

# Program Analysis

## 6. Abstract Interpretation (2): Abstract Semantics

Kihong Heo



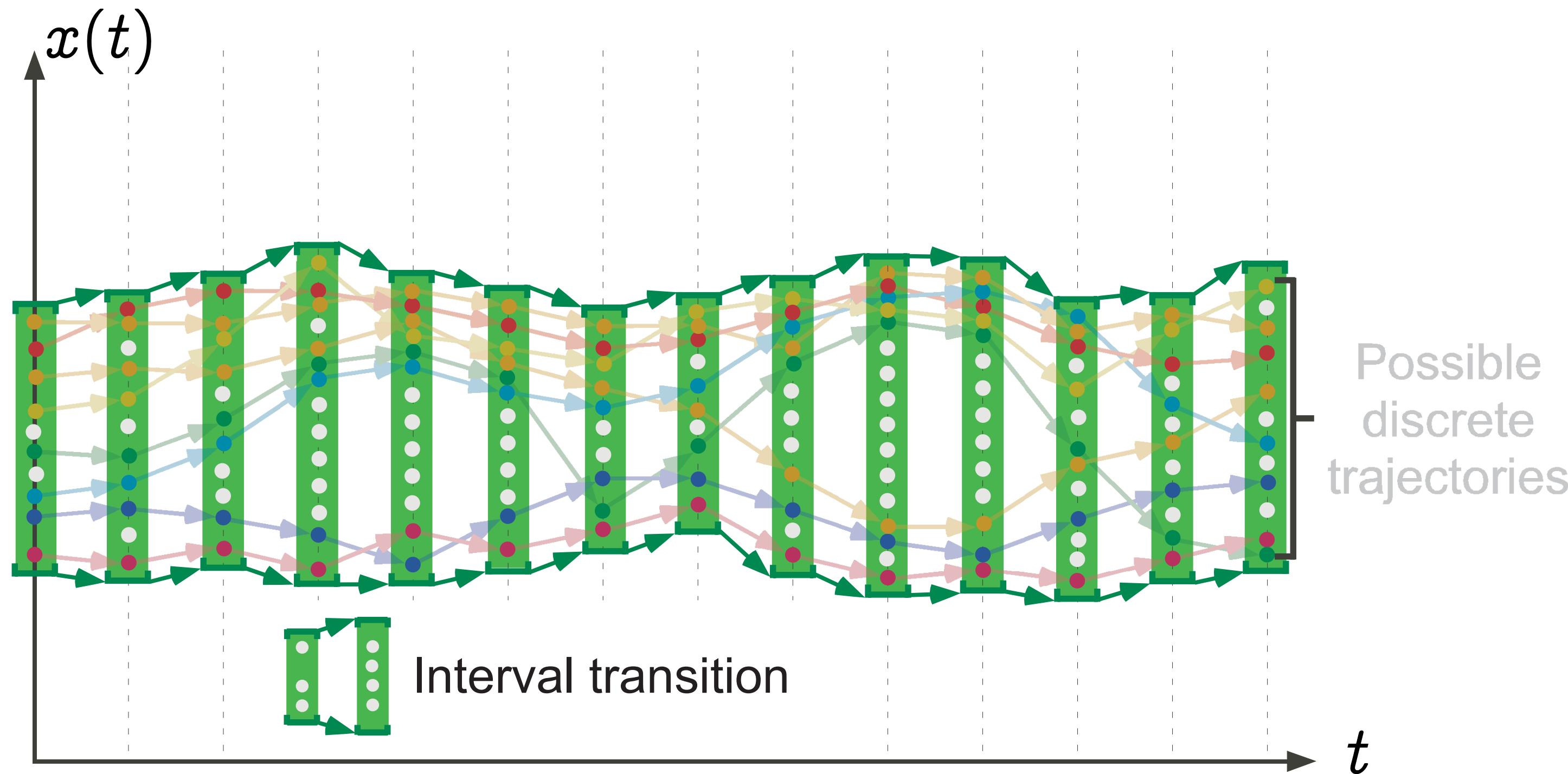
# Design of Static Analysis

- Goal: **conservative** and **terminating** static analysis
- Design principles:
  - Define **concrete semantics**
  - Define **abstract semantics** (sound w.r.t the concrete semantics)
- Computation & implementation:
  - Abstract semantics of a program: **the least fixed point** of the semantic function
  - Static analyzer: **compute** the least fixed point within **finite time**

# Step 2: Design Abstract Semantics

- Formalization of **abstract** program executions
  - Soundly subsume concrete executions
- How to subsume: different choices depending on the purposes
  - Some are more expressive than others
- Example: abstraction of {1, 3, 5, 7}
  - Integer, Positive, Odd, [1, 7], etc

# Transitions of Abstract States



\*from Patrick Cousot's slides

# Abstract Semantics

- Define an abstract domain  $\mathbb{D}^\sharp$  (CPO)
- Define an abstract semantic function  $F^\sharp : \mathbb{D}^\sharp \rightarrow \mathbb{D}^\sharp$  (monotone or extensive)

**(Monotone)**  $\forall x^\sharp, y^\sharp \in \mathbb{D}^\sharp. x^\sharp \sqsubseteq y^\sharp \implies F^\sharp(x^\sharp) \sqsubseteq F^\sharp(y^\sharp)$

