

Discrete Algebraic Structures

WiSe 2025/2026

Prof. Dr. Antoine Wiehe
Research Group for Theoretical Computer Science

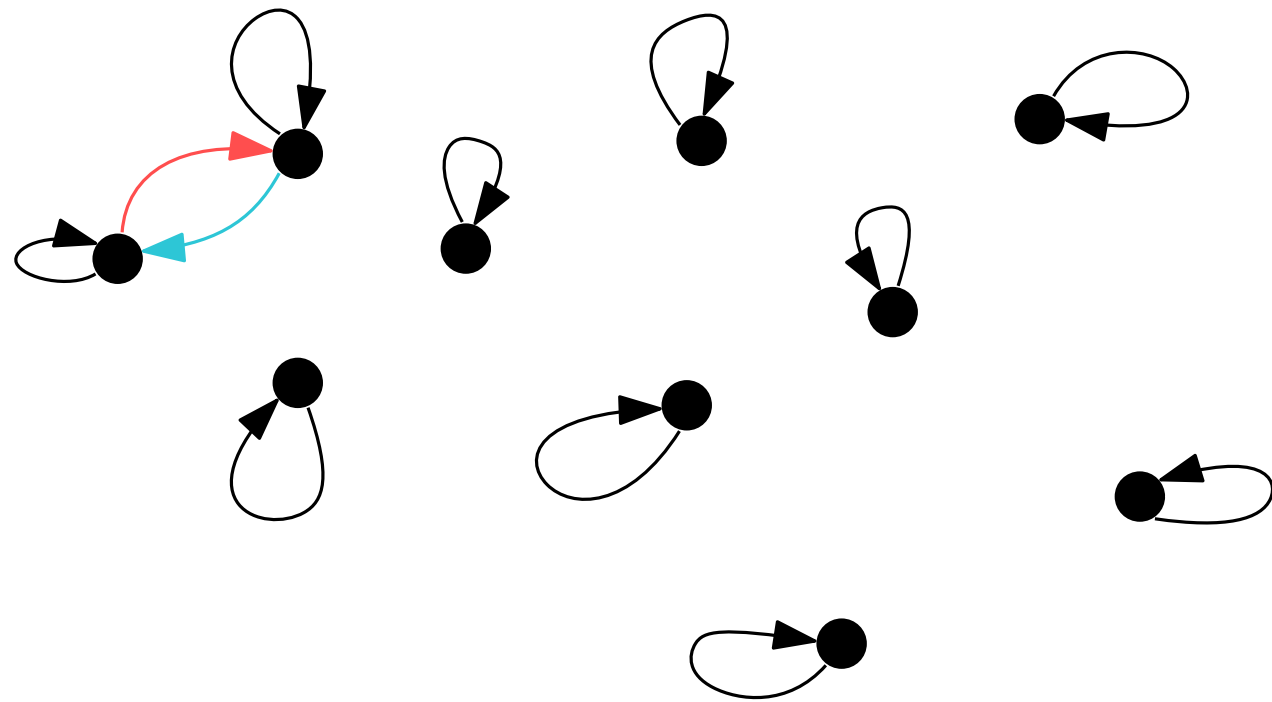


- What a relation is
- How to draw a relation $R \subseteq A \times B$
- How to compute the composition and transpose of binary relations
- The basic properties
(anti)reflexivity, (anti)symmetry, transitivity
- How to compute the closures

Relations we encounter in “real life” are often of one of two types:

Things can share a **common property**:

- $x = y$: share the same value
- x, y are numbers that end with the same digit
- x, y are in the same family
- x, y work in the same company

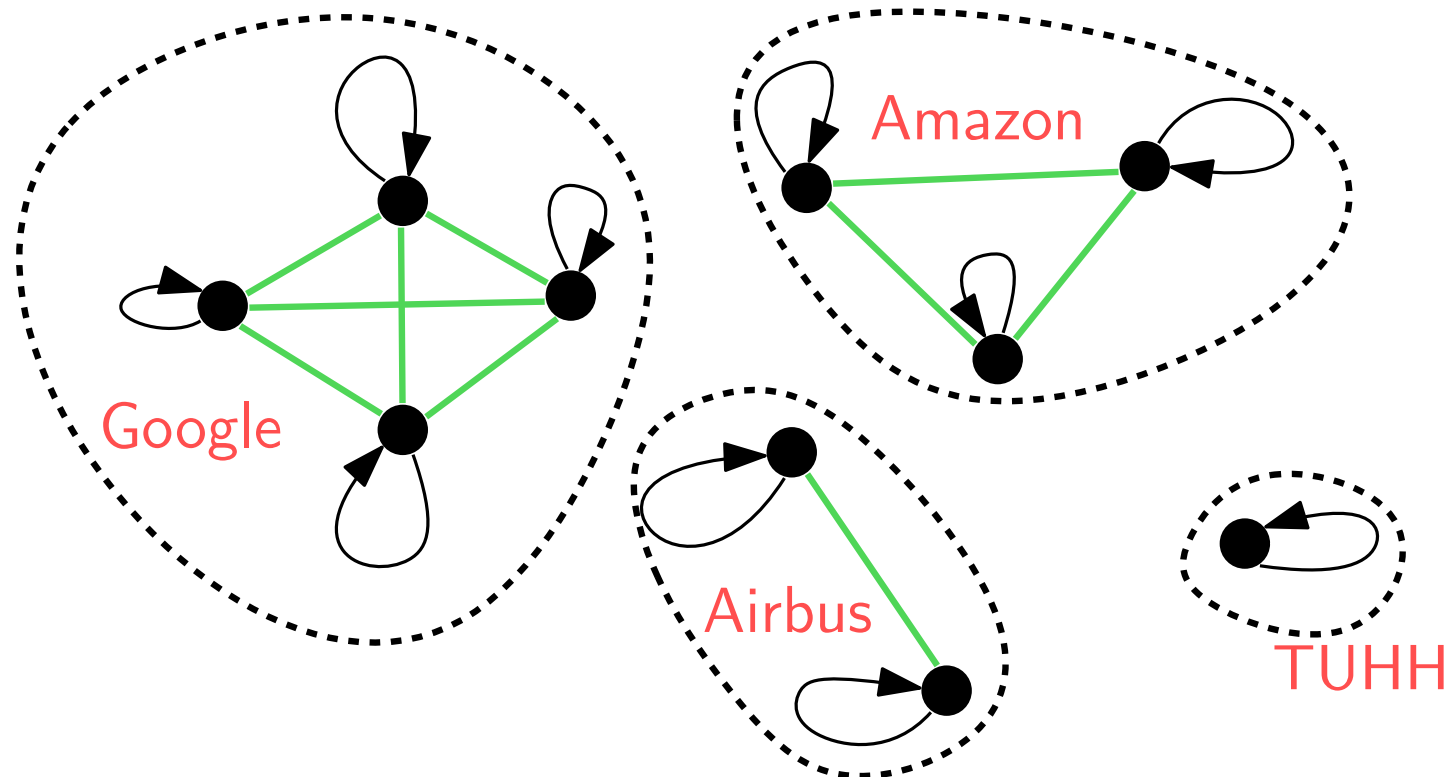


SameCompany $\subseteq$ People $\times$ People

Relations we encounter in “real life” are often of one of two types:

Things can share a **common property**:

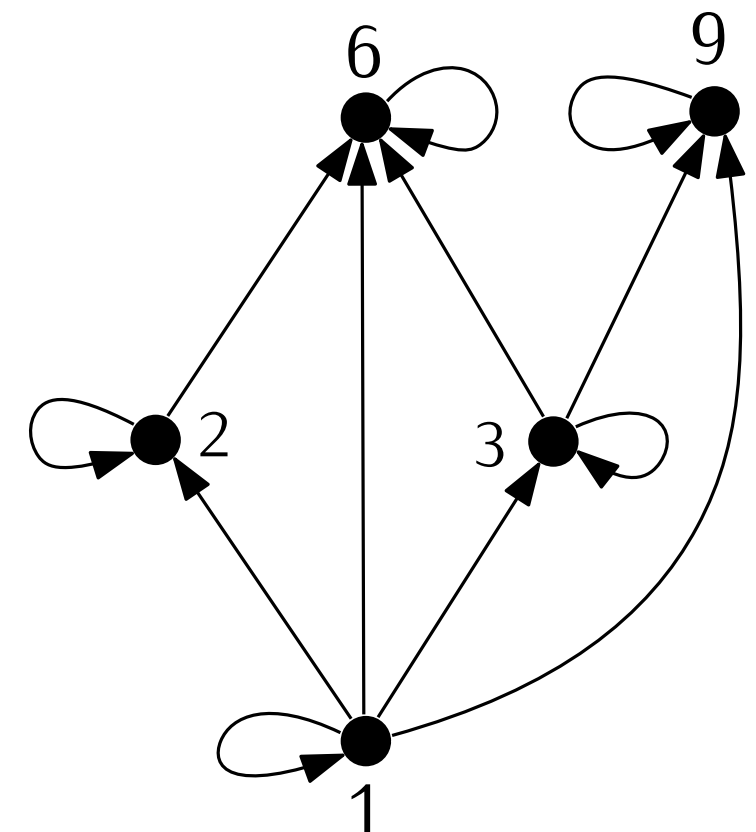
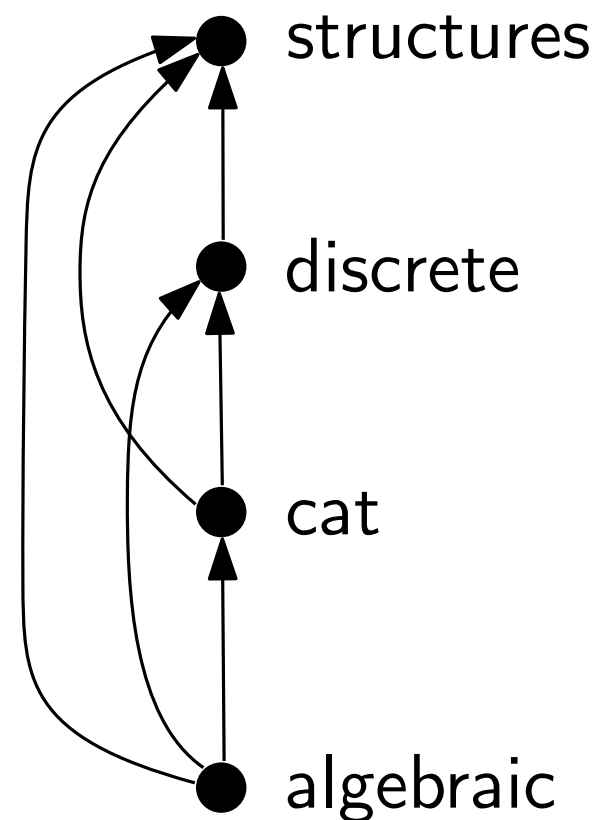
- $x = y$: share the same value
- x, y are numbers that end with the same digit
- x, y are in the same family
- x, y work in the same company



$\text{SameCompany} \subseteq \text{People} \times \text{People}$

Things can be ordered:

- x appears before y in the dictionary
- The string x is not longer than the string y
- x is taller than y
- y is a multiple of x



- Definition.** A relation $R \subseteq A \times A$ is:
- **reflexive**: if for all $a \in A$, $(a, a) \in R$
 - **antireflexive**: if for all $a \in A$, $(a, a) \notin R$
 - **symmetric**: if for all $a, b \in A$, if $(a, b) \in R$, then $(b, a) \in R$
 - **antisymmetric**: if for all $a, b \in A$, if $(a, b) \in R$ and $a \neq b$ then $(b, a) \notin R$
 - **transitive**: if for all $a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$.

