AN INTRODUCTION TO ABSTRACT INTERPRETATION

P. Cousot

Patrick.Cousot@ens.fr http://www.di.ens.fr/~cousot

Biarritz IFIP-WG 2.3 meeting (1)

23 — 28 mars 2003, Hotel Miramar, Biarritz, France

2.2 A Short Introduction to Abstract Interpretation Theory (see Sec. 5 of [POPL '79])

Reference

[POPL '79] P. Cousot & R. Cousot. Systematic design of program analysis frameworks. In 6^{th} *POPL*, pages 269–282, San Antonio, TX, 1979. ACM Press. 9, 99

2.2.1 Moore Family-Based Abstraction

See Sec. 5.1 of [POPL '79].

Reference

[POPL '79] P. Cousot & R. Cousot. Systematic design of program analysis frameworks. In 6^{th} *POPL*, pages 269–282, San Antonio, TX, 1979. ACM Press. 10

PROPERTIES

- We represent properties P of objects $s \in \Sigma$ as sets of objects $P \in \wp(\Sigma)$ (which have the property in question);

  Example: the property "*to be an even natural number*" is $\{0, 2, 4, 6, \ldots\}$

Complete Lattice of Properties

- The set of properties of objects Σ is a complete boolean lattice:

$$\langle \wp(\Sigma),\ \subseteq,\ \emptyset,\ \Sigma,\ \cup,\ \cap,\ \neg \rangle\ .$$

ABSTRACTION

A reasoning/computation such that:

- only some properties can be used;
- the properties that can be used are called "*abstract*";
- so, the (other concrete) properties must be approximated by the abstract ones;

Direction of Approximation

- Approximation from above: approximate P by $\overline{P}$ such that $P \subseteq \overline{P}$;
- Approximation from below: approximate P by $\underline{P}$ such that $\underline{P} \subseteq P$ (dual).

Abstract Properties

- Abstract Properties: a set $\overline{\mathcal{A}} \subsetneq \wp(\Sigma)$ of properties of interest (the only one which can be used to approximate others).

In Absence of (Upper) Approximation

- What to say when some property has no (computable) abstraction?
  - loop?
  - block?
  - ask for help?
  - say something!

I don't know

- Any property should be approximable from above by I don't know (i.e. "true" or Σ).

Minimal Approximations

- A concrete property $P \in \wp(\Sigma)$ is most precisely abstracted by any minimal upper approximation $\overline{P} \in \overline{\mathcal{A}}$:

$$P \subseteq \overline{P}$$
$$\nexists \overline{P'} \in \overline{\mathcal{A}} : P \subseteq \overline{P'} \subsetneq \overline{P}$$

- So, an abstract property $\overline{P} \in \overline{\mathcal{A}}$ is best approximated by itself.

Which Minimal Approximation is Most Useful?

- Which minimal approximation is most useful depends upon the circumstances;
- **Example** (rule of signs):
  - 0 is better approximated as positive in "$3 + 0$";
  - 0 is better approximated as negative in "$-3 + 0$".

Avoiding Backtracking

- We don't want to exhaustively try all minimal approximations;
- We want to use only one of the minimal approximations;

Which Minimal Abstraction to Use?

- Which minimal abstraction to choose?
  - make a circumstantial choice [1];
  - make a definitive arbitrary choice [2];
  - require the existence of a best choice [3].

Reference

[JLC '92] P. Cousot & R. Cousot. Abstract interpretation frameworks. *J. Logic and Comp.*, 2(4):511–547, 1992.

1 [JLC '92] uses a concretization function.
2 [JLC '92] uses an abstraction function.
3 [JLC '92] uses an abstraction/concretization Galois connection (this talk).

Best Abstraction

- We require that all concrete property $P \in \wp(\Sigma)$ have a best abstraction $\overline{P} \in \overline{\mathcal{A}}$:

$$P \subseteq \overline{P}$$
$$\forall \overline{P'} \in \overline{\mathcal{A}} : (P \subseteq \overline{P'}) \Longrightarrow (\overline{P} \subseteq \overline{P'})$$

- So, by definition of the greatest lower bound/meet $\cap$:

$$\overline{P} = \bigcap \{\overline{P'} \in \overline{\mathcal{A}} \mid P \subseteq \overline{P'}\} \in \overline{\mathcal{A}}$$

Moore Family

- So, the hypothesis that any concrete property $P \in \wp(\Sigma)$ has a best abstraction $\overline{P} \in \overline{\mathcal{A}}$ implies that:

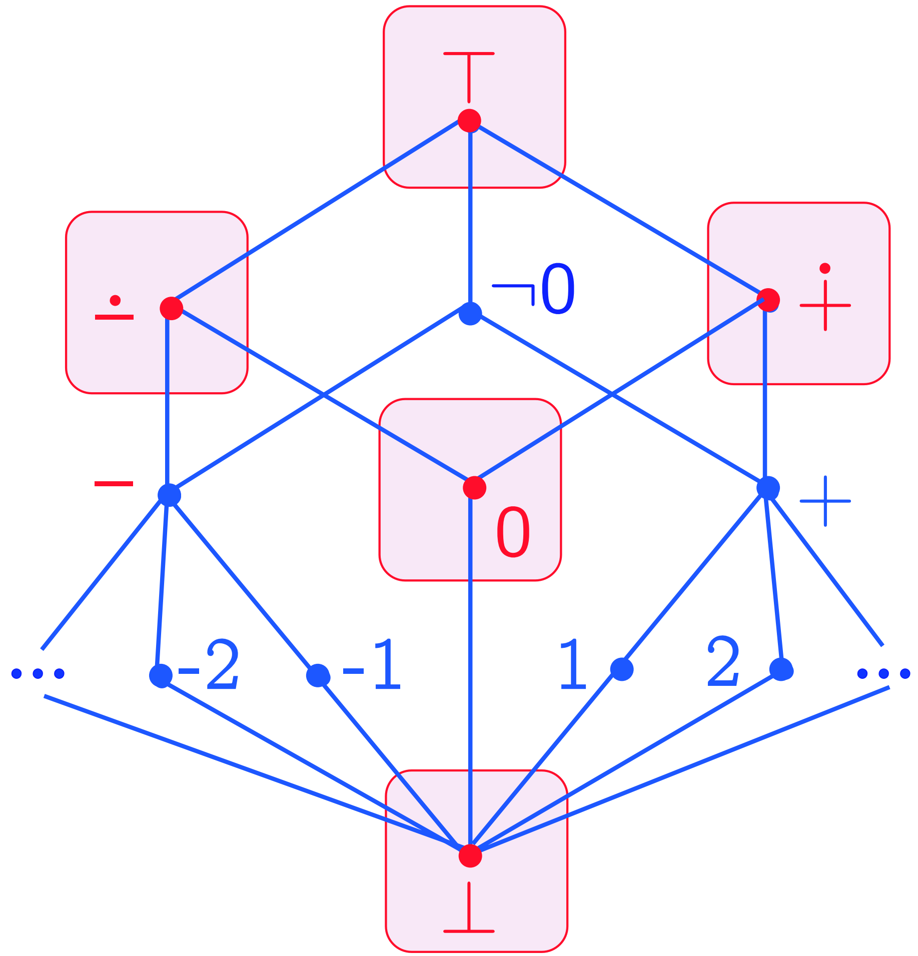
  $\overline{\mathcal{A}}$ is a Moore family

  i.e. it is closed under intersection $\bigcap$:

$$\forall S \subseteq \overline{\mathcal{A}} : \bigcap S \in \overline{\mathcal{A}}$$

- In particular $\bigcap \emptyset = \Sigma \in \overline{\mathcal{A}}$.

Example of Moore Family-Based Abstraction



The Lattice of Abstractions (1)

- The set $\mathcal{M}(\wp(\wp(\Sigma)))$ of all abstractions i.e. of Moore families on the set $\wp(\Sigma)$ of concrete properties is the complete lattice of abstractions

$$\langle \mathcal{M}(\wp(\wp(\Sigma))),\ \supseteq,\ \wp(\Sigma),\ \{\Sigma\},\ \lambda S \boldsymbol{\cdot} \mathcal{M}(\cup S),\ \cap \rangle$$

where:

$$\mathcal{M}(\overline{\mathcal{A}}) = \{\bigcap S \mid S \subseteq \overline{\mathcal{A}}\}$$

is the $\subseteq$-least Moore family containing $\overline{\mathcal{A}}$.

2.2.2 Closure Operator-Based Abstraction

See Sec. 5.2 of [POPL '79]).

