TRANSFORMING ABSTRACT INTERPRETATIONS BY ABSTRACT INTERPRETATIONS

MODELLING SYSTEMS AS AI TRANSFORMERS

Roberto Giacobazzi

(and A. Banerjee, **I. Mastroeni**, E. Quintarelli, F. Ranzato, F. Scozzari)

SAS'08, Valencia July 2008

Abstract Interpretation

[Cousot & Cousot '79]

- A program P
- A domain of computation for P: C typically a complete lattice
- Semantic specification (interpreter): $[\![P]\!] : C \longrightarrow C$
- (Approximate) observable properties: $\rho \in uco(C)$
- DERIVE A SOUND APPROXIMATE SPECIFICATION $[\![P]\!]^\sharp$

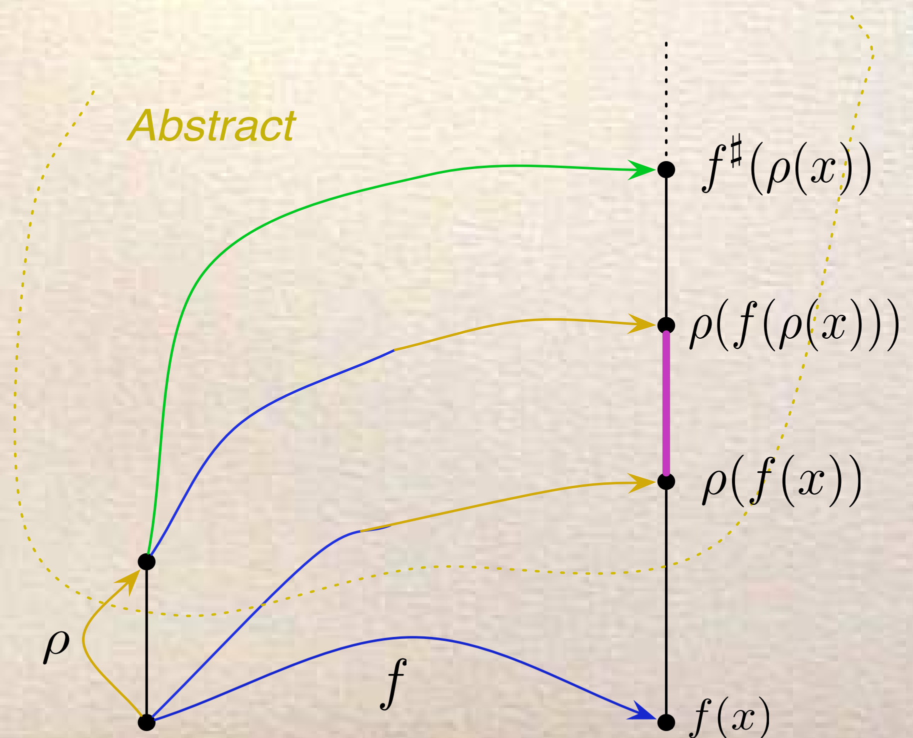
$$\rho([\![P]\!](x)) \leq [\![P]\!]^\sharp(x)$$

- THE LIMIT CASE: COMPLETENESS

$$\rho([\![P]\!](x)) = [\![P]\!]^\sharp(x) \text{ iff } \rho([\![P]\!](x)) = \rho([\![P]\!](\rho(x)))$$

