Abstract Interpretation Framework

Woosuk Lee

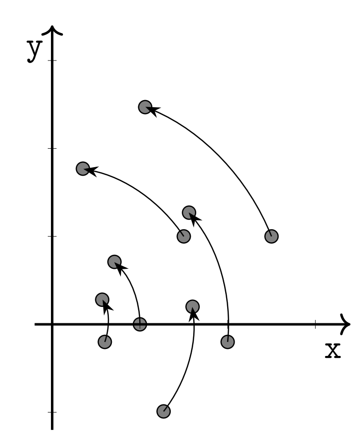
CSE 6049 Program Analysis

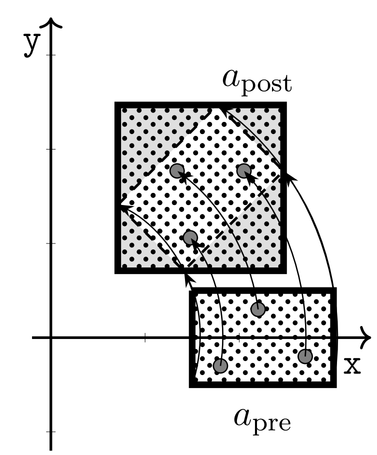
Hanyang University, Korea

Abstract Interpretation Framework

real execution	$[\![P]\!] = \text{fix } F \in D$
abstract execution	$[\![\hat{P}]\!] = \text{fix } \hat{F} \in \hat{D}$
correctness	$[\![P]\!] \approx [\![\hat{P}]\!]$
implementation	computation of $[\![\hat{P}]\!]$

- The framework requires:
  - a relation between D and $\hat{D}$
  - a relation between $F \in D \to D$ and $\hat{F} \in \hat{D} \to \hat{D}$
- The framework guarantees:
  - correctness and implementation
  - freedom: any such $\hat{D}$ and $\hat{F}$ are fine.





Abstract Interpretation Framework

real execution	$[\![P]\!] = \text{fix}\ F \in D$
abstract execution	$[\![\hat{P}]\!] = \text{fix}\ \hat{F} \in \hat{D}$
correctness	$[\![P]\!] \approx [\![\hat{P}]\!]$
implementation	computation of $[\![\hat{P}]\!]$

A domain of concrete states (e.g., a set of integers)

A domain of abstract states (e.g., a set of intervals)

- The framework requires:
  - a relation between D and $\hat{D}$
  - a relation between $F \in D \to D$ and $\hat{F} \in \hat{D} \to \hat{D}$
- The framework guarantees:
  - correctness and implementation
  - freedom: any such $\hat{D}$ and $\hat{F}$ are fine.

A function corresponding to one-step real execution

A function corresponding to one-step abstract execution

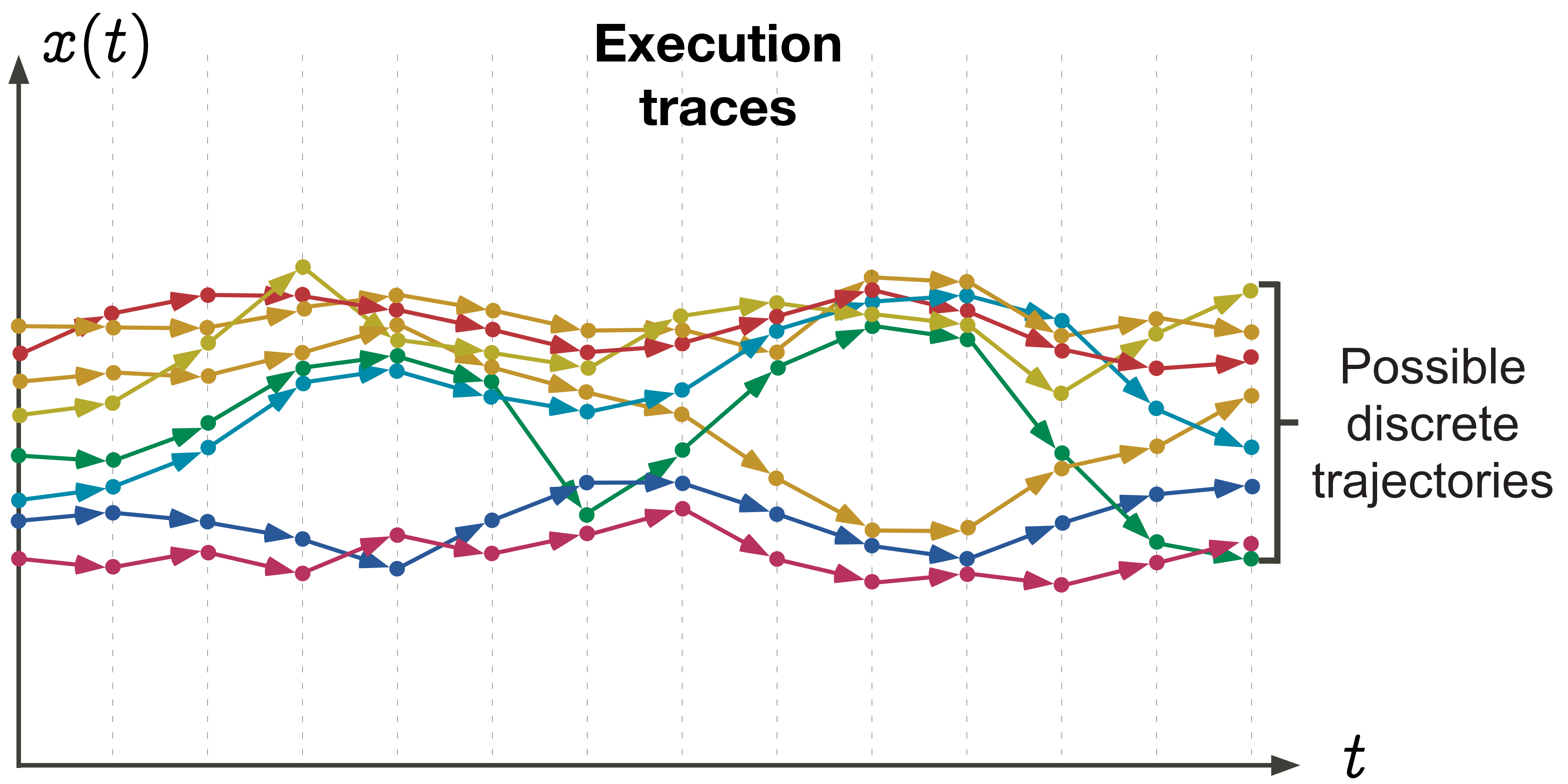
Steps

- Step 1: Define standard semantics
- Step 2: Define concrete semantics
- Step 3: Define abstract semantics

Step 1: Define Standard Semantics

- Formalization of **a single program execution**
- Operational semantics (transitional style)
  - Big-step / small-step
- Denotational semantics (compositional style)
- $State \rightarrow State$

Step 1: Define Standard Semantics



*from Patrick Cousot's slides

Semantics Style: Compositional vs. Transitional

- Compositional semantics is defined by the semantics of sub-parts of a program.

$$[\![AB]\!] = \cdots [\![A]\!] \cdots [\![B]\!] \cdots$$

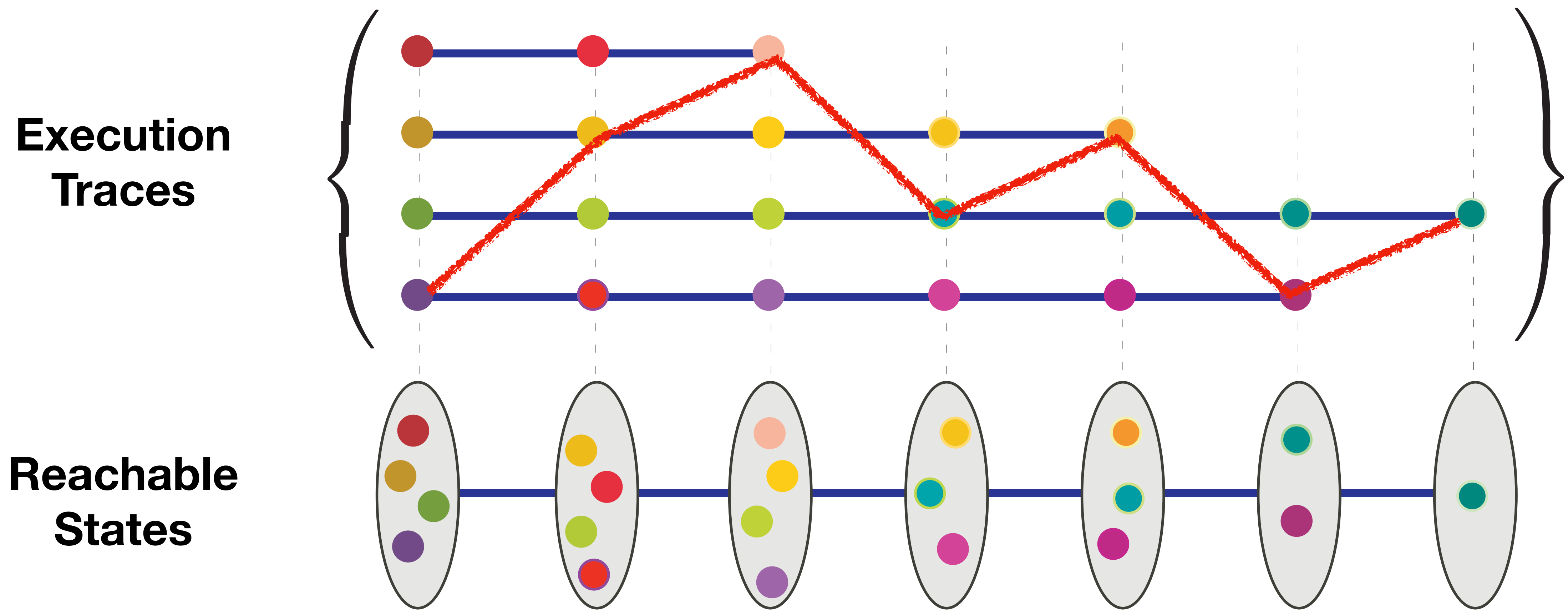
- For some realistic languages, even defining their compositional ("denotational") semantics is a hurdle.
  - goto, exceptions, function calls
- Transitional-style ("operational") semantics avoids the hurdle.

