurlyeq be a partial order on a set A . A *Hasse diagram* of \preccurlyeq satisfies the following condition for all $x, y \in A$:

If $x \prec y$ and no $z \in A$ is such that $x \prec z \prec y$, then x is placed below y and there is a line joining x to y , else no line joins x to y .

Read \preccurlyeq as “(curly) less than or equal to”.

Example 7.3.14

Consider $\{1, 2, 3, 4\}$ partially ordered by the non-strict less-than relation \leq .

A Hasse diagram is as follows:



Min and max

minimal



smallest

Definition 7.4.1

- (1) c is a **minimal element** if no $x \in A$ is strictly \preccurlyeq -less than c , i.e.,

$$\forall x \in A (x \preccurlyeq c \Rightarrow c = x).$$

- (2) c is a **maximal element** if no $x \in A$ is strictly \preccurlyeq -bigger than c , i.e.,

$$\forall x \in A (c \preccurlyeq x \Rightarrow c = x).$$

- (3) c is the **smallest element** (or the **minimum element**) if all $x \in A$ are \preccurlyeq -bigger than or equal to c , i.e.,

$$\forall x \in A (c \preccurlyeq x).$$

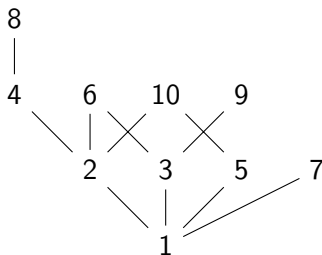
- (4) c is the **largest element** (or the **maximum element**) if all $x \in A$ are \preccurlyeq -less than or equal to c , i.e.,

$$\forall x \in A (x \preccurlyeq c).$$

Let \preccurlyeq be a partial order on a set A , and $c \in A$.

Example 7.4.2

The divisibility relation $|$ on $\{1, 2, \dots, 10\}$ is represented by the Hasse diagram



- ▶ The only minimal element is 1.
- ▶ The maximal elements are 6, 7, 8, 9, 10.
- ▶ The smallest element is 1.
- ▶ There is no largest element.

No min/max

minimal

$\forall \bullet$
 \exists

c
 \times
 \bullet

smallest

Definition 7.4.1

- (1) c is a **minimal element** if no $x \in A$ is strictly \preccurlyeq -less than c , i.e.,

$$\forall x \in A (x \preccurlyeq c \Rightarrow c = x).$$

- (2) c is a **maximal element** if no $x \in A$ is strictly \preccurlyeq -bigger than c , i.e.,

$$\forall x \in A (c \preccurlyeq x \Rightarrow c = x).$$

- (3) c is the **smallest element** (or the **minimum element**) if all $x \in A$ are \preccurlyeq -bigger than or equal to c , i.e.,

$$\forall x \in A (c \preccurlyeq x).$$

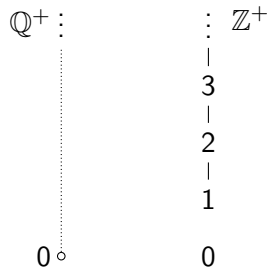
- (4) c is the **largest element** (or the **maximum element**) if all $x \in A$ are \preccurlyeq -less than or equal to c , i.e.,

$$\forall x \in A (x \preccurlyeq c).$$

Let \preccurlyeq be a partial order on a set A , and $c \in A$.

Example 7.4.3

- (1) \mathbb{Q}^+ under the non-strict less-than relation \leq has neither a minimal element nor a maximal element.
- (2) \mathbb{Z}^+ under the non-strict less-than relation \leq has a smallest element but no maximal element.



Implication

minimal



smallest

Definition 7.4.1

- (1) c is a **minimal element** if no $x \in A$ is strictly \preccurlyeq -less than c , i.e.,

$$\forall x \in A (x \preccurlyeq c \Rightarrow c = x).$$

- (2) c is a **maximal element** if no $x \in A$ is strictly \preccurlyeq -bigger than c , i.e.,

$$\forall x \in A (c \preccurlyeq x \Rightarrow c = x).$$

- (3) c is the **smallest element** (or the **minimum element**) if all $x \in A$ are \preccurlyeq -bigger than or equal to c , i.e.,

$$\forall x \in A (c \preccurlyeq x).$$

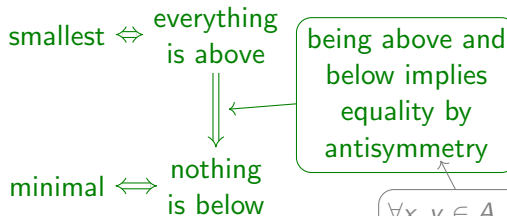
- (4) c is the **largest element** (or the **maximum element**) if all $x \in A$ are \preccurlyeq -less than or equal to c , i.e.,

$$\forall x \in A (x \preccurlyeq c).$$

Let \preccurlyeq be a partial order on a set A , and $c \in A$.