Reference

[POPL '79] P. Cousot & R. Cousot. Systematic design of program analysis frameworks. In 6^{th} *POPL*, pages 269–282, San Antonio, TX, 1979. ACM Press. 26

Closure Operator Induced by an Abstraction

The map $\rho_{\overline{\mathcal{A}}}$ mapping a concrete property $P \in \wp(\Sigma)$ to its best abstraction $\rho_{\overline{\mathcal{A}}}(P)$ in $\overline{\mathcal{A}}$ is:

$$\rho_{\overline{\mathcal{A}}}(P) = \bigcap \{\overline{P} \in \overline{\mathcal{A}} \mid P \subseteq \overline{P}\} \ .$$

It is a closure operator:

- extensive,
- idempotent,
- isotone/monotonic;

such that

$$P \in \bar{\mathcal{A}} \Longleftrightarrow P = \rho_{\overline{\mathcal{A}}}(P)$$

hence

$$\overline{\mathcal{A}} = \rho_{\overline{\mathcal{A}}}(\wp(\Sigma)).$$

Abstraction Induced by a Closure Operator

- Any closure operator ρ on the set of properties $\wp(\Sigma)$ induces an abstraction:

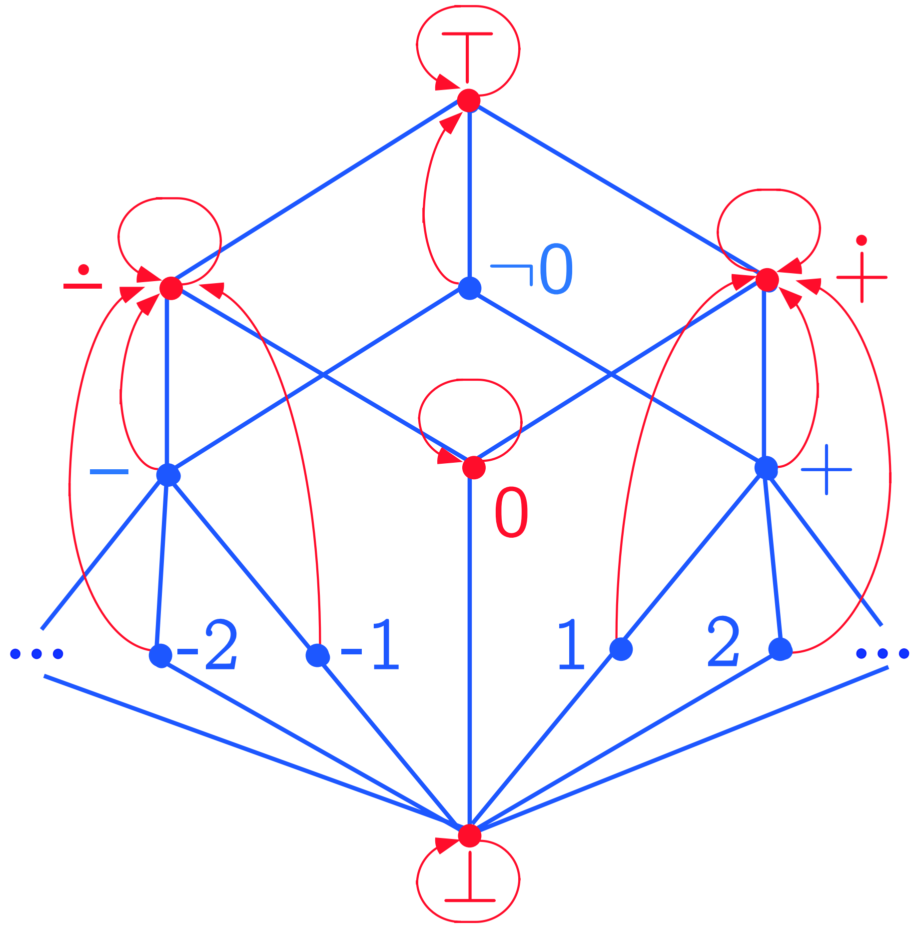
$$\rho(\wp(\Sigma)).$$

Examples:

  - $\lambda P \cdot P$ the most precise abstraction (identity),
  - $\lambda P \cdot \Sigma$ the most imprecise abstraction (I don't know).

- Closure operators are isomorphic to the Moore families (i.e. their fixpoints).

Example of Closure Operator-Based Abstraction



The Lattice of Abstractions (2)

- The set $\mathbf{clo}(\wp(\Sigma) \longmapsto \wp(\Sigma))$ of all abstractions, i.e. isomorphically, closure operators ρ on the set $\wp(\Sigma)$ of concrete properties is the complete lattice of abstractions for pointwise inclusion [4]:

$$\langle \mathbf{clo}(\wp(\Sigma) \longmapsto \wp(\Sigma)),\ \dot{\subseteq},\ \lambda P \cdot P,\ \lambda P \cdot \Sigma,\ \lambda S \cdot \mathbf{ide}(\dot{\bigcup} S),\ \dot{\bigcap} \rangle$$

where:

  - the lub $\lambda S \cdot \mathbf{ide}(\dot{\bigcup} S)$ is the reduced product;
  - $\mathbf{ide}(\rho) = \mathrm{lfp}_{\rho}^{\dot{\subseteq}}\ \lambda f \cdot f \circ f$ is the $\dot{\subseteq}$-least idempotent operator on $\wp(\Sigma)$ $\dot{\subseteq}$-greater than ρ.

[4] M. Ward, *The closure operators of a lattice*, Annals Math., 43(1942), 191–196.

2.2.4 Galois Connection-Based Abstraction

See Sec. 5.3 of [POPL '79]).

Reference

[POPL '79] P. Cousot & R. Cousot. Systematic design of program analysis frameworks. In 6^{th} *POPL*, pages 269–282, San Antonio, TX, 1979. ACM Press. 38

Correspondance Between Concrete and Abstract Properties

- For closure operators ρ, we have:

$$\rho(P) \subseteq \rho(P') \;\Leftrightarrow\; P \subseteq \rho(P')$$

written:

$$\langle \wp(\Sigma),\ \subseteq\rangle \xleftrightarrows[\rho]{1} \langle \rho(\wp(\Sigma)),\ \subseteq\rangle$$

where 1 is the identity and:

$$\langle \wp(\Sigma),\ \subseteq\rangle \xleftrightarrows[\alpha]{\gamma} \langle \overline{\mathcal{D}},\ \sqsubseteq\rangle$$

means that $\langle \alpha,\ \gamma\rangle$ is a Galois connection:

– $\forall P \in \wp(\Sigma), \overline{P} \in \overline{\mathcal{D}} : \alpha(P) \sqsubseteq \overline{P} \;\Leftrightarrow\; P \subseteq \gamma(\overline{P})$;

– α is onto (equivalently $\alpha \circ \gamma = 1$ or γ is one-to-one).

Abstract Domain

- Abstract Domain: an isomorphic representation $\overline{\mathcal{D}}$ of the set $\overline{\mathcal{A}} \subsetneq \wp(\Sigma) = \rho(\wp(\Sigma))$ of abstract properties (up to some order-isomorphism ι).

Galois Surjection [6]

- We have the Galois surjection:

$$\langle \wp(\Sigma),\ \subseteq\rangle \xleftarrow[\iota\circ\rho]{\iota^{-1}} \rightarrow\!\!\!\!\rightarrow \langle \overline{\mathcal{D}},\ \sqsubseteq\rangle$$

- More generally:

$$\langle \wp(\Sigma),\ \subseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \overline{\mathcal{D}},\ \sqsubseteq\rangle$$