$$[\![AB]\!] = \{s_1 \to s_2 \to \cdots\}$$

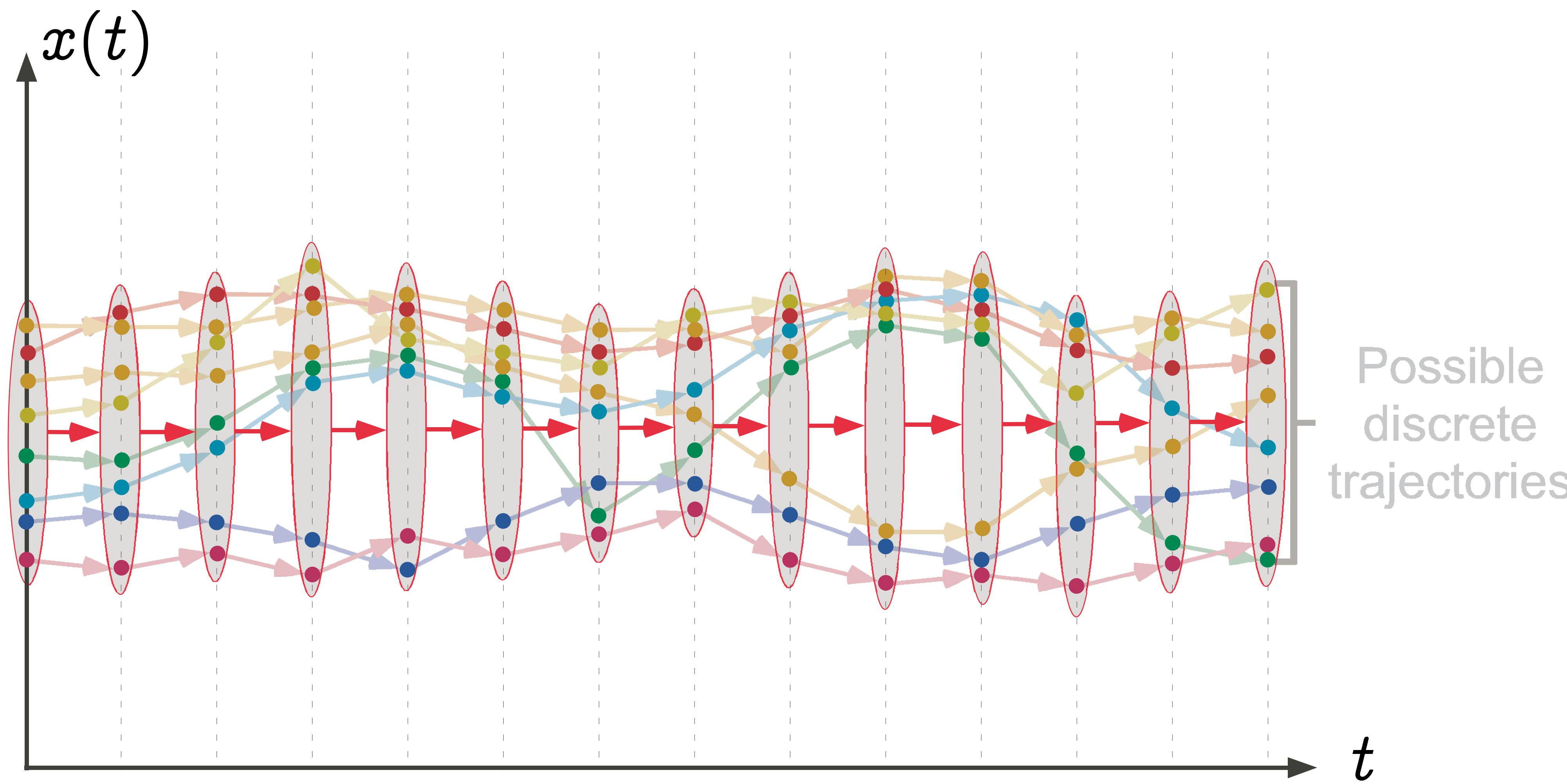
Step 2: Define Concrete Semantics

- Formalization of **all possible program executions**
- Also called collecting semantics
- Simple extension of the standard semantics in general
- $2^{State} \rightarrow 2^{State}$

Traces vs. Reachable States



Transitions of Sets of States



*from Patrick Cousot's slides

Step 2: Define Concrete Semantics

- Define a semantic domain D, which is a CPO
- Define a semantic function $F : D \to D$, which is ***continuous***.
- Then, the concrete semantics is the least fixed point of semantic function

$$\mathit{fix} F = \bigsqcup_{i \in N} F^i(\bot).$$

Plan: define an abstraction that captures $\mathit{fix} F$

Step 3: Define Abstract Semantics

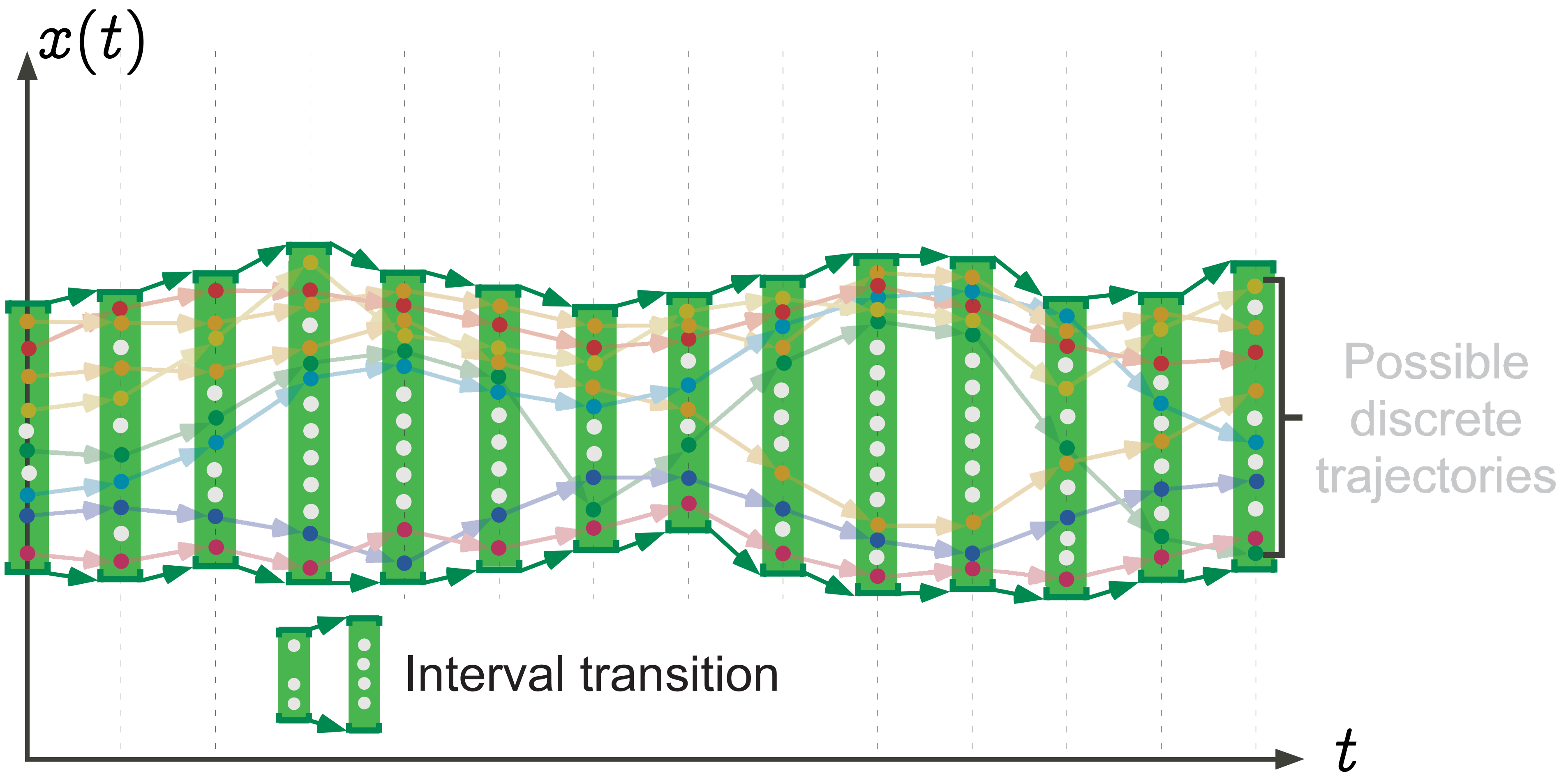
- Define an abstract domain CPO $\hat{D}$
  - Intuition: $\hat{D}$ is an abstraction of D
- Define an abstract semantic function $\hat{F} : \hat{D} \to \hat{D}$
  - Intuition: $\hat{F}$ is an abstraction of F
  - $\hat{F}$ must be monotone:

$$\forall \hat{x}, \hat{y} \in \hat{D}.\ \hat{x} \sqsubseteq \hat{y} \implies \hat{F}(\hat{x}) \sqsubseteq \hat{F}(\hat{y})$$

(or extensive: $\forall x \in \hat{D}.\ x \sqsubseteq \hat{F}(x)$)

Plan: define an abstraction that captures $\mathit{fix} F$ by using $\hat{F}$

Transitions of Abstract States



*from Patrick Cousot's slides

Sound Static Analysis

- Static analysis is to compute an upper bound of the chain:

$$\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot})$$

- How can we ensure the abstract semantics soundly subsume the concrete semantics?
  - Abstract interpretation framework guarantees if some requirements are met.