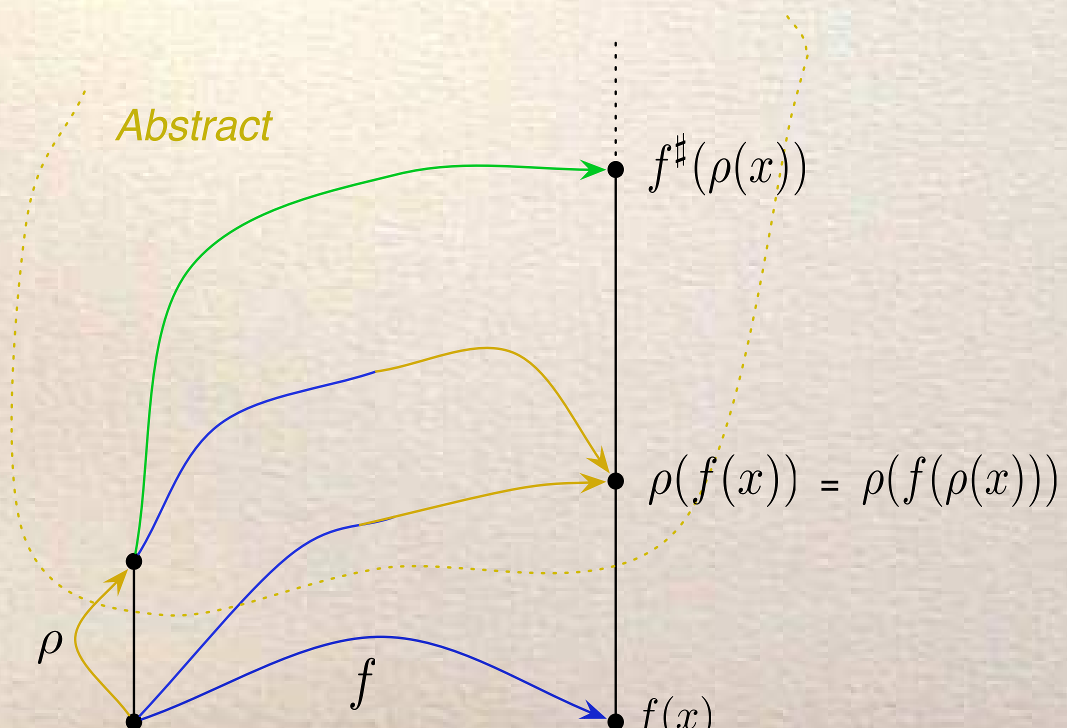
Completeness in Abstract Interpretation

- Backward Soundness: no information is lost by approximating the input/output
- $\rho \circ f \leq \rho \circ f \circ \rho$



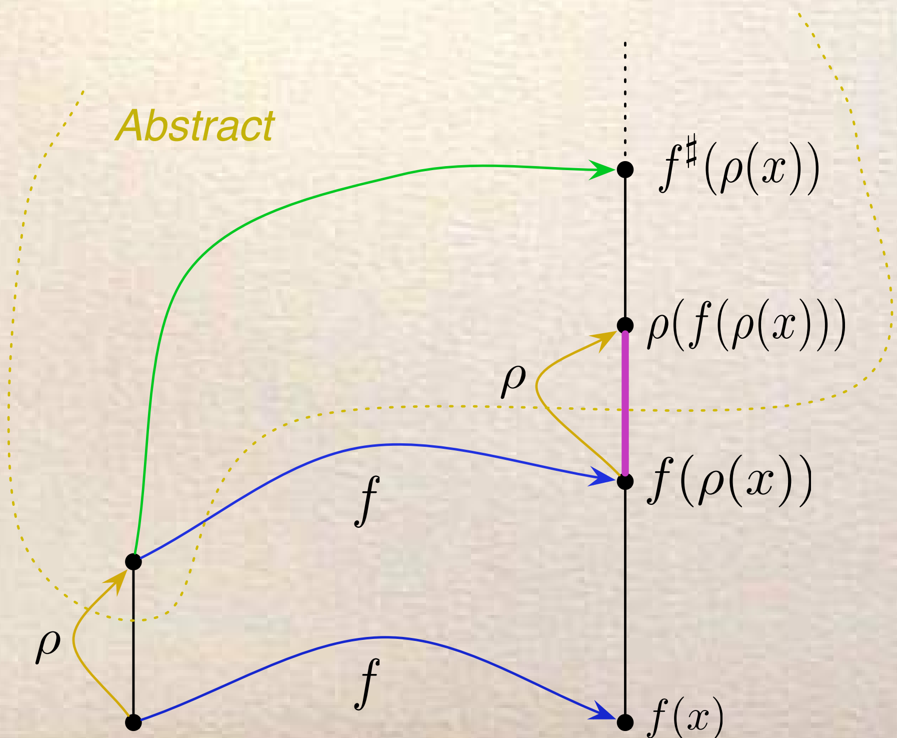
COMPLETENESS IN ABSTRACT INTERPRETATION

- BACKWARD COMPLETENESS: NO LOSS OF PRECISION IS ACCUMULATED BY APPROXIMATING THE INPUT
- $\rho \circ f = \rho \circ f \circ \rho$



