Modeling & Verification

Tarski's Fixed Point Theorem

Max Tschaikowski (tschaikowski@cs.aau.dk)
Slides Courtesy of Giorgio Bacci

in the last Lecture

- Model Checking (idea & motivations)
- Hennessy-Milner Logic (syntax & semantics)
- Correspondence with Strong Bisimilarity
- example in CAAL

in this Lecture

- Limit of expressibility of Hennessy-Milner logic
- Tarski's Fixed Point Theorem (+ a bit of lattice theory)
- Computing fixed points on finite lattices

Verifying Correctness

Equivalence Checking

Impl $\equiv$ **Spec**

e.g., strong or weak bisimilarity

Model Checking

Impl $\models$ **Property**

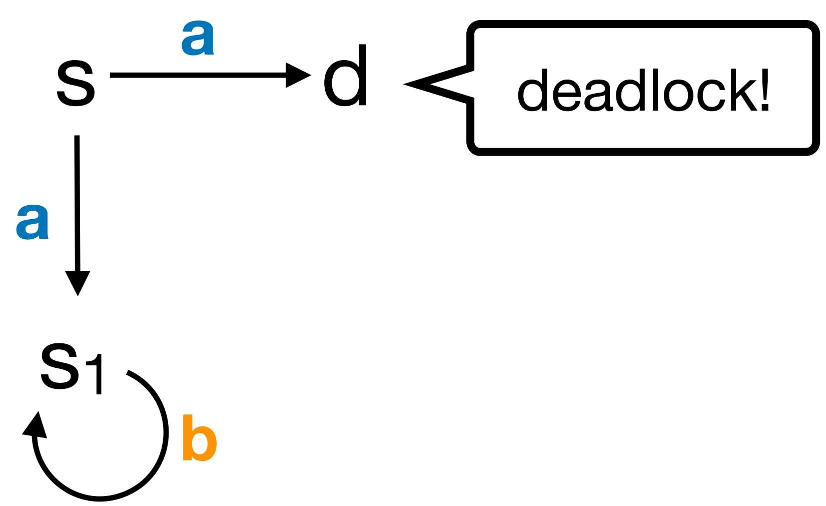
Hennessy-Milner logic

Theorem (Hennessy-Milner)

Let (Proc, Act, $\{\xrightarrow{\alpha} \mid \alpha \in \mathrm{Act}\}$) be an *image-finite LTS*, p,q$\in$Proc two states. Then

$$p \sim q \quad \text{iff} \quad \text{for all } \phi \in \mathcal{M}.\ (\, p \models \phi \Leftrightarrow q \models \phi \,)$$

Can we detect deadlocks?



$d \models [a]\mathrm{ff}$

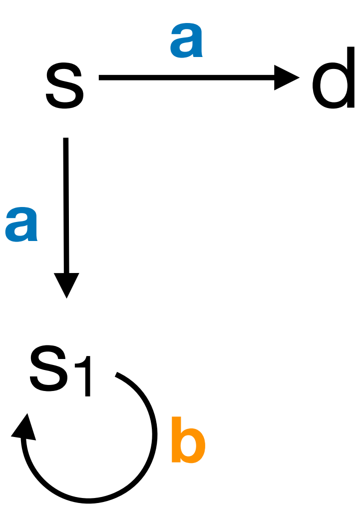
"cannot perform an a-move"

is this enough to say that d is a deadlock state?

$s_1 \models [a]\mathrm{ff}$ but $s_1 \not\models [a]\mathrm{ff} \wedge [b]\mathrm{ff}$

Can we detect deadlocks?

Act = {a, b}



deadlock!

All states reachable with an A-move satisfy ϕ

Let $A=\{a_1,\ldots, a_n\}\subseteq Act$, then $[A]\phi = [a_1]\phi \wedge \ldots \wedge [a_n]\phi$

and $\langle A\rangle\phi = \langle a_1\rangle\phi \vee \ldots \vee \langle a_n\rangle\phi$