	Reflexive	Antireflexive	Symmetric	Antisymmetric	Transitive
Equivalence relation	✓		✓		✓
Order	✓			✓	✓
Strict order		✓		✓	✓
Quasi-order	✓				✓

Equivalence relations

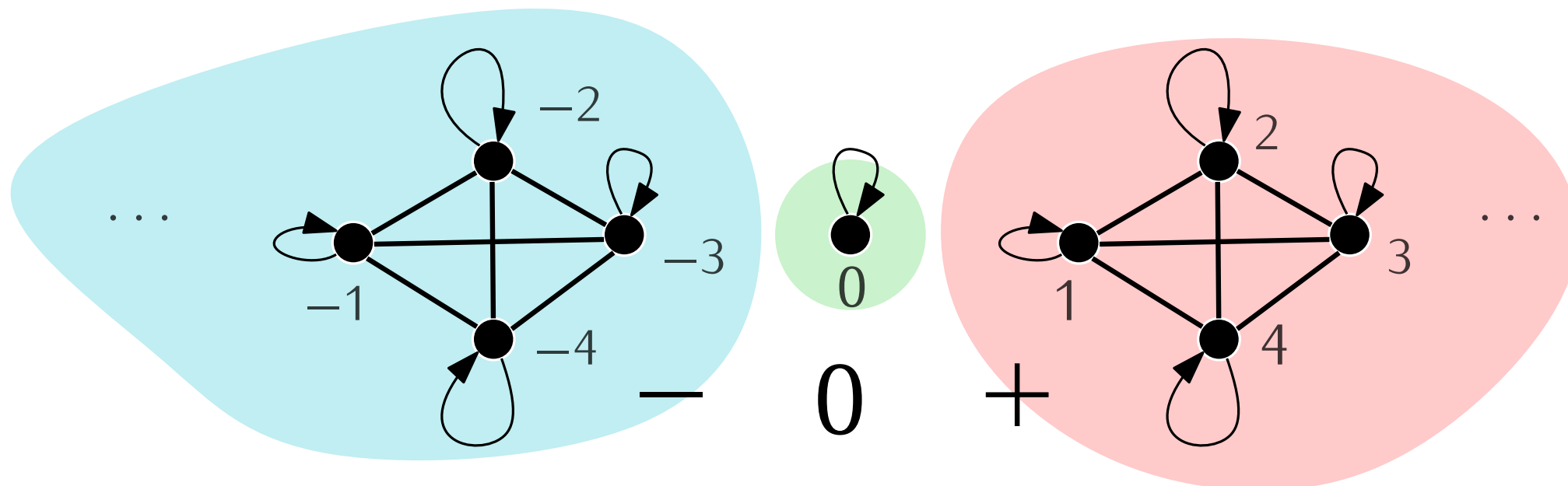
Definition. A relation $R \subseteq A \times A$ is an **equivalence relation** if it is reflexive, symmetric, and transitive.

Examples. All of these are equivalence relations:

- $\{(x, y) \in \mathbb{Z}^2 \mid x, y \text{ have the same sign}\}$ $\{0, +, -\}$
- $\{(x, y) \in (\mathbb{N}_0)^2 \mid x, y \text{ have the same parity}\}$ $\{\text{even}, \text{odd}\}$
- $\{(x, y) \in \text{People}^2 \mid x, y \text{ have the same height}\}$ $\mathbb{N}_0$
- $\{(\varphi, \psi) \in \text{PropositionalFormulas}^2 \mid \varphi \equiv \psi\}$
- $\{(x, y) \in A^2 \mid x = y\}$
- A^2

We use symbols like $\sim, \simeq, \equiv$ for relations that are equivalence relations

We then write $a \simeq b$ instead of $(a, b) \in \simeq$



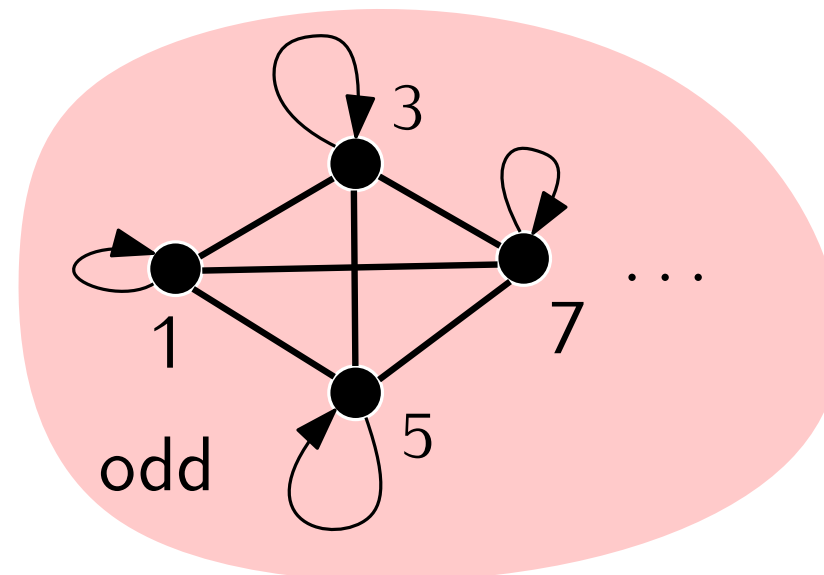
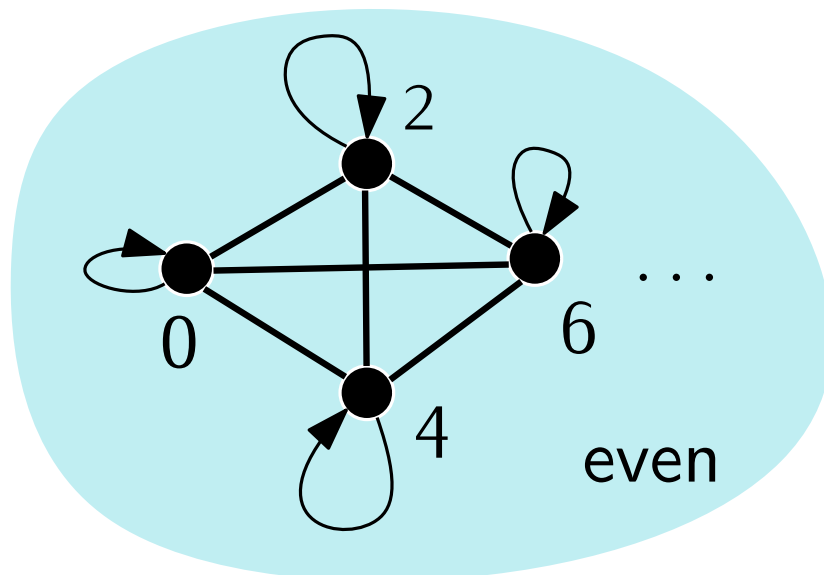
Definition. A relation $R \subseteq A \times A$ is an **equivalence relation** if it is reflexive, symmetric, and transitive.

Examples. All of these are equivalence relations:

- $\{(x, y) \in \mathbb{Z}^2 \mid x, y \text{ have the same sign}\}$ $\{0, +, -\}$
- $\{(x, y) \in (\mathbb{N}_0)^2 \mid x, y \text{ have the same parity}\}$ $\{\text{even}, \text{odd}\}$
- $\{(x, y) \in \text{People}^2 \mid x, y \text{ have the same height}\}$ $\mathbb{N}_0$
- $\{(\varphi, \psi) \in \text{PropositionalFormulas}^2 \mid \varphi \equiv \psi\}$
- $\{(x, y) \in A^2 \mid x = y\}$
- A^2

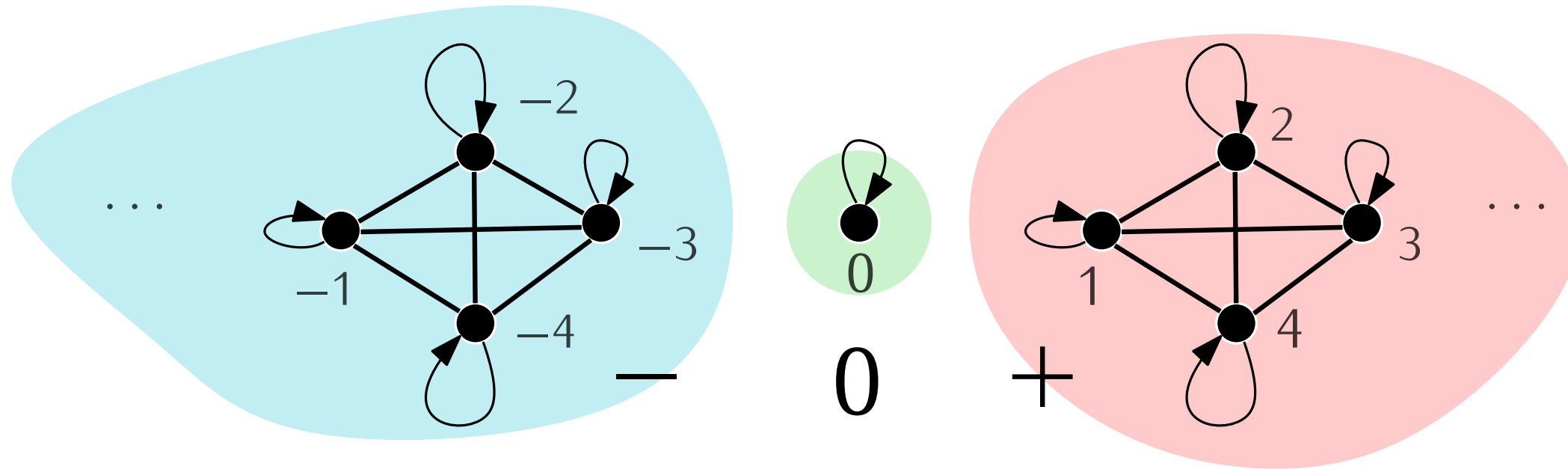
We use symbols like $\sim, \simeq, \equiv$ for relations that are equivalence relations

We then write $a \simeq b$ instead of $(a, b) \in \simeq$



Definition. Let $\sim$ be an equivalence relation on A , and let $a \in A$. The **equivalence class** of a is

$$[a]_{\sim} = \{b \in A \mid a \sim b\}$$



$$[-1]_{\sim} =$$

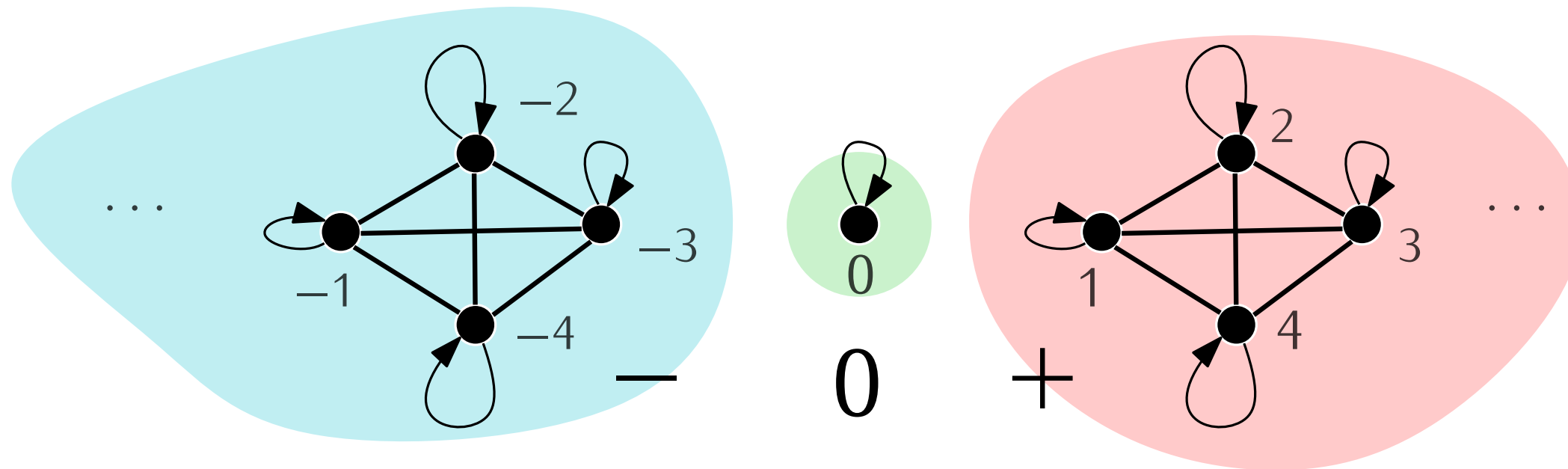
$$[0]_{\sim} =$$

$$[1]_{\sim} =$$

$$[-2]_{\sim} =$$

Definition. Let $\sim$ be an equivalence relation on A , and let $a \in A$. The **equivalence class** of a is

$$[a]_{\sim} = \{b \in A \mid a \sim b\}$$



Define $a \sim b$ on $\mathbb{N}_0$ as “ a and b have the same parity”.
What is $[0]_{\sim}$?