Requirement 1: about $\hat{D}$ in relation with D

$\boldsymbol{D}$ and $\hat{\boldsymbol{D}}$ must be related with Galois-connection:

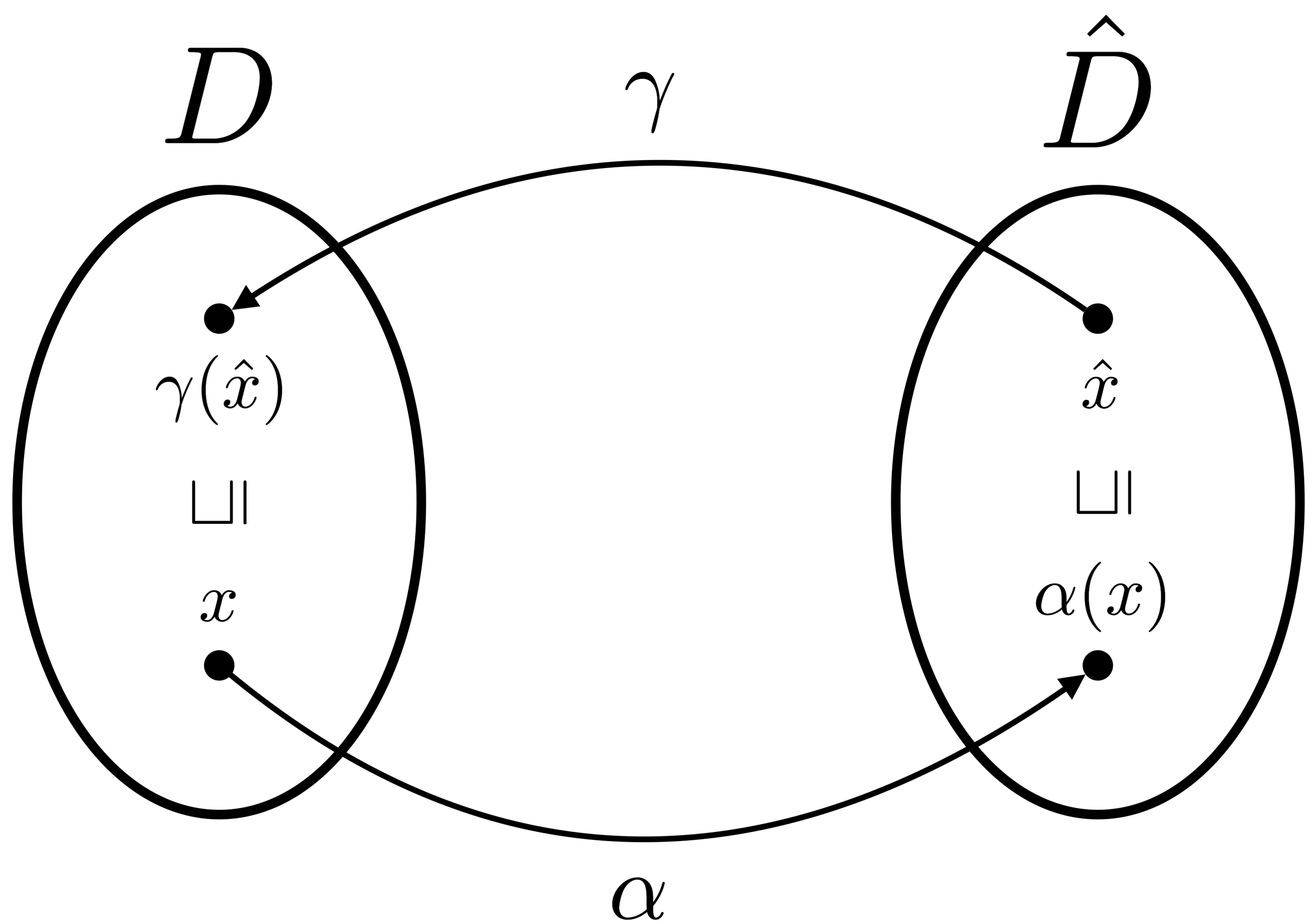
$$\boldsymbol{D} \underset{\boldsymbol{\alpha}}{\overset{\gamma}{\leftrightarrows}} \hat{\boldsymbol{D}}$$

That is, we have

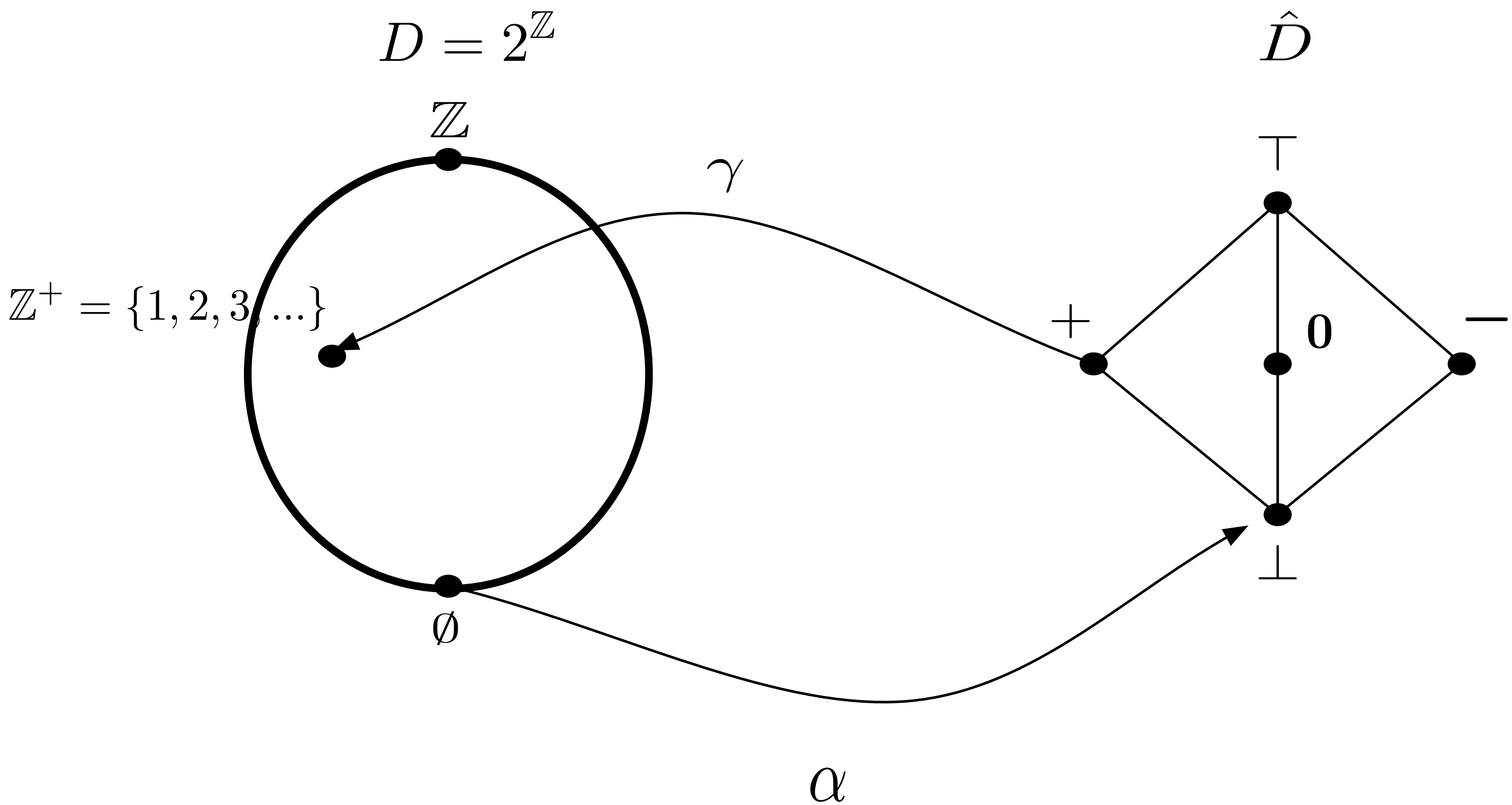
- *abstraction function*: $\boldsymbol{\alpha} \in \boldsymbol{D} \to \hat{\boldsymbol{D}}$
  - represents elements in $\boldsymbol{D}$ as elements of $\hat{\boldsymbol{D}}$
- *concretization function*: $\gamma \in \hat{\boldsymbol{D}} \to \boldsymbol{D}$
  - gives the meaning of elements of $\hat{\boldsymbol{D}}$ in terms of $\boldsymbol{D}$
- $\forall \boldsymbol{x} \in \boldsymbol{D}, \hat{\boldsymbol{x}} \in \hat{\boldsymbol{D}}.\ \boldsymbol{\alpha}(\boldsymbol{x}) \sqsubseteq \hat{\boldsymbol{x}} \iff \boldsymbol{x} \sqsubseteq \gamma(\hat{\boldsymbol{x}})$
  - $\boldsymbol{\alpha}$ and γ respect the orderings of $\boldsymbol{D}$ and $\hat{\boldsymbol{D}}$

Plan: static analysis is computing an upper bound of $\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot})$

Galois Connection



Example: Sign Abstraction



Example: Sign Abstraction

Sign abstraction:

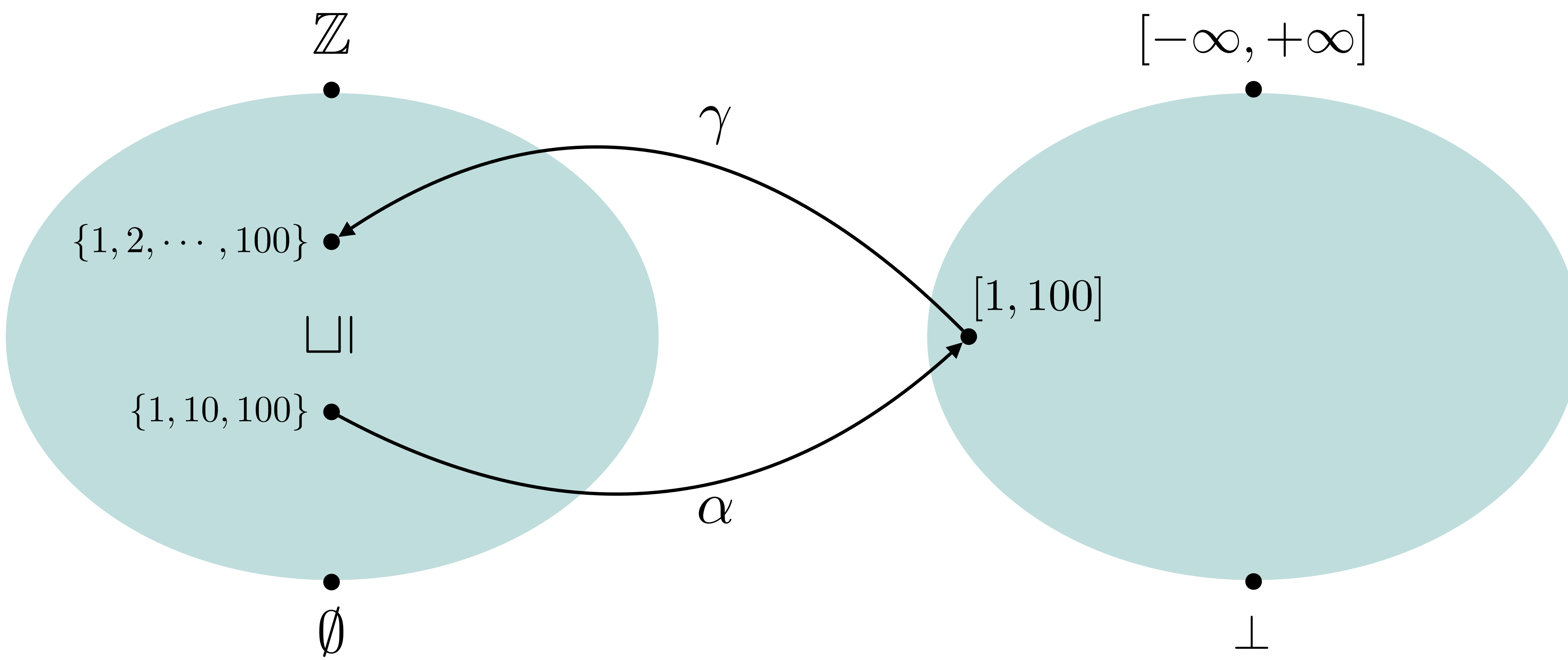
$$\wp(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot, +, 0, -\top\}$$