**(Extensive)**  $\forall x^\sharp \in \mathbb{D}. x^\sharp \sqsubseteq F^\sharp(x^\sharp)$

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

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp)$$

**Q. How to ensure that the abstract semantics soundly subsume the concrete semantics?**

# Requirement 1: Galois Connection (1)

$$\mathbb{D} \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}^\sharp$$

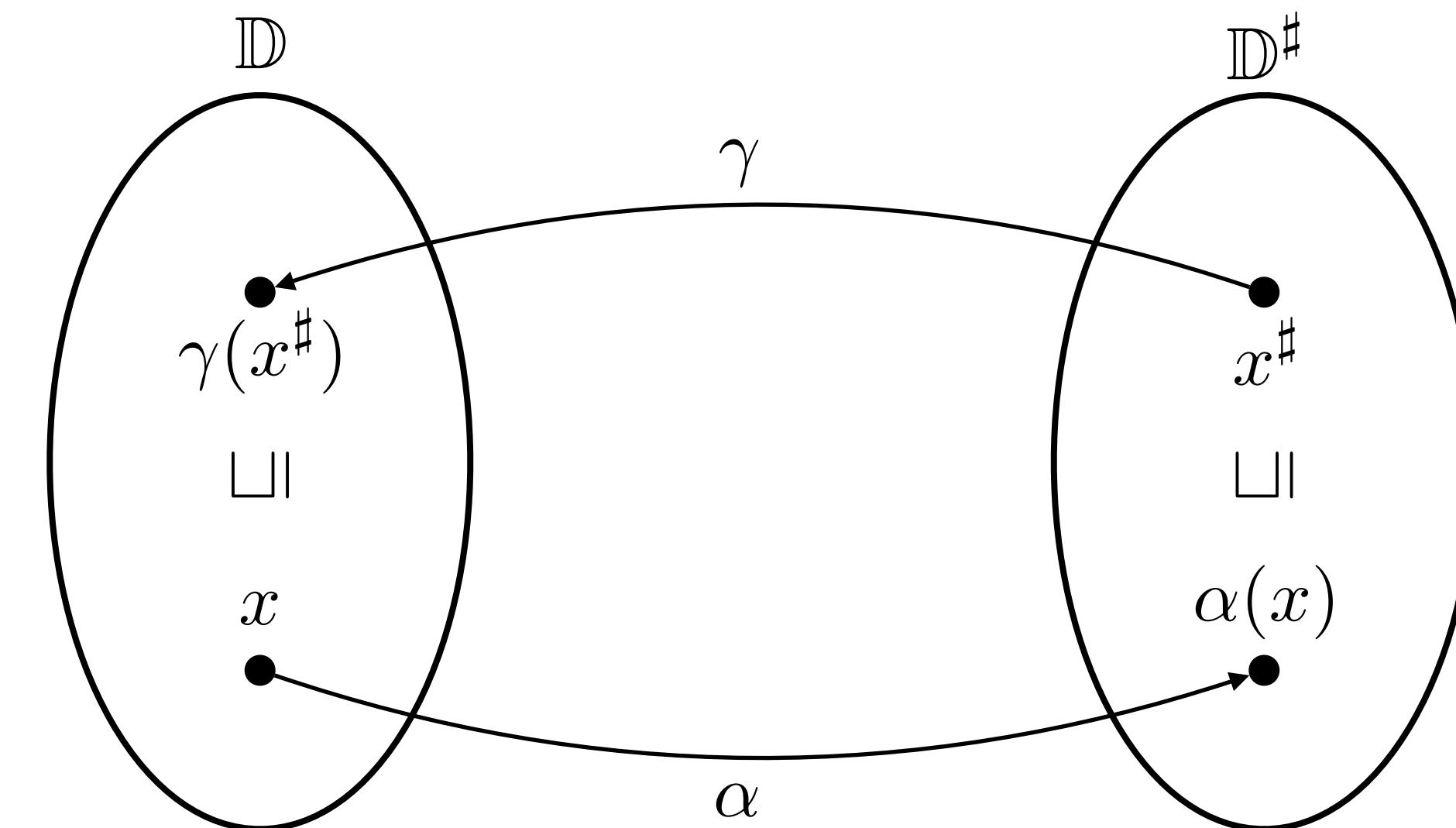
- $\mathbb{D}$  and  $\mathbb{D}^\sharp$  must be related with a Galois connection where

- Abstraction function:  $\alpha \in \mathbb{D} \rightarrow \mathbb{D}^\sharp$
- Concretization function:  $\gamma \in \mathbb{D}^\sharp \rightarrow \mathbb{D}$

$$\forall x \in \mathbb{D}, x^\sharp \in \mathbb{D}^\sharp. \alpha(x) \sqsubseteq x^\sharp \iff x \sqsubseteq \gamma(x^\sharp)$$

# Requirement 1: Galois Connection (2)

- Intuition: order preservation between two semantic domains



# Galois Connection



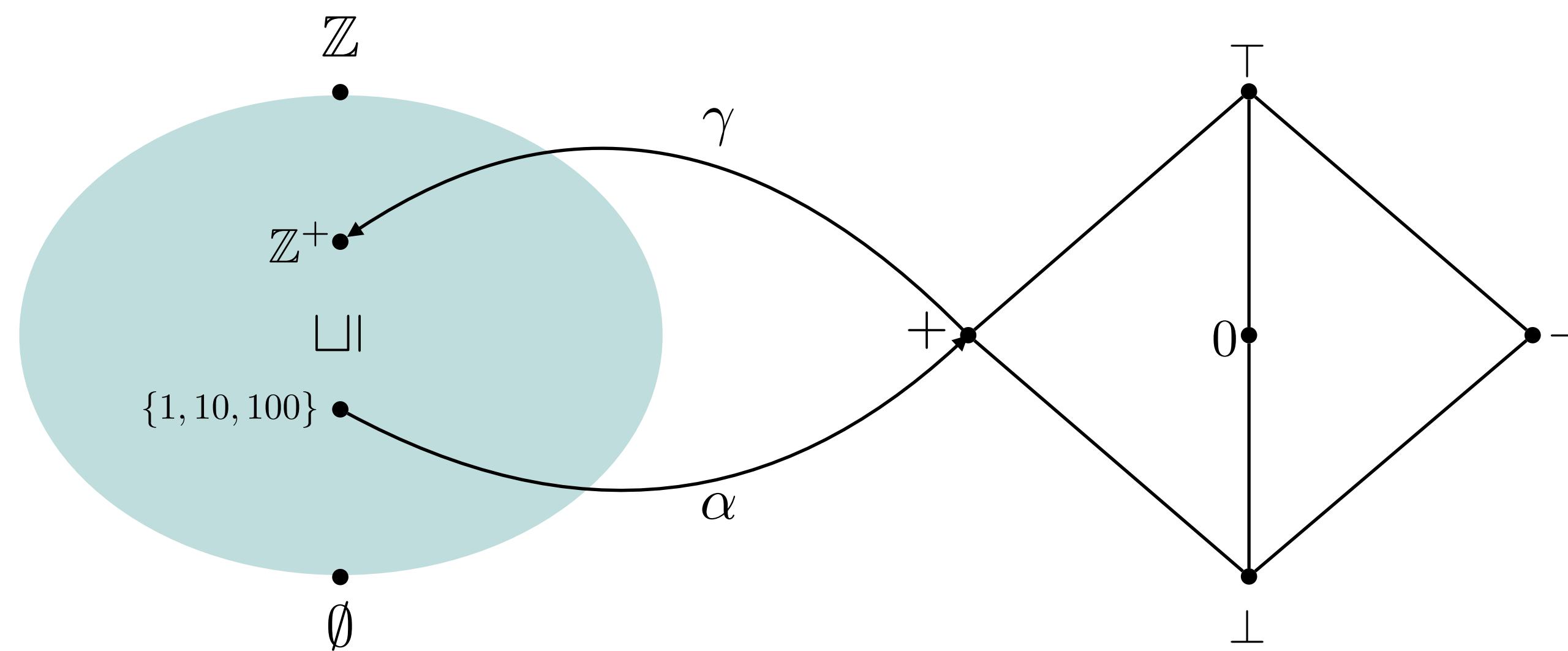
*A robot on a starry night watching himself  
in the water surface,  
in the style of vaporwave*

by Youngseok Choi, 2022



# Example: Sign Abstraction (1)

$$\wp(\mathbb{Z}) \xrightleftharpoons[\alpha]{\gamma} \{\perp, -, 0, +, \top\}$$



# Example: Sign Abstraction (2)

$$\wp(\mathbb{Z}) \xrightleftharpoons[\alpha]{\gamma} \{\perp, -, 0, +, \top\}$$

$$\alpha(Z) = \begin{cases} \perp & Z = \emptyset \\ + & \forall z \in Z. z > 0 \\ 0 & Z = \{0\} \\ - & \forall z \in Z. z < 0 \\ \top & \text{otherwise} \end{cases}$$