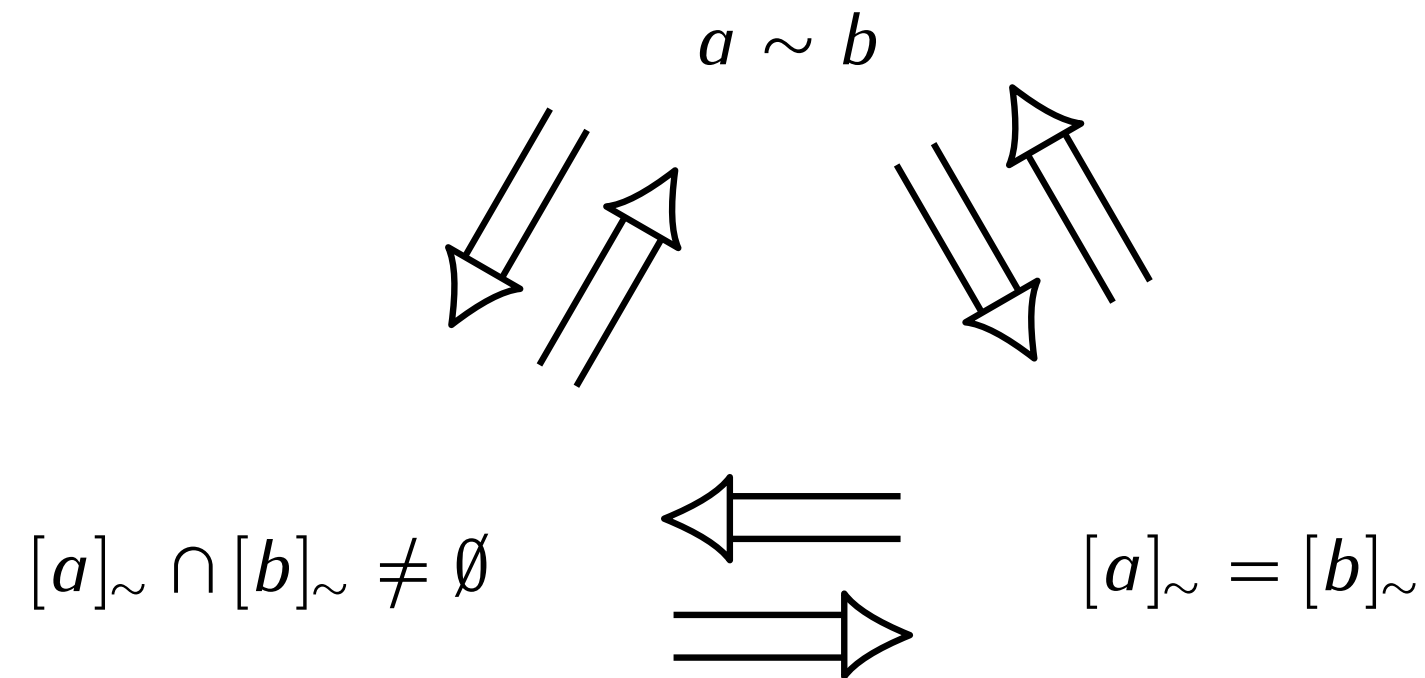
Definition. Let $\sim$ be an equivalence relation on A , and let $a \in A$. The **equivalence class** of a is

$$[a]_{\sim} = \{b \in A \mid a \sim b\}$$

Theorem. Let $\sim$ be an equivalence relation on A , and let $a, b \in A$. The following are equivalent:

1. $a \sim b$
2. $[a]_{\sim} = [b]_{\sim}$
3. $[a]_{\sim} \cap [b]_{\sim} \neq \emptyset$

Theoretically, one needs to prove **6 implications**:



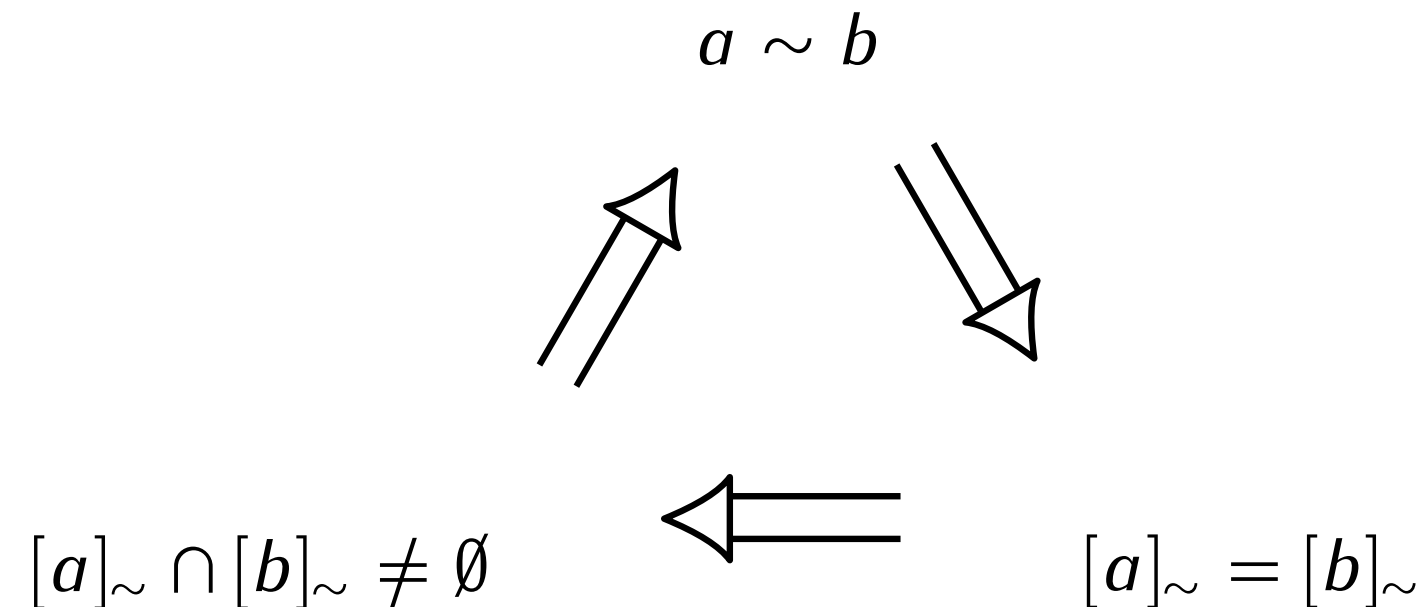
Definition. Let $\sim$ be an equivalence relation on A , and let $a \in A$. The **equivalence class** of a is

$$[a]_{\sim} = \{b \in A \mid a \sim b\}$$

Theorem. Let $\sim$ be an equivalence relation on A , and let $a, b \in A$. The following are equivalent:

1. $a \sim b$
2. $[a]_{\sim} = [b]_{\sim}$
3. $[a]_{\sim} \cap [b]_{\sim} \neq \emptyset$

Theoretically, one needs to prove **6 implications**:

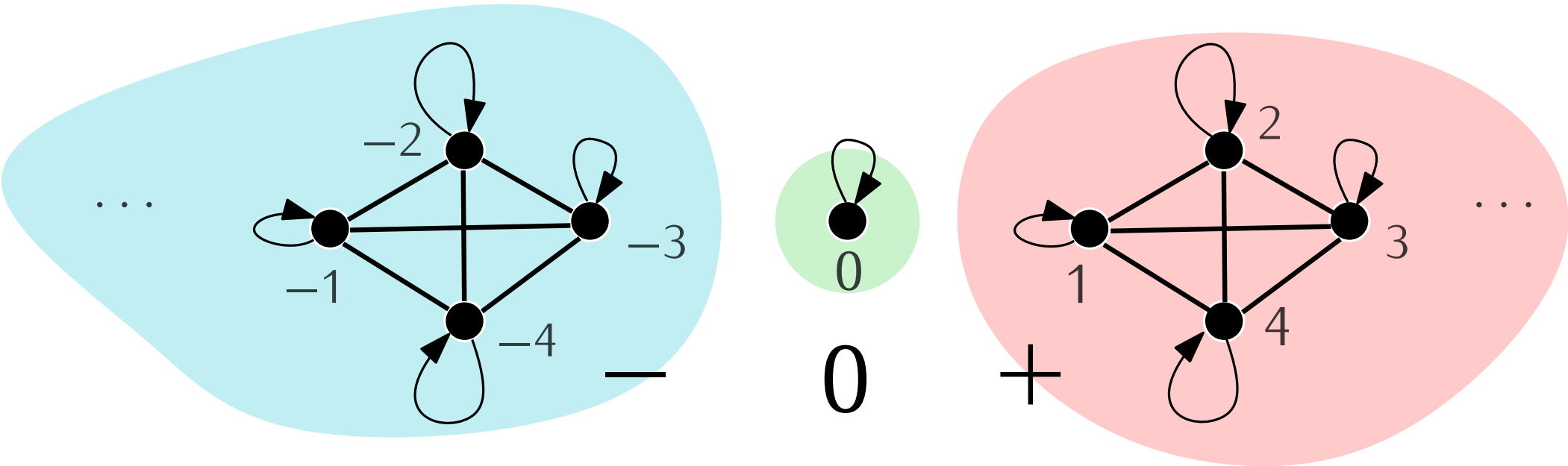


By **logical equivalence**, it suffices to prove **3 implications**!

Definition. Let A be a set. A **partition** of A is a set P of **subsets of A** , called the **parts**, such that:

- the parts are not empty
- every $a \in A$ belongs to one of the parts of P
- distinct parts in P are disjoint.

$\forall S \in P \ S \neq \emptyset$
 $\forall a \in A \exists S \in P : a \in S$
 $\forall S, T \in P (S \neq T \Rightarrow S \cap T = \emptyset)$



$P = \{\mathbb{Z}_-, \{0\}, \mathbb{Z}_+\}$
is a partition of $\mathbb{Z}$

f : equivalence relation $\sim \mapsto$ partition $\{[a]_\sim \mid a \in A\}$

g : partition $P \mapsto \{(a, b) \in A^2 \mid a, b \text{ belong to the same part}\}$

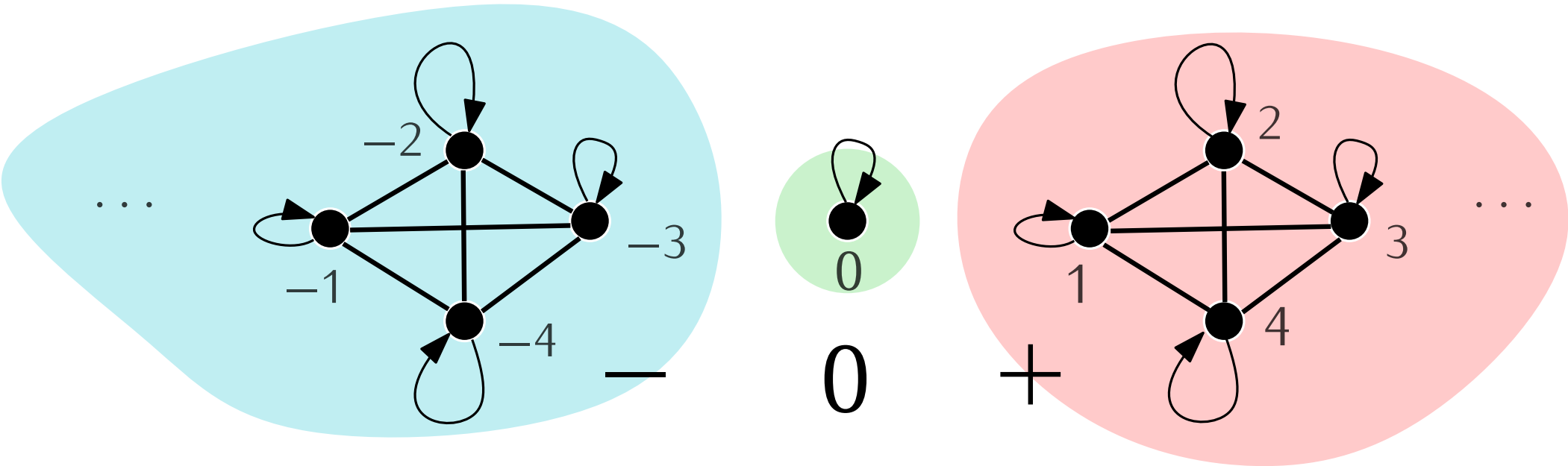
these two functions are inverse of each other!

$(g \circ f)(\sim) = \sim$
 $(f \circ g)(P) = P$

Definition. Let A be a set. A **partition** of A is a set P of **subsets of A** , called the **parts**, such that:

- the parts are not empty
- every $a \in A$ belongs to one of the parts of P
- distinct parts in P are disjoint.

$$\forall S \in P \ S \neq \emptyset$$
$$\forall a \in A \exists S \in P : a \in S$$
$$\forall S, T \in P (S \neq T \Rightarrow S \cap T = \emptyset)$$



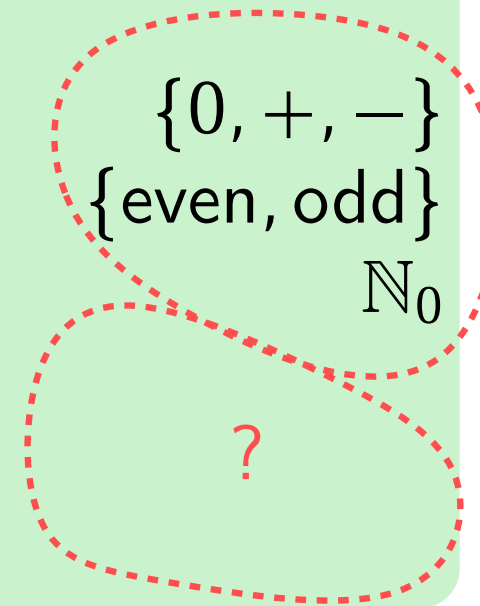
$P = \{\mathbb{Z}_-, \{0\}, \mathbb{Z}_+\}$
is a partition of $\mathbb{Z}$

We have proved:

Theorem. There exists a bijection between the set of all equivalence relations on A , and the set of all partitions of A .