where

$$\begin{array}{rcl}
\alpha(Z) & = & \begin{cases} \bot & Z = \emptyset \\ + & \forall z \in Z.\ z > 0 \\ 0 & Z = \{0\} \\ - & \forall z \in Z.\ z < 0 \\ \top & \text{otherwise} \end{cases} \\
\gamma(\bot) & = & \emptyset \\
\gamma(\top) & = & \mathbb{Z} \\
\gamma(+) & = & \{z \in \mathbb{Z} \mid z > 0\} \\
\gamma(0) & = & \{0\} \\
\gamma(-) & = & \{z \in \mathbb{Z} \mid z < 0\}
\end{array}$$

Example: Interval Abstraction

$$\wp(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot\} \cup \{[a,b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\}$$



Example: Interval Abstraction

$$\wp(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot\} \cup \{[a,b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\}$$

$$\begin{array}{rcl} \gamma(\bot) & = & \emptyset \\ \gamma([a,b]) & = & \{z \in \mathbb{Z} \mid a \leq z \leq b\} \\ \gamma([a,+\infty]) & = & \{z \in \mathbb{Z} \mid z \geq a\} \\ \gamma([-\infty,b]) & = & \{z \in \mathbb{Z} \mid z \leq b\} \\ \gamma([-\infty,+\infty]) & = & \mathbb{Z} \end{array}$$

Requirement 2: about $\hat{F}$

- $\hat{F}$ must be monotonic:

$$\forall x, y \in \hat{D} : x \sqsubseteq y \Rightarrow \hat{F}(x) \sqsubseteq \hat{F}(y)$$

  or extensive:

$$\forall x \in \hat{D} : x \sqsubseteq \hat{F}(x).$$

Plan: static analysis is computing an upper bound of $\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot})$

Requirement 3: $\hat{F}$ in relation with F

- For any $x \in D, \hat{x} \in \hat{D}$, $\hat{\boldsymbol{F}}$ and $\boldsymbol{F}$ must satisfy

$$\boldsymbol{\alpha}(\boldsymbol{x}) \sqsubseteq \hat{\boldsymbol{x}} \implies \boldsymbol{\alpha}(\boldsymbol{F}(\boldsymbol{x})) \sqsubseteq \hat{\boldsymbol{F}}(\hat{\boldsymbol{x}})$$

  - Intuition: the result of one-step abstract execution subsumes that of one-step real execution.

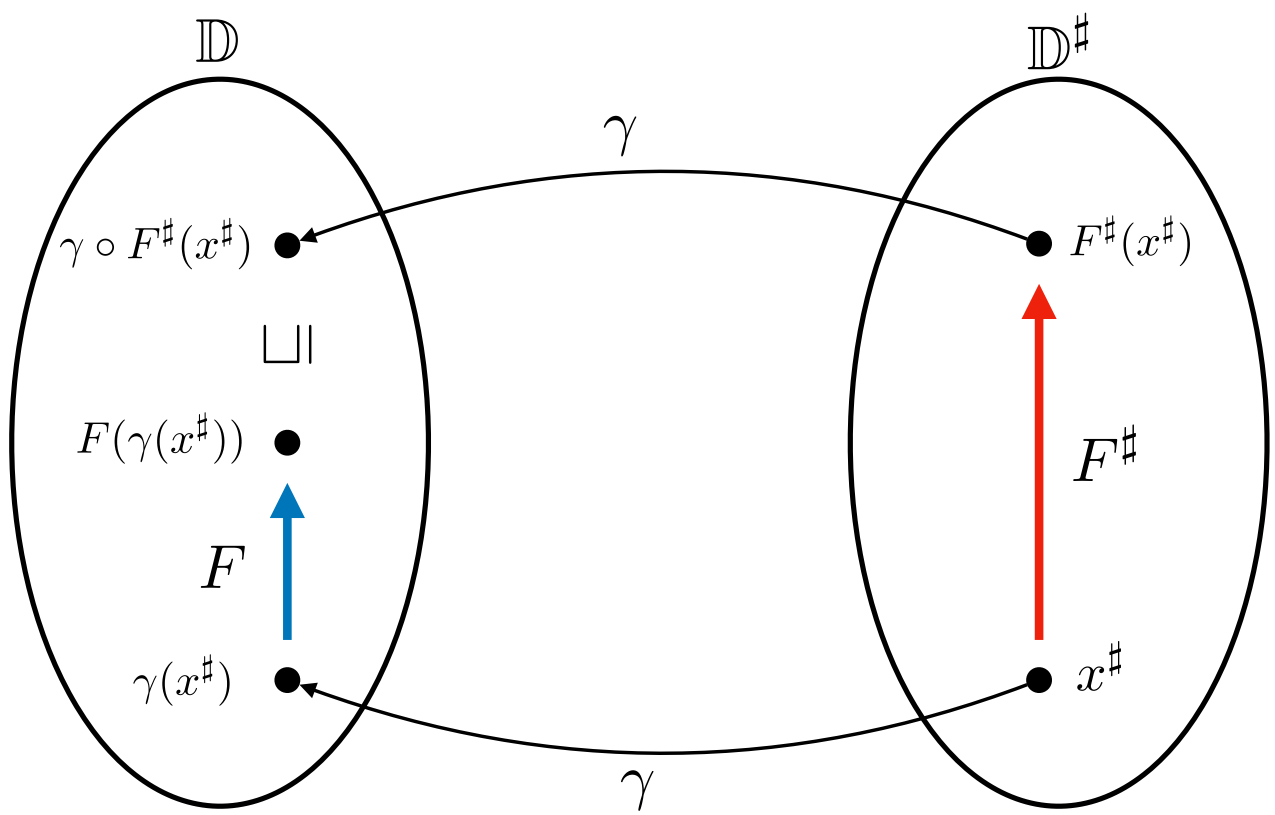
- or, alternatively,

$$\boldsymbol{\alpha} \circ \boldsymbol{F} \sqsubseteq \hat{\boldsymbol{F}} \circ \boldsymbol{\alpha} \quad \text{(i.e., } \boldsymbol{F} \circ \boldsymbol{\gamma} \sqsubseteq \boldsymbol{\gamma} \circ \hat{\boldsymbol{F}}\text{)}$$

Plan: static analysis is computing an upper bound of $\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot})$

Requirement 3: $\hat{F}$ in relation with F

$$F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$$



Intuition: the result of one-step abstract execution ($F^\sharp$) subsumes that of one-step concrete execution (F)

Then: a Correct Static Analysis

static analysis = computing an upper bound of $\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot})$.

- Such an upper bound $\hat{\mathcal{A}}$ is correct:

$$\alpha(\mathit{fix} F) \sqsubseteq \hat{\mathcal{A}}, \quad \text{that is,}$$
$$\mathit{fix} F \sqsubseteq \gamma \hat{\mathcal{A}}$$

  Theorem[fixpoint-transfer]

- Analysis result $\hat{\mathcal{A}}$ subsumes the real executions $\mathit{fix} F$

How to Compute an Upper Bound of $\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot})$

- If abstract domain $\hat{D}$ is finite (i.e., all chains are finite), we can directly compute