Proof?

$$\gamma(\perp) = \emptyset$$

$$\gamma(+) = \{z \in \mathbb{Z} \mid z > 0\}$$

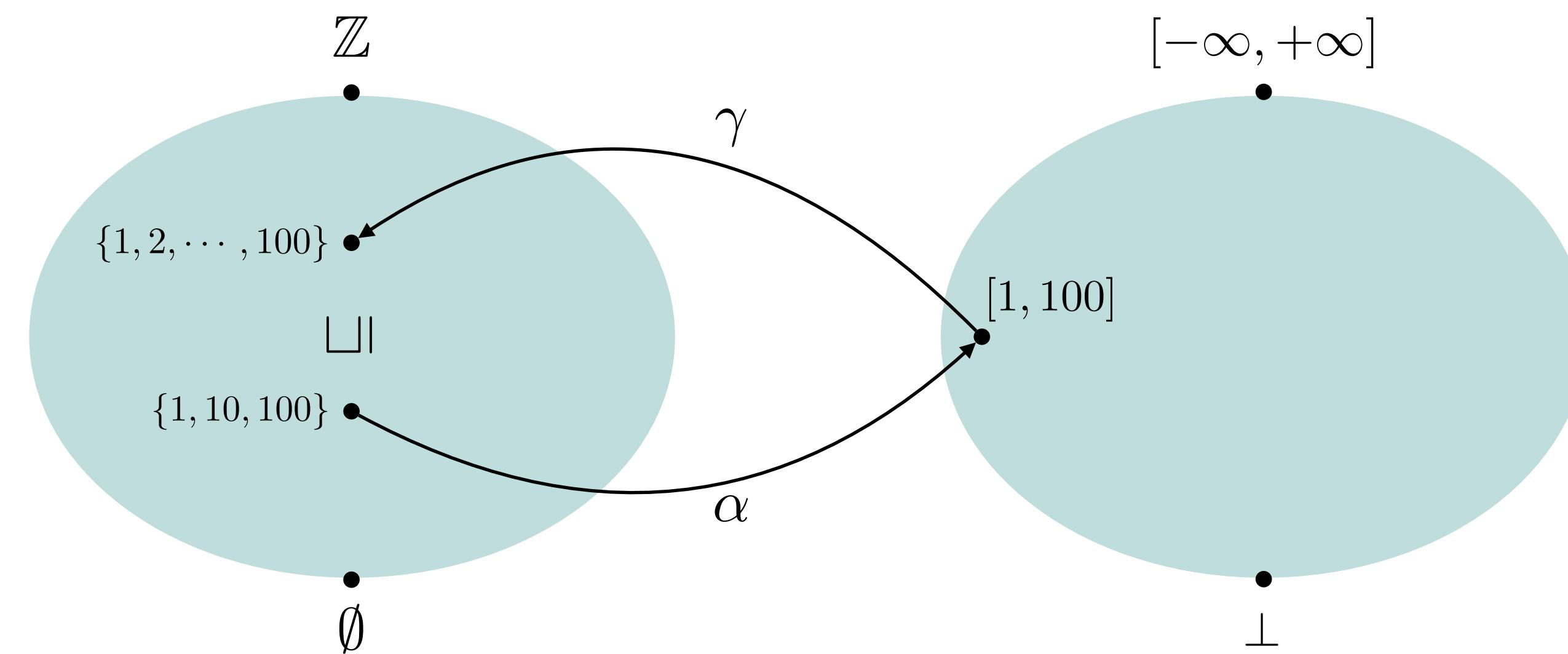
$$\gamma(0) = \{0\}$$

$$\gamma(-) = \{z \in \mathbb{Z} \mid z < 0\}$$

$$\gamma(\top) = \mathbb{Z}$$

# Example: Interval Abstraction (1)

$$\wp(\mathbb{Z}) \xrightleftharpoons[\alpha]{\gamma} \{\perp\} \cup \{[a, b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\}$$



# Example: Interval Abstraction (2)

$$\wp(\mathbb{Z}) \xrightleftharpoons[\alpha]{\gamma} \{\perp\} \cup \{[a, b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\}$$

Proof?

$$\alpha(\emptyset) = \perp$$

$$\alpha(X) = [\min X, \max X]$$

$$\gamma(\perp) = \emptyset$$

$$\gamma([a, b]) = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$$

# Properties of Galois Connection

$$\forall x \in \mathbb{D}, x^\# \in \mathbb{D}^\#. \alpha(x) \sqsubseteq x^\# \iff x \sqsubseteq \gamma(x^\#)$$

- $id \sqsubseteq \gamma \circ \alpha$

$$\iff \alpha(x) \sqsubseteq \alpha(x) \\ \iff x \sqsubseteq \gamma(\alpha(x)) \quad (\text{by Galois connection})$$

- $\alpha \circ \gamma \sqsubseteq id$

$$\iff \gamma(x^\#) \sqsubseteq \gamma(x^\#) \\ \iff \alpha(\gamma(x^\#)) \sqsubseteq x^\# \quad (\text{by Galois connection})$$

- $\alpha$  is monotone

$$\implies x \sqsubseteq y \\ \implies x \sqsubseteq \gamma(\alpha(y)) \quad (id \sqsubseteq \gamma \circ \alpha) \\ \iff \alpha(x) \sqsubseteq \alpha(y) \quad (\text{by Galois connection})$$

- $\gamma$  is monotone

$$\implies x^\# \sqsubseteq y^\# \\ \implies \alpha(\gamma(x^\#)) \sqsubseteq y^\# \quad (\alpha \circ \gamma \sqsubseteq id) \\ \iff \gamma(x^\#) \sqsubseteq \gamma(x^\#) \quad (\text{by Galois connection})$$