Proposition 7.4.4(1)

Consider a partial order \preccurlyeq on a set A . Any smallest element is minimal.



$$\forall x, y \in A \\ (x R y \wedge y R x) \\ \Rightarrow x = y$$

Proof

1. Let c be a smallest element.
2. Take any $x \in A$ such that $x \preccurlyeq c$.
3. By smallestness, we know $c \preccurlyeq x$ too.
4. So $c = x$ by antisymmetry. \square

Existence of minimal elements

Proposition 7.4.6

With respect to any partial order \preccurlyeq on a finite set $A \neq \emptyset$, one can find a minimal element.

Definition 6.2.4(3). R is *transitive* if $\forall x, y, z \in A (x R y \wedge y R z \Rightarrow x R z)$.

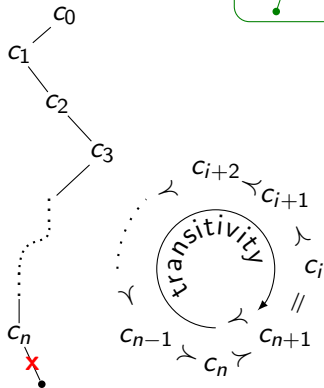
Definition 7.3.1(1). R is *antisymmetric* if $\forall x, y \in A (x R y \wedge y R x \Rightarrow x = y)$.

Proof (optional material)

1. Take any $c_0 \in A$. This is possible since $A \neq \emptyset$.
2. If c_0 is not minimal, then find $c_1 \in A$ such that $c_1 \prec c_0$.
3. Continue this process: if c_n is not minimal, then find $c_{n+1} \in A$ such that $c_{n+1} \prec c_n$.
4. Note that $c_{n+1} \neq c_i$ for any $i \in \{0, 1, \dots, n\}$ because if $i \in \{0, 1, \dots, n\}$ such that $c_{n+1} = c_i$, then
 - 4.1. $c_n \prec c_{n-1} \prec \dots \prec c_i = c_{n+1}$;
 - 4.2. so $c_n \preccurlyeq c_{n+1}$ by transitivity;
 - 4.3. so $c_n = c_{n+1}$ by antisymmetry as $c_{n+1} \prec c_n$;
 - 4.4. so we have a contradiction with $c_{n+1} \prec c_n$.
5. Since A is finite, this process must end, say with c_n .
6. c_n must be minimal for this process to end. \square

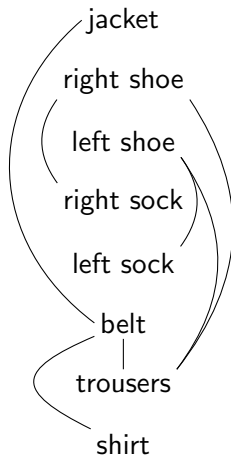
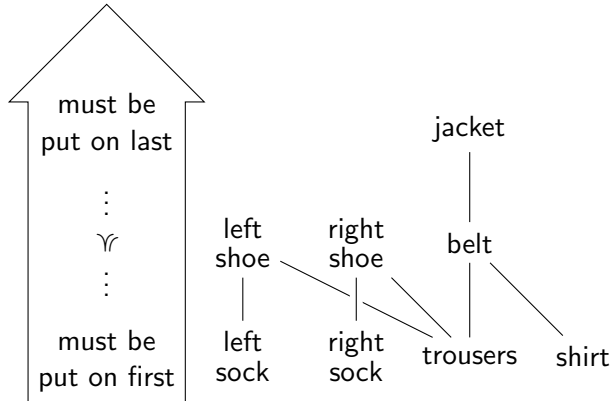
Keep picking smaller elements until minimal.

minimal



Linearization in terms of Hasse diagrams

A way to draw a Hasse diagram for the partial order in which all the items are in one vertical line.