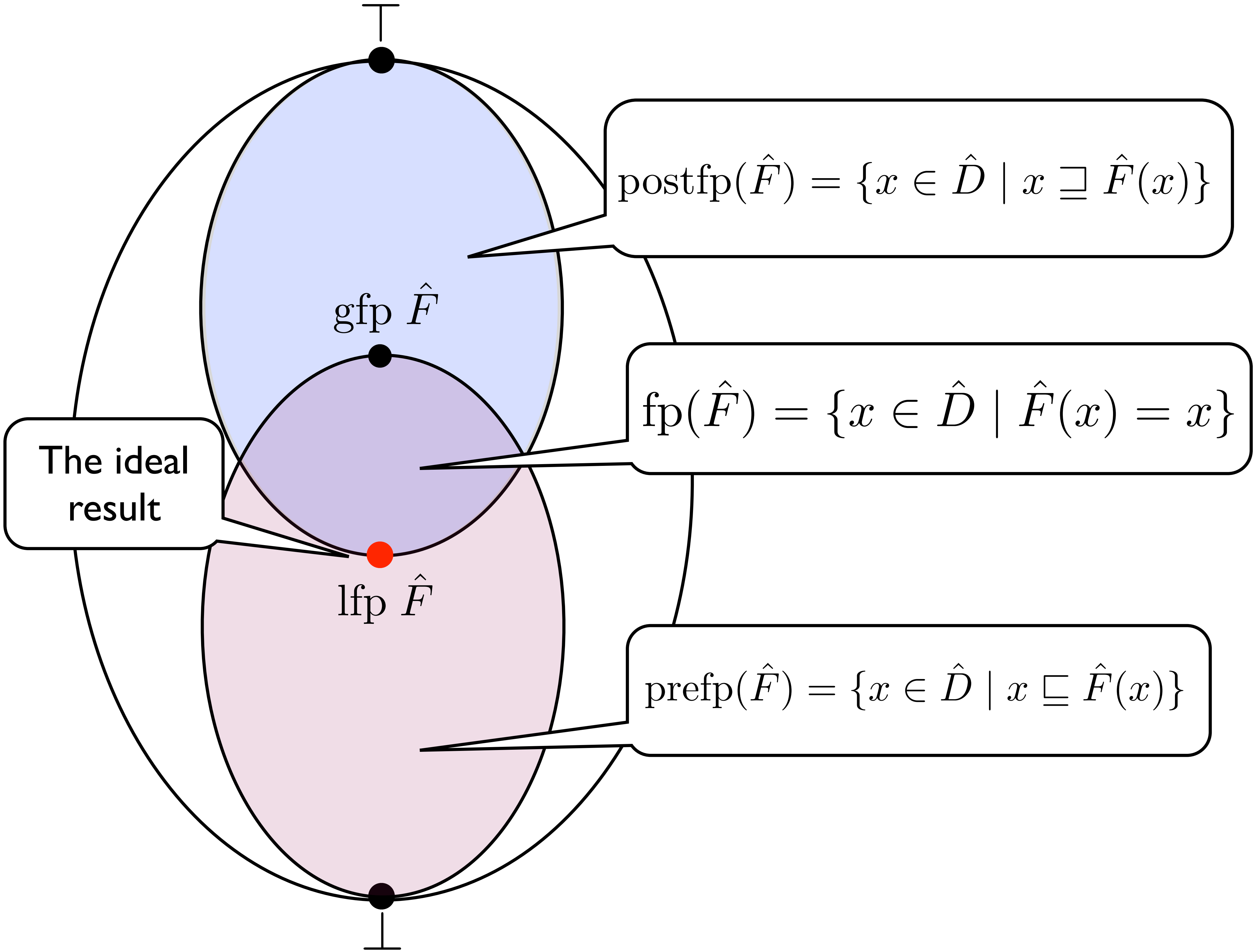
$$\bigsqcup_{i \in \mathbb{N}} \hat{\boldsymbol{F}}^{\boldsymbol{i}}(\hat{\bot}).$$

  The computation always terminate.

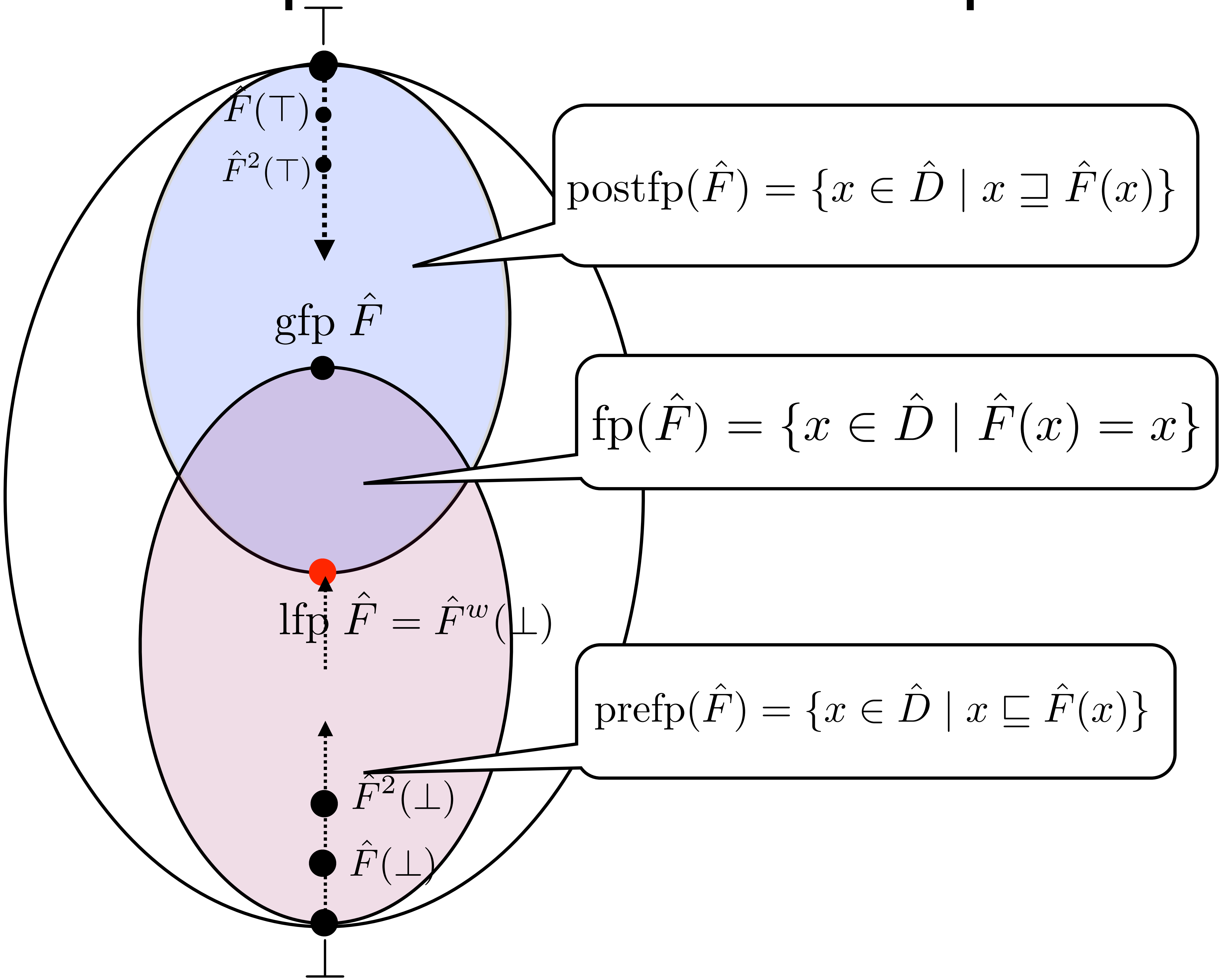
- Otherwise, we compute a finite chain $\hat{\boldsymbol{X}}_{\boldsymbol{0}} \sqsubseteq \hat{\boldsymbol{X}}_{\boldsymbol{1}} \sqsubseteq \hat{\boldsymbol{X}}_{\boldsymbol{2}} \sqsubseteq \ldots$ such that

$$\bigsqcup_{i \in \mathbb{N}} \hat{\boldsymbol{F}}^{\boldsymbol{i}}(\hat{\bot}) \sqsubseteq \lim_{i \in \mathbb{N}} \hat{\boldsymbol{X}}_{\boldsymbol{i}}$$