# Deriving Galois Connections (1)

- Pointwise lifting:

Given a Galois connection  $\mathbb{D} \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}^\sharp$  and a set  $\mathbb{S}$

$$\mathbb{S} \rightarrow \mathbb{D} \xrightleftharpoons[\alpha']{\gamma'} \mathbb{S} \rightarrow \mathbb{D}^\sharp$$

where  $\alpha'(f) = \lambda x \in \mathbb{S}. \alpha(f(x))$  and  $\gamma'(f^\sharp) = \lambda x \in \mathbb{S}. \gamma(f^\sharp(x))$

- Example

- $\wp(\mathbb{Z}) \xrightleftharpoons[\alpha]{\gamma} \{\perp, -, 0, +, \top\}$

- $\mathbb{S} = \{x, y, z\}$

# Deriving Galois Connections (2)

- Composition:

Given two galois connections  $\mathbb{D}_1 \xrightleftharpoons[\alpha_1]{\gamma_1} \mathbb{D}_2 \xrightleftharpoons[\alpha_2]{\gamma_2} \mathbb{D}_3$

$$\mathbb{D}_1 \xrightleftharpoons[\alpha_2 \circ \alpha_1]{\gamma_1 \circ \gamma_2} \mathbb{D}_3$$

- Example

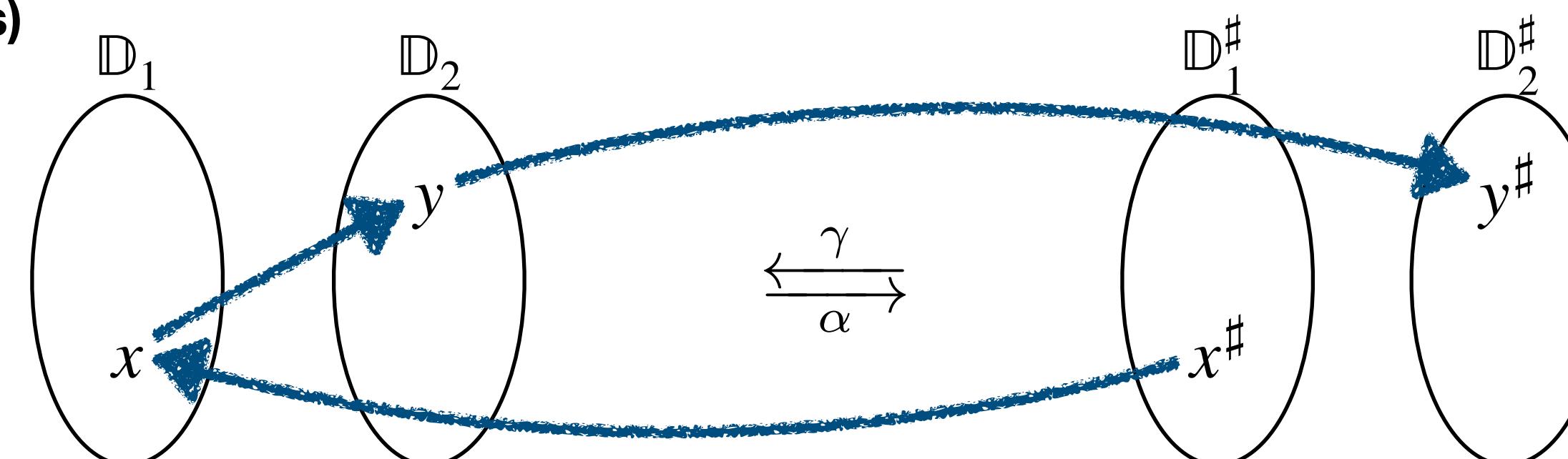
- $(\mathbb{S} \rightarrow \wp(\mathbb{Z})) \xrightleftharpoons[\alpha_1]{\gamma_1} \wp(\mathbb{Z}) \xrightleftharpoons[\alpha_2]{\gamma_2} \{\perp, -, 0, +, \top\}$

# Deriving Galois Connections (3)

Given two Galois connections  $\mathbb{D}_1 \xrightleftharpoons[\alpha_1]{\gamma_1} \mathbb{D}_1^\sharp$  and  $\mathbb{D}_2 \xrightleftharpoons[\alpha_2]{\gamma_2} \mathbb{D}_2^\sharp$

- $\mathbb{D}_1 \times \mathbb{D}_2 \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}_1^\sharp \times \mathbb{D}_2^\sharp$  where  $\alpha = \lambda \langle x, y \rangle. \langle \alpha_1(x), \alpha_2(y) \rangle$
- $\mathbb{D}_1 + \mathbb{D}_2 \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}_1^\sharp + \mathbb{D}_2^\sharp$  where  $\alpha = \lambda x. \begin{cases} \alpha_1(x) & \text{if } x \in \mathbb{D}_1 \\ \alpha_2(x) & \text{if } x \in \mathbb{D}_2 \end{cases}$
- $\mathbb{D}_1 \rightarrow \mathbb{D}_2 \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}_1^\sharp \rightarrow \mathbb{D}_2^\sharp$  where  $\alpha = \lambda f. \alpha_2 \circ f \circ \gamma_1$

(set of monotone functions)



# Deriving Galois Connections (4)

Given two Galois connections  $\wp(\mathbb{A}) \xrightleftharpoons[\alpha_1]{\gamma_1} \mathbb{D}_1^\sharp$  and  $\wp(\mathbb{B}) \xrightleftharpoons[\alpha_2]{\gamma_2} \mathbb{D}_2^\sharp$

- $\wp(\mathbb{A} \times \mathbb{B}) \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}_1^\sharp \times \mathbb{D}_2^\sharp$  where  $\alpha = \lambda X. \langle \alpha_1(\{a \mid \langle a, b \rangle \in X\}), \alpha_2(\{b \mid \langle a, b \rangle \in X\}) \rangle$
- $\wp(\mathbb{A} \times \mathbb{B}) \xrightleftharpoons[\alpha]{\gamma} \mathbb{A}' \rightarrow \mathbb{D}_2^\sharp$  where  $\alpha = \lambda X. \{a \mapsto \alpha_2(S) \mid \langle a, b \rangle \in X, S = \{b \mid \langle a, b \rangle \in X\}\}$  and  $\mathbb{A}' \subseteq \mathbb{A}$
- $\wp(\mathbb{A} + \mathbb{B}) \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}_1^\sharp \times \mathbb{D}_2^\sharp$  where  $\alpha = \lambda X. \langle \alpha_1(X \cap \mathbb{A}), \alpha_2(X \cap \mathbb{B}) \rangle$
- $\wp(\mathbb{A}) \rightarrow \wp(\mathbb{B}) \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}_1^\sharp \rightarrow \mathbb{D}_2^\sharp$  where  $\alpha = \lambda f. \alpha_2 \circ f \circ \gamma_1$   
**(set of monotone functions)**