there is a state reachable with an A-move satisfying ϕ

$d \models [Act]ff$

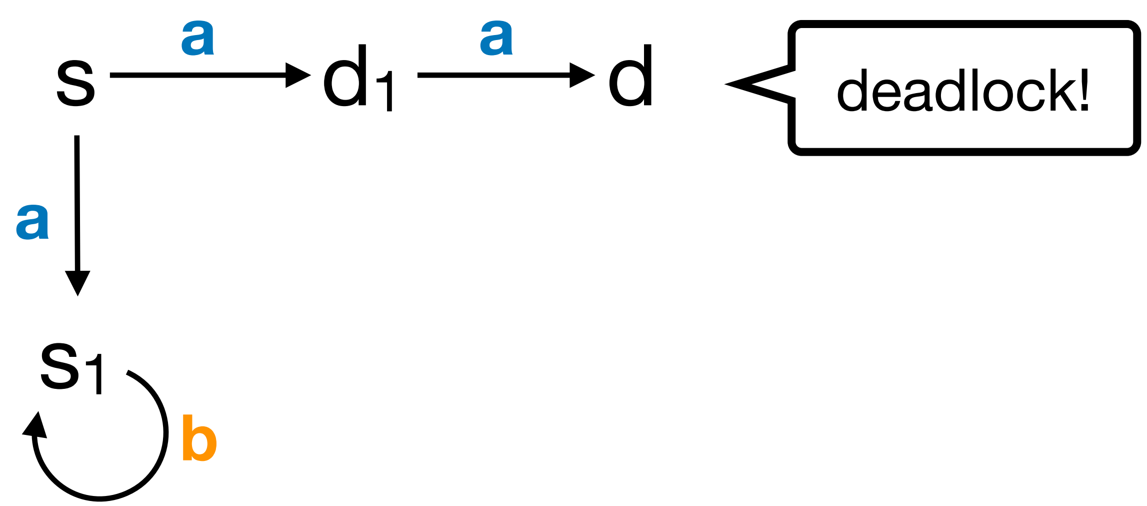
"cannot perform any move"

$s \models \langle Act\rangle[Act]ff$

"in one move it reaches a deadlock state"

Can we detect deadlocks?

$Act = \{a, b\}$



Let $A=\{a_1,\ldots, a_n\}\subseteq Act$, then $[A]\phi = [a_1]\phi \wedge \ldots \wedge [a_n]\phi$

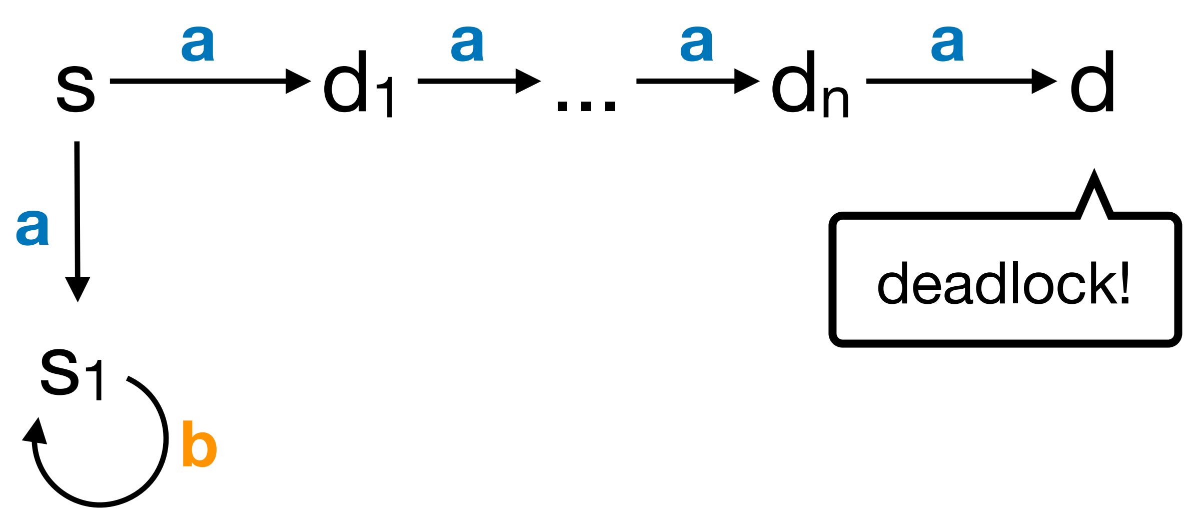
and $\langle A\rangle\phi = \langle a_1\rangle\phi \vee \ldots \vee \langle a_1\rangle\phi$

$s \not\models \langle Act\rangle[Act]ff$ "in *one* move it reaches a deadlock state"

$s \models \langle Act\rangle\langle Act\rangle[Act]ff$ "in *two* moves it reaches a deadlock state"

Can we detect deadlocks?