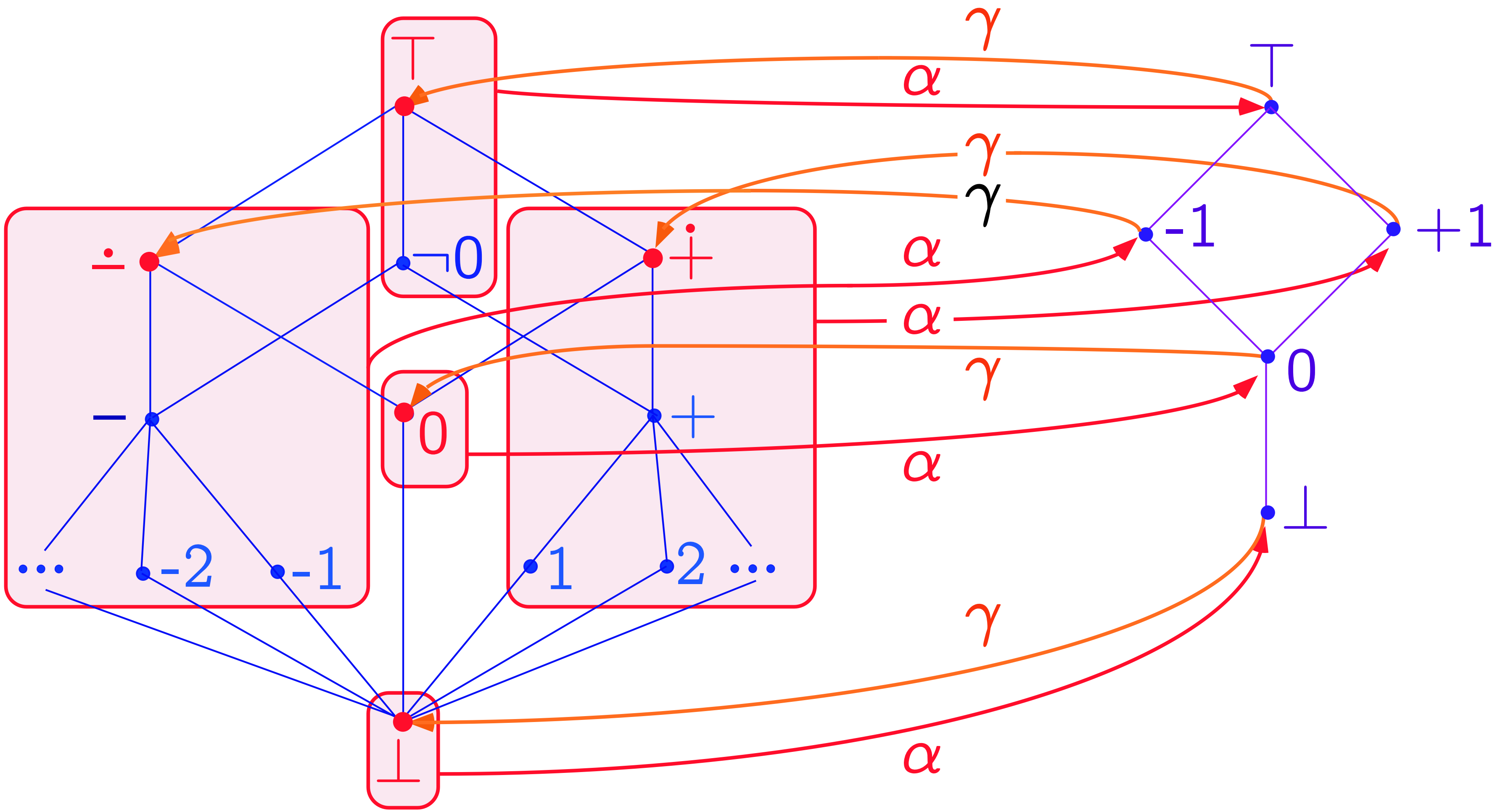
denoting (again) the fact that:

– $\forall P \in \wp(\Sigma), \overline{P} \in \overline{\mathcal{D}} : \alpha(P) \sqsubseteq \overline{P} \ \Leftrightarrow\ P \subseteq \gamma(\overline{P})$;

– α is onto (equivalently $\alpha \circ \gamma = 1$ or γ is one-to-one).

[6] Also called Galois insertion since γ is injective.

Example of Galois Surjection-Based Abstraction



Galois Connection

- Relaxing the condition that α is onto:

$$\langle \wp(\Sigma),\ \subseteq \rangle \xleftrightarrow[\alpha]{\gamma} \langle \overline{\mathcal{D}},\ \sqsubseteq \rangle$$

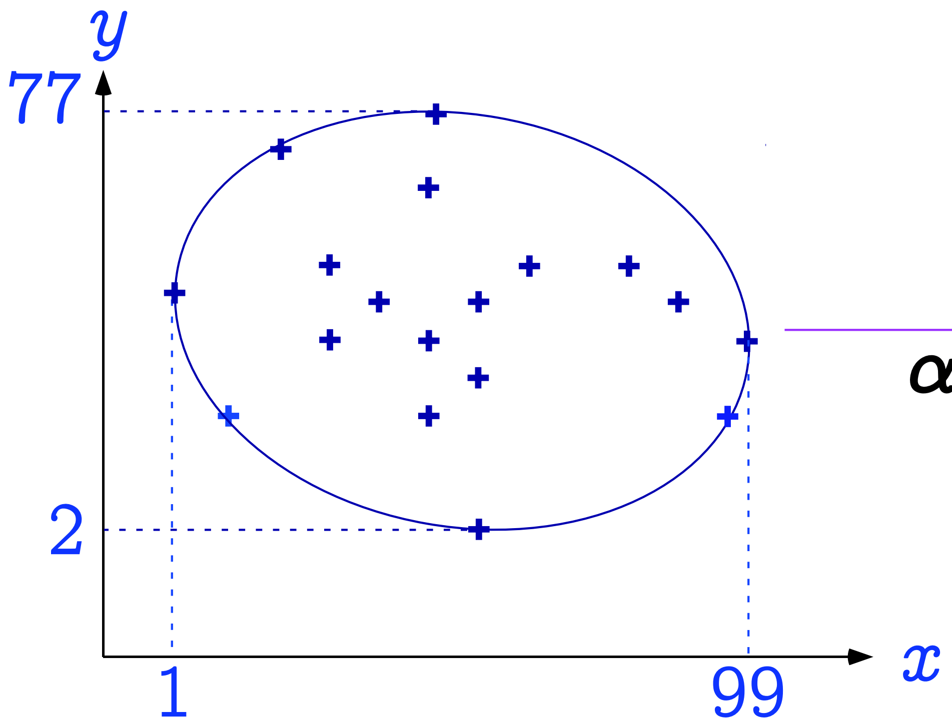
  that is to say:

$$\forall P \in \wp(\Sigma), \overline{P} \in \overline{\mathcal{D}} : \alpha(P) \sqsubseteq \overline{P} \iff P \subseteq \gamma(\overline{P});$$

- i.e. ρ is now $\gamma \circ \alpha$;

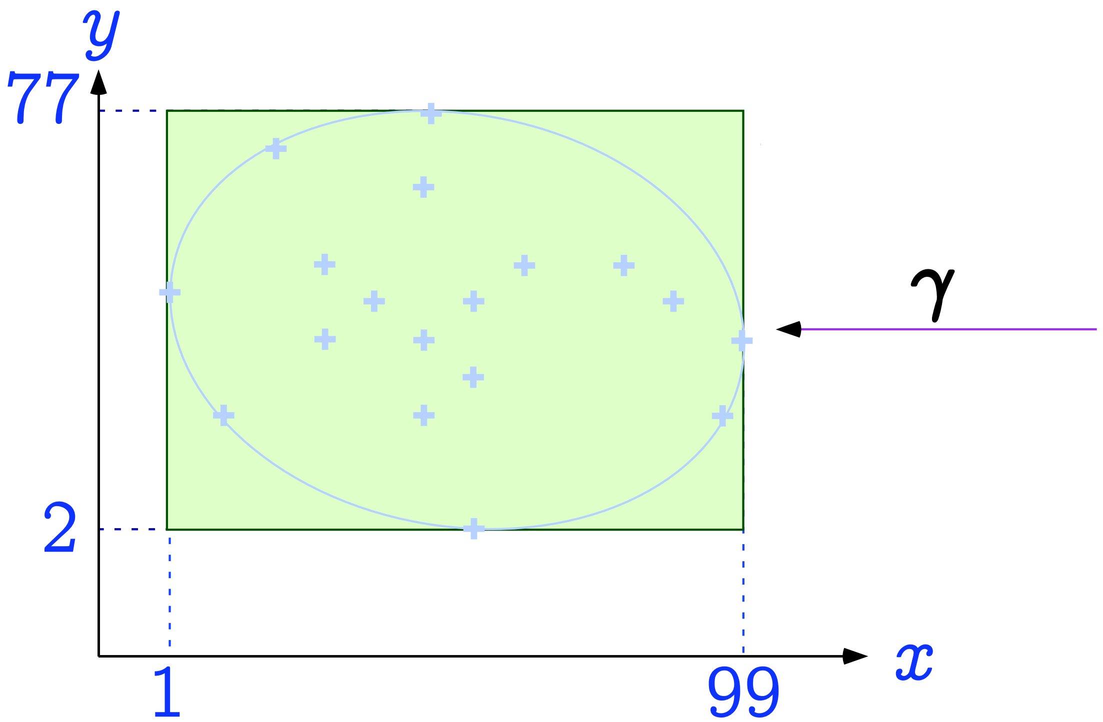
  We can now have different representations of the same abstract property.