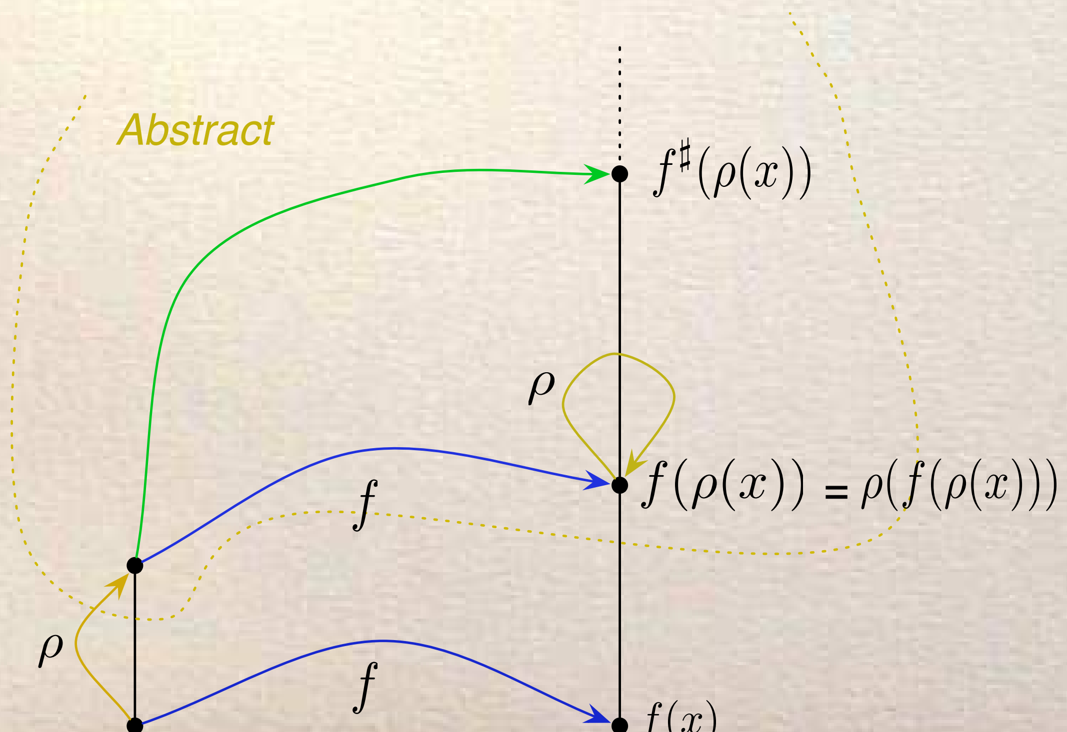
Completeness in Abstract Interpretation

- Forward Completeness: no information is lost by approximating the output
- $f \circ \rho \leq \rho \circ f \circ \rho$