Act = {a, b}



Let $A=\{a_1,\ldots, a_n\}\subseteq Act$, then $[A]\phi = [a_1]\phi \wedge \ldots \wedge [a_n]\phi$

and $\langle A\rangle\phi = \langle a_1\rangle\phi \vee \ldots \vee \langle a_1\rangle\phi$

$D_0 = [Act]ff$ and $D_{n+1} = \langle Act\rangle D_n$

$D = \bigvee_{n\geq 0} D_n$

"it reaches a deadlock state"

not a formula!
(infinite disjunction)

Typical Temporal Properties *not* Expressible in HML

Let $A=\{a_1,\ldots, a_n\}\subseteq Act$, then $[A]\phi = [a_1]\phi \wedge \ldots \wedge [a_n]\phi$

and $\langle A\rangle\phi = \langle a_1\rangle\phi \vee \ldots \vee \langle a_1\rangle\phi$

Possibility

$$Pos_0(\phi) = \phi$$
$$Pos_{n+1}(\phi) = \langle Act\rangle Pos_n(\phi)$$

$$Pos(\phi) = \bigvee_{n\geq 0} Pos_n(\phi)$$

Invariance

$$Inv_0(\phi) = \phi$$
$$Inv_{n+1}(\phi) = [Act]Inv_n(\phi)$$

$$Inv(\phi) = \bigwedge_{n\geq 0} Inv_n(\phi)$$

Infinite disjunction and conjunctions are not expressible!

Solutions of Equations

Given two formulas $\phi,\psi\in\mathcal{M}$, we write $\phi \equiv \psi$ whenever $⟪\phi⟫=⟪\psi⟫$.

Pos and Inv satisfy the following equations:

$$\mathrm{Pos}(\phi) \equiv \phi \vee \langle \mathrm{Act} \rangle \mathrm{Pos}(\phi) \qquad \mathrm{Inv}(\phi) \equiv \phi \wedge [\mathrm{Act}]\mathrm{Inv}(\phi)$$

recursive equation!

recursive equation!

Possibility

$$\mathrm{Pos}_0(\phi) = \phi$$
$$\mathrm{Pos}_{n+1}(\phi) = \langle \mathrm{Act} \rangle \mathrm{Pos}_n(\phi)$$

$$\mathrm{Pos}(\phi) = \bigvee_{n\geq 0} \mathrm{Pos}_n(\phi)$$

Invariance

$$\mathrm{Inv}_0(\phi) = \phi$$
$$\mathrm{Inv}_{n+1}(\phi) = [\mathrm{Act}]\mathrm{Inv}_n(\phi)$$

$$\mathrm{Inv}(\phi) = \bigwedge_{n\geq 0} \mathrm{Inv}_n(\phi)$$

Recursion vs Infinite $\vee/\wedge$

Properties expressible by Pos and Inv are very useful in real life applications (e.g. *safety properties* or *liveness properties*)

"nothing bad can happen"

"something good will happen"

Two options:

- extend Hennessy-Milner Logic with *infinitary* $\vee$ *and* $\wedge$;
- extend Hennessy-Milner Logic with *recursion*.

Even if theoretically possible, infinite formulas are not easy to handle: *infinitely long, hard using them as input of an algorithm*

Solving Equations...

Equations over natural numbers $n \in \mathbb{N}$

$n = 2 \cdot n$ (unique solution $n = 0$)

$n = n+1$ (no solutions)

$n = 1 \cdot n$ (many solutions: every $n \in \mathbb{N}$)

Equations over sets of natural numbers $M \subseteq \mathbb{N}$

$M = (\{7\} \cap M) \cup \{7\}$ (unique solution $M = \{7\}$)

$M = \mathbb{N} \setminus M$ (no solutions)

$M = M \cup N$ (many solutions: every $M \supseteq N$)

What about equations over formulas (i.e. subsets of states)?

Fixed Points

The general approach to look at solutions of equations is as fixed point of some function on a domain D

Definition (Fixed Point)

For a set D and a function $f : D \longrightarrow D$, a *fixed point* for f is an element $d \in D$ such that

$$d = f(d) .$$

It does not need to exist, and if it exists may not be unique

Example:

- $D = \mathbb{N}$, $f(n) = 2 \cdot n$, then $0 = f(0)$ is *the* fixed point of f
- $D = 2^{\mathbb{N}}$, $f(M) = M \cup N$, then $N = f(N)$ is *a* fixed point of f

break?