Abstraction α



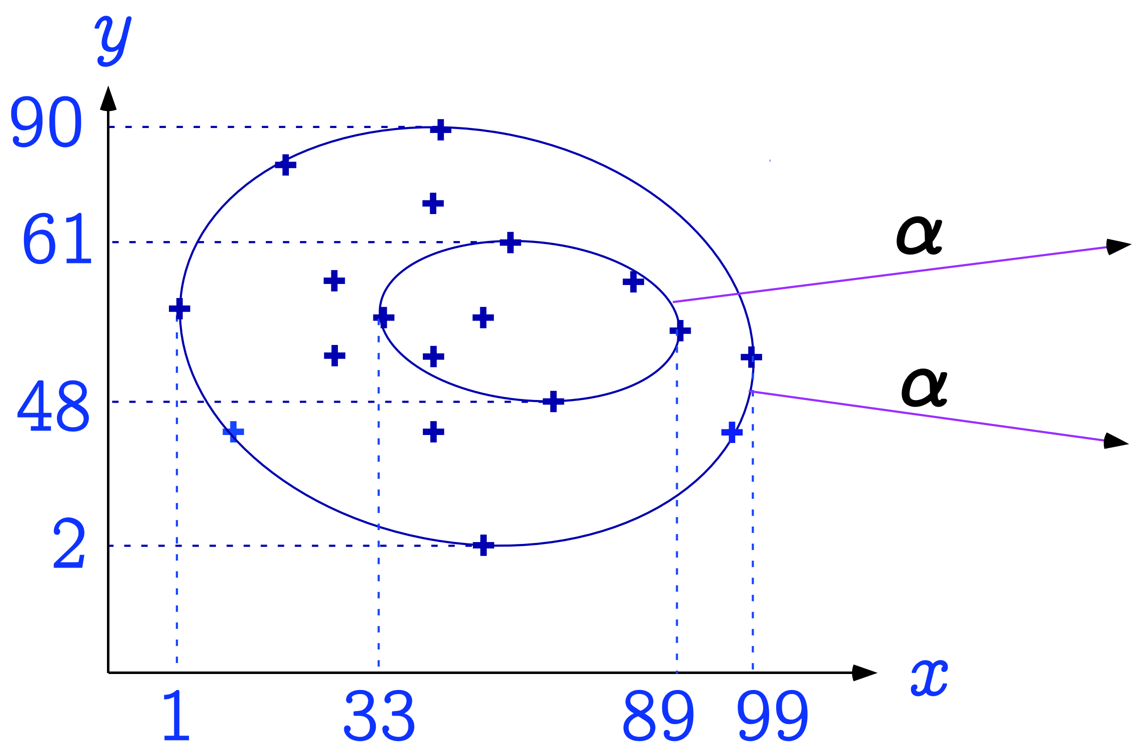
$$\xrightarrow{\boldsymbol{\alpha}} \{x : [1, 99], y : [2, 77]\}$$

Concretization γ



$\{x : [1, 99], y : [2, 77]\}$

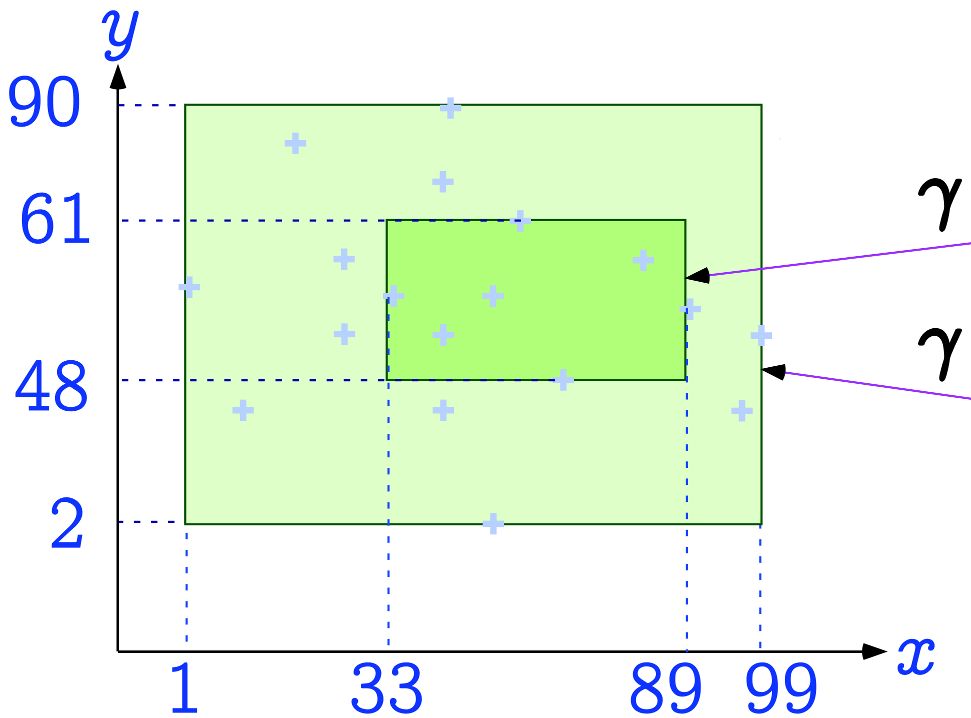
The Abstraction α is Monotone



$$\{x : [33, 89], y : [48, 61]\}$$
$$\sqsubseteq$$
$$\{x : [1, 99], y : [2, 90]\}$$