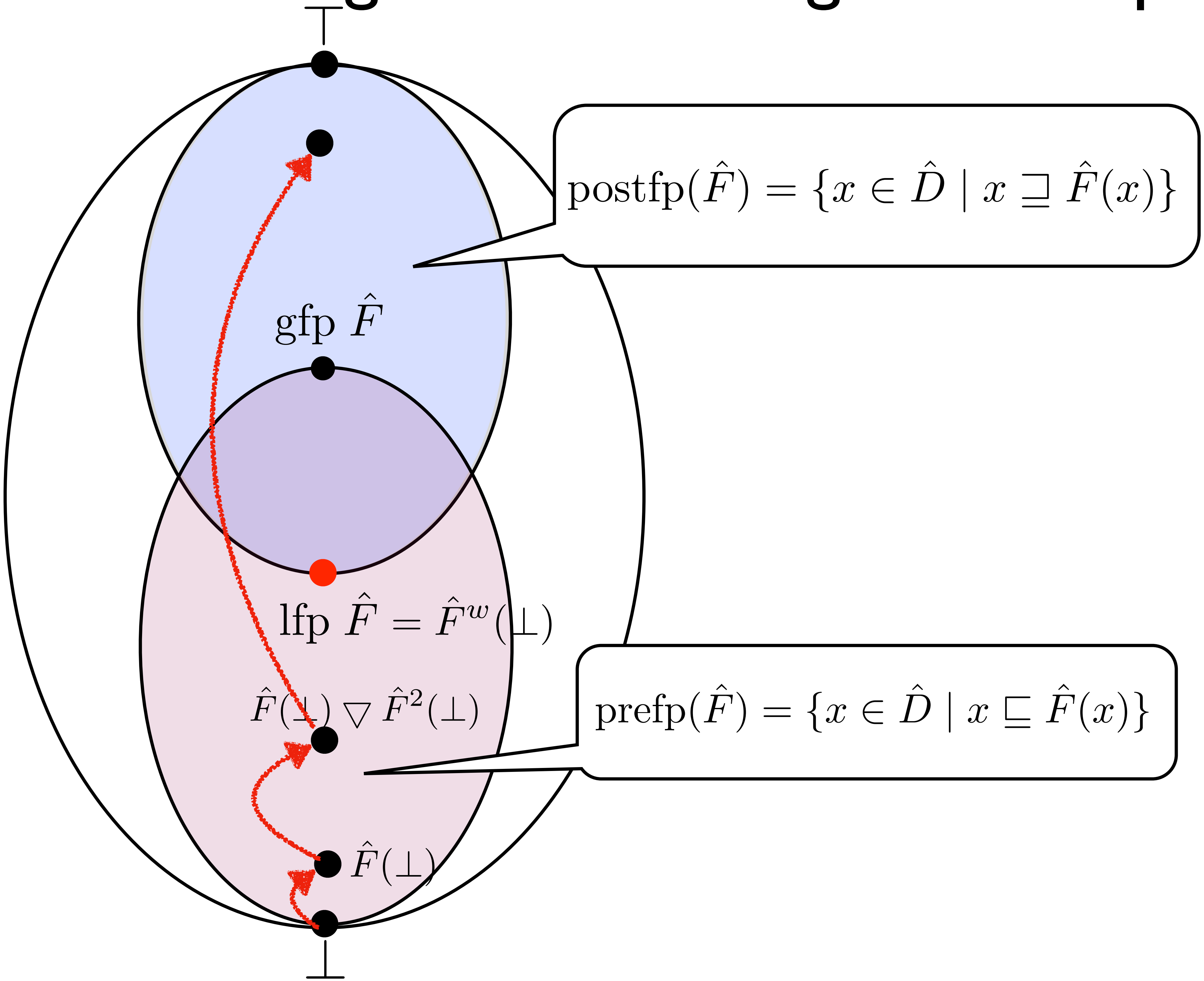
Abstract Domain



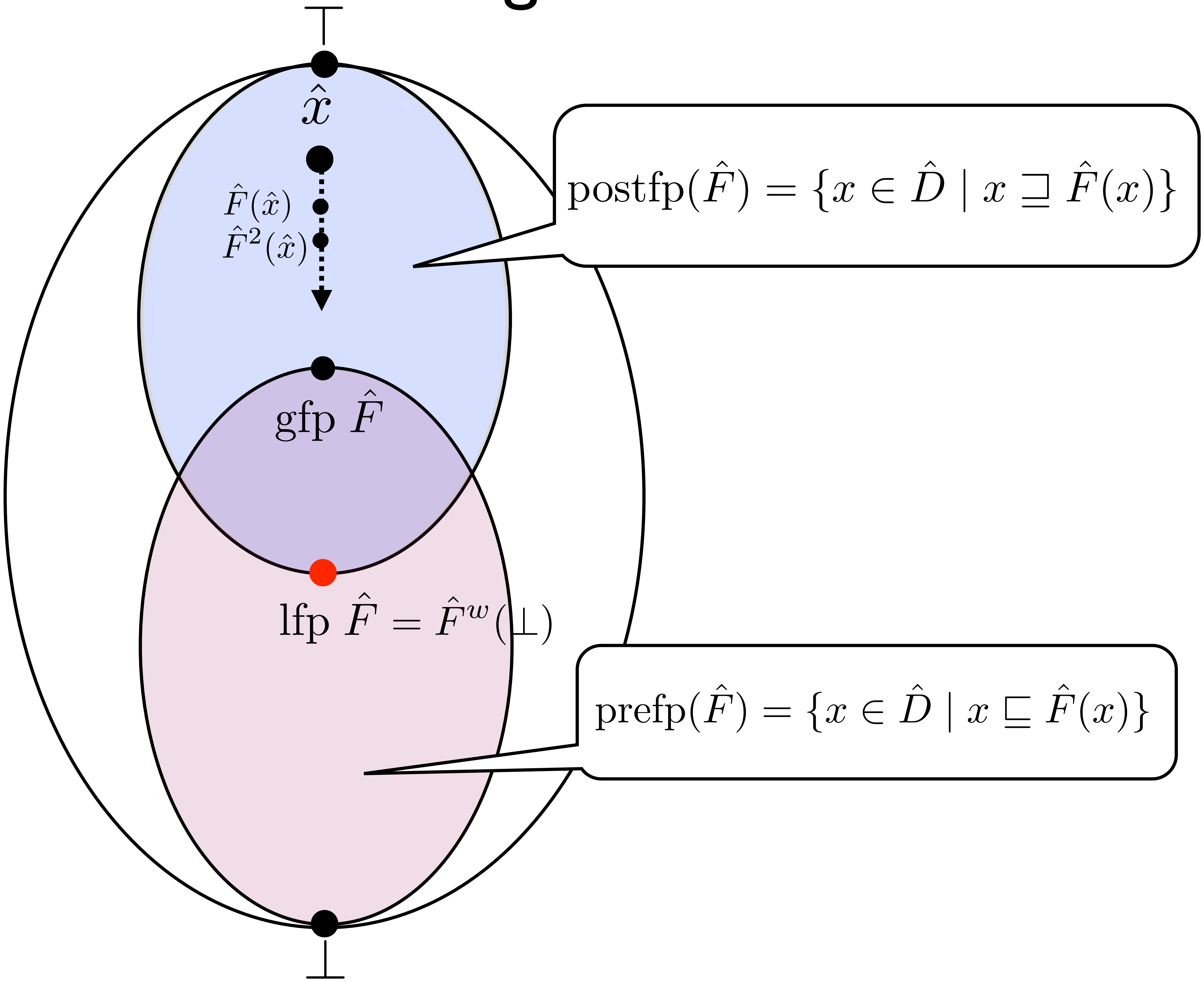
Basic Upward/Downward Fixpoint Iteration



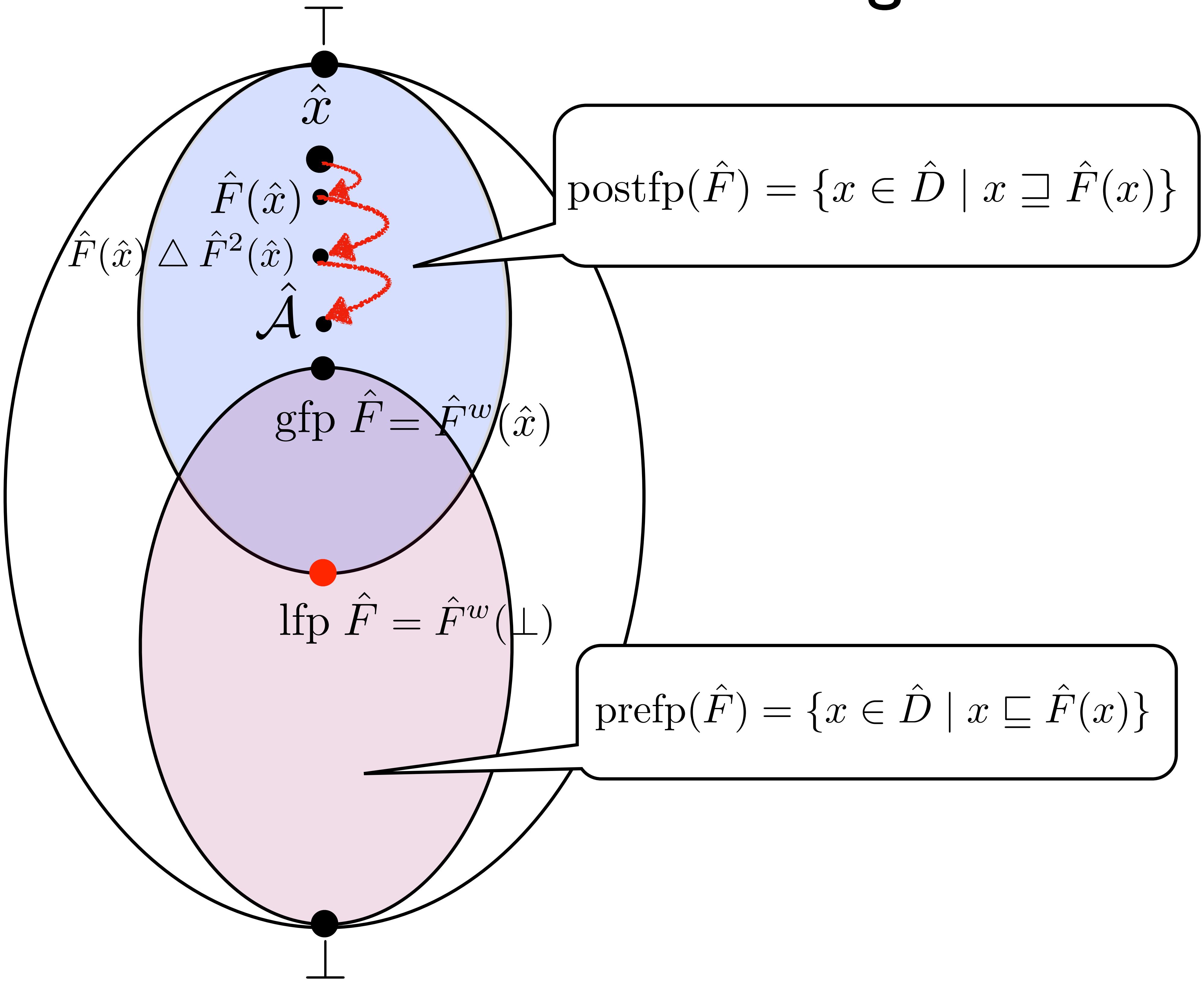
Widening: Overshooting via Extrapolation



Refining the Widened Result



Narrowing



$\top$
$\hat{x}$
$\hat{F}(\hat{x})$
$\hat{F}(\hat{x}) \triangle \hat{F}^2(\hat{x})$
$\hat{\mathcal{A}}$
gfp $\hat{F} = \hat{F}^w(\hat{x})$
lfp $\hat{F} = \hat{F}^w(\bot)$
$\bot$
postfp$(\hat{F}) = \{x \in \hat{D} \mid x \sqsupseteq \hat{F}(x)\}$
prefp$(\hat{F}) = \{x \in \hat{D} \mid x \sqsubseteq \hat{F}(x)\}$

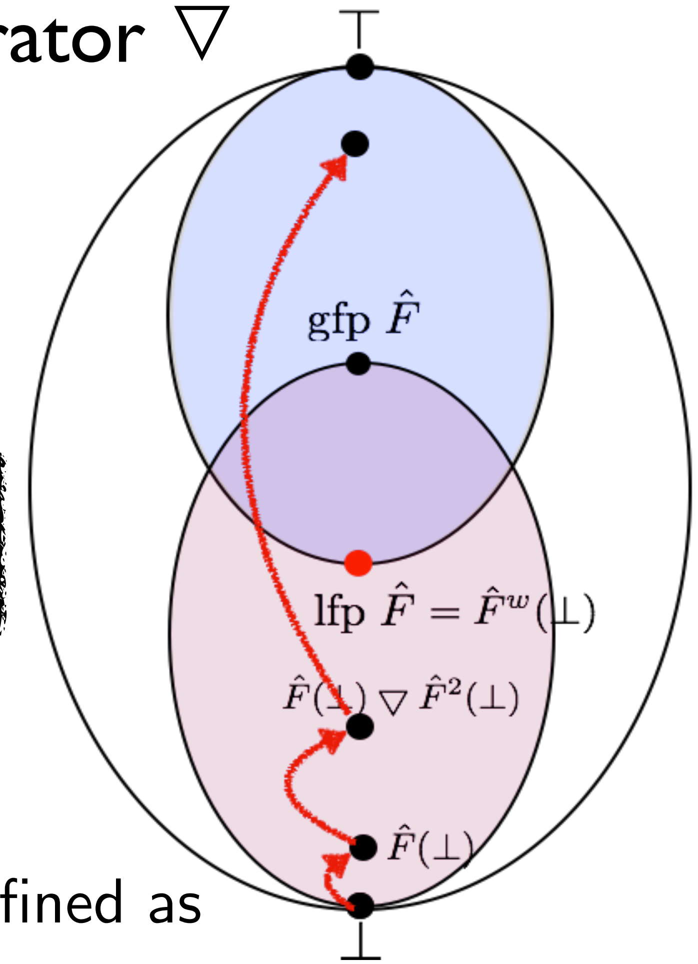
Widening

- We can define a finite chain with an widening operator $\triangledown$

$$\hat{X}_0 = \hat{\bot}$$

$$\hat{X}_{i+1} = \begin{cases} \hat{X}_i & \text{if } \hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i \\ \hat{X}_i \triangledown \hat{F}(\hat{X}_i) & \text{o.w.} \end{cases}$$

Stop if a postfix is reached



- Conditions on $\triangledown$:
  - $\forall a, b \in \ddot{D}.\ (a \sqsubseteq a \triangledown b) \ \wedge \ (b \sqsubseteq a \triangledown b)$
  - For all increasing chains $(x_i)_i$, the increasing chain $(y_i)_i$ defined as

$$y_i = \begin{cases} x_0 & \text{if } i = 0 \\ y_{i-1} \triangledown x_i & \text{if } i > 0 \end{cases}$$

eventually stabilizes (i.e., the chain is finite).