Examples. All of these are equivalence relations:

- $\{(x, y) \in \mathbb{Z}^2 \mid x, y \text{ have the same sign}\}$
- $\{(x, y) \in (\mathbb{N}_0)^2 \mid x, y \text{ have the same parity}\}$
- $\{(x, y) \in \text{People}^2 \mid x, y \text{ have the same height}\}$
- $\{(\varphi, \psi) \in \text{PropositionalFormulas}^2 \mid \varphi \equiv \psi\}$
- $\{(x, y) \in A^2 \mid x = y\}$
- A^2



partition associated
with the equivalence
relation

“thing” shared by the
elements that are
equivalent

Notation. We write $A/\sim$ for the partition of A given by the equivalence classes of $\sim$.

$$A/\sim = \{[a]_\sim \mid a \in A\}$$

Partitions and quotients will appear many many times in your studies, for example:

- modular arithmetic, Lagrange’s theorem (later this semester): **RSA** cryptosystem
- quotient of vector spaces, V/W (Math 2 or 3): **persistent homology**, recognizing patterns in big data
- automata theory (2nd semester)

Intuition: forget some differences between elements,
only remember some specific aspects

Orders

- Generalize properties of $(\mathbb{N}, <)$ and $(\mathbb{Q}, <)$ to other sets
- Having an order can help to design good algorithms (binary search)
- Many problems (in math, in CS, natural sciences) are solved by computing minimal elements for some order

Question. What properties does the relation $\leq$ have (on $\mathbb{N}, \mathbb{Z}, \dots$)?

- Reflexive
- Antireflexive
- Symmetric
- Antisymmetric
- Transitive

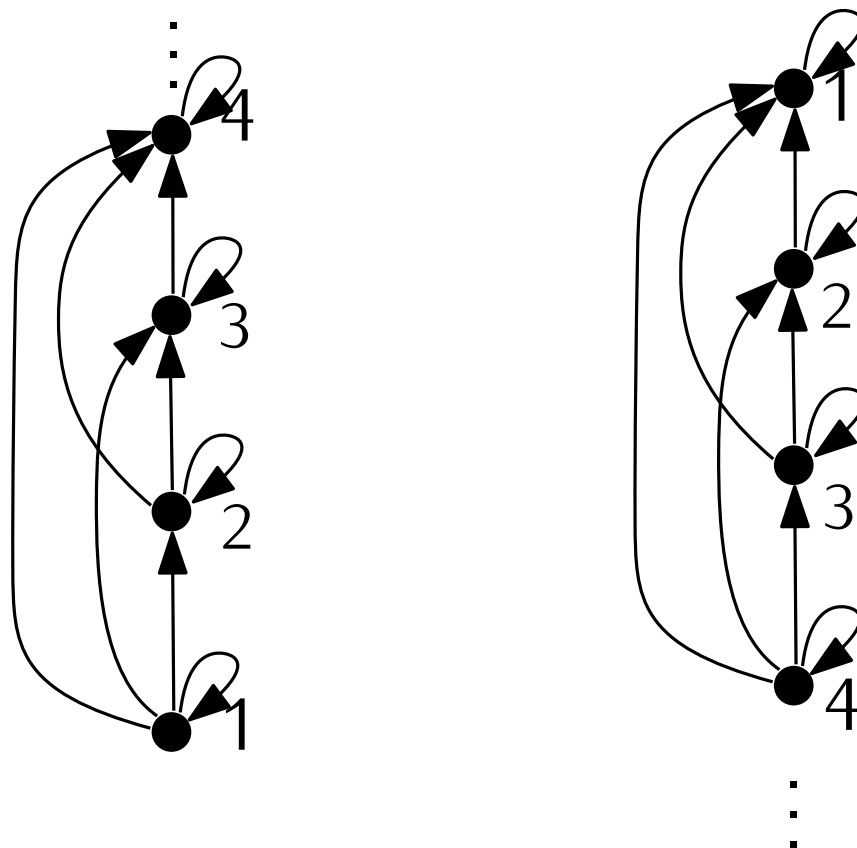


Definition. A relation $R \subseteq A \times A$ is an **order** if it is reflexive, antisymmetric, and transitive.

Examples. The following relations are all orders:

- $\{(n, m) \in \mathbb{N}^2 \mid n \leq m\}$
- $\{(n, m) \in \mathbb{N}^2 \mid n \geq m\}$
- $\{(n, m) \in \mathbb{N}^2 \mid n \text{ divides } m\}$
- $\{(S, T) \in \mathcal{P}(A)^2 \mid S \subseteq T\}$
- $\{(s, t) \in \text{BinaryStrings}^2 \mid s \text{ is a prefix of } t\}$

Notation: (A, R) is a **poset**.

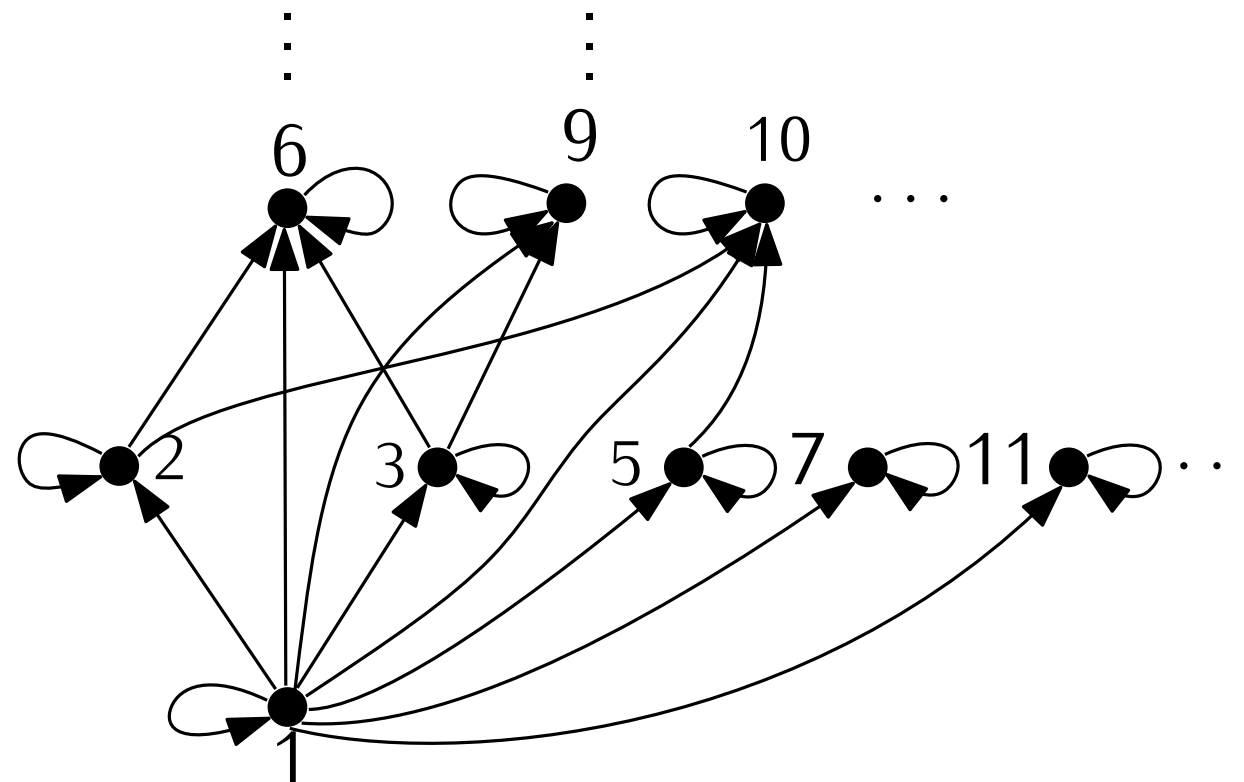


Definition. A relation $R \subseteq A \times A$ is an **order** if it is reflexive, antisymmetric, and transitive.

Examples. The following relations are all orders:

- $\{(n, m) \in \mathbb{N}^2 \mid n \leq m\}$
- $\{(n, m) \in \mathbb{N}^2 \mid n \geq m\}$
- $\{(n, m) \in \mathbb{N}^2 \mid n \text{ divides } m\}$
- $\{(S, T) \in \mathcal{P}(A)^2 \mid S \subseteq T\}$
- $\{(s, t) \in \text{BinaryStrings}^2 \mid s \text{ is a prefix of } t\}$

Notation: (A, R) is a **poset**.

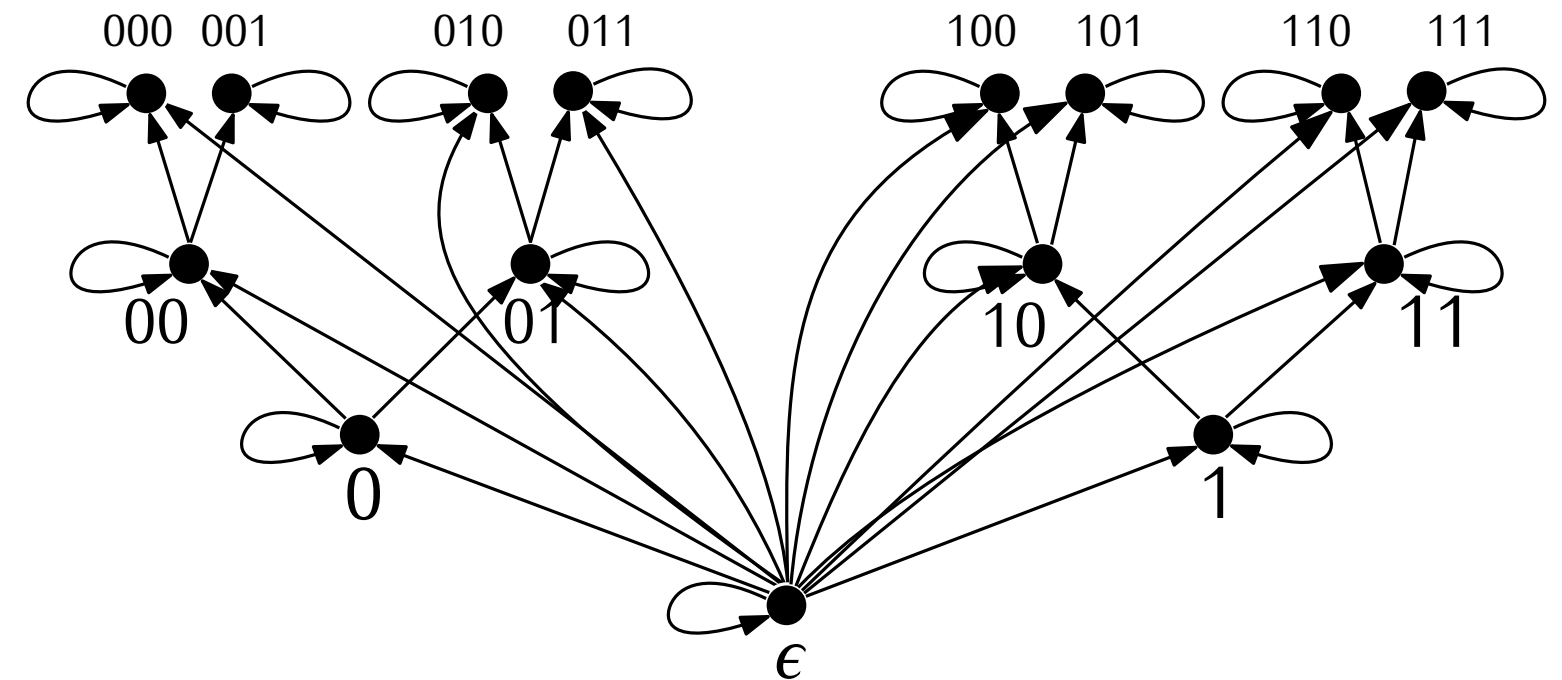
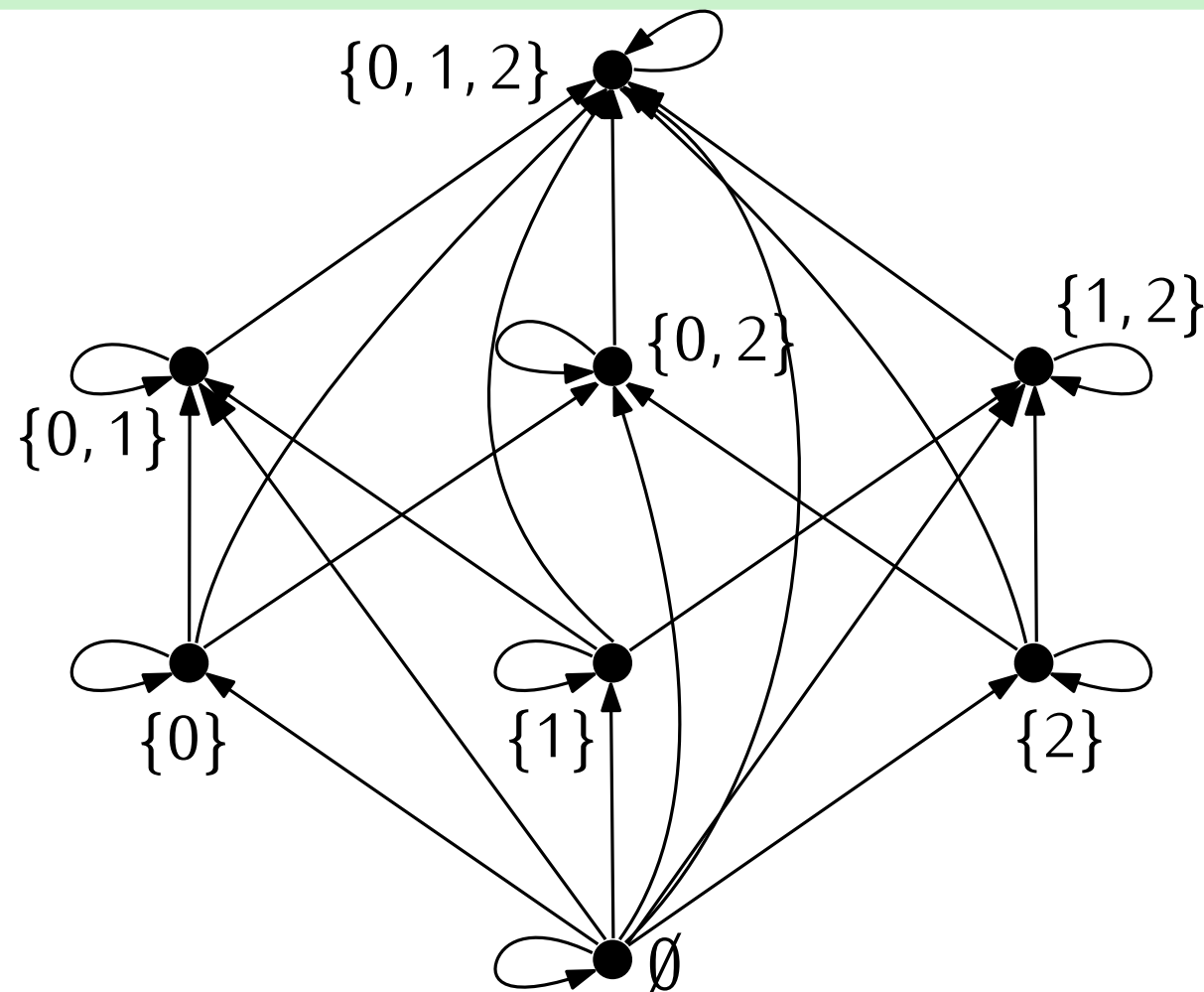