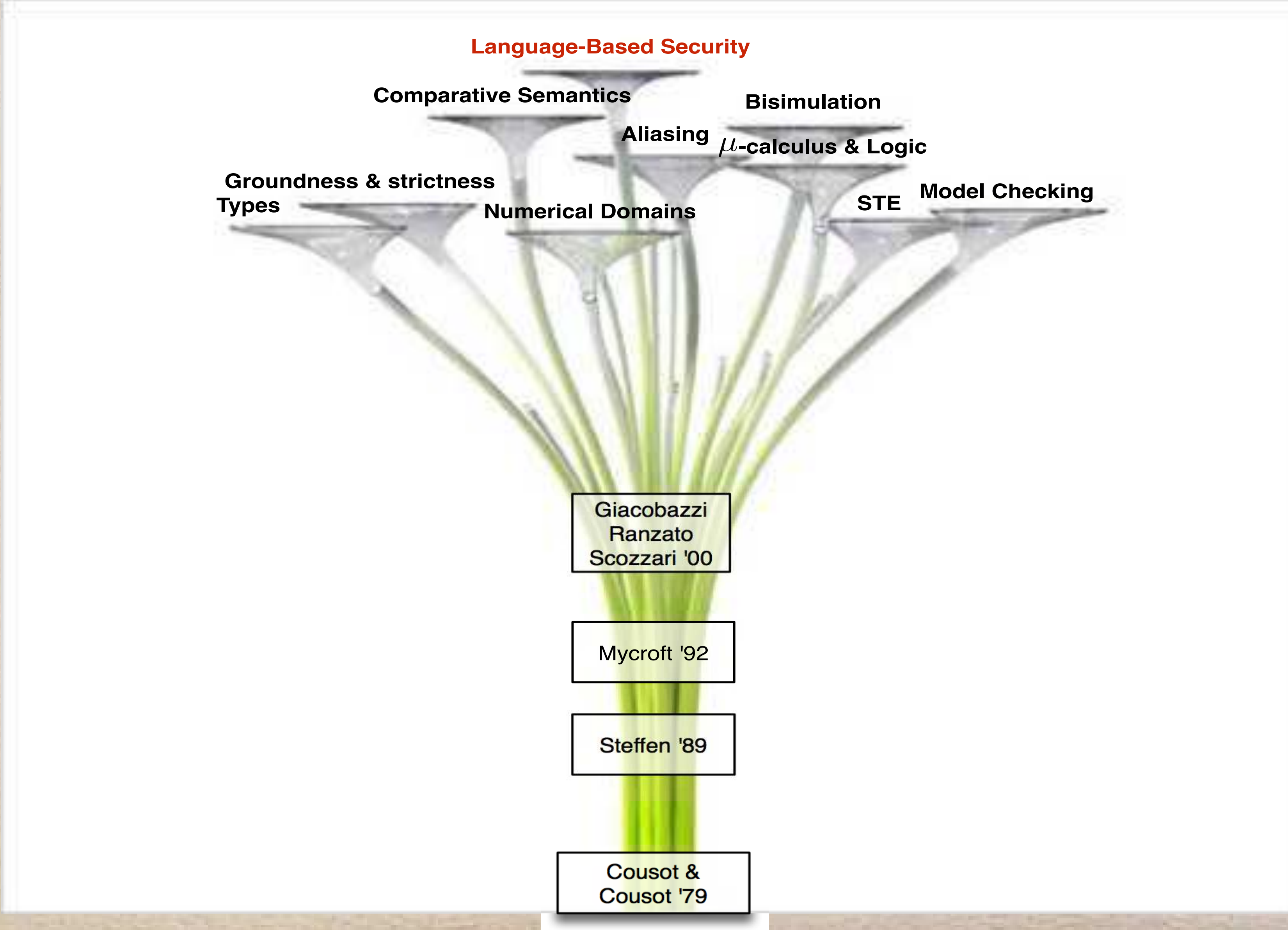


Completeness in Abstract Interpretation

- Forward Completeness: no information is lost by approximating the output
- $f \circ \rho = \rho \circ f \circ \rho$