Lattice Theory

as a basis to solve
fixed point equations

Partial Order

Definition (Partially Ordered Set)

A *partially ordered set* (or simply *partial order*) is a pair $(D, \sqsubseteq)$ such that

- D is a set, and
- $\sqsubseteq \; \subseteq D \times D$ is a binary relation on D such that
  - **(reflexive)** $\forall d \in D.\ d \sqsubseteq d$;
  - **(antisymmetric)** $\forall d, e \in D.$ if $d \sqsubseteq e$ and $e \sqsubseteq d$, then $d = e$;
  - **(transitive)** $\forall d, e, f \in D.$ if $d \sqsubseteq e$ and $e \sqsubseteq f$, then $d \sqsubseteq f$.

Example: $(\mathbb{N}, \leq)$ and $(2^{\mathbb{N}}, \subseteq)$ are partial orders.

Infimum & Supremum

Definition (Lower/Upper Bound)

Let $(D,\sqsubseteq)$ be a partial order and $F \subseteq D$, then $d \in D$

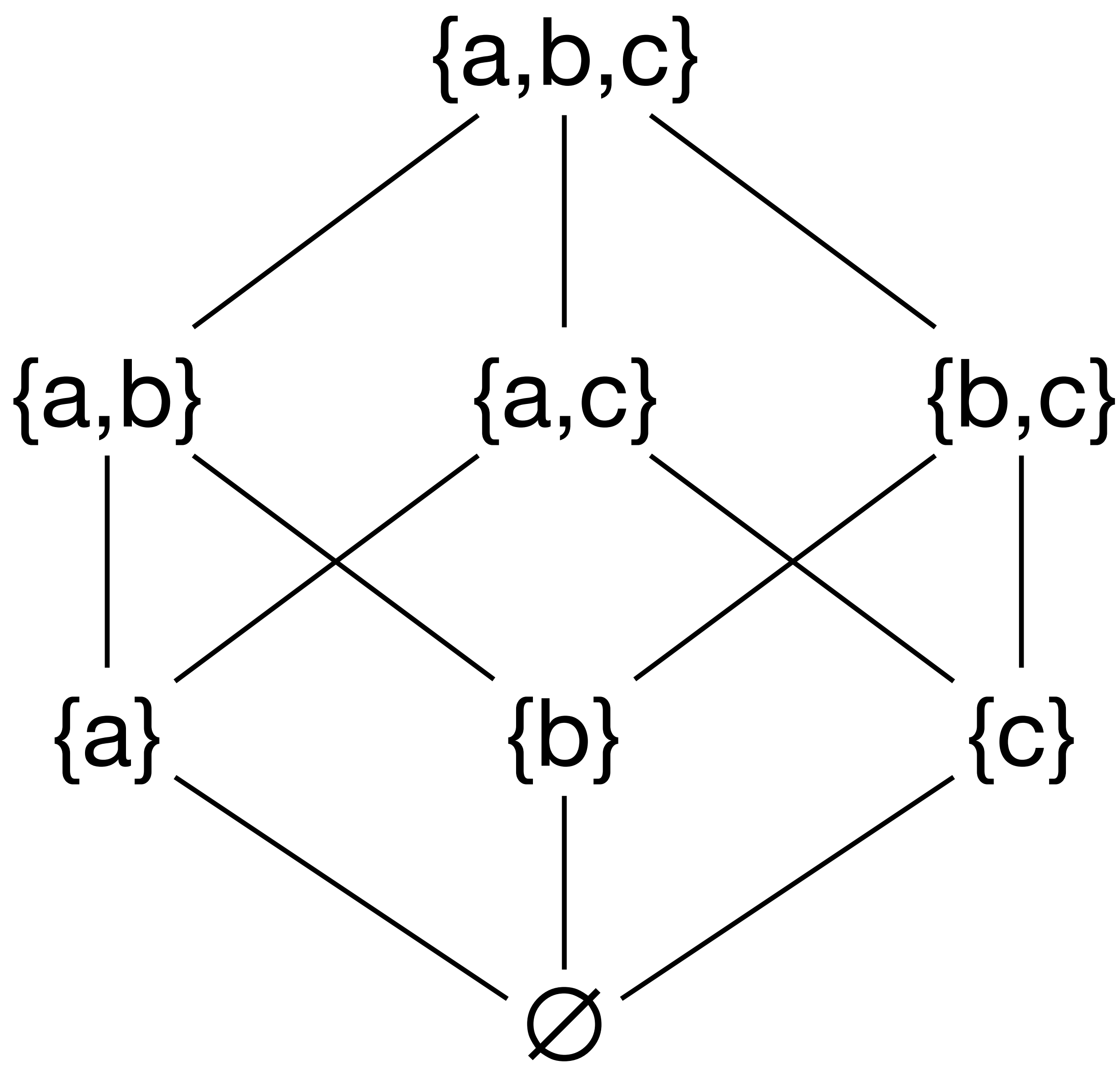
- is a *lower bound* for F, written $d \sqsubseteq F$, iff $\forall f \in F.\ d \sqsubseteq f$;
- is an *upper bound* for F, written $F \sqsubseteq d$, iff $\forall f \in F.\ f \sqsubseteq d$.