Widening

- Then
  - $\hat{X}_0 \sqsubseteq \hat{X}_1 \sqsubseteq \cdots \sqsubseteq \hat{X}_n$ is a finite chain.
  - Its limit is correct:

$$\bigsqcup_{i \in \mathbb{N}} (\hat{F}^i(\hat{\bot})) \sqsubseteq \lim_{i \in \mathbb{N}} (\hat{X}_i).$$

Theorem [widen's safety]

Narrowing

- We can define a finite chain with a narrowing operator $\triangle$:

$$\hat{Y}_0 = \hat{A} \text{ s.t. } \hat{A} \in \text{postfp}(\hat{F})$$
$$\hat{Y}_{i+1} = \hat{Y}_i \triangle \hat{F}(\hat{Y}_i)$$

- Conditions
  - $\forall a, b \in \hat{D}.\ a \sqsupseteq b \implies a \sqsupseteq a \triangle b \sqsupseteq b$
  - $\forall$decreasing chain$\{a_i\}_i$: chain$y_0 = a_0, y_{i+1} = y_i \triangle a_{i+1}$is finite
- Then
  - $\{\hat{Y}_i\}_i$ is a finite chain.
  - Its limit is still correct:

$$\bigsqcup_{i \in \mathbb{N}} (\hat{F}^i(\hat{\bot})) \sqsubseteq \lim_{i \in \mathbb{N}} (\hat{Y}_i).$$

Theorem [narrow's safety]

Why Above Prescription Is Correct?

Fixpoint Transfer Theorem

Theorem (fixpoint transfer)

Let CPOs D *and* $\hat{D}$ *are Galois-connected. Function* $F : D \to D$ *is continuous.* $\hat{F} : \hat{D} \to \hat{D}$ *is either monotonic or extensive. Either* $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$ *or* $\alpha\ f \sqsubseteq \hat{f}$ *implies* $\alpha(F\ f) \sqsubseteq \hat{F}\ \hat{f}$*. Then,*

$$\alpha(\mathit{fix} F) \sqsubseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot}).$$

Why Above Prescription Is Correct?

Widening/Narrowing Theorems

Theorem (widen's safety)

Let $\hat{F} : \hat{D} \to \hat{D}$ *be monotonic over CPO* $\hat{D}$*. Let widening operator* $\bigtriangledown : \hat{D} \times \hat{D} \to \hat{D}$ *satisfies the widending conditions. Then the widened chain* $\{\hat{X}_i\}_i$ *is finite and its limit satisfies* $\lim_{i \in \mathbb{N}} \hat{X}_i \sqsupseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot})$.

Theorem (narrow's safety)

Let $\hat{F} : \hat{D} \to \hat{D}$ *be monotonic over CPO* $\hat{D}$*. Let narrowing operator* $\bigtriangleup : \hat{D} \times \hat{D} \to \hat{D}$ *satisfies the narrowng conditions. If* $\hat{F}(\hat{\mathcal{A}}) \sqsubseteq \hat{\mathcal{A}}$ *then the narrowed chain* $\{\hat{Y}_i\}_i$ *is finite and its limit satisfies* $\lim_{i \in \mathbb{N}} \hat{Y}_i \sqsupseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\bot})$.

More Properties of Galois Connections

Properties of Galois Connections

$$D \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{D}$$

Theorem 1. $\alpha(\bot) = \hat{\bot}$

Proof. $\alpha(\bot) \sqsubseteq \hat{\bot}$ because $\bot \sqsubseteq \gamma(\hat{\bot})$. By the definition of $\hat{\bot}$, $\hat{\bot} \sqsubseteq \alpha(\bot)$. Therefore, $\alpha(\bot) = \hat{\bot}$. □

Theorem 2. $id \sqsubseteq \gamma \circ \alpha$

Proof. $\alpha(x) \sqsubseteq \alpha(x)$. By the definition of galois connection, $x \sqsubseteq \gamma(\alpha(x))$. □

Theorem 3. $\alpha \circ \gamma \sqsubseteq id$

Proof. $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{x})$. By the definition of galois connection, $\alpha(\gamma(\hat{x})) \sqsubseteq \hat{x}$. □

Properties of Galois Connections

Theorem 4. γ *is monotone.*

Proof. Suppose $\hat{x} \sqsubseteq \hat{y}$. Because $\alpha \circ \gamma \sqsubseteq id$, $\alpha \circ \gamma(\hat{x}) \sqsubseteq \hat{y}$. By the definition of galois connection, $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{y})$.

$\square$

Theorem 5. α *is monotone.*

Proof. Suppose $x \sqsubseteq y$. Then $x \sqsubseteq \gamma \circ \alpha(y)$ because $id \sqsubseteq \gamma \circ \alpha$. By the definition of galois connection, $\alpha(x) \sqsubseteq \alpha(y)$. $\square$

Properties of Galois Connections

Theorem 6. *α is continuous.*

Proof. We show that for any chain S in D,

$$\alpha(\bigsqcup_{x \in S} x) = \bigsqcup_{x \in S} \alpha(x).$$

- ($\sqsupseteq$): Because α is monotone, $\alpha(\bigsqcup_{x \in S} x) \sqsupseteq \bigsqcup_{x \in S} \alpha(x)$.
- ($\sqsubseteq$): $\bigsqcup_{x \in S} x \sqsubseteq \gamma(\bigsqcup_{x \in S} \alpha(x))$ because

$$\bigsqcup_{x \in S} x \sqsubseteq \bigsqcup_{x \in S} \gamma(\alpha(x)) \qquad (id \sqsubseteq \gamma \circ \alpha)$$

$$\bigsqcup_{x \in S} \gamma(\alpha(x)) \sqsubseteq \gamma(\bigsqcup_{x \in S} \alpha(x)) \qquad (\gamma \text{ is monotone})$$

By the definition of galois connection, $\alpha(\bigsqcup_{x \in S} x) \sqsubseteq \bigsqcup_{x \in S} \alpha(x)$.

□

Compositional Constructions of Galois Connections

- Suppose $A \underset{\alpha_A}{\overset{\gamma_A}{\leftrightarrows}} \hat{A}$ and $B \underset{\alpha_B}{\overset{\gamma_B}{\leftrightarrows}} \hat{B}$. Then,

- $A \times B \underset{\alpha_{A \times B}}{\overset{\gamma_{A \times B}}{\leftrightarrows}} \hat{A} \times \hat{B}$
  - with $\alpha_{A \times B} = \lambda \langle a, b \rangle .\ \langle \alpha_A(a), \alpha_B(b) \rangle$

- $A + B \underset{\alpha_{A+B}}{\overset{\gamma_{A+B}}{\leftrightarrows}} \hat{A} + \hat{B}$
  - with $\alpha_{A+B} = \lambda x.\ \begin{cases} \alpha_A(x) & (x \in A) \\ \alpha_B(x) & (\text{otherwise}) \end{cases}$

Compositional Constructions of Galois Connections

- $A \to B \underset{\alpha_{A \to B}}{\overset{\gamma_{A \to B}}{\longleftrightarrows}} \hat{A} \to \hat{B}$
  - with $\alpha_{A \to B} = \lambda f.\, \alpha_B \circ f \circ \gamma_{\hat{A}}$

Compositional Constructions of Galois Connections

Theorem 7. *If* $A \xleftrightarrow[\alpha_A]{\gamma_A} \hat{A}$ *and* $B \xleftrightarrow[\alpha_B]{\gamma_B} \hat{B}$*, then* $A \to B \xleftrightarrow[\alpha_{A\to B}]{\gamma_{A\to B}} \hat{A} \to \hat{B}$ *where* $\alpha_{A\to B} = \lambda f.\ \alpha_B \circ f \circ \gamma_{\hat{A}}$ *and* $\gamma_{\hat{A}\to\hat{B}} = \lambda \hat{f}.\ \gamma_{\hat{B}} \circ \hat{f} \circ \alpha_A$.

Proof. We will show

$$\forall f \in A \to B, \hat{f} \in \hat{A} \to \hat{B}.\ \alpha_{A\to B}(f) \sqsubseteq \hat{f} \iff f \sqsubseteq \gamma_{\hat{A}\to\hat{B}}(\hat{f}).$$

- Case ($\Rightarrow$): for $f \in A \to B, \hat{f} \in \hat{A} \to \hat{B}$, $\alpha_{A\to B}(f) \sqsubseteq \hat{f}$.

$$\begin{array}{lr}
\alpha_B \circ f \circ \gamma_{\hat{A}} \sqsubseteq \hat{f} & \\
\gamma_{\hat{B}} \circ \alpha_B \circ f \circ \gamma_{\hat{A}} \sqsubseteq \gamma_{\hat{B}} \circ \hat{f} & (\gamma_{\hat{B}} \text{ monotone}) \\
f \circ \gamma_{\hat{A}} \sqsubseteq \gamma_{\hat{B}} \circ \hat{f} & (id \sqsubseteq \gamma_{\hat{B}} \circ \alpha_B) \\
f \circ \gamma_{\hat{A}} \circ \alpha_A \sqsubseteq \gamma_{\hat{B}} \circ \hat{f} \circ \alpha_A & \\
f \sqsubseteq \gamma_{\hat{B}} \circ \hat{f} \circ \alpha_A & (f \text{ monotone}, id \sqsubseteq \gamma_{\hat{A}} \circ \alpha_A)
\end{array}$$

- Case ($\Leftarrow$): similar to the above case.