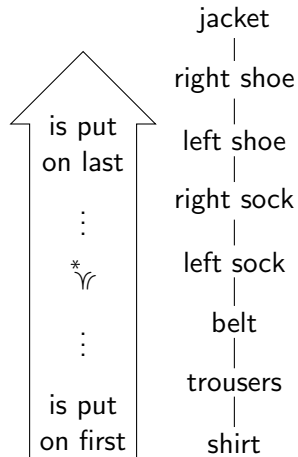
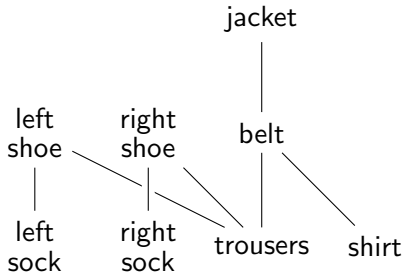
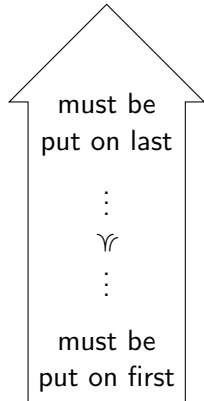
Linearization in terms of tasks and dependencies

a total order \preceq^*

A sequential way to complete the tasks such that tasks that must be done first are done first.

$$\forall x, y (x \preceq y \Rightarrow x \preceq^* y)$$

$\preceq \subseteq \preceq^*$



Linearization defined

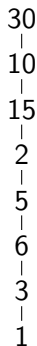
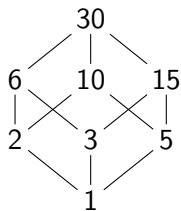
Definition 7.4.8

Let A be a set and \preccurlyeq be a partial order on A . A *linearization* of \preccurlyeq is a total order \preccurlyeq^* on A such that

$$\forall x, y \in A \quad (x \preccurlyeq y \Rightarrow x \preccurlyeq^* y).$$

Question 7.4.9

Is the total order \preccurlyeq^* represented by the bottom Hasse diagram a linearization of the partial order \preccurlyeq represented by the top Hasse diagram?



Linearizations exist

Keep collecting
minimal elements.

Definition 7.4.8

Let A be a set and \preceq be a partial order on A . A **linearization** of \preceq is a total order \preceq^* on A such that

$$\forall x, y \in A \quad (x \preceq y \Rightarrow x \preceq^* y).$$

Theorem 7.4.10

Every partial order \preceq has a linearization \preceq^* .

Proposition 7.4.6

With respect to any partial order \preceq on a finite set $A \neq \emptyset$, one can find a minimal element.

Note 7.4.12

In step (2.1), there may be several minimal elements to choose from. Different choices give different linearizations.

Kahn's Algorithm (1962)

Input: a finite set A , a partial order \preceq on A .

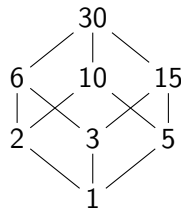
- (1) Set $A_0 := A$ and $i := 0$.
- (2) Repeat until $A_i = \emptyset$:
 - (2.1) find a minimal element c_i of A_i wrt \preceq ;
 - (2.2) set $A_{i+1} := A_i \setminus \{c_i\}$;
 - (2.3) set $i := i + 1$.

Output: a linearization \preceq^* of \preceq defined by setting, for all indices i, j ,

$$c_i \preceq^* c_j \quad \Leftrightarrow \quad i \leq j.$$

A run of Kahn's Algorithm

Keep collecting
minimal elements.



Example 7.4.13

Consider $\{d \in \mathbb{Z}^+ : d \mid 30\}$ partially ordered by the divisibility relation \mid .

- ▶ Set $A_0 := \{d \in \mathbb{Z}^+ : d \mid 30\}$.
- ▶ 1 is the only minimal element of A_0 .
- ▶ 2, 3, 5 are the minimal elements of A_1 .
- ▶ 2, 5 are the minimal elements of A_2 .
- ▶ 5, 6 are the minimal elements of A_3 .
- ▶ 5 is the only minimal element of A_4 .
- ▶ 10, 15 are the minimal elements of A_5 .
- ▶ 10 is the only minimal element of A_6 .
- ▶ 30 is the only (minimal) element of A_7 .
- ▶ $A_8 = \emptyset$ and so we stop.
- ▶ A linearization is given by $1 \preceq^* 3 \preceq^* 2 \preceq^* 6 \preceq^* 5 \preceq^* 15 \preceq^* 10 \preceq^* 30$.

Set $c_0 := 1$ and $A_1 := A_0 \setminus \{1\}$.

Set $c_1 := 3$ and $A_2 := A_1 \setminus \{3\}$.

Set $c_2 := 2$ and $A_3 := A_2 \setminus \{2\}$.