Definition (Infimum/Supremum)

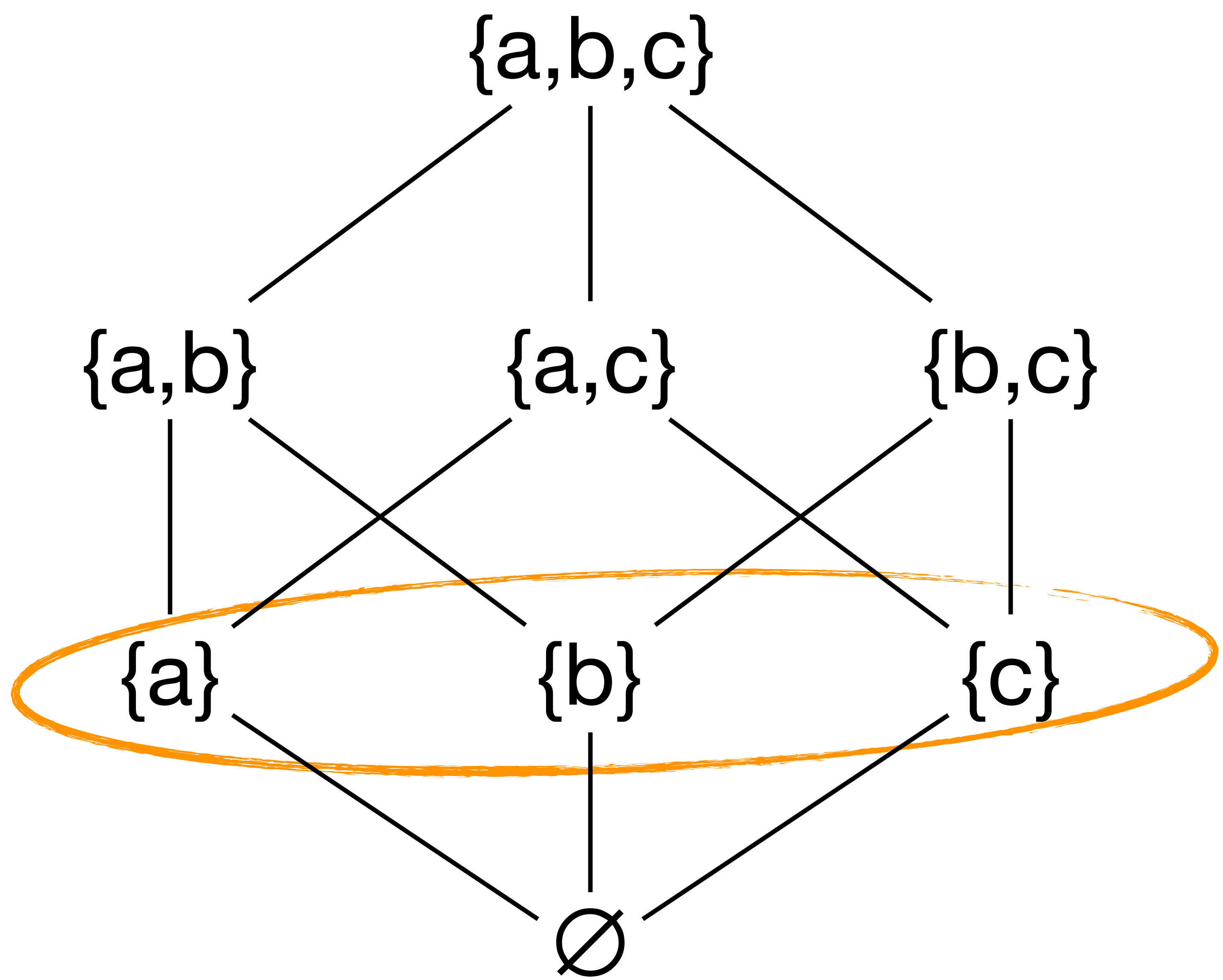
Let $(D,\sqsubseteq)$ be a partial order and $F \subseteq D$, then $d \in D$