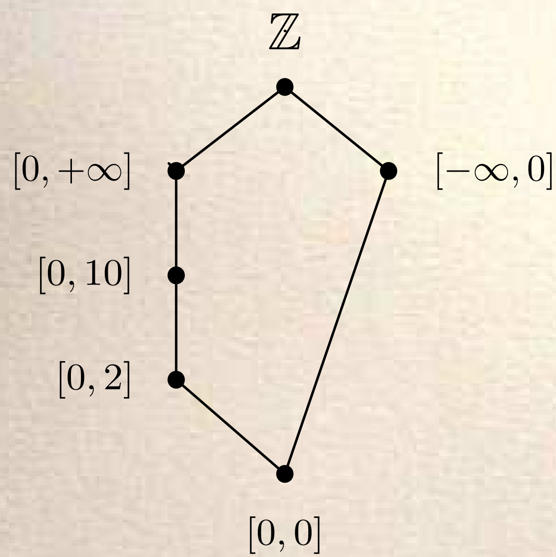


COMPLETENESS IN ABSTRACT INTERPRETATION



IN NUMERICAL DOMAINS

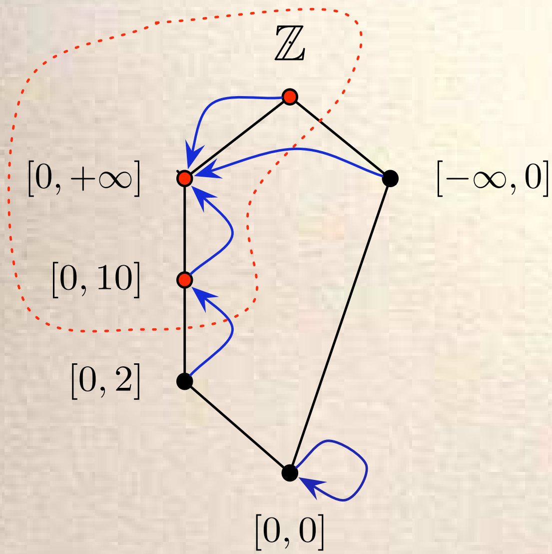
A SIMPLE EXAMPLE IN INTERVAL ANALYSIS



- A simple domain of intervals

In Numerical Domains

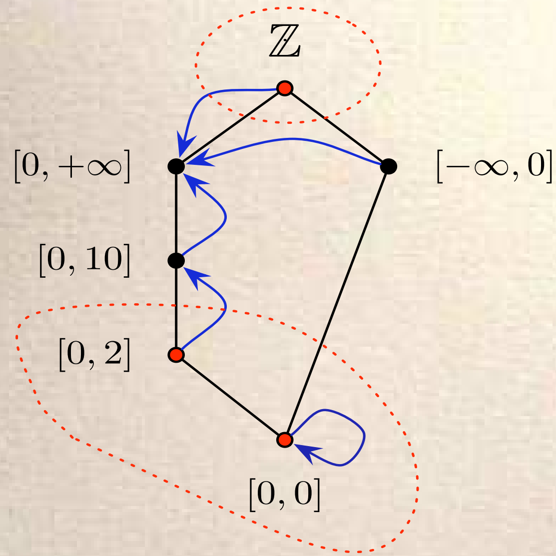
A simple example in Interval analysis



- A simple domain of intervals
- $sq(X) = \left\{ x^2 \;\middle|\; x \in X \right\}$
- $\{\mathbb{Z}, [0,+\infty], [0,10]\}$ is Forward but not Backward complete

IN NUMERICAL DOMAINS

A SIMPLE EXAMPLE IN INTERVAL ANALYSIS

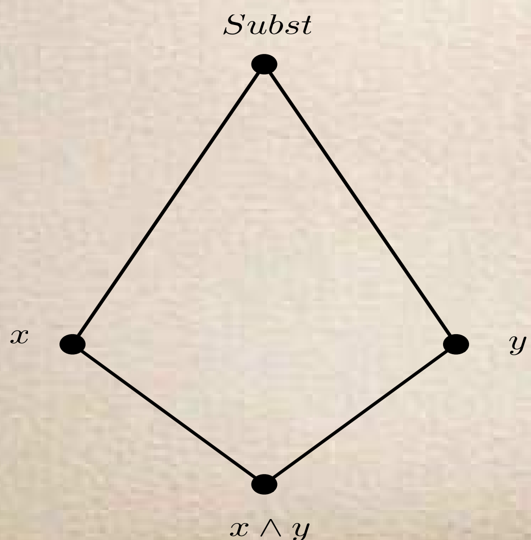


- A simple domain of intervals
- $sq(X) = \left\{ x^2 \;\middle|\; x \in X \right\}$
- $\{\mathbb{Z}, [0, +\infty], [0, 10]\}$ is Forward but not Backward complete
- $\{\mathbb{Z}, [0, 2], [0, 0]\}$ is Backward but not Forward complete

IN GROUNDNESS: HEYTING COMPLETION

GROUNDNESS ANALYSIS DETERMINES WHETHER A VARIABLE IS DEFINITIVELY INSTANTIATED

- $(\wp(Subst)^{\downarrow}, \cap)$ is a complete Heyting Algebra
- $\Theta_1 \cap \Theta_2 \leq \Theta_3 \iff \Theta_2 \leq \Theta_1 \xrightarrow{\cap} \Theta_3 = \bigcup \left\{ \Theta \;\middle|\; \Theta_1 \cap \Theta \leq \Theta_3 \right\}$
- $A \xrightarrow{\cap} B = \left\{ \Theta_1 \xrightarrow{\cap} \Theta_3 \;\middle|\; \Theta_1 \in A, \Theta_2 \in B \right\}$