$$X \subseteq Y \Rightarrow \alpha(X) \sqsubseteq \alpha(Y)$$

The Concretization γ is Monotone



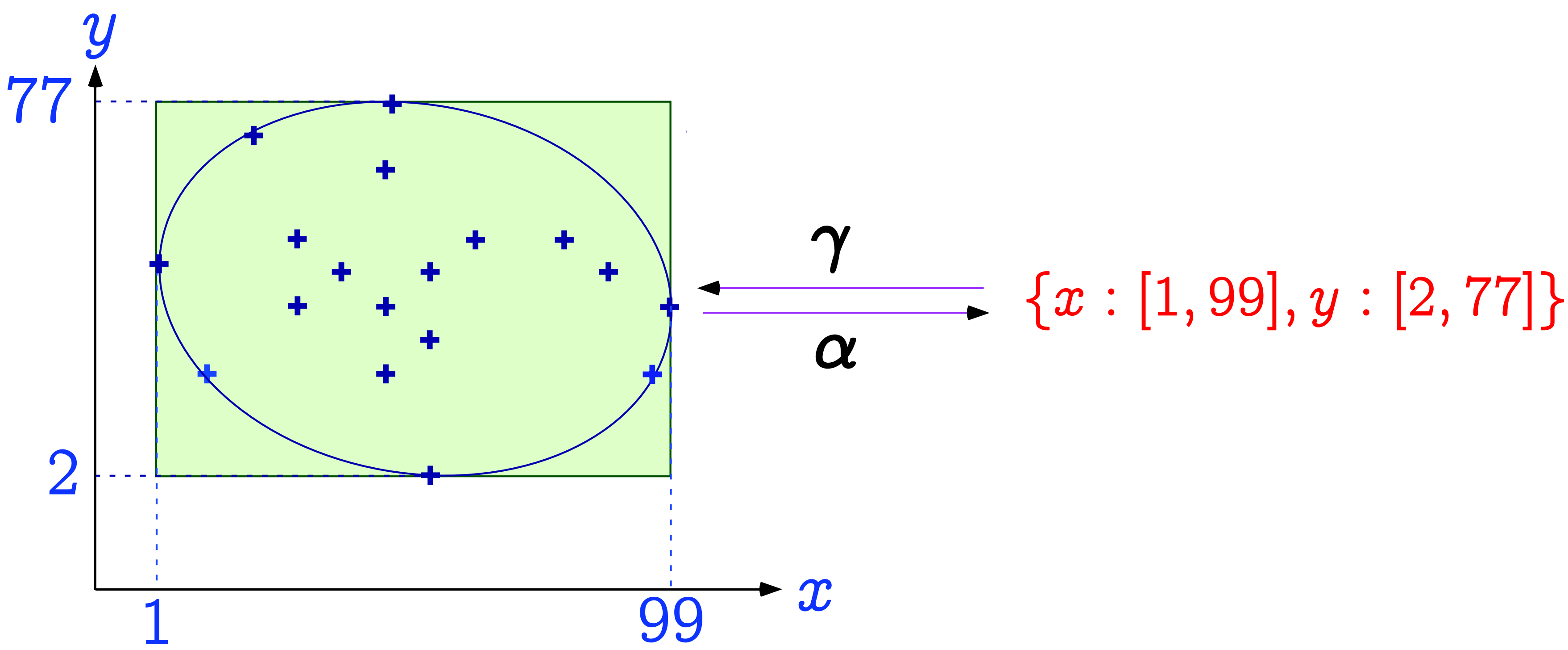
$\{x : [33, 89], y : [48, 61]\}$

$\sqsubseteq$

$\{x : [1, 99], y : [2, 90]\}$

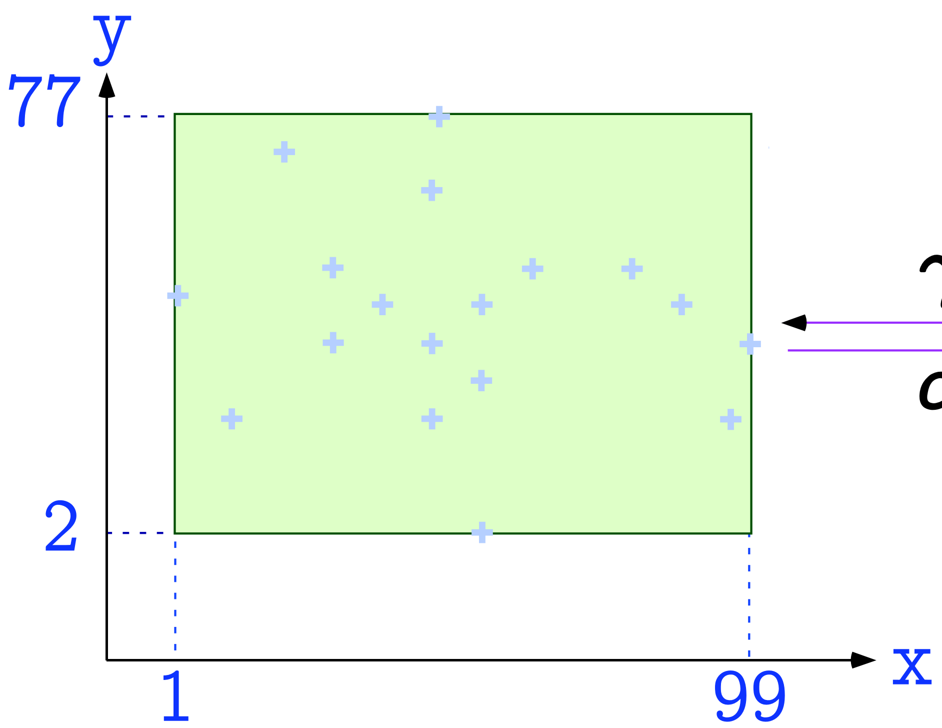
$$X \sqsubseteq Y \Rightarrow \gamma(X) \subseteq \gamma(Y)$$

The $\gamma \circ \alpha$ Composition is Extensive



$$X \subseteq \gamma \circ \alpha(X)$$

The $\alpha \circ \gamma$ Composition is Reductive



$$\{x : [1, 99], y : [2, 77]\} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}}$$

$$\{x : [1, 99], y : [2, 77]\}$$
$$=/\sqsubseteq$$
$$\{x : [1, 99], y : [2, 77]\}$$

$$\alpha \circ \gamma(Y) =/\sqsubseteq Y$$

Composition of Galois Connections

The composition of Galois connections:

$$\langle L,\ \leq\rangle \xleftarrow[\alpha_1]{\gamma_1} \langle M,\ \sqsubseteq\rangle$$

and:

$$\langle M,\ \sqsubseteq\rangle \xleftarrow[\alpha_2]{\gamma_2} \langle N,\ \preceq\rangle$$

is a Galois connection:

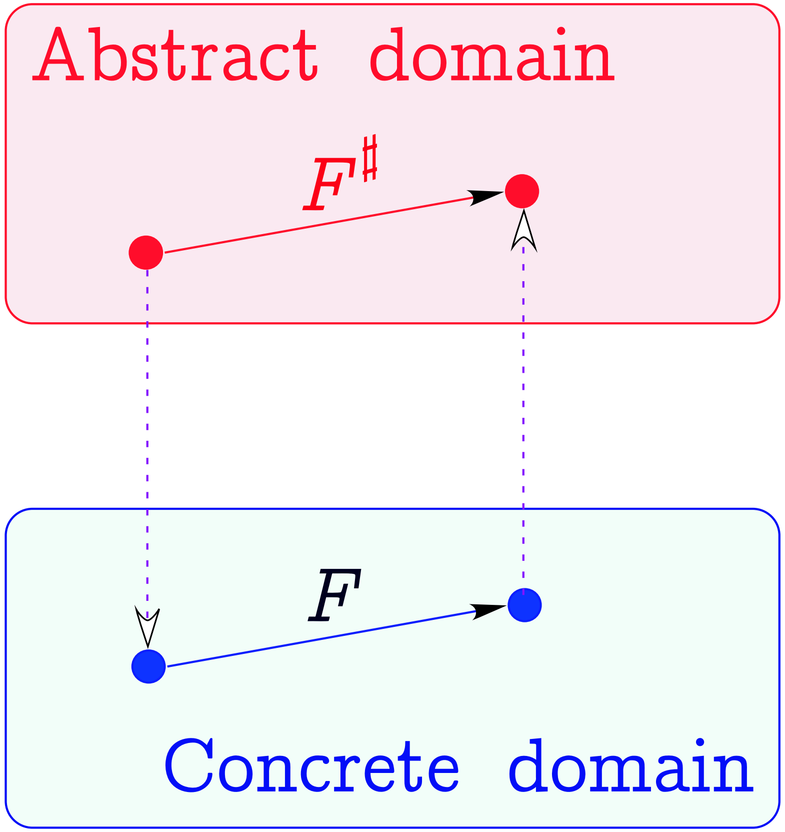
$$\langle L,\ \leq\rangle \xleftarrow[\alpha_2 \circ \alpha_1]{\gamma_1 \circ \gamma_2} \langle N,\ \preceq\rangle$$

2.2.5 Function Abstraction

See Sec. 7.2 of[POPL '79].

Reference

[POPL '79] P. Cousot & R. Cousot. Systematic design of program analysis frameworks. In *6th POPL*, pages 269–282, San Antonio, TX, 1979. ACM Press. 51



Function Abstraction

$$F^\sharp = \alpha \circ F \circ \gamma$$

i.e. $F^\sharp = \rho \circ F$

$$\langle P, \subseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q, \sqsubseteq\rangle \Rightarrow$$

$$\langle P \xrightarrow{\text{mon}} P, \dot{\subseteq}\rangle \underset{\lambda F \bullet \alpha \circ F \circ \gamma}{\overset{\lambda F^\sharp \bullet \gamma \circ F^\sharp \circ \alpha}{\leftrightarrows}} \langle Q \xrightarrow{\text{mon}} Q, \dot{\sqsubseteq}\rangle$$

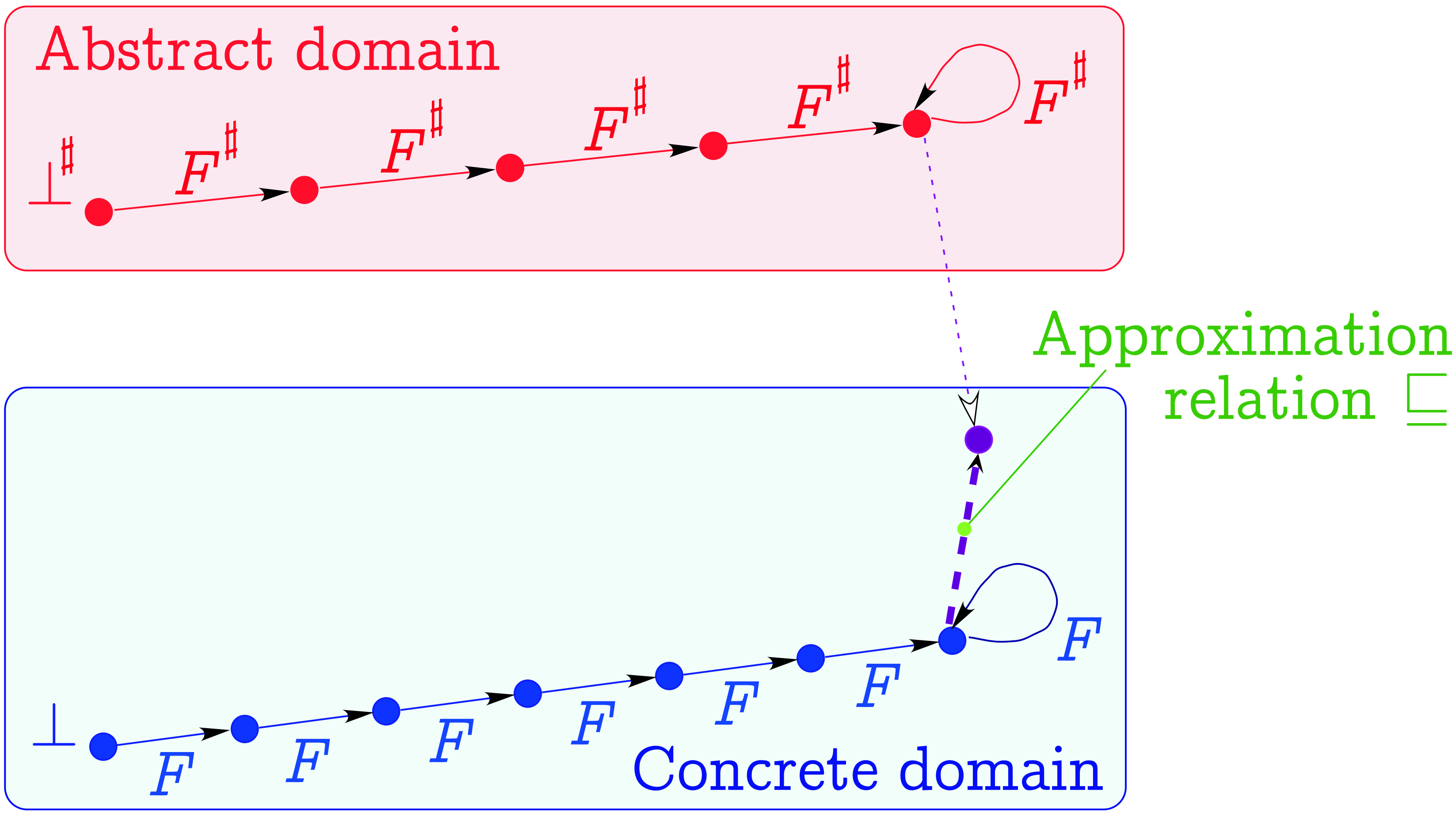
2.2.6 Fixpoint Abstraction

See Sec. 7.1 of [POPL '79].