Set $c_3 := 6$ and $A_4 := A_3 \setminus \{6\}$.

Set $c_4 := 5$ and $A_5 := A_4 \setminus \{5\}$.

Set $c_5 := 15$ and $A_6 := A_5 \setminus \{15\}$.

Set $c_6 := 10$ and $A_7 := A_6 \setminus \{10\}$.

Set $c_7 := 30$ and $A_8 := A_7 \setminus \{30\}$.

Kahn's Algorithm stops

Keep collecting
minimal elements.

- ▶ The input set A is finite.
- ▶ Each time the repeat-until loop is run, one element is taken out of A .
- ▶ So this loop is run exactly $|A|$ times.
- ▶ Then the set of remaining elements is empty, and the stopping condition is satisfied.

Kahn's Algorithm (1962)

Input: a finite set A , a partial order \preceq on A .

- (1) Set $A_0 := A$ and $i := 0$.
- (2) Repeat until $A_i = \emptyset$:
 - (2.1) find a minimal element c_i of A_i wrt \preceq ;
 - (2.2) set $A_{i+1} := A_i \setminus \{c_i\}$;
 - (2.3) set $i := i + 1$.

Output: a linearization \preceq^* of \preceq defined by setting, for all indices i, j ,

$$c_i \preceq^* c_j \iff i \leq j.$$

Kahn's Algorithm is correct

Want \preceq^* a total order and $\forall x, y \in A$ ($x \preceq y \Rightarrow x \preceq^* y$)

Proof (optional material)

2. Suppose the run produces $A_0, A_1, \dots, A_n, c_0, c_1, \dots, c_{n-1}$ and \preceq^* .
3. Note $A = \{c_0, c_1, \dots, c_{n-1}\}$ because the removal of c_0, c_1, \dots, c_{n-1} from A makes the set empty.
4. Note also that \preceq^* is a total order on A because it is by definition only a renaming of the total order \leq on $\{0, 1, \dots, n-1\}$.
5.
 - 5.1. Take $x \in A$ and $c_j \in A$ such that $x \prec c_j$.
 - 5.2. Then $x \notin A_j$ as c_j is minimal in A_j .
 - 5.3. So $x \in A \setminus A_j = \{c_0, c_1, \dots, c_{j-1}\}$ by the choices of $A_0, A_1, \dots, A_j, c_0, c_1, \dots, c_{j-1}$.
 - 5.4. Let $i \in \{0, 1, \dots, j-1\}$ such that $x = c_i$.
 - 5.5. Then $x = c_i \preceq^* c_j$ by the definition of \preceq^* , as $i \leq j-1 < j$.



Kahn's Algorithm (1962)

Input: a finite set A , a partial order \preceq on A .

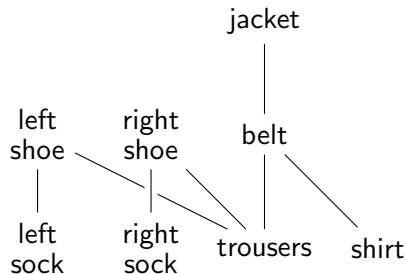
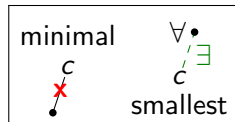
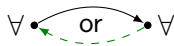
- (1) Set $A_0 := A$ and $i := 0$.
- (2) Repeat until $A_i = \emptyset$:
 - (2.1) find a minimal element c_i of A_i wrt \preceq ;
 - (2.2) set $A_{i+1} := A_i \setminus \{c_i\}$;
 - (2.3) set $i := i + 1$.

Output: a linearization \preceq^* of \preceq defined by setting, for all indices i, j ,

$$c_i \preceq^* c_j \iff i \leq j.$$

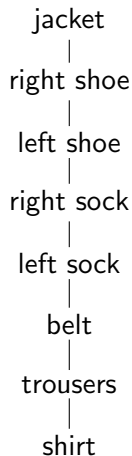
Checkpoint

- ▶ antisymmetric relations: if $x R y$ and $y R x$, then $x = y$.
- ▶ partial orders: reflexive, antisymmetric, transitive
- ▶ total order: a partial order in which any two elements are comparable
- ▶ minimal/maximal vs smallest/largest
- ▶ linearization: a sequential way to complete the tasks such that tasks that must be done first are done first
- ▶ Kahn's Algorithm, with a proof of its termination and correctness



[T]he things themselves are not what [science] can reach, as the naive dogmatists think, but only the relations between things. Outside of these relations there is no knowable reality.

Poincaré 1902



Next:
induction