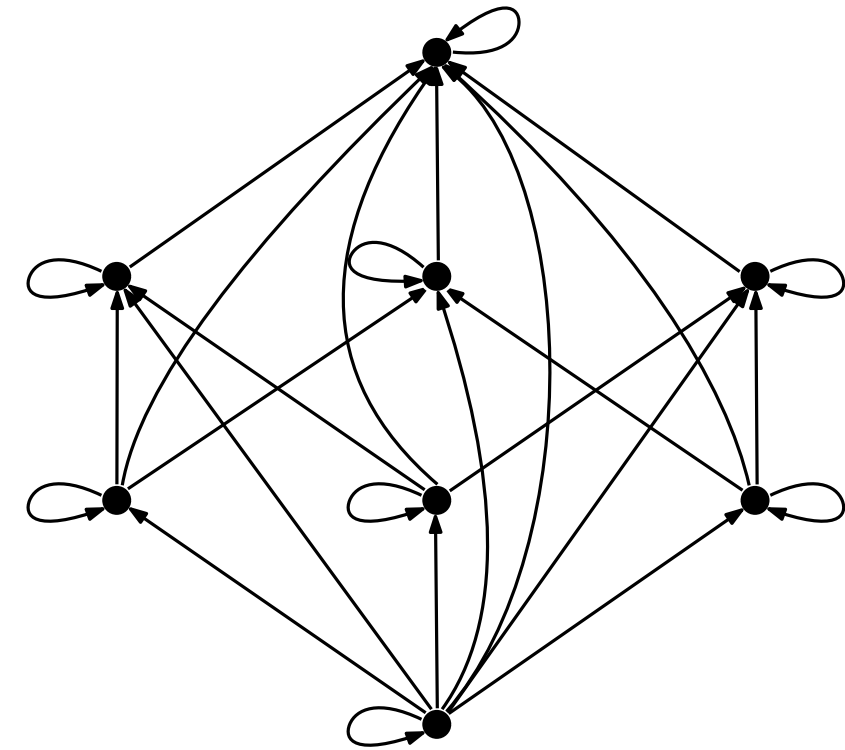
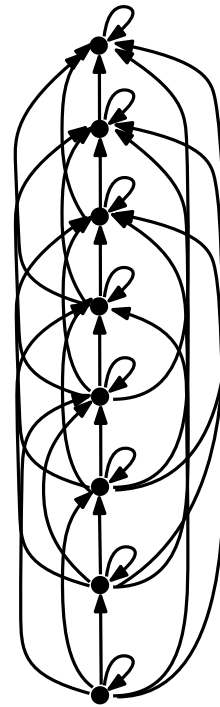
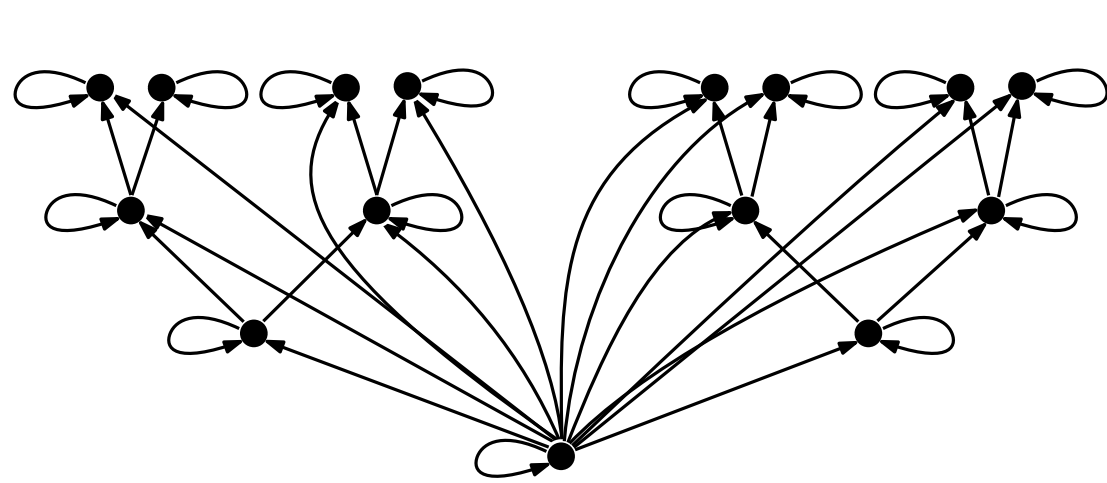
Definition. A relation $R \subseteq A \times A$ is an **order** if it is reflexive, antisymmetric, and transitive.

Examples. The following relations are all orders:

- $\{(n, m) \in \mathbb{N}^2 \mid n \leq m\}$
- $\{(n, m) \in \mathbb{N}^2 \mid n \geq m\}$
- $\{(n, m) \in \mathbb{N}^2 \mid n \text{ divides } m\}$
- $\{(S, T) \in \mathcal{P}(A)^2 \mid S \subseteq T\}$
- $\{(s, t) \in \text{BinaryStrings}^2 \mid s \text{ is a prefix of } t\}$

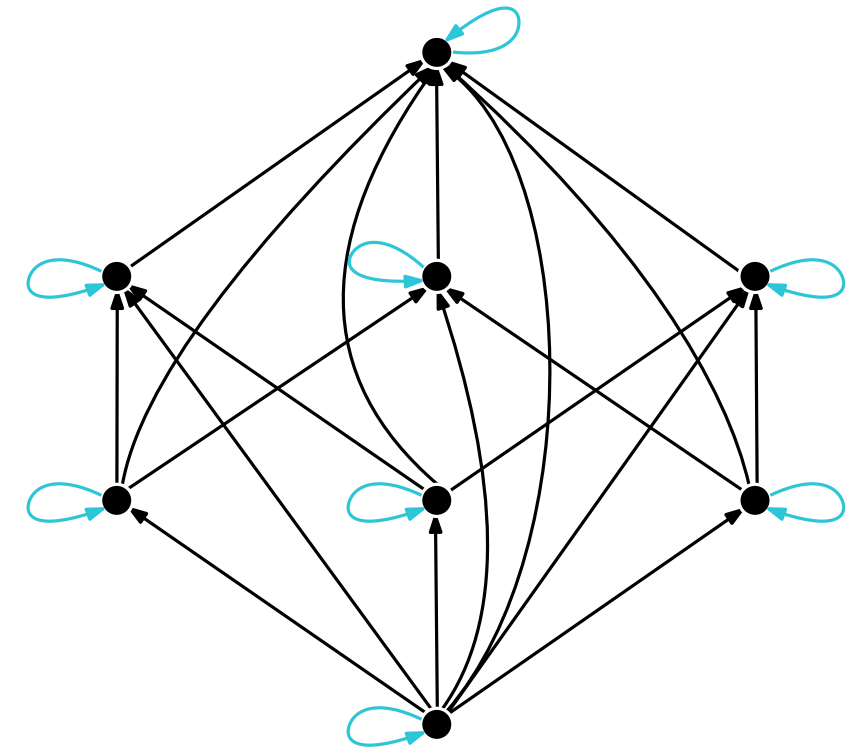
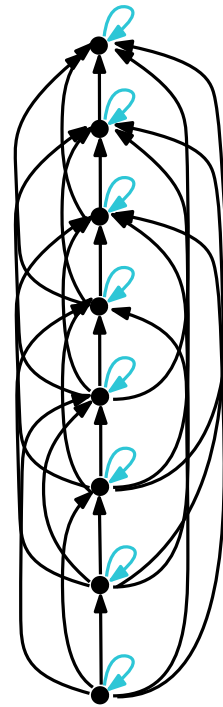
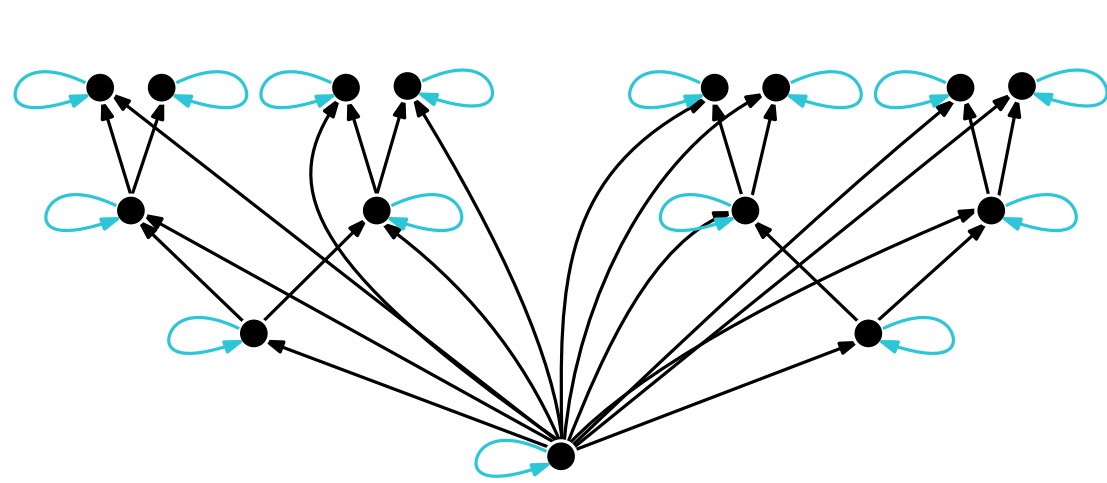
Notation: (A, R) is a **poset**.





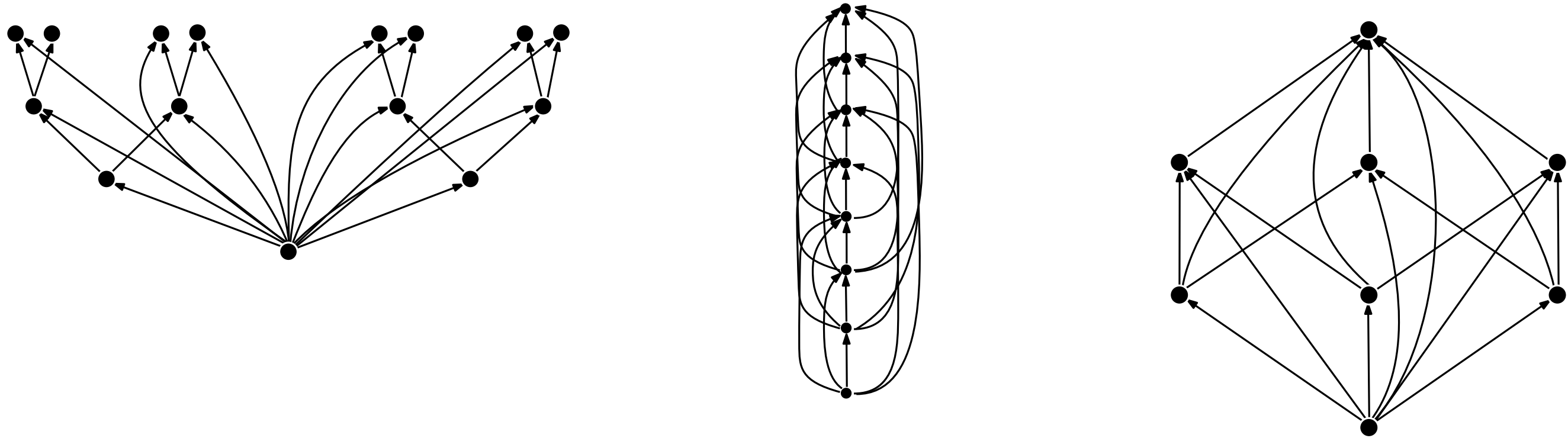
Question. How much information is actually necessary to “remember” the order we are drawing?