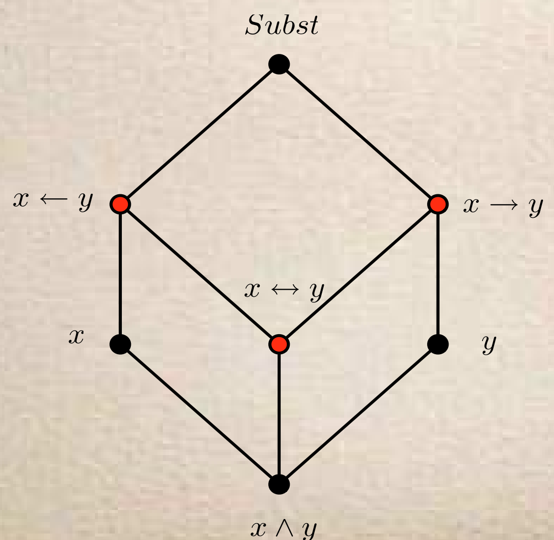


$$X = \mathcal{G} \sqcap (X \xrightarrow{\cap} X)$$

In Groundness: Heyting completion

Groundness analysis determines whether a variable is definitively instantiated

- $(\wp(Subst)^{\downarrow}, \cap)$ is a complete Heyting Algebra
- $$\Theta_1 \cap \Theta_2 \leq \Theta_3 \iff \Theta_2 \leq \Theta_1 \xrightarrow{\cap} \Theta_3 = \bigcup \left\{ \Theta \;\middle|\; \Theta_1 \cap \Theta \leq \Theta_3 \right\}$$
- $$A \xrightarrow{\cap} B = \left\{ \Theta_1 \xrightarrow{\cap} \Theta_3 \;\middle|\; \Theta_1 \in A,\, \Theta_2 \in B \right\}$$



$$X = \mathcal{G} \sqcap (X \xrightarrow{\cap} X)$$

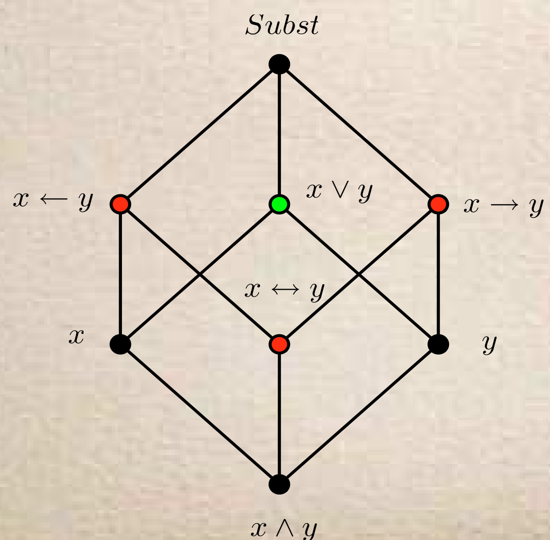
IN GROUNDNESS: HEYTING COMPLETION

GROUNDNESS ANALYSIS DETERMINES WHETHER A VARIABLE IS DEFINITIVELY INSTANTIATED

- $(\wp(Subst)^{\downarrow}, \cap)$ is a complete Heyting Algebra

- $$\Theta_1 \cap \Theta_2 \leq \Theta_3 \iff \Theta_2 \leq \Theta_1 \xrightarrow{\cap} \Theta_3 = \bigcup \left\{ \Theta \;\middle|\; \Theta_1 \cap \Theta \leq \Theta_3 \right\}$$

- $$A \xrightarrow{\cap} B = \left\{ \Theta_1 \xrightarrow{\cap} \Theta_3 \;\middle|\; \Theta_1 \in A, \Theta_2 \in B \right\}$$



$$X = \mathcal{G} \sqcap (X \xrightarrow{\cap} X)$$

$\boxed{\Rightarrow \text{A COMPLETENESS PROBLEM}}$

[Giacobazzi & Scozzari '98]

In Comparative Semantics

Condensing generalises the lifting lemma from SLD-resolution to arbitrary semantics [Giacobazzi et al. '05]

$$[\![a \otimes b]\!] = a \otimes [\![b]\!]$$

$$\boxed{\begin{array}{llll} \textit{Program} & P & ::= & \varnothing \mid p(\overline{x}) \leftarrow A \mid P.P \\ \textit{Agent} & A & ::= & \theta \mid p(\overline{x}) \mid A \otimes A \mid \bigvee_{i=1}^{n} A_i \end{array}}$$