# Example

- Concrete domain:  $\mathbb{D} = \wp(\mathbb{M}) \rightarrow \wp(\mathbb{M})$  where  $\mathbb{M} = \mathbb{X} \rightarrow \mathbb{Z}$
- Abstract domain:  $\mathbb{D}^\sharp = \mathbb{M}^\sharp \rightarrow \mathbb{M}^\sharp$  where  $\mathbb{M}^\sharp = \mathbb{X} \rightarrow \mathbb{Z}^\sharp$
- Galois connection:  $\mathbb{D} \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}^\sharp$ 
  - Memory abstraction:  $\wp(\mathbb{M}) \xrightleftharpoons[\alpha_{\mathbb{M}}]{\gamma_{\mathbb{M}}} \mathbb{M}^\sharp$  via  $\wp(\mathbb{X} \rightarrow \mathbb{Z}) \xrightleftharpoons[\alpha_{\mathbb{M}_1}]{\gamma_{\mathbb{M}_1}} \mathbb{X} \rightarrow \wp(\mathbb{Z}) \xrightleftharpoons[\alpha_{\mathbb{M}_2}]{\gamma_{\mathbb{M}_2}} \mathbb{X} \rightarrow \mathbb{Z}^\sharp$ 
$$\alpha_{\mathbb{M}_1} : \wp(\mathbb{X} \rightarrow \mathbb{Z}) \rightarrow (\mathbb{X} \rightarrow \wp(\mathbb{Z}))$$
$$\alpha_{\mathbb{M}_1} = \lambda M. \lambda x. \bigcup_{m \in M} m(x)$$
$$\alpha_{\mathbb{M}_2} : (\mathbb{X} \rightarrow \wp(\mathbb{Z})) \rightarrow (\mathbb{X} \rightarrow \mathbb{Z}^\sharp)$$
$$\alpha_{\mathbb{M}_2} = \lambda m. \lambda x. \alpha_{\mathbb{Z}}(m(x))$$
  - Value abstraction:  $\wp(\mathbb{Z}) \xrightleftharpoons[\alpha_{\mathbb{Z}}]{\gamma_{\mathbb{Z}}} \mathbb{Z}^\sharp$

# Requirement 2: $F$ and $F^\#$

- $F^\#$  is a sound abstraction of  $F$  (option 1)

$$F \circ \gamma \sqsubseteq \gamma \circ F^\#$$

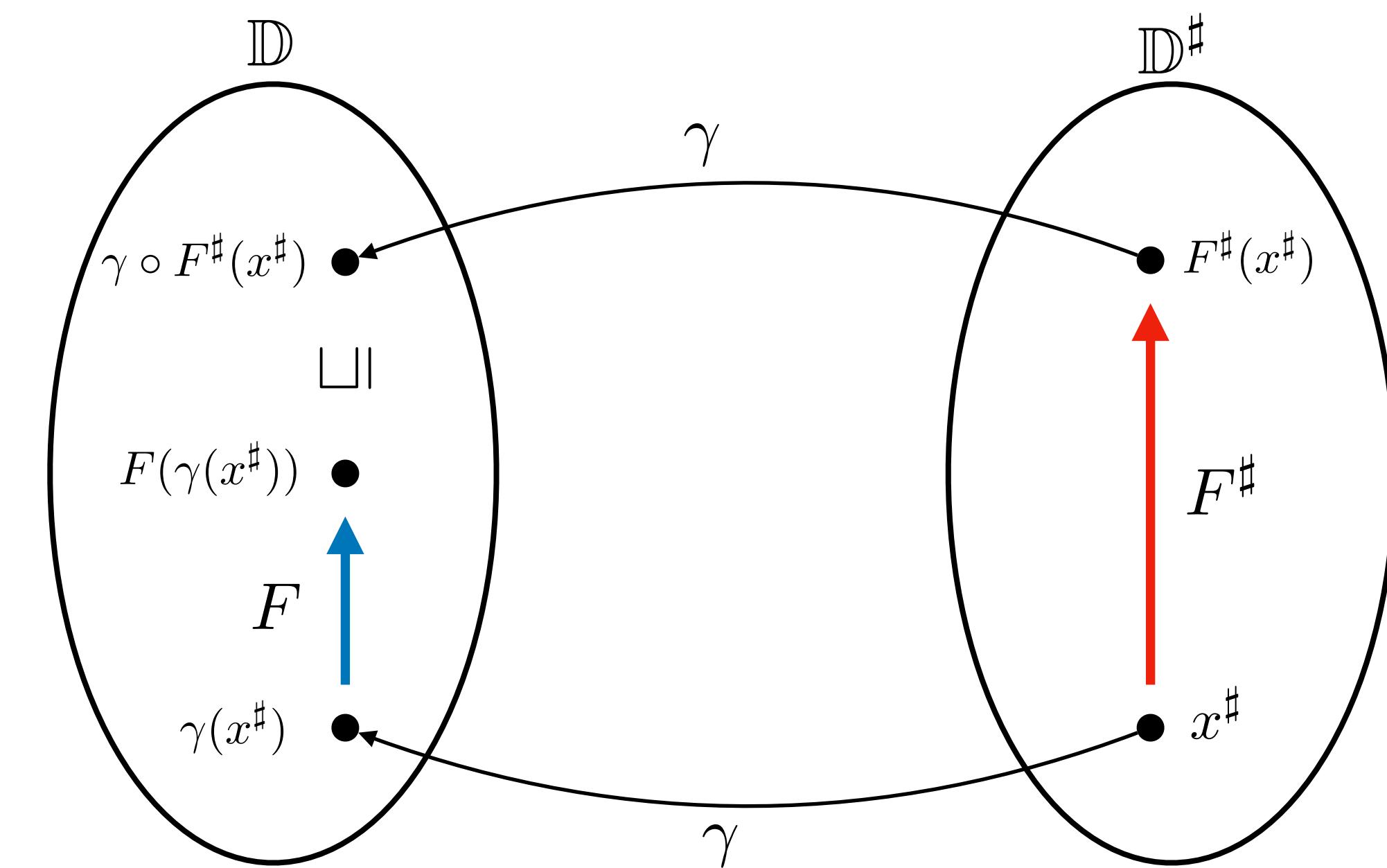
- $F^\#$  is a sound abstraction of  $F$  (option 2)