Reference

[POPL '79] P. Cousot & R. Cousot. Systematic design of program analysis frameworks. In *6th POPL*, pages 269–282, San Antonio, TX, 1979. ACM Press. 53

Approximate Fixpoint Abstraction



$$\alpha(\mathrm{lfp}\, F) \sqsubseteq \mathrm{lfp}\, F^\sharp$$

Approximate/Exact Fixpoint Abstraction

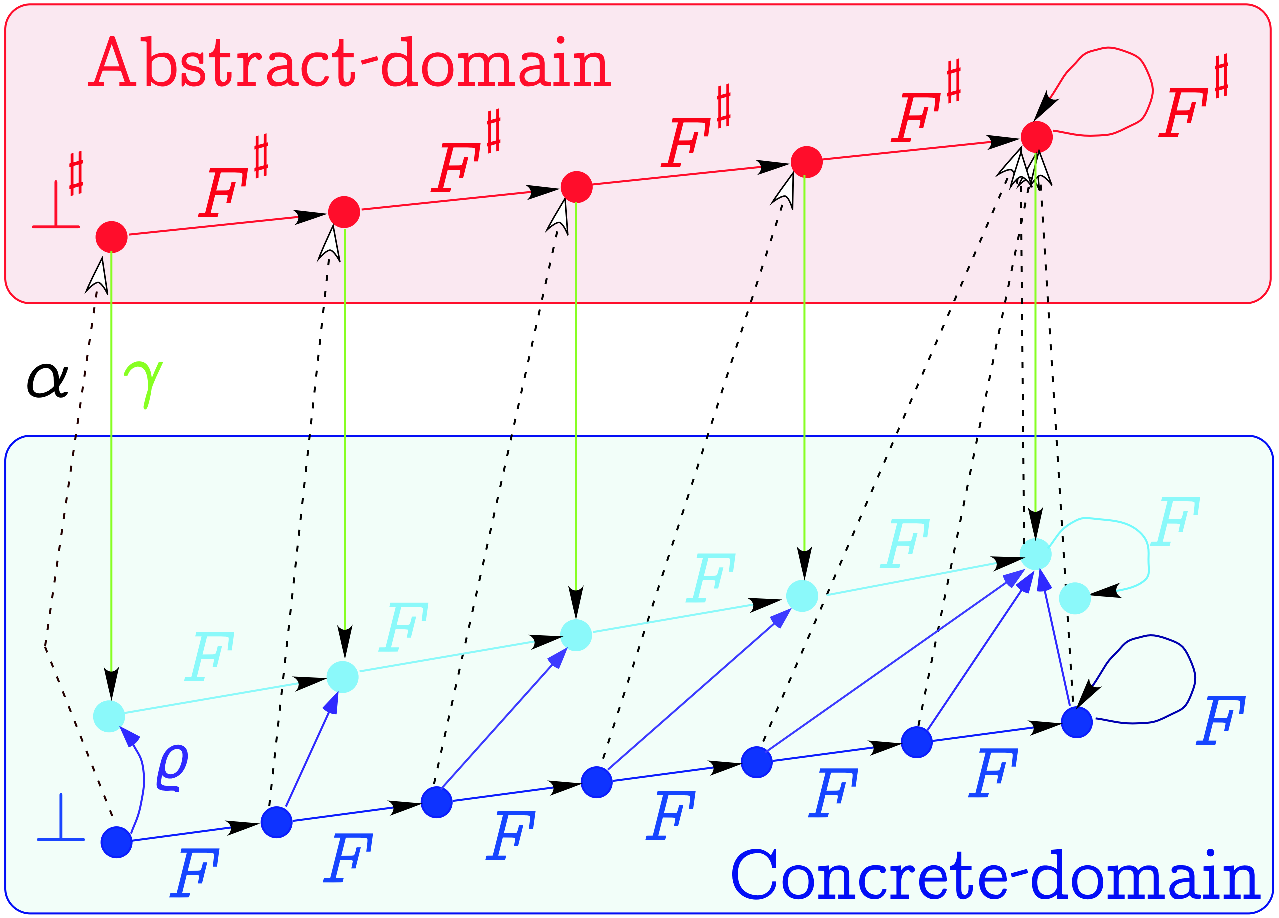
Exact Abstraction:

$$\alpha(\operatorname{lfp} F) = \operatorname{lfp} F^\sharp$$

Approximate Abstraction:

$$\alpha(\operatorname{lfp} F) \sqsubseteq^\sharp \operatorname{lfp} F^\sharp$$

Exact Fixpoint Abstraction



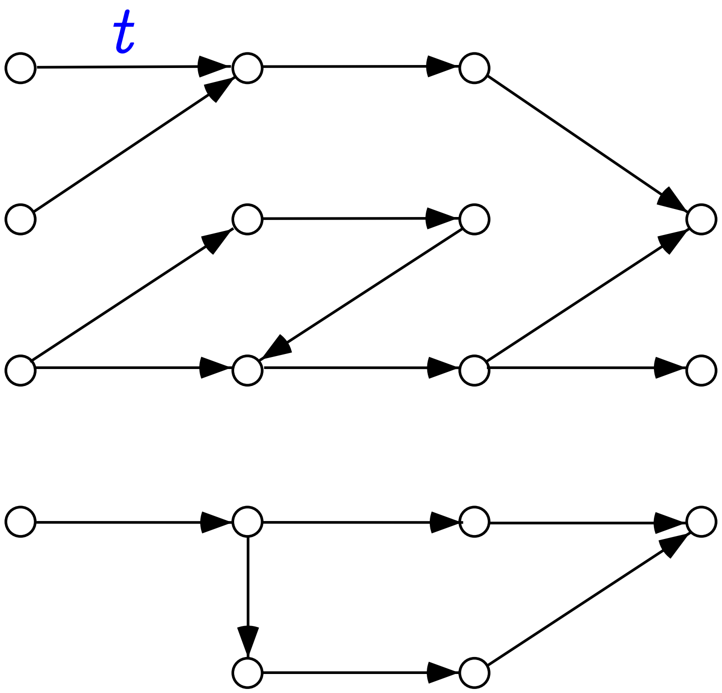
$$\alpha \circ F = F^\sharp \circ \alpha \;\Rightarrow\; \alpha(\operatorname{lfp} F) = \operatorname{lfp} F^\sharp$$

2.3 Application to Reachability

Transition systems

- $\langle S, t \rangle$ where:
  - S is a set of states/vertices/...
  - $t \in \wp(S \times S)$ is a transition relation/set of arcs/...