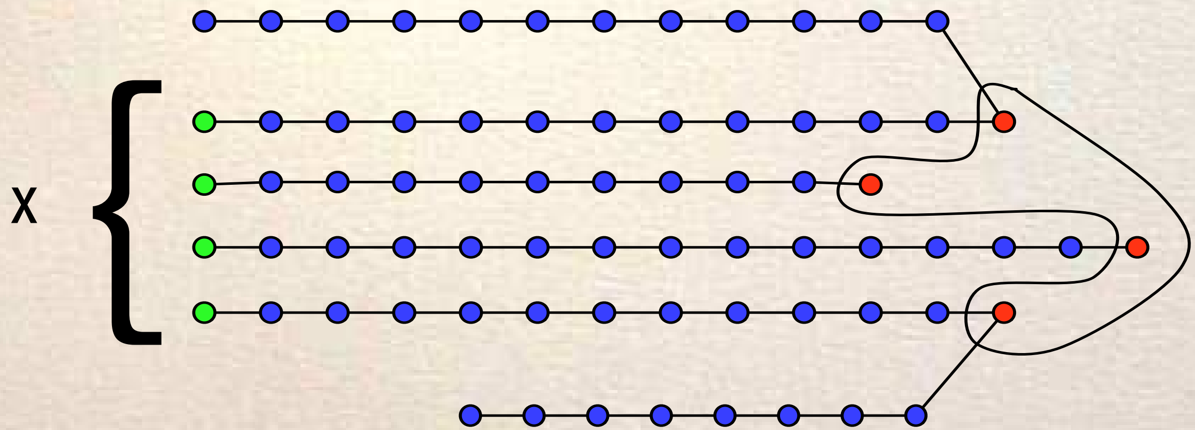
- $\otimes$ is a tensor operator (e.g. unification)
- $$a \otimes b \leq c \iff b \leq a \multimap c = \bigvee \left\{ b \in C \,\middle|\, a \otimes b \leq c \right\}$$
- $$A \xrightarrow{\otimes} B = \left\{ a \multimap b \in C \,\middle|\, a \in A,\ b \in B \right\}$$
- X is condensing iff $X = X \sqcap (X \xrightarrow{\otimes} X)$ iff X is complete for $F_X = \left\{ \lambda y.x \otimes y \,\middle|\, x \in X \right\}$.

$\boxed{\Rightarrow \text{A completeness problem}}$

In Comparative Semantics

$$[\![P_1; P_2]\!]^A = [\![P_1]\!]^A \diamond [\![P_2]\!]^A$$

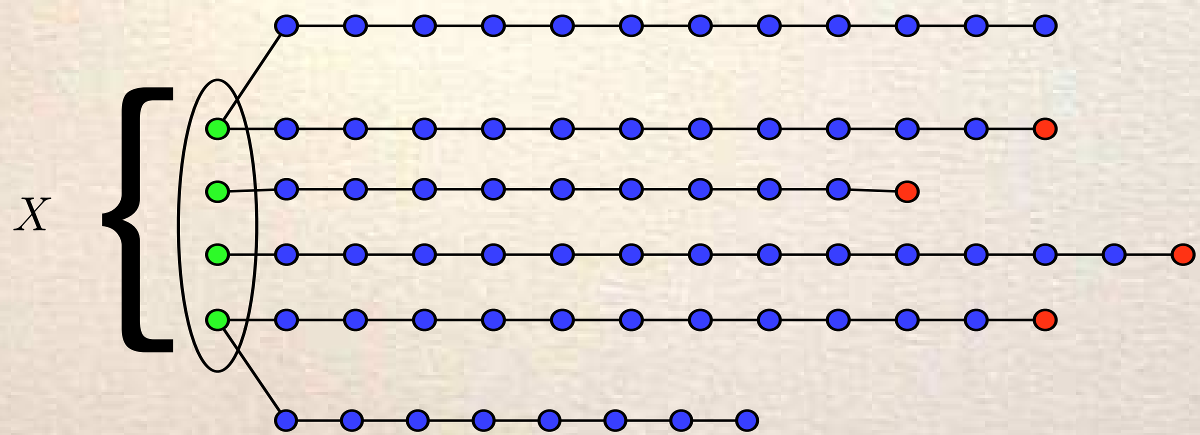
- *Forward termination*: $Pot^{\rightarrow ?}(X) = \left\{ \sigma \;\middle|\; \delta \in X^+ \wedge \sigma_\dashv = \delta_\dashv \right\}$