$$x \sqsubseteq \gamma(x^\#) \implies F(x) \sqsubseteq \gamma(F^\#(x^\#))$$

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

# Sound Abstract Semantics (1)

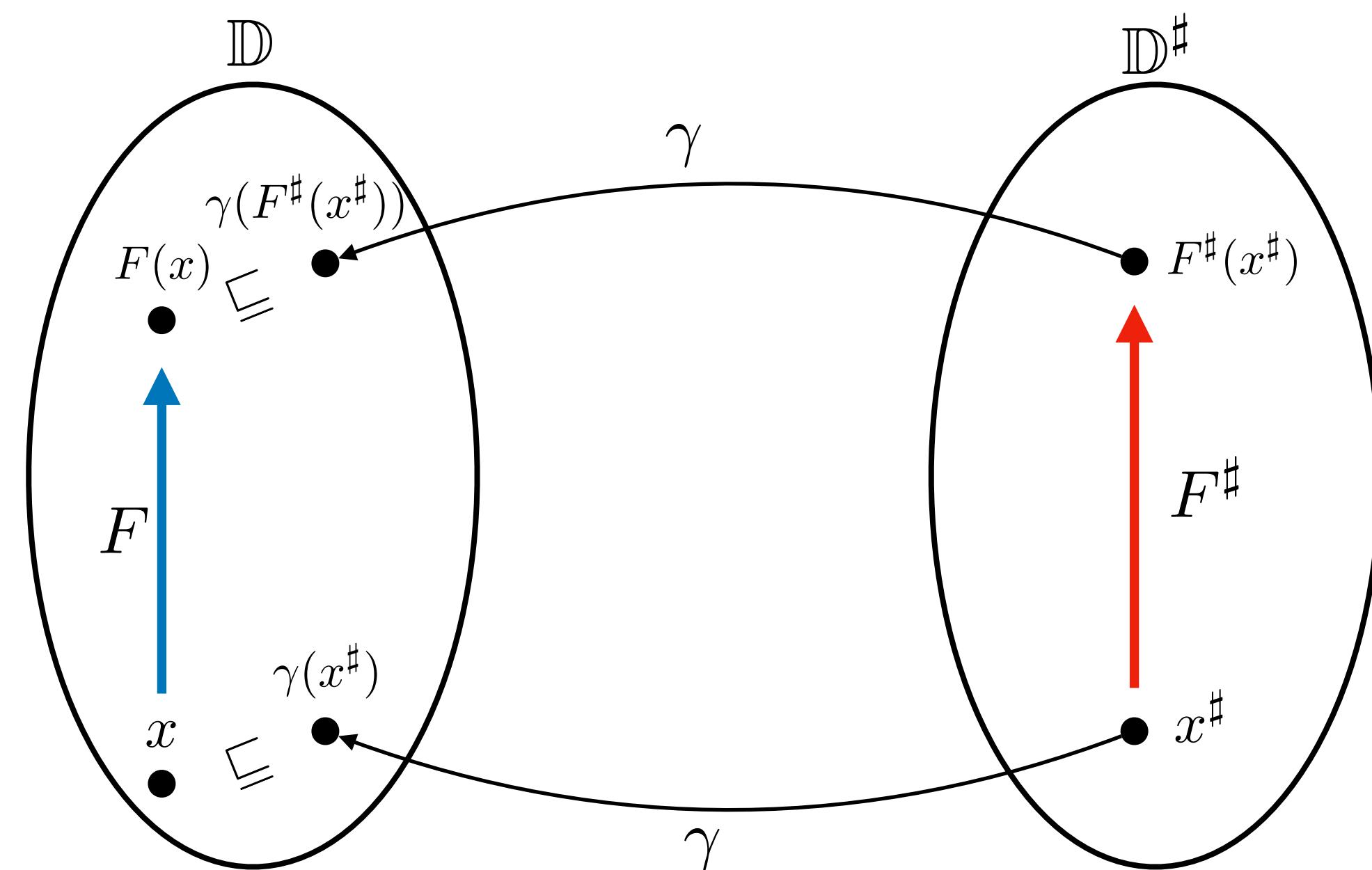
$$F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$$



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

# Sound Abstract Semantics (2)

$$x \sqsubseteq \gamma(x^\sharp) \implies F(x) \sqsubseteq \gamma(F^\sharp(x^\sharp))$$



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

# Soundness

- Static analysis result  $\bigsqcup_{i \geq 0} F^{\sharp i}(\perp)$  soundly subsumes all possible executions

$$\text{lfp } F \sqsubseteq \gamma\left(\bigsqcup_{i \geq 0} F^{\sharp i}(\perp)\right)$$

- How to guarantee the soundness?
- How to compute the sound result within finite time?

# Fixpoint Transfer Theorems

- With option 1

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

$$\text{lfp } F \sqsubseteq \gamma \left( \bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp) \right).$$

- With option 2

**Theorem** (Fixpoint Transfer 2). *Let  $\mathbb{D}$  and  $\mathbb{D}^\sharp$  be related by Galois connection  $\mathbb{D} \xrightleftharpoons[\alpha]{\gamma} \mathbb{D}^\sharp$ . Let  $F : \mathbb{D} \rightarrow \mathbb{D}$  be a continuous function and  $F^\sharp : \mathbb{D}^\sharp \rightarrow \mathbb{D}^\sharp$  be a monotone or extensive function such that  $x \sqsubseteq \gamma(x^\sharp) \implies F(x) \sqsubseteq \gamma(F^\sharp(x^\sharp))$ . Then,*

$$\text{lfp } F \sqsubseteq \gamma \left( \bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp) \right).$$

# Proof

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

$$\text{lfp } F \sqsubseteq \gamma\left(\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp)\right).$$

## Proof.

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

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

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

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

# Abstraction of Compositions

- Composition of sound semantic functions is also sound

$$\begin{array}{ccc} \mathbb{D}_1 & \xrightleftharpoons[\alpha_1]{\gamma_1} & \mathbb{D}_1^\# \\ f \downarrow & & \downarrow f^\# \\ \mathbb{D}_2 & \xrightleftharpoons[\alpha_2]{\gamma_2} & \mathbb{D}_2^\# \\ g \downarrow & & \downarrow g^\# \\ \mathbb{D}_3 & \xrightleftharpoons[\alpha_3]{\gamma_3} & \mathbb{D}_3^\# \end{array} \longrightarrow g \circ f \circ \gamma_1 \sqsubseteq \gamma_3 \circ g^\# \circ f^\#$$