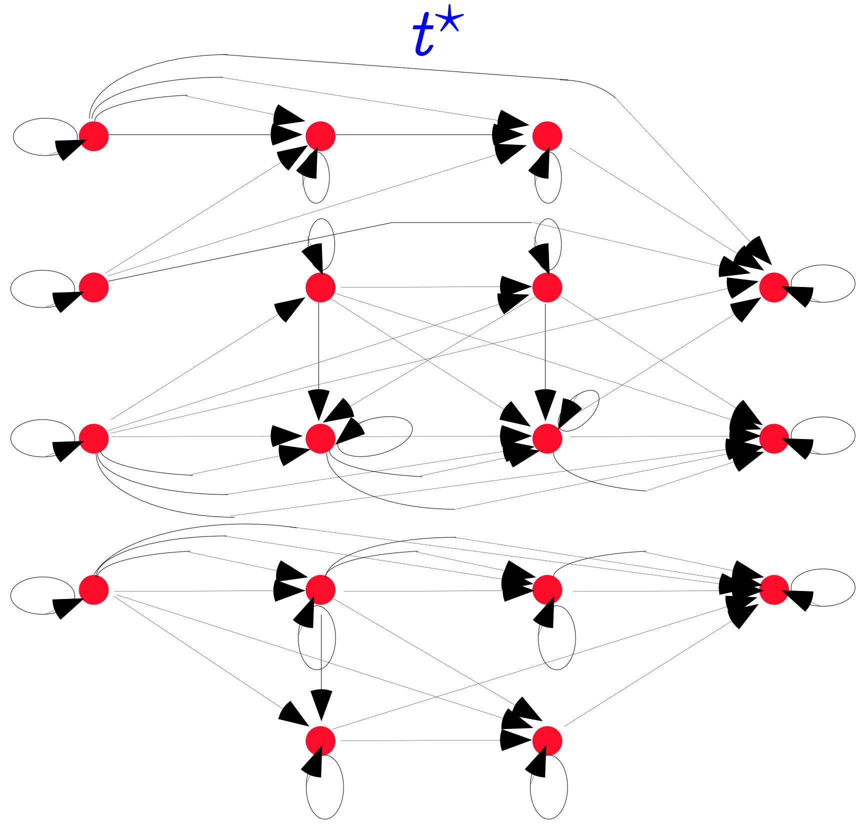
Example of transition system



Reflexive transitive closure

- Composition:
  - $t \circ t' \stackrel{\text{def}}{=} \{\langle s, s''\rangle \mid \exists s' : \langle s, s"\rangle \in t \wedge \langle s', s''\rangle \in t'\}$
- Powers:
  - $t^0 \stackrel{\text{def}}{=} \{\langle s, s\rangle \mid s \in S\}$
  - $t^{n+1} \stackrel{\text{def}}{=} t^n \circ t \qquad n \geq 0$
- Reflexive transitive closure:
  - $t^* = \bigcup_{n \geq 0} t^n$

Example of transitive reflexive closure



Reflexive transitive closure in fixpoint form

$$t^* = \text{lfp}^{\subseteq} \lambda X \cdot t^0 \cup X \circ t$$

Proof

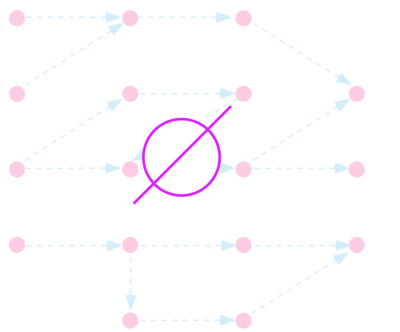
$$\begin{aligned}
X^0 &= \emptyset \\
X^1 &= t^0 \cup X^0 \circ t = t^0 \\
X^2 &= t^0 \cup X^1 \circ t = {}^0 \cup t^0 \circ t = t^0 \cup t^1 \\
\ldots & \quad \ldots \\
X^n &= \bigcup_{0 \leq i < n} t^i \qquad \text{(induction hypothesis)}
\end{aligned}$$

$$
\begin{aligned}
X^{n+1} &= t^0 \cup X^n \circ t \\
&= t^0 \cup \Big(\bigcup_{0 \le i < n} t^i\Big) \circ t \\
&= t^0 \cup \bigcup_{0 \le i < n} \big(t^i \circ t\big) \\
&= t^0 \cup \bigcup_{1 \le i+1 < n+1} \big(t^{i+1}\big) \\
&= t^0 \cup \Big(\bigcup_{1 \le j < n+1} t^j\Big) \circ t \\
&= \bigcup_{0 \le i < n+1} t^i \\
\ldots \quad & \quad \ldots
\end{aligned}
$$

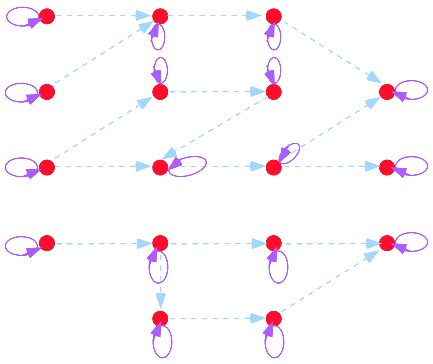
$$
\begin{aligned}
X^{\omega} &= \bigcup_{n \geq 0} X^{n} \\
&= \bigcup_{n \geq 0} \bigcup_{0 \leq i < n} t^{i} \\
&= \bigcup_{n \geq 0} t^{n} \\
&= t^{*}
\end{aligned}
$$

$$
\begin{aligned}
X^{\omega+1} &= t^0 \cup X^\omega \circ t \\
&= t^0 \cup \Big(\bigcup_{n\geq 0} t^n\Big) \circ t \\
&= t^0 \cup \bigcup_{n\geq 0} \big(t^n \circ t\big) \\
&= t^0 \cup \bigcup_{n\geq 0} t^{n+1} \\
&= t^0 \cup \bigcup_{k\geq 1} t^k \\
&= \bigcup_{n\geq 0} t^n \\
&= t^*
\end{aligned}
$$

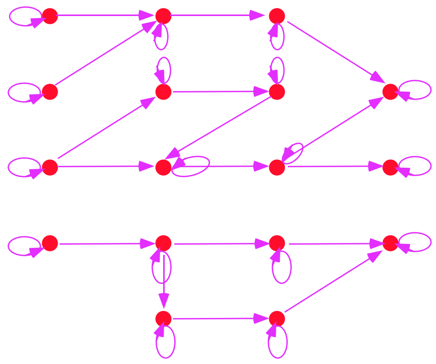
Iterates



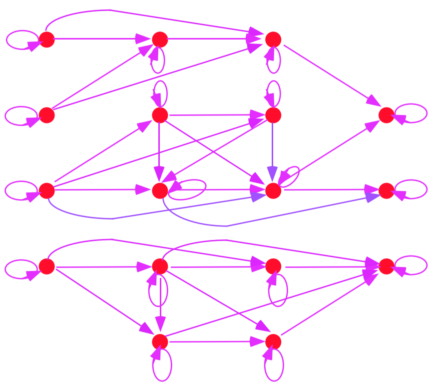
X^0



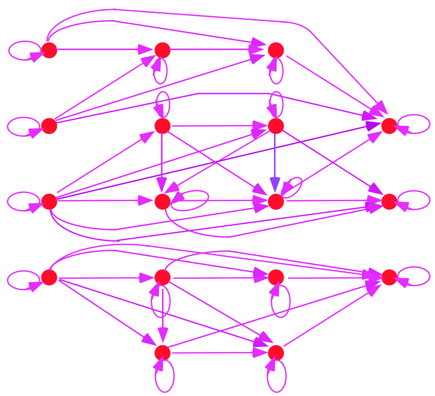
X^1



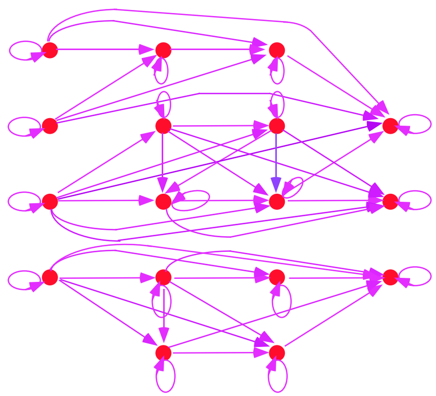
X^2



X^3



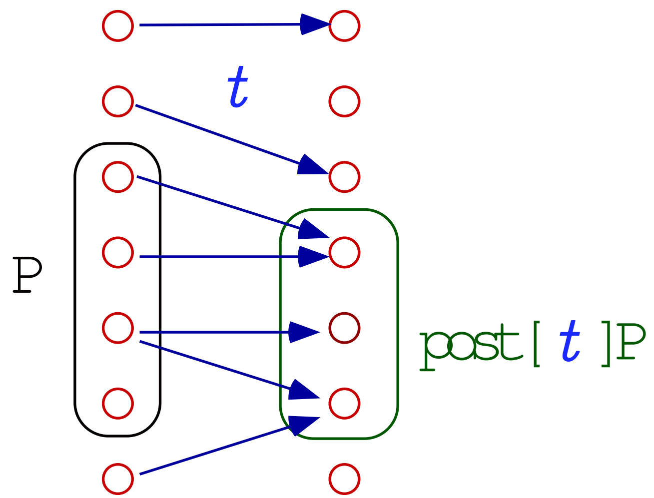
X^4



$X^5 = t^*$

Post-image

$$\text{post}[t]I = \{s' \mid \exists s \in I : \langle s, s' \rangle \in t\}$$



We have $\text{post}[\bigcup_{i \in \Delta} t^i]I = \bigcup_{i \in \Delta} \text{post}[t^i]I$ so $\alpha = \lambda t \cdot \text{post}[t]I$ is the lower adjoint of a Galois connection.