- It’s reflexive, so we know the loops are there



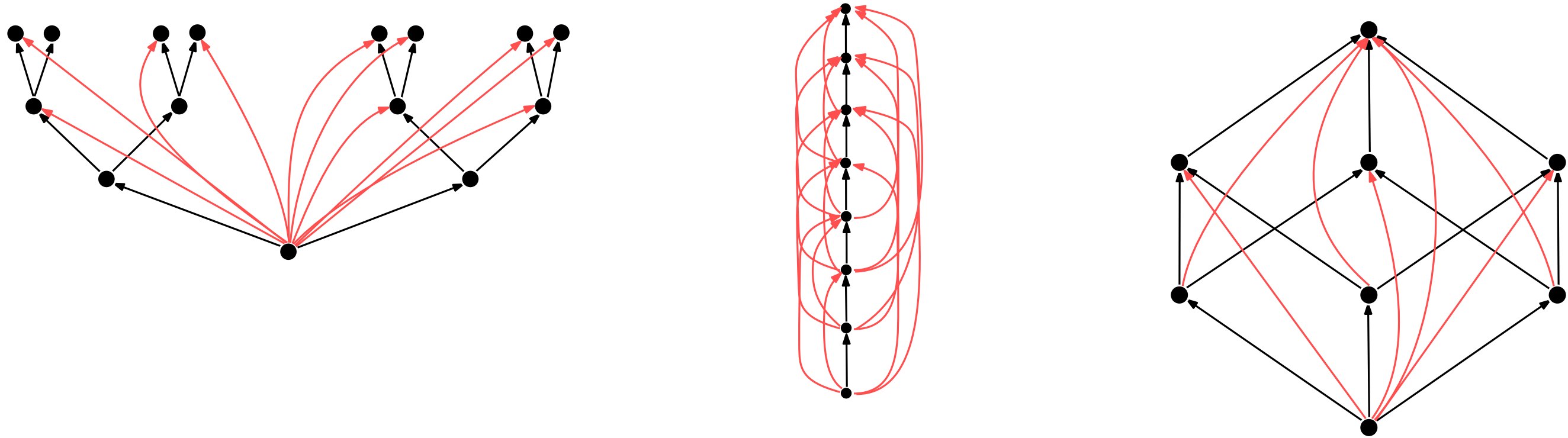
Question. How much information is actually necessary to “remember” the order we are drawing?

- It’s reflexive, so we know the loops are there



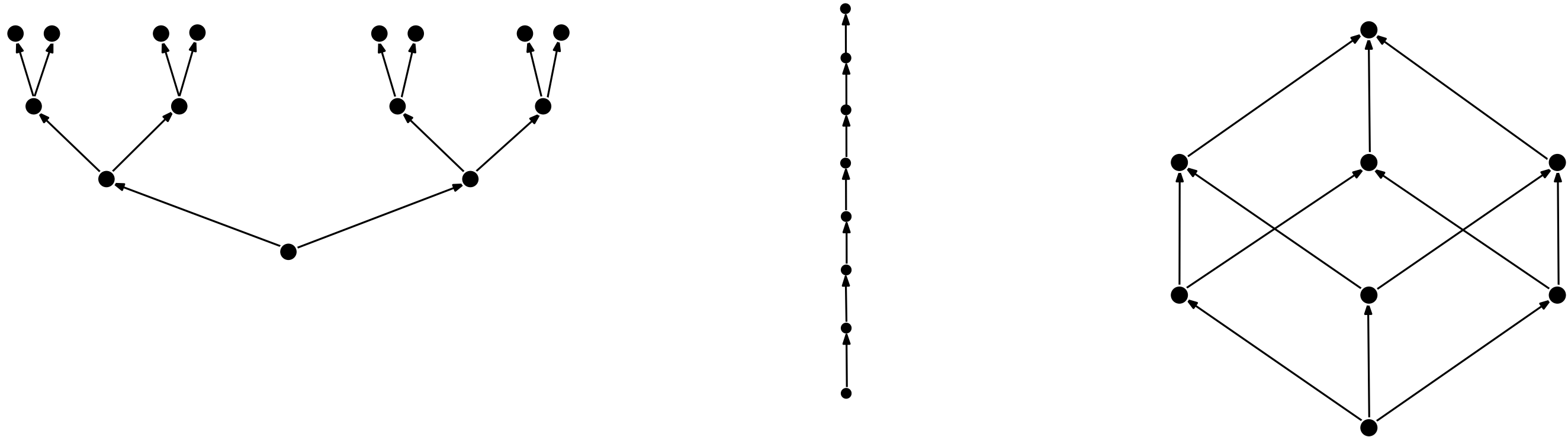
Question. How much information is actually necessary to “remember” the order we are drawing?

- It's reflexive, so we know the loops are there
- It's transitive, so some edges are implied by others



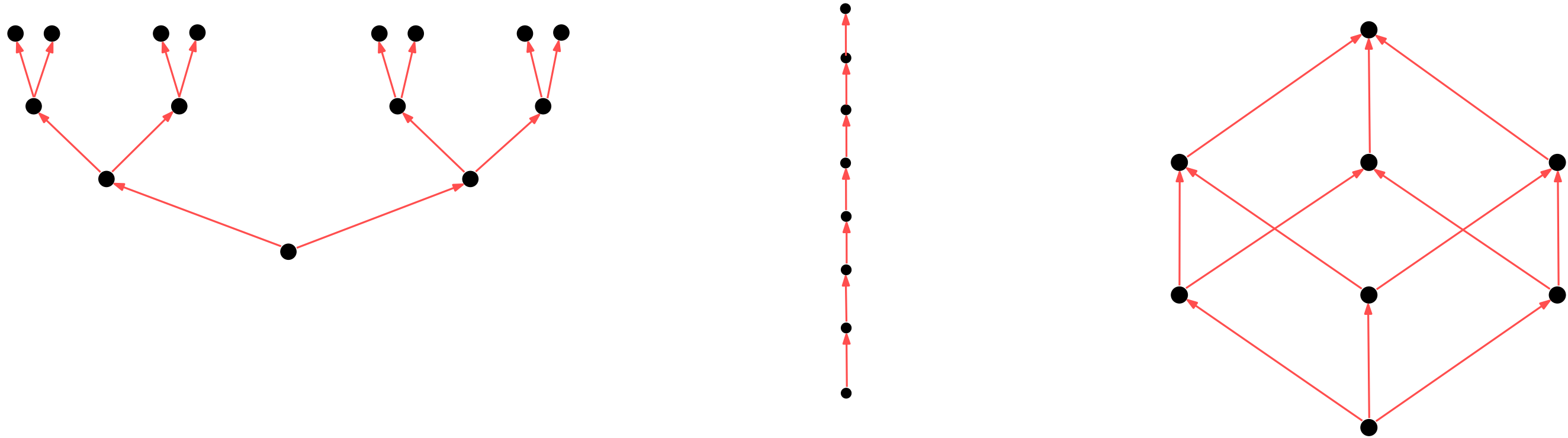
Question. How much information is actually necessary to “remember” the order we are drawing?

- It's reflexive, so we know the loops are there
- It's transitive, so some edges are implied by others



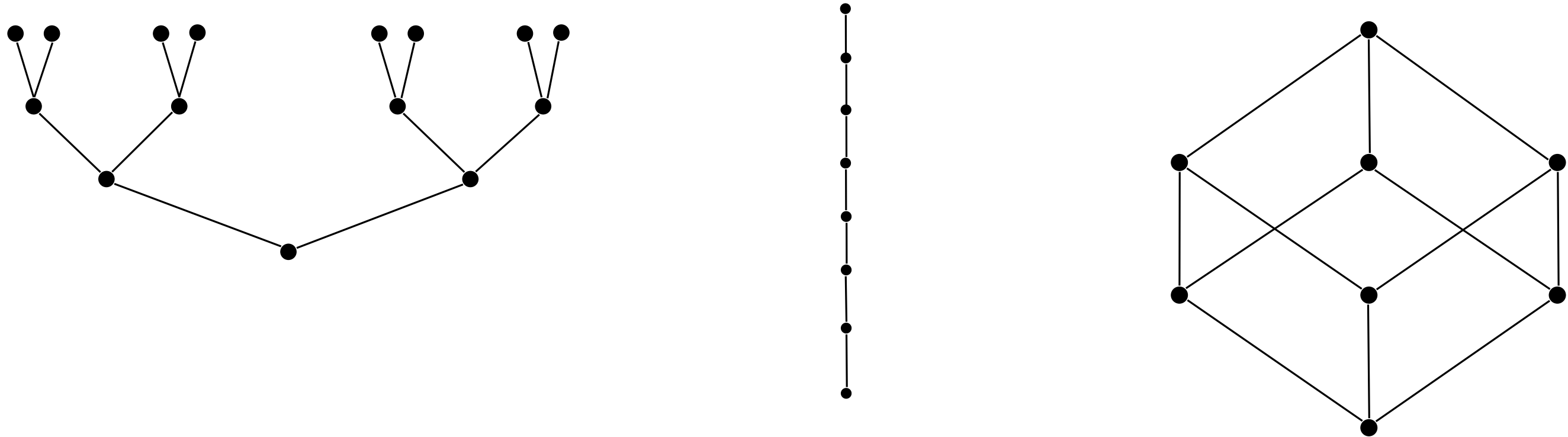
Question. How much information is actually necessary to “remember” the order we are drawing?

- It's reflexive, so we know the loops are there
- It's transitive, so some edges are implied by others
- The increasing direction is already shown by going up, so arrows are not necessary



Question. How much information is actually necessary to “remember” the order we are drawing?

- It's reflexive, so we know the loops are there
- It's transitive, so some edges are implied by others
- The increasing direction is already shown by going up, so arrows are not necessary



Question. How much information is actually necessary to “remember” the order we are drawing?

- It’s reflexive, so we know the loops are there
- It’s transitive, so some edges are implied by others
- The increasing direction is already shown by going up, so arrows are not necessary

These are the **Hasse diagrams** of the orders.

In general: consider an order $\leq$ on A and $a, b \in A$ distinct with $a \leq b$

We say b **covers** a if there is nothing between a and b $\forall c \in A (a \leq c \leq b \Rightarrow c \in \{a, b\})$

Definition. If A is finite, then a **Hasse diagram** of $\leq$ is a drawing of $\leq_{\text{cover}} = \{(a, b) \in A^2 \mid b \text{ covers } a\}$, where if $a \leq_{\text{cover}} b$, then b is above a .

We say b **covers** a if there is nothing between a and b

$$\forall c \in A (a \leq c \leq b \Rightarrow c \in \{a, b\})$$

Definition. If A is finite, then a **Hasse diagram** of $\leq$ is a drawing of $\leq_{\text{cover}} = \{(a, b) \in A^2 \mid b \text{ covers } a\}$, where if $a \leq_{\text{cover}} b$, then b is above a .

For infinite orders, sometimes it is not possible to draw a Hasse diagram:

in $\mathbb{Q}$ with the usual ordering, does 1 cover 0?

In this case, $\leq_{\text{cover}}$ is the empty set!

Let $A = \{n \in \mathbb{N} \mid n \text{ divides } 12\}$, and let $R = \{(n, m) \in A^2 \mid n \text{ divides } m\}$.
Draw the Hasse diagram of R .

Definition. A relation $R \subseteq A \times A$ is an **order** if it is reflexive, antisymmetric, and transitive.

Question. Is $<$ an order?

- Reflexive? 
- Antisymmetric? 
- Transitive? 

Definition. A relation is a **strict order** if it is **antireflexive**, antisymmetric, and transitive.

Definition. A relation $R \subseteq A \times A$ is an **order** if it is reflexive, antisymmetric, and transitive.