- Implication: soundness proof can be compositional

# Abstract Semantics of Expressions

$$\llbracket E \rrbracket^\sharp : \mathbb{M}^\sharp \rightarrow \mathbb{Z}^\sharp$$

$$\llbracket n \rrbracket^\sharp = \lambda m^\sharp. \alpha(\{n\})$$

$$\llbracket x \rrbracket^\sharp = \lambda m^\sharp. m^\sharp(x)$$

$$\llbracket E_1 \odot E_2 \rrbracket^\sharp = \lambda m^\sharp. \llbracket E_1 \rrbracket^\sharp(m^\sharp) \odot^\sharp \llbracket E_2 \rrbracket^\sharp(m^\sharp)$$

- Example
  - Sign domain  $\mathbb{Z}^\sharp = \{\perp, -, 0, +, \top\}$
  - Interval domain  $\mathbb{Z}^\sharp = \{\perp\} \cup \{[a, b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\}$
  - Soundness:  $\llbracket E \rrbracket_\wp \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{Z}} \circ \llbracket E \rrbracket^\sharp$

# Example: Binary Operator

$$\wp(\mathbb{Z}) \xrightleftharpoons[\alpha]{\gamma} \{\perp, -, 0, +, \top\}$$

- Define an abstract addition operator  $+^\sharp : \mathbb{Z}^\sharp \rightarrow \mathbb{Z}^\sharp \rightarrow \mathbb{Z}^\sharp$  (as precise as possible)

	$\perp$	$-$	$0$	$+$	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
$-$	$\perp$	$-$	$-$	$\top$	$\top$
$0$	$\perp$	$-$	$0$	$+$	$\top$
$+$	$\perp$	$\top$	$+$	$+$	$\top$
$\top$	$\perp$	$\top$	$\top$	$\top$	$\top$

# Soundness Proof

$$\llbracket E \rrbracket_{\wp} \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{Z}} \circ \llbracket E \rrbracket^{\sharp}$$

- $E : n$

$$\begin{aligned}\llbracket n \rrbracket_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) &= \{n\} \\ &= \gamma_{\mathbb{Z}} \circ \llbracket n \rrbracket^{\sharp}(m^{\sharp})\end{aligned}$$

- $E : x$

$$\begin{aligned}\llbracket x \rrbracket_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) &= \llbracket x \rrbracket_{\wp} \{m \mid \forall x. m(x) \in \gamma_{\mathbb{Z}}(m^{\sharp}(x))\} \\ &= \{m(x) \mid \forall x. m(x) \in \gamma_{\mathbb{Z}}(m^{\sharp}(x))\} \\ &= \gamma_{\mathbb{Z}}(m^{\sharp}(x)) \\ &= \gamma_{\mathbb{Z}} \circ \llbracket x \rrbracket^{\sharp}(m^{\sharp})\end{aligned}$$

- $E : E_1 \odot E_2$

- Exercise!
- For each operator, prove using induction

# Abstract Semantics of Conditions

$$\llbracket B \rrbracket^\# : \mathbb{M}^\# \rightarrow \mathbb{M}^\#$$

$$\llbracket \text{true} \rrbracket^\# = \lambda m^\#. m^\#$$

$$\llbracket \text{false} \rrbracket^\# = \lambda m^\#. \perp$$

- Example

- Sign domain

$$\llbracket x < 0 \rrbracket^\# = \lambda m^\#. \begin{cases} \perp & \text{if } m^\#(x) \in \{+, 0, \perp\} \\ m^\# \{x \mapsto -\} & \text{o.w.} \end{cases}$$

- Interval domain

$$\llbracket x < n \rrbracket^\# = \lambda m^\#. \begin{cases} \perp & \text{if } m^\#(x) = [a, b] \wedge a > n \\ m^\# \{x \mapsto [a, n-1]\} & \text{if } a \leq n \leq b \\ m^\# & \text{if } b < n \end{cases}$$

- Soundness:  $\llbracket B \rrbracket_\wp \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ \llbracket B \rrbracket^\#$

# Soundness Proof

$$\llbracket B \rrbracket_{\wp} \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ \llbracket B \rrbracket^{\sharp}$$

- $B : x < 0$  and  $\llbracket x < 0 \rrbracket^{\sharp} = \lambda m^{\sharp}. \begin{cases} \perp & \text{if } m^{\sharp}(x) \in \{+, 0, \perp\} \\ m^{\sharp}\{x \mapsto -\} & \text{o.w.} \end{cases}$

$$\begin{aligned} \llbracket x < 0 \rrbracket_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) &= \llbracket x < 0 \rrbracket_{\wp}\{m \mid \forall i. m(i) \in \gamma_{\mathbb{Z}}(m^{\sharp}(i))\} \\ &= \{m \mid \forall i. m(i) \in \gamma_{\mathbb{Z}}(m^{\sharp}(i)), m(x) < 0\} \end{aligned}$$

- Case 1:  $m^{\sharp}(x) \in \{+, 0, \perp\}$

$$LHS = \emptyset = RHS$$

- Case 2:  $m^{\sharp}(x) \in \{-, \top\}$

$$\begin{aligned} \gamma_{\mathbb{M}} \circ \llbracket x < 0 \rrbracket^{\sharp}(m^{\sharp}) &= \gamma_{\mathbb{M}}(m^{\sharp}\{x \mapsto -\}) \\ &= \{m \mid \forall i. m(i) \in \gamma_{\mathbb{Z}}(m^{\sharp}\{x \mapsto -\}(i)), m(x) < 0\} \\ &= LHS \end{aligned}$$

# Abstract Semantics of Commands

$$\llbracket C \rrbracket^\# : \mathbb{M}^\# \rightarrow \mathbb{M}^\#$$

$$\llbracket \text{skip} \rrbracket^\# = \lambda m^\#. m^\#$$

$$\llbracket C_0 ; C_1 \rrbracket^\# = \lambda m^\#. \llbracket C_1 \rrbracket^\# \circ \llbracket C_0 \rrbracket^\#(m^\#)$$

$$\llbracket x := E \rrbracket^\# = \lambda m^\#. m^\# \{x \mapsto \llbracket E \rrbracket^\#(m^\#)\}$$

$$\llbracket \text{input}(x) \rrbracket^\# = \lambda m^\#. m^\# \{x \mapsto \alpha(\mathbb{Z})\}$$

$$\llbracket \text{if } B \text{ then } C_1 \text{ else } C_2 \rrbracket^\# = \lambda m^\#. \llbracket C_1 \rrbracket^\# \circ \llbracket B \rrbracket^\#(m^\#) \sqcup \llbracket C_2 \rrbracket^\# \circ \llbracket \neg B \rrbracket^\#(m^\#)$$

$$\llbracket \text{while } B \text{ } C \rrbracket^\# = \lambda m^\#. \llbracket \neg B \rrbracket^\# \left( \bigsqcup_{i \geq 0} F^{\#i}(\perp) \right)$$

$$\text{where } F^\# = \lambda X. m^\# \sqcup \llbracket C \rrbracket^\# \circ \llbracket B \rrbracket^\#(X)$$