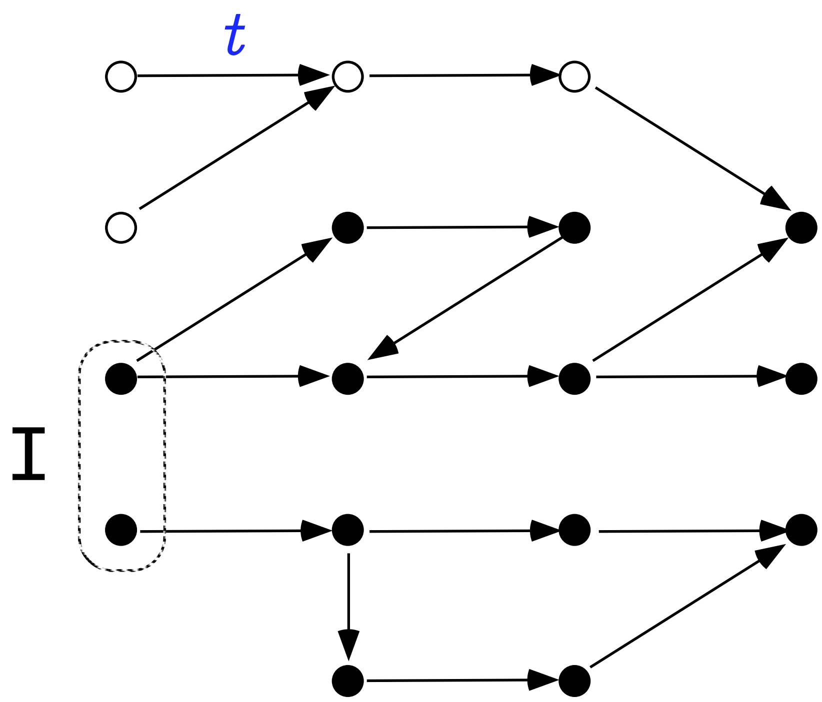
Postimage Galois connection

Given $I \in \wp(S)$,

$$\langle \wp(S \times S), \subseteq \rangle \underset{\lambda t \cdot \text{post}[t]I}{\overset{\gamma}{\leftrightarrows}} \langle \wp(S), \subseteq \rangle$$

$$\begin{aligned}
& \text{post}[t]I \subseteq R \\
\Leftrightarrow\ & \{s' \mid \exists s \in I : \langle s, s' \rangle \in t\} \subseteq R \\
\Leftrightarrow\ & \forall s' \in S : (\exists s \in I : \langle s, s' \rangle \in t) \Rightarrow (s' \in R) \\
\Leftrightarrow\ & \forall s', s \in S : (s \in I \wedge \langle s, s' \rangle \in t) \Rightarrow (s' \in R) \\
\Leftrightarrow\ & \forall s', s \in S : \langle s, s' \rangle \in t \Rightarrow ((s \in I) \Rightarrow (s' \in R)) \\
\Leftrightarrow\ & t \subseteq \{\langle s, s' \rangle \mid (s \in I) \Rightarrow (s' \in R)\} \stackrel{\text{def}}{=} \gamma(R)
\end{aligned}$$

Reachable states



$$\text{post}[t^*]\mathcal{I}$$

Fixpoint abstraction, once again

Let $F \in L \overset{m}{\longmapsto} L$ and $\overline{F} \in \overline{L} \overset{m}{\longmapsto} \overline{L}$ be respective monotone maps on the cpos $\langle L, \bot, \sqsubseteq\rangle$ and $\langle \overline{L}, \overline{\bot}, \overline{\sqsubseteq}\rangle$ and $\langle L, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \overline{L}, \overline{\sqsubseteq}\rangle$ such that $\alpha \circ F \circ \gamma \,\dot{\overline{\sqsubseteq}}\, \overline{F}$. Then [10]:

- $\forall \delta \in \mathbb{O}$: $\alpha(F^\delta) \mathrel{\overline{\sqsubseteq}} \overline{F}^\delta$ (iterates from the infimum);
- The iteration order of $\overline{F}$ is $\leq$ to that of F;
- $\alpha(\mathrm{lfp}^{\sqsubseteq} F) \mathrel{\overline{\sqsubseteq}} \mathrm{lfp}^{\overline{\sqsubseteq}}\, \overline{F}$;

Soundness: $\mathrm{lfp}^{\overline{\sqsubseteq}}\, \overline{F} \mathrel{\overline{\sqsubseteq}} \overline{P} \Rightarrow \mathrm{lfp}^{\sqsubseteq} F \sqsubseteq \gamma(\overline{P})$.

[10] P. Cousot & R. Cousot. *Systematic design of program analysis frameworks.* ACM POPL'79, pp. 269–282, 1979. Numerous variants!

Fixpoint abstraction (continued)

Moreover, the *commutation condition* $\overline{F} \circ \alpha = \alpha \circ F$ implies [11]:

- $\overline{F} = \alpha \circ F \circ \gamma$, and
- $\alpha(\text{lfp}^{\sqsubseteq} F) = \text{lfp}^{\overline{\sqsubseteq}} \overline{F}$;

Completeness: $\text{lfp}^{\sqsubseteq} F \sqsubseteq \gamma(\overline{P}) \Rightarrow \text{lfp}^{\overline{\sqsubseteq}} \overline{F} \mathrel{\overline{\sqsubseteq}} \overline{P}$.

[11] P. Cousot & R. Cousot. *Systematic design of program analysis frameworks.* ACM POPL'79, pp. 269–282, 1979. Numerous variants!

Reachable states in fixpoint form

$$
\begin{aligned}
& \mathrm{post}[t^*]I, \quad I \text{ given} \\
= \; & \alpha(t^*) \qquad \text{where} \quad \alpha(t) = \mathrm{post}[t]I = \{s' \mid \exists s \in I : \langle s, s' \rangle \in t\} \\
= \; & \alpha(\mathrm{lfp}^{\subseteq} \lambda X \cdot t^0 \cup X \circ t) \\
= \; & \mathrm{lfp}^{\subseteq} \overline{F} \; ???
\end{aligned}
$$

DISCOVERING $\overline{F}$ BY CALCULUS

$$
\begin{aligned}
& \alpha \circ (\lambda X \cdot t^0 \cup X \circ t) \\
= \ & \lambda X \cdot \alpha(t^0 \cup X \circ t) \\
= \ & \lambda X \cdot \alpha(t^0) \cup \alpha(X \circ t) \\
= \ & \lambda X \cdot \mathrm{post}[t^0]I \cup \mathrm{post}[X \circ t]I
\end{aligned}
$$

$$
\begin{aligned}
& \operatorname{post}[t^0]I \\
= & \ \{s' \mid \exists s \in I : \langle s, s' \rangle \in t^0\} \\
= & \ \{s' \mid \exists s \in I : \langle s, s' \rangle \in \{\langle s, s \rangle \mid s \in S\}\} \\
= & \ \{s' \mid \exists s \in I\} \\
= & \ I
\end{aligned}
$$

$$
\begin{aligned}
& \operatorname{post}[X \circ t]I \\
= {} & \{s' \mid \exists s \in I : \langle s, s' \rangle \in (X \circ t)\} \\
= {} & \{s' \mid \exists s \in I : \langle s, s' \rangle \in \{\langle s, s'' \rangle \mid \exists s' : \langle s, s" \rangle \in X \wedge \langle s', s'' \rangle \in t\}\} \\
= {} & \{s' \mid \exists s \in I : \exists s'' \in S : \langle s, s" \rangle \in X \wedge \langle s', s'' \rangle \in t\} \\
= {} & \{s' \mid \exists s'' \in S : (\exists s \in I : \langle s, s" \rangle \in X) \wedge \langle s', s'' \rangle \in t\} \\
= {} & \{s' \mid \exists s'' \in S : s'' \in \{s'' \mid \exists s \in I : \langle s, s" \rangle \in X\} \wedge \langle s', s'' \rangle \in t\} \\
= {} & \{s' \mid \exists s'' \in S : s'' \in \operatorname{post}[X]I \wedge \langle s', s'' \rangle \in t\} \\
= {} & \operatorname{post}[t](\operatorname{post}[X]I) \\
= {} & \operatorname{post}[t](\alpha(X))
\end{aligned}
$$

$$
\begin{aligned}
& \alpha \circ (\lambda X \cdot t^0 \cup X \circ t) \\
= \; & \ldots \\
= \; & \lambda X \cdot \mathrm{post}[t^0]I \cup \mathrm{post}[X \circ t]I \\
= \; & \lambda X \cdot I \cup \mathrm{post}[t](\alpha(X)) \\
= \; & \lambda X \cdot \overline{F}(\alpha(X))
\end{aligned}
$$

by defining:

$$\overline{F} = \lambda X \cdot I \cup \mathrm{post}[t](X)$$

proving:

$$\mathrm{post}[t^*](I) = \mathrm{lfp}^{\subseteq} \lambda X \cdot I \cup \mathrm{post}[t](X) \tag{2}$$

Example of iteration