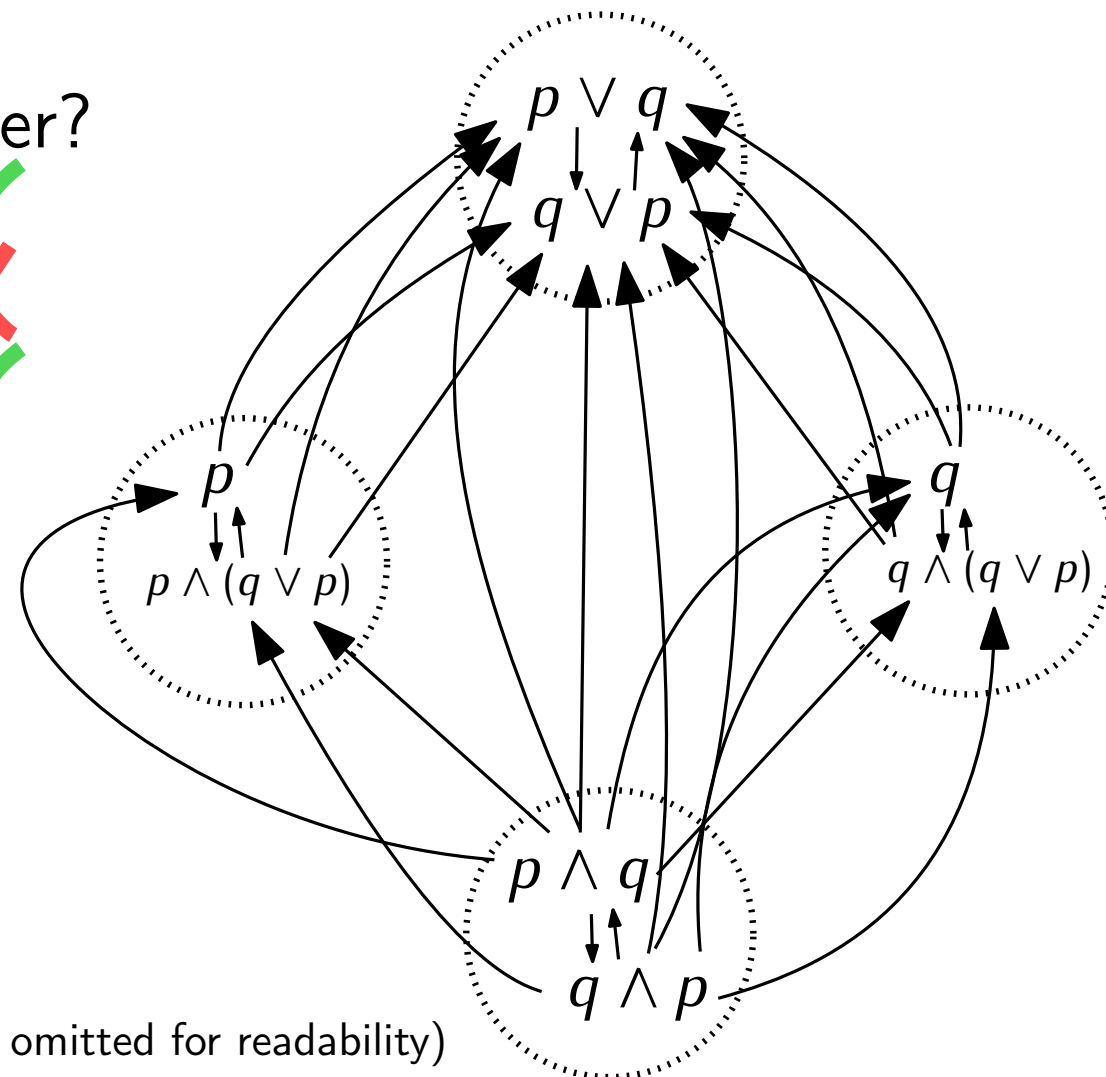
Consider the relation R defined by $\{(\varphi, \psi) \mid \text{if } \varphi \text{ is true, then } \psi \text{ is true}\}$

- $(p, p \vee q) \in R$
- $((p \Rightarrow q) \wedge p, q) \in R$
- $(p \wedge q, q \wedge p) \in R$
- $(p, p \wedge q) \notin R$

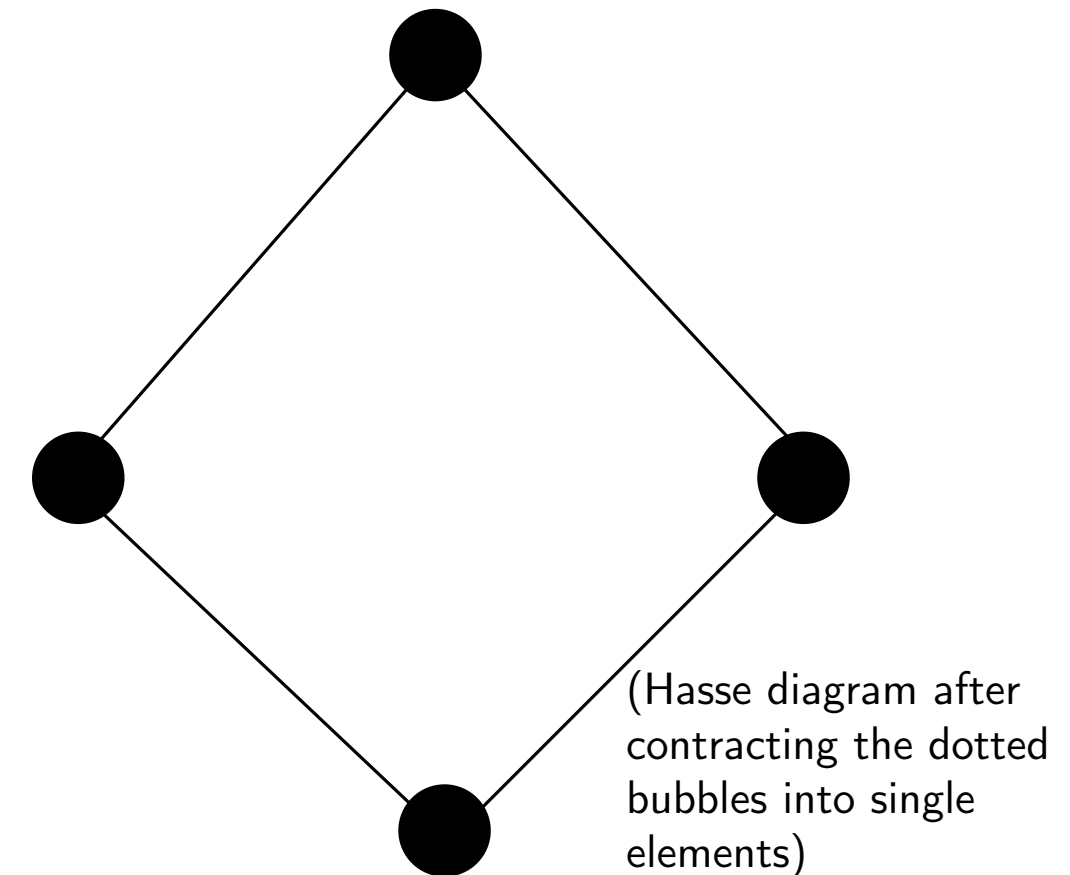
Definition. A relation is a **quasiorder** if it is reflexive and transitive.

Question. Is R an order?

- Reflexive? ✓
- Antisymmetric? ✗
- Transitive? ✓



$\rightsquigarrow$



Definition. A relation $R \subseteq A \times A$ is an **order** if it is reflexive, antisymmetric, and transitive.

Consider R defined by $\{(x, y) \in \mathbb{N}^2 \mid x \leq y\}$.

Question. Is R an order?

- Reflexive? ✓
- Antisymmetric? ✓
- Transitive? ✓

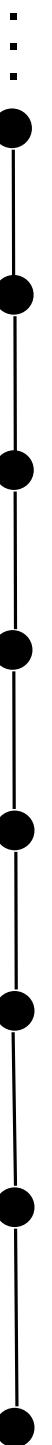
Definition. We say an order is **linear** if for every $a, b \in A$, we have $a \leq b$ or $b \leq a$.

In other words: any two elements can be compared using the order.

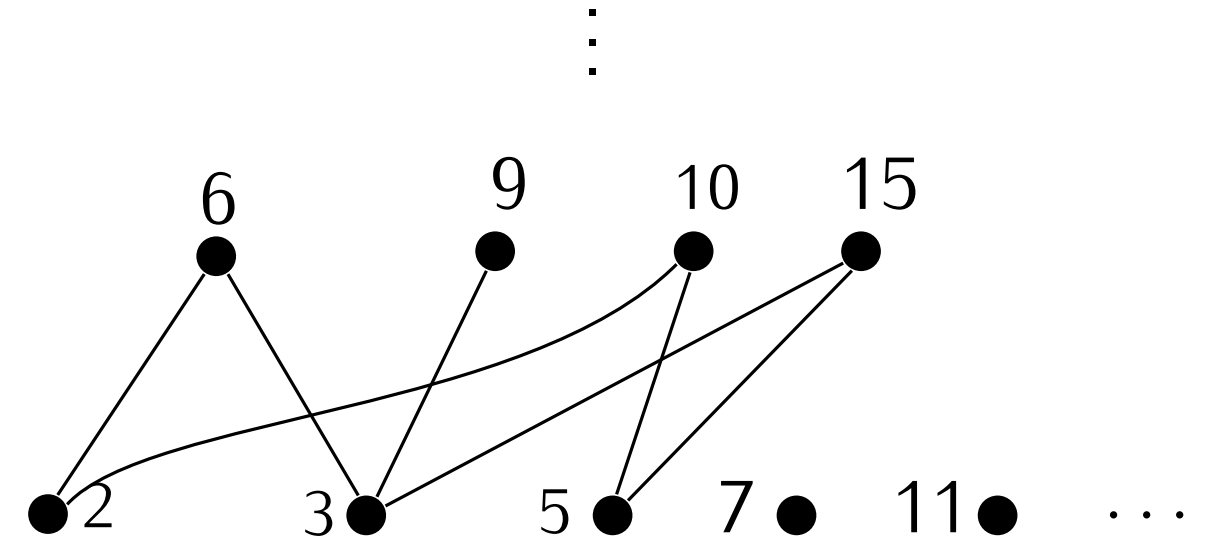
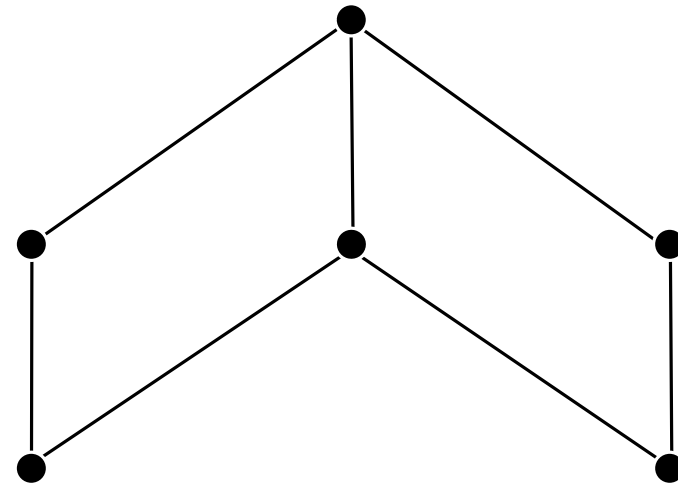
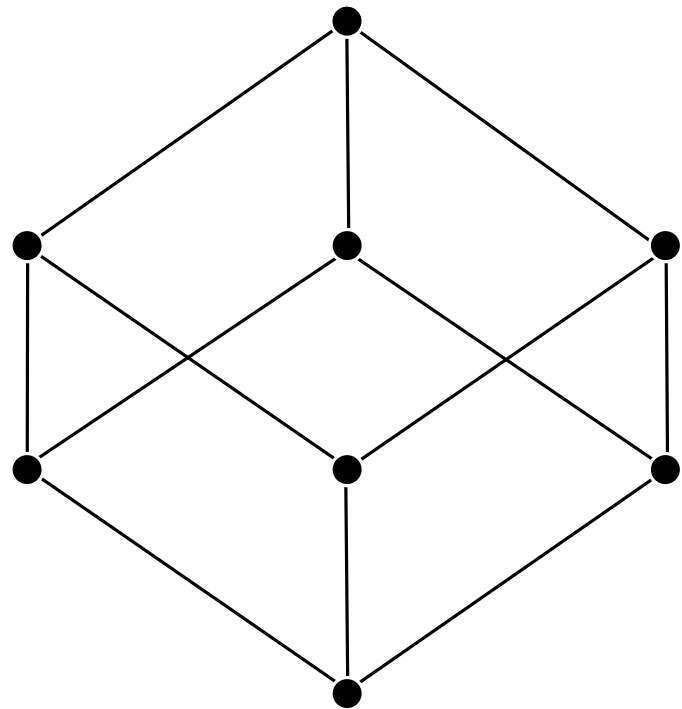
The Hasse diagram (if it exists) looks like a line.

Which of the following orders are linear?