- Soundness:  $\llbracket C \rrbracket_\wp \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ \llbracket C \rrbracket^\#$  and  $\cup \circ (\gamma_{\mathbb{M}}, \gamma_{\mathbb{M}}) \subseteq \gamma_{\mathbb{M}} \circ \sqcup$

# Soundness Proof (1)

$$\llbracket C \rrbracket_{\wp} \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ \llbracket C \rrbracket^{\sharp}$$

- $C_1 ; C_2$
- $\text{if } B \text{ then } C_1 \text{ else } C_2$

$$\begin{aligned}\llbracket C_0 ; C_1 \rrbracket_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) &= \llbracket C_0 \rrbracket_{\wp} \circ \llbracket C_1 \rrbracket_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) \\ &\subseteq \llbracket C_0 \rrbracket_{\wp} \circ \gamma_{\mathbb{M}} \circ \llbracket C_1 \rrbracket^{\sharp}(m^{\sharp}) \\ &\subseteq \gamma_{\mathbb{M}} \circ \llbracket C_0 \rrbracket^{\sharp} \circ \llbracket C_1 \rrbracket^{\sharp}(m^{\sharp}) \\ &= \gamma_{\mathbb{M}} \circ \llbracket C_0 ; C_1 \rrbracket^{\sharp}(m^{\sharp})\end{aligned}$$

$$\begin{aligned}&\llbracket \text{if } B \text{ then } C_1 \text{ else } C_2 \rrbracket_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) \\ &= \llbracket C_1 \rrbracket_{\wp} \circ \llbracket B \rrbracket_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) \cup \llbracket C_2 \rrbracket_{\wp} \circ \llbracket \neg B \rrbracket_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) \\ &\subseteq \llbracket C_1 \rrbracket_{\wp} \circ \gamma_{\mathbb{M}} \circ \llbracket B \rrbracket^{\sharp}(m^{\sharp}) \cup \llbracket C_2 \rrbracket_{\wp} \circ \gamma_{\mathbb{M}} \circ \llbracket B \rrbracket^{\sharp}(m^{\sharp}) \\ &\subseteq \gamma_{\mathbb{M}} \circ \llbracket C_1 \rrbracket^{\sharp} \circ \llbracket B \rrbracket^{\sharp}(m^{\sharp}) \cup \gamma_{\mathbb{M}} \circ \llbracket C_2 \rrbracket^{\sharp} \circ \llbracket B \rrbracket^{\sharp}(m^{\sharp}) \\ &\subseteq \gamma_{\mathbb{M}} (\llbracket C_1 \rrbracket^{\sharp} \circ \llbracket B \rrbracket^{\sharp}(m^{\sharp}) \sqcup \llbracket C_2 \rrbracket^{\sharp} \circ \llbracket B \rrbracket^{\sharp}(m^{\sharp})) \\ &= \gamma_{\mathbb{M}} \circ \llbracket \text{if } B \text{ then } C_1 \text{ else } C_2 \rrbracket^{\sharp}(m^{\sharp})\end{aligned}$$

# Soundness Proof (2)

$$\llbracket C \rrbracket_{\wp} \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ \llbracket C \rrbracket^{\sharp}$$

- `while B C`

$$\llbracket \text{while } B \text{ } C \rrbracket_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp})$$

$$= \llbracket \neg B \rrbracket_{\wp} (\text{lfp} \lambda X. \gamma_{\mathbb{M}}(m^{\sharp}) \cup \llbracket C \rrbracket_{\wp} \circ \llbracket B \rrbracket_{\wp}(X))$$

$$\subseteq \llbracket \neg B \rrbracket_{\wp} \circ \gamma_{\mathbb{M}} \left( \bigsqcup_{i \geq 0} F^{\sharp i}(\perp) \right)$$

$$\subseteq \gamma_{\mathbb{M}} \circ \llbracket \neg B \rrbracket^{\sharp} \left( \bigsqcup_{i \geq 0} F^{\sharp i}(\perp) \right)$$

where  $F^{\sharp} = \lambda X. m^{\sharp} \sqcup \llbracket C \rrbracket^{\sharp} \circ \llbracket B \rrbracket^{\sharp}(X)$

- $(\text{lfp} \lambda X. \gamma_{\mathbb{M}}(m^{\sharp}) \cup \llbracket C \rrbracket_{\wp} \circ \llbracket B \rrbracket_{\wp}(X)) \subseteq \gamma_{\mathbb{M}} \left( \bigsqcup_{i \geq 0} F^{\sharp i}(\perp) \right)$

This holds by the fixed point transfer theorem if  $F \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ F^{\sharp}$

$$(\lambda X. \gamma_{\mathbb{M}}(m^{\sharp}) \cup \llbracket C \rrbracket_{\wp} \circ \llbracket B \rrbracket_{\wp}(X)) \circ \gamma_{\mathbb{M}}(m^{\sharp})$$

$$= \gamma_{\mathbb{M}}(m^{\sharp}) \cup \llbracket C \rrbracket_{\wp} \circ \llbracket B \rrbracket_{\wp}(\gamma_{\mathbb{M}}(m^{\sharp}))$$

$$\subseteq \gamma_{\mathbb{M}}(m^{\sharp}) \cup \llbracket C \rrbracket_{\wp} \circ \gamma_{\mathbb{M}} \circ \llbracket B \rrbracket^{\sharp}(m^{\sharp})$$

$$\subseteq \gamma_{\mathbb{M}}(m^{\sharp}) \cup \gamma_{\mathbb{M}} \circ \llbracket C \rrbracket^{\sharp} \circ \llbracket B \rrbracket^{\sharp}(m^{\sharp})$$

$$\subseteq \gamma_{\mathbb{M}}(m^{\sharp} \sqcup \llbracket C \rrbracket^{\sharp} \circ \llbracket B \rrbracket^{\sharp}(m^{\sharp}))$$

$$= \gamma_{\mathbb{M}} \circ (\lambda X. m^{\sharp} \sqcup \llbracket C \rrbracket^{\sharp} \circ \llbracket B \rrbracket^{\sharp}(X))(m^{\sharp})$$

# Summary

- Abstract semantics: a **sound approximation** of the concrete semantics
- **Soundness guarantee** by Fixpoint transfer theorem
  - Galois connection, sound abstract semantic function
- Static analysis design: design of **precise and efficient** abstract semantics
- Plan: compute the abstract semantics within a **finite time**