- is the *greatest lower bound* (or *infimum*) for F, written $\sqcap F$, iff $d \sqsubseteq F$ and $\forall d' \in D.$ if $d' \sqsubseteq F$, then $d' \sqsubseteq d$;
- is the *least upper bound* (or *supremum*) for F, written $\sqcup F$, iff $F \sqsubseteq d$ and $\forall d' \in D.$ if $F \sqsubseteq d'$, then $d \sqsubseteq d'$;

Let consider the partial order of subsets of {a,b,c} wrt ⊆

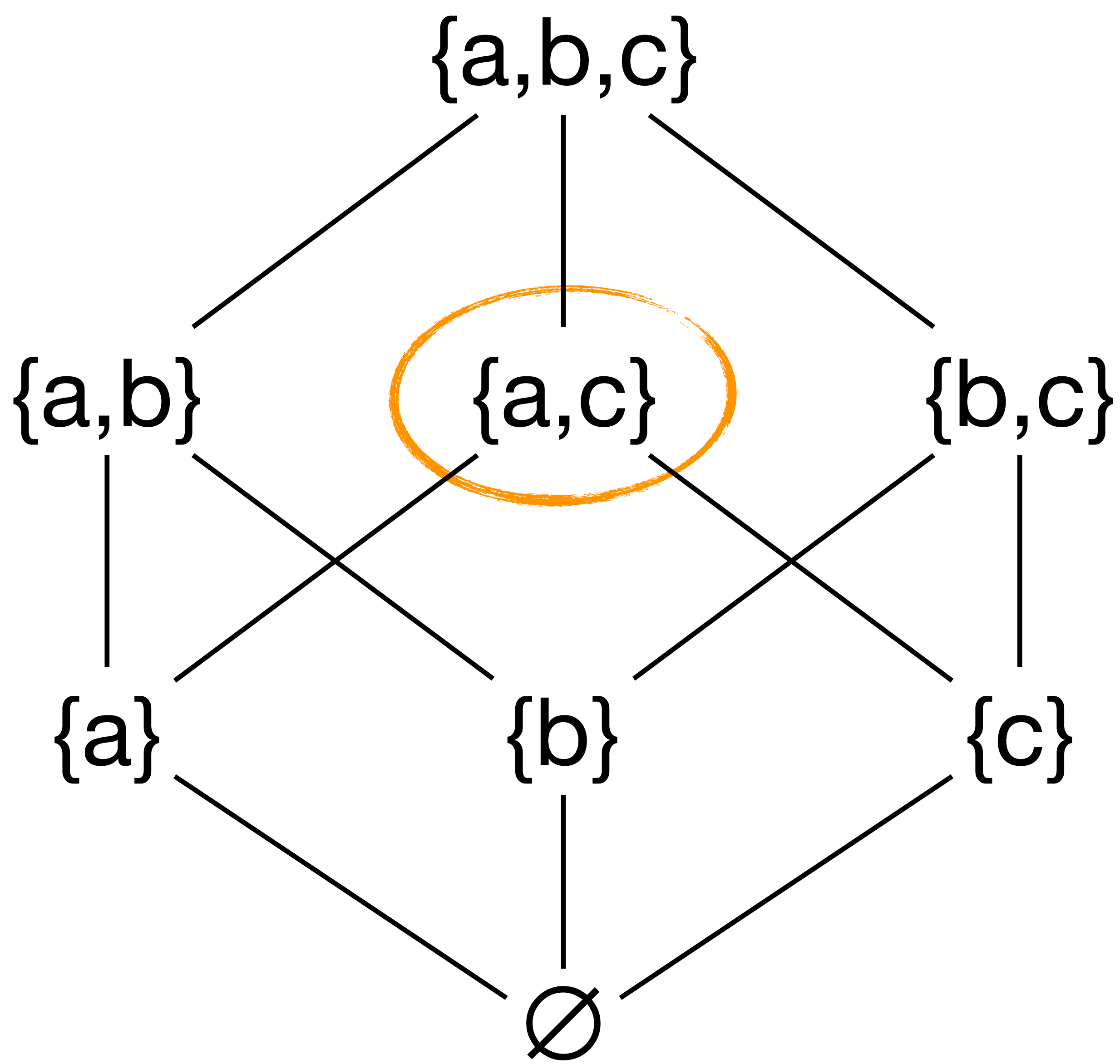


Let consider the partial order of subsets of {a,b,c} wrt ⊆



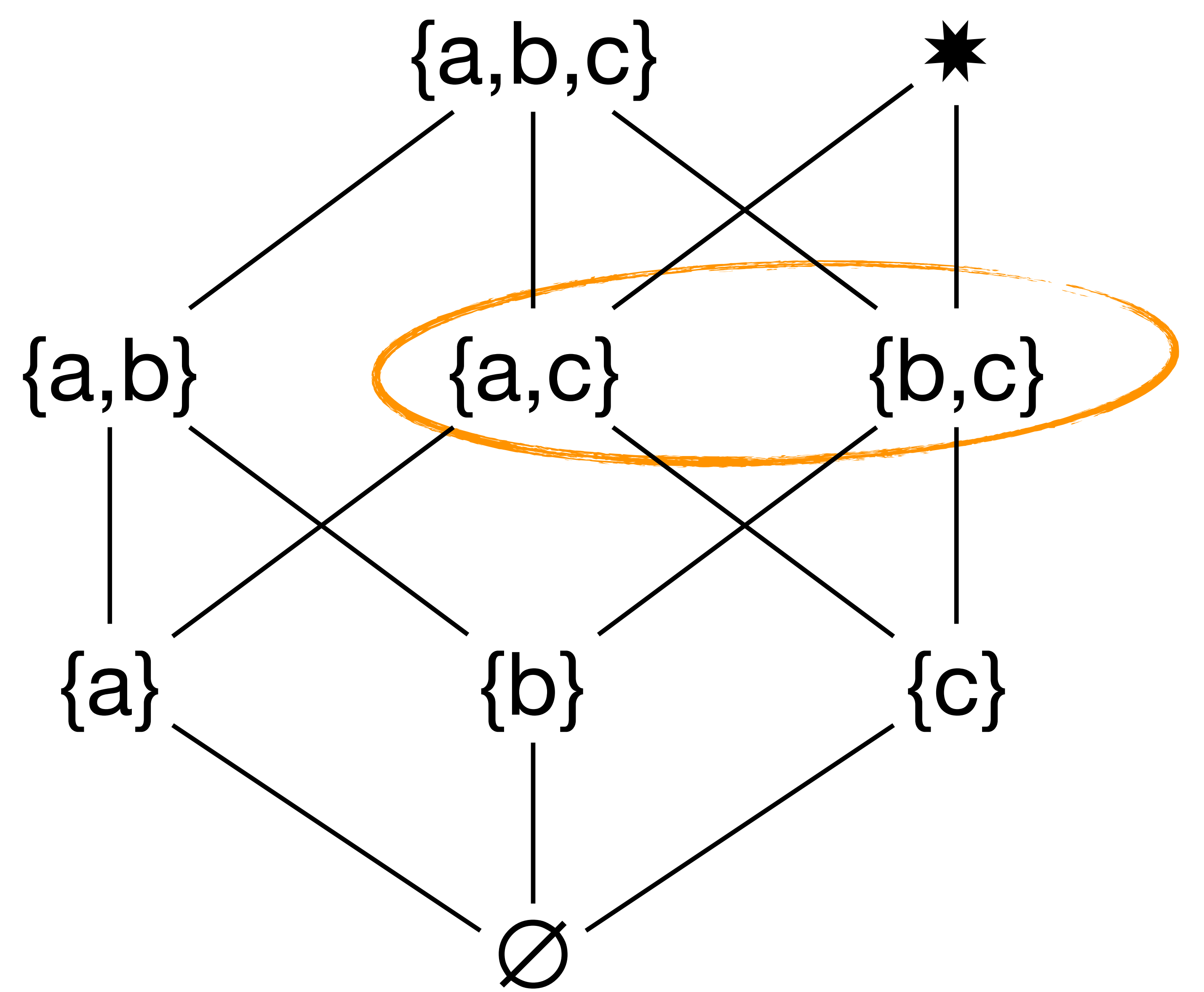
What are the infimum and supremum of F = {{a},{b},{c}}?