- $\leq$ on $\mathbb{Q}$
- $\preceq_{\text{prefix}}$ on binary strings
- $\leq$ on $\mathbb{R}$
- $\subseteq$ on $\mathcal{P}(A)$



Definition. Let $\leq$ be an order on A and $a \in A$.
We say that a is **minimal** if there is no $b \in A \setminus \{a\}$ such that $b \leq a$.



Many problems in IT/science can be rephrased as finding a minimal element in a given order.
Being able to formalize the order you care about allows you to use known algorithms/methods.

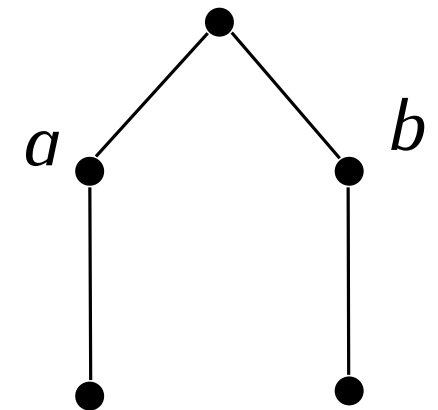
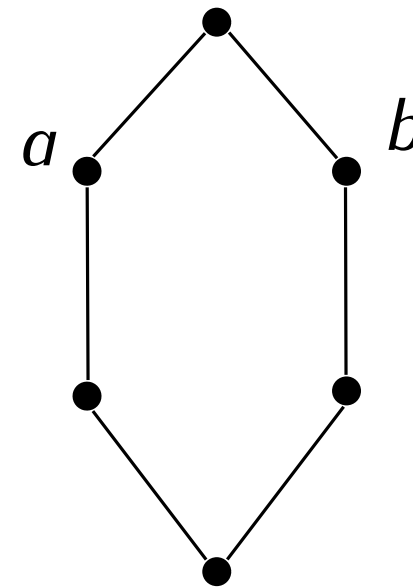
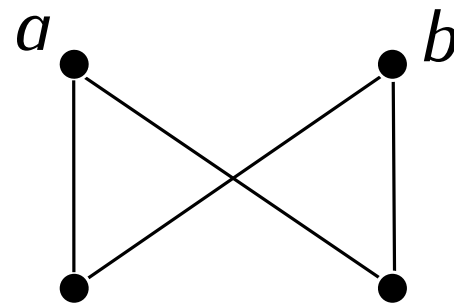
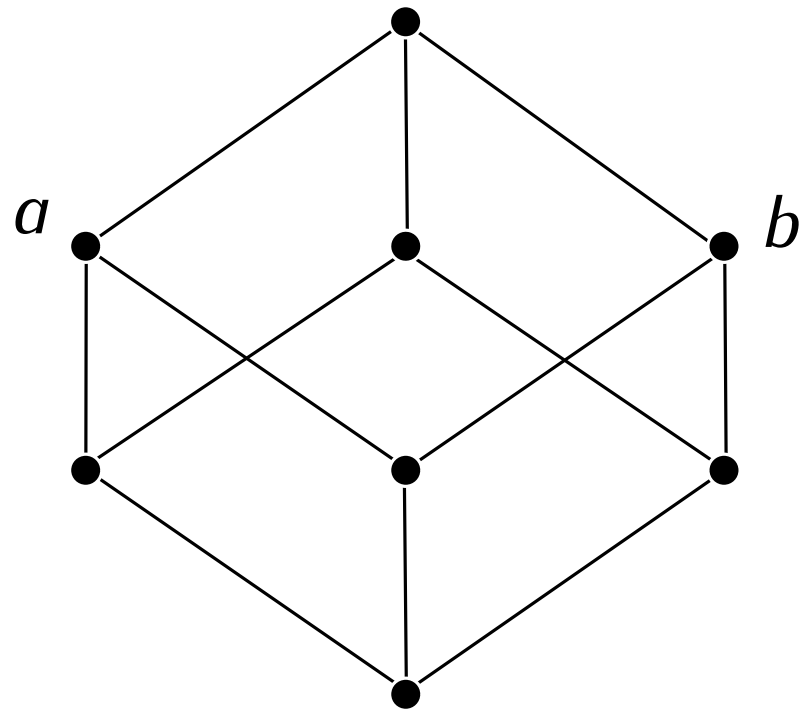
Theorem. Every non-empty finite order has a minimal element.

Proof by contradiction!

Definition. Let $\leq$ be an order on A , $S \subseteq A$, and $a \in A$. We say:

- a is a **lower bound** of S if for all $s \in S$, we have $a \leq s$
- a is a **greatest lower bound** of S if it is a lower bound and for every lower bound b of S , we have $b \leq a$.

We write $a \wedge b$ for the greatest lower bound of $\{a, b\}$, if it exists.

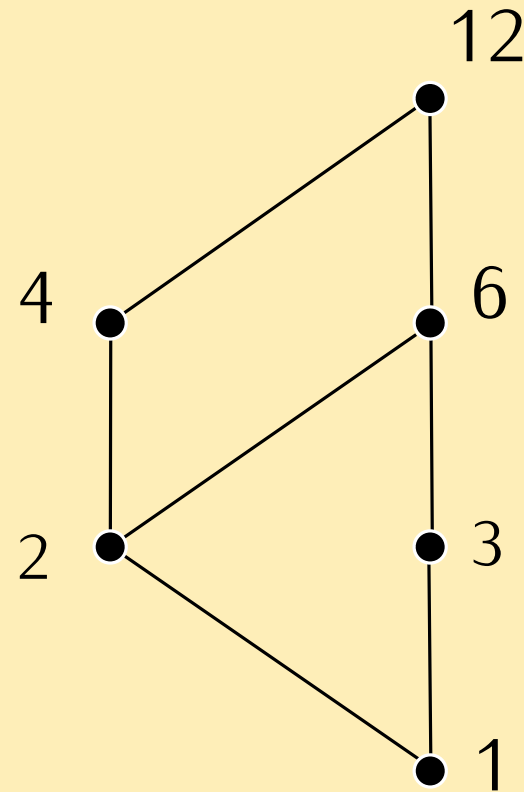


Definition. Let $\leq$ be an order on A , $S \subseteq A$, and $a \in A$. We say:

- a is a **lower bound** of S if for all $s \in S$, we have $a \leq s$
- a is a **greatest lower bound** of S if it is a lower bound and for every lower bound b of S , we have $b \leq a$.

We write $a \wedge b$ for the greatest lower bound of $\{a, b\}$, if it exists.

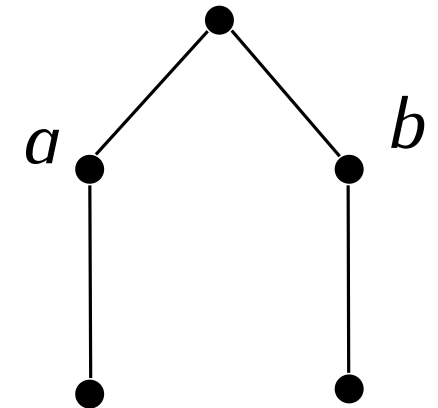
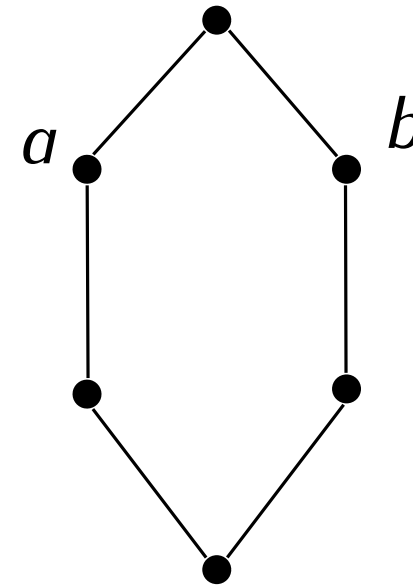
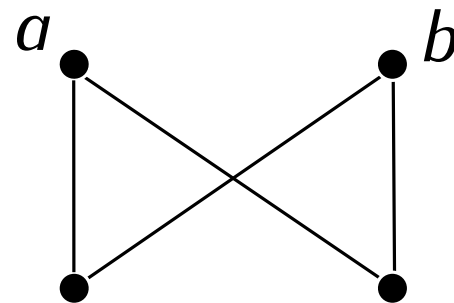
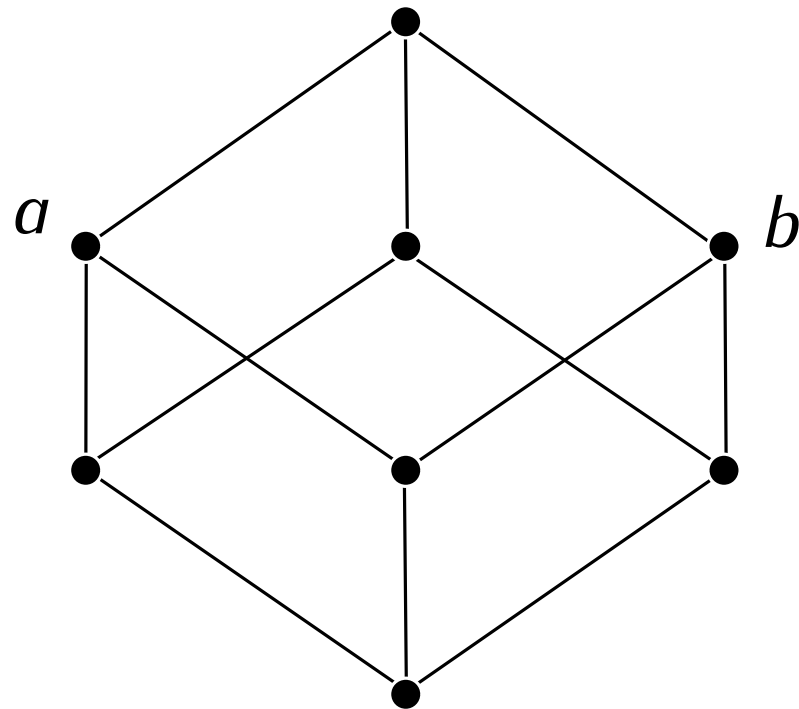
Let $A = \{n \in \mathbb{N} \mid n \text{ divides } 12\}$, and let $R = \{(n, m) \in A^2 \mid n \text{ divides } m\}$.
What is $4 \wedge 3$?



Definition. Let $\leq$ be an order on A , $S \subseteq A$, and $a \in A$. We say:

- a is an **upper bound** of S if for all $s \in S$, we have $s \leq a$
- a is a **lowest upper bound** of S if it is an upper bound and for every upper bound b of S , we have $a \leq b$.

We write $a \vee b$ for the lowest upper bound of $\{a, b\}$, if it exists.

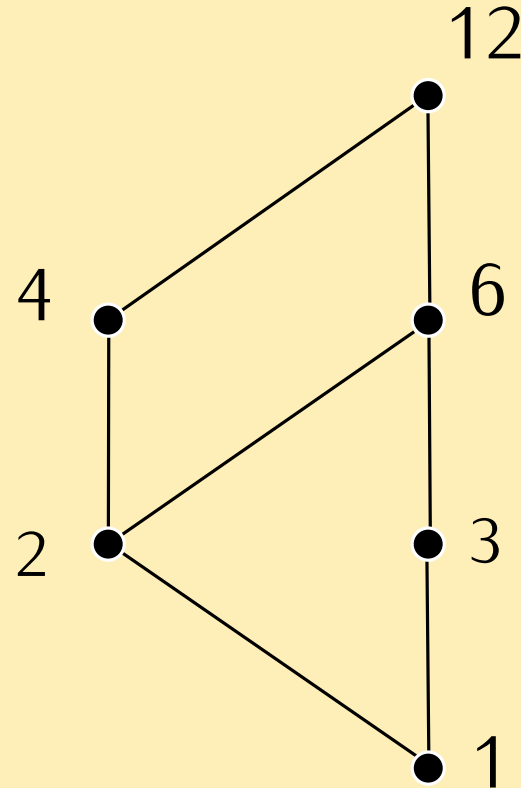


Definition. Let $\leq$ be an order on A , $S \subseteq A$, and $a \in A$. We say:

- a is an **upper bound** of S if for all $s \in S$, we have $s \leq a$
- a is a **lowest upper bound** of S if it is an upper bound and for every upper bound b of S , we have $a \leq b$.

We write $a \vee b$ for the lowest upper bound of $\{a, b\}$, if it exists.

Let $A = \{n \in \mathbb{N} \mid n \text{ divides } 12\}$, and let $R = \{(n, m) \in A^2 \mid n \text{ divides } m\}$.
What is $2 \vee 3$?



- How to recognize an equivalence relation, an order
- Compute equivalence classes
- Compute $A/\sim$
- Draw a Hasse diagram
- Recognize minimal/maximal elements
- Recognize lower/upper bounds

	Reflexive	Antireflexive	Symmetric	Antisymmetric	Transitive
Equivalence relation	✓		✓		✓
Order	✓			✓	✓
Strict order		✓		✓	✓
Quasi-order	✓				✓