$\square$

Best Abstract Semantics

- Let $f \in A \to B$ be a concrete semantic function and

$$A \underset{\alpha_A}{\overset{\gamma_{A^\sharp}}{\leftrightarrows}} A^\sharp \qquad B \underset{\alpha_B}{\overset{\gamma_{B^\sharp}}{\leftrightarrows}} B^\sharp$$

- $f^\sharp \in A^\sharp \to B^\sharp$ is a monotone abstract semantic function. Then, the "best" (most precise) abstract semantic function is $f^\sharp = \alpha_B \circ f \circ \gamma_{A^\sharp}$

- Why? we can show

  - $f \circ \gamma_{A^\#} \sqsubseteq \gamma_{B^\#} \circ f^\#$
  - For any $g \in A^\# \to B^\#$, if $f \circ \gamma_{A^\#} \sqsubseteq \gamma_{B^\#} \circ g^\#$, then $f^\# \sqsubseteq g^\#$

Soundness Proofs

Fixpoint Transfer Theorems

Theorem (Fixpoint Transfer 1). *Let $\mathbb{D}$ and $\mathbb{D}^\sharp$ be related by Galois connection $\mathbb{D} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}^\sharp$. Let $F : \mathbb{D} \to \mathbb{D}$ be a continuous function and $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ be a monotone or extensive function such that $F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$. Then,*

$$\mathbf{lfp} F \sqsubseteq \gamma(\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp)).$$

Fixpoint Transfer Theorem

Theorem (Fixpoint Transfer 1). *Let* $\mathbb{D}$ *and* $\mathbb{D}^\sharp$ *be related by Galois connection* $\mathbb{D} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}^\sharp$. *Let* $F : \mathbb{D} \to \mathbb{D}$ *be a continuous function and* $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ *be a monotone or extensive function such that* $F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$. *Then,*

$$\mathbf{lfp} F \sqsubseteq \gamma(\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp)).$$

Proof. First we prove $\forall n \in \mathbb{N}.\ F^n(\bot) \sqsubseteq \gamma(F^{\sharp n}(\bot^\sharp))$ by induction. The base case is trivial. The inductive case is as follows:

$$\begin{aligned} F^{n+1}(\bot) &= F \circ F^n(\bot) \\ &\sqsubseteq F \circ \gamma(F^{\sharp n}(\bot^\sharp)) && \text{(by induction hypothesis and monotonicity of } F) \\ &\sqsubseteq \gamma \circ F^\sharp \circ F^{\sharp n}(\bot^\sharp) && \text{(by assumption } F \circ \gamma \sqsubseteq \gamma \circ F^\sharp) \\ &= \gamma(F^{\sharp n+1}(\bot^\sharp)) \end{aligned}$$

$\{F^i(\bot)\}_i$ is a chain because F is continuous (so monotone). Then, the least upper bound of the chain $\bigsqcup_{i \geq 0} F^i(\bot)$ exists because $\mathbb{D}$ is a CPO. $\{F^{\sharp i}(\bot^\sharp)\}_i$ is a chain because $F^\sharp$ is monotone or extensive. Then, $\{\gamma(F^{\sharp i}(\bot^\sharp))\}_i$ is also a chain because γ is monotone. Therefore, the least upper bound of the chain $\bigsqcup_{i \geq 0} \{\gamma(F^{\sharp i}(\bot^\sharp))\}_i$ exists.

$$\begin{aligned} \mathbf{lfp} F = \bigsqcup_{i \geq 0} F^i(\bot) &\sqsubseteq \bigsqcup_{i \geq 0} \gamma(F^{\sharp i}(\bot^\sharp)) \\ &\sqsubseteq \gamma(\bigsqcup_{i \geq 0} (F^{\sharp i}(\bot^\sharp))) && \text{(by monotonicity of } \gamma) \end{aligned}$$

Widening's Safety

Theorem (Widening's Safety). *Let* $\mathbb{D}^\sharp$ *be a CPO,* $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ *be a monotone function, and* $\nabla : \mathbb{D}^\sharp \times \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ *be a widening operator. Then, chain* $\{Y_i^\sharp\}_i$ *eventually stabilizes and*

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Y^\sharp_{\lim}$$

where $Y^\sharp_{\lim}$ *is the greatest element of the chain.*

Widening's Safety

Theorem (Widening's Safety). *Let $\mathbb{D}^\sharp$ be a CPO, $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ be a monotone function, and $\nabla : \mathbb{D}^\sharp \times \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ be a widening operator. Then, chain $\{Y_i^\sharp\}_i$ eventually stabilizes and*

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Y_{\lim}^\sharp$$

where $Y_{\lim}^\sharp$ is the greatest element of the chain.

Proof. First we prove chain $\{Y_i^\sharp\}_i$ is finite. According to the second condition on widening operator, it is enough to show that chain $\{F^\sharp(Y_i^\sharp)\}_i$ is increasing. The chain is increasing because 1) $F^\sharp(Y_{i+1}^\sharp)$ is either $F^\sharp(Y_i^\sharp)$ or $F^\sharp(Y_i^\sharp \nabla F^\sharp(Y_i^\sharp))$, 2) $Y_i^\sharp \sqsubseteq Y_i^\sharp \nabla F^\sharp(Y_i^\sharp)$ according to the first condition on widening, and 3) $F^\sharp$ is monotone.

Second, we prove $\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Y_{\lim}^\sharp$. It is enough to show that $\forall i \in \mathbb{N}.\ F^{\sharp i}(\bot^\sharp) \sqsubseteq Y_i^\sharp$ that can be proven by induction. The base case is trivial. The inductive case is as follows:

$$\begin{aligned} F^{\sharp i+1}(\bot^\sharp) &= F^\sharp(F^{\sharp i}(\bot^\sharp)) \\ &\sqsubseteq F^\sharp(Y_i^\sharp) \qquad \text{(by induction hypothesis and monotonicity of } F^\sharp\text{)} \end{aligned}$$

If $F^\sharp(Y_i^\sharp) \sqsubseteq Y_i^\sharp$, then $Y_{i+1}^\sharp = Y_i^\sharp$ by definition. Therefore, $F^{\sharp i+1}(\bot^\sharp) \sqsubseteq Y_{i+1}^\sharp$.

If $F^\sharp(Y_i^\sharp) \sqsupset Y_i^\sharp$, then $Y_{i+1}^\sharp = Y_i^\sharp \ \nabla\ F^\sharp(Y_i^\sharp)$ by definition. According to the first condition on widening, $F^\sharp(Y_i^\sharp) \sqsubseteq Y_i^\sharp \ \nabla\ F^\sharp(Y_i^\sharp)$. Therefore, $F^{\sharp i+1}(\bot^\sharp) \sqsubseteq Y_{i+1}^\sharp$.

Narrowing's Safety

Theorem (Narrowing's Safety)**.** *Let* $\mathbb{D}^\sharp$ *be a CPO,* $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ *be a monotone function, and* $\triangle : \mathbb{D}^\sharp \times \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ *be a narrowing operator. Then, chain* $\{Z_i^\sharp\}_i$ *eventually stabilizes and*

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Z^\sharp_{\lim}$$

where $Z^\sharp_{\lim}$ *is the least element of the chain.*

Narrowing's Safety

Theorem (Narrowing's Safety). *Let $\mathbb{D}^\sharp$ be a CPO, $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ be a monotone function, and $\triangle : \mathbb{D}^\sharp \times \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ be a narrowing operator. Then, chain $\{Z_i^\sharp\}_i$ eventually stabilizes and*

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Z_{\mathrm{lim}}^\sharp$$

where $Z_{\mathrm{lim}}^\sharp$ is the least element of the chain.

Proof. First we prove chain $\{Z_i^\sharp\}_i$ is finite. According to the second condition on narrowing operator, it is enough to show that chain $\{F^\sharp(Z_i^\sharp)\}_i$ is decreasing. The chain is decreasing if $\forall i \in \mathbb{N}.\ Z_i^\sharp \sqsupseteq F^\sharp(Z_i^\sharp)$, because

$$\begin{array}{lr}
Z_i^\sharp \sqsupseteq F^\sharp(Z_i^\sharp) & \\
\Longrightarrow Z_i^\sharp \sqsupseteq (Z_i^\sharp \triangle F^\sharp(Z_i^\sharp)) \sqsupseteq F^\sharp(Z_i^\sharp) & \text{(by the first condition on narrowing)} \\
\Longrightarrow F^\sharp(Z_i^\sharp) \sqsupseteq F^\sharp(Z_i^\sharp \triangle F^\sharp(Z_i^\sharp)) & \text{(by monotonicity of } F^\sharp) \\
\Longrightarrow F^\sharp(Z_i^\sharp) \sqsupseteq F^\sharp(Z_{i+1}^\sharp) & \text{(by definition of } Z_{i+1}^\sharp)
\end{array}$$

We prove $\forall i \in \mathbb{N}.\ Z_i^\# \sqsupseteq F^{\# i}(\bot)$ by induction. The base case is trivial because $F^{\#0}(\bot) = \bot$. The inductive step is as follows: By IH, we have $Z_i^\# \sqsupseteq F^{\# i}(\bot)$. We need to show that $Z_{i+1}^\# \sqsupseteq F^{\# i+1}(\bot)$. Because $F^\#$ is monotone, we have $F^\#(Z_i^\#) \sqsubseteq F^{\# i+1}(\bot)$. Because $F^\#(Z_i^\#) \sqsubseteq Z_i^\#$, $Z_i^\# \triangle F^\#(Z_i^\#) \sqsupseteq F^\#(Z_i^\#)$ by the first condition of the narrowing operator. Therefore, $F^{\# i+1}(\bot) \sqsubseteq F^\#(Z_i^\#) \sqsubseteq Z_i^\# \triangle F^\#(Z_i^\#) \sqsubseteq Z_{i+1}^\#$.