Let consider the partial order of subsets of {a,b,c} wrt ⊆



What are the infimum and supremum of F = {{a,c}}?

Let's extend the partial order with the element ✷ ordered as follows



What are the infimum and supremum of F = {{a,c},{b,c}}?

Tarski's
Fixed Point Theorem

Alfred Tarski (1901-1983)

Complete Lattice

Definition (Complete Lattice)

A partial order $(D, \sqsubseteq)$ is a *complete lattice* if for all $F \subseteq D$, $\sqcap F$ (infimum) and $\sqcup F$ (supremum) exist.

By definition a complete lattice $(D, \sqsubseteq)$ has always

a *top element* $\top \stackrel{\text{def}}{=} \sqcup D$

and

a *bottom element* $\bot \stackrel{\text{def}}{=} \sqcap D$

Example: $(2^{\mathbb{N}}, \subseteq)$ is a complete lattice, but $(\mathbb{N}, \leq)$ is not.

Monotonic Functions

Definition (Monotonic Function)

Let $(D, \sqsubseteq)$ be a partial order. A function $f : D \longrightarrow D$ is monotonic if $\forall d, e \in D$,

$$d \sqsubseteq e \quad \text{implies} \quad f(d) \sqsubseteq f(e) \; .$$

It preserves the order of elements

Example: the functions $f(n) = 2 \cdot n$ and $g(n) = 0$ in $\mathbb{N}$ are monotonic. while the function $F(M) = \mathbb{N} \setminus M$ on $2^{\mathbb{N}}$ is not!

Tarski's Fixed Point Theorem

The following theorem is the basis of many important results in computer sciences!

Theorem (Tarski)

Let $(D, \sqsubseteq)$ be a complete lattice and $f : D \longrightarrow D$ a monotonic function on D. Then

1. The set of fixed points of f is a complete lattice
2. The least and greatest fixed point of f exists and are given as follows

(least fixed point) $\quad lfp(f) = \sqcap \{ d \in D \mid f(d) \sqsubseteq \underbrace{d}_{\text{post-fixpoint}} \}$

(greatest fixed point) $\quad gfp(f) = \sqcup \{ d \in D \mid \underbrace{d}_{\text{pre-fixpoint}} \sqsubseteq f(d) \}$

Computing fixed points on *finite* Complete Lattices

Computing by iterations

Let $(D,\sqsubseteq)$ be a complete lattice and $f : D \longrightarrow D$, then for all $n \geq 0$ define the function $f^n : D \longrightarrow D$ as follows

$$f^0(d) = d \quad \text{and} \quad f^{n+1}(d) = f(\, f^n(d)\,)$$

$$\text{i.e.,} \qquad f^n(d) = \underbrace{f(f(\ \dots\ f}_{\text{n-times}}(d)\ \dots\ ))$$

Theorem

Let $(D,\sqsubseteq)$ be a finite complete lattice and $f : D \longrightarrow D$ a monotonic function on D. Then exist $M,m \geq 0$ such that

$$\mathrm{lfp}(f) = f^m(\bot) \quad \text{and} \quad \mathrm{gfp}(f) = f^M(\top)\ .$$

the sequence stabilises in a finite number of steps

Least Fixed Point:

$$\bot \sqsubseteq f^1(\bot) \sqsubseteq \ldots \sqsubseteq f^{m-1}(\bot) \sqsubseteq f^m(\bot) = f^{m+1}(\bot)$$

similarly...

Greatest Fixed Point:

$$f^{M+1}(\top) = f^M(\top) \sqsubseteq f^{M-1}(\top) \sqsubseteq \ldots \sqsubseteq f^1(\top) \sqsubseteq \top$$

Hence we have a terminating algorithm to compute fixed points, i.e. solutions of equations on a finite complete lattice!