In Comparative Semantics

$$[\![P_1;P_2]\!]^A = [\![P_1]\!]^A \diamond [\![P_2]\!]^A$$

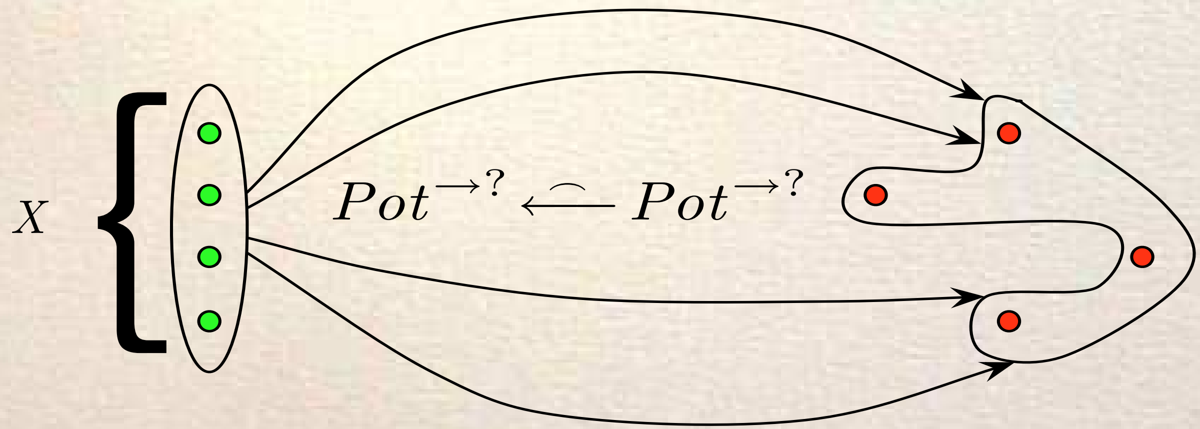
- *Backward termination*: $Pot^{\leftarrow ?}(X) = \left\{ \sigma \;\middle|\; \delta \in X^+ \wedge \sigma_\vdash = \delta_\vdash \right\}$



In Comparative Semantics

$$[\![P_1;P_2]\!]^A = [\![P_1]\!]^A \diamond [\![P_2]\!]^A$$

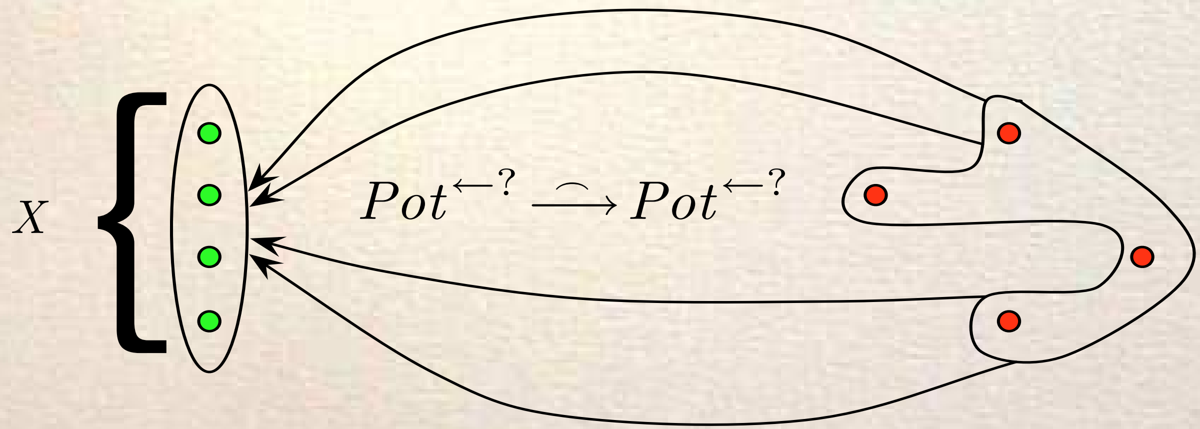
- $X = Pot^{\rightarrow ?} \sqcap (X \stackrel{\frown}{\longrightarrow} X)$ and the solution: $Pot^{\rightarrow ?} \stackrel{\frown}{\longleftarrow} Pot^{\rightarrow ?} = [\![\cdot]\!]$.



In Comparative Semantics

$$[\![P_1;P_2]\!]^A = [\![P_1]\!]^A \diamond [\![P_2]\!]^A$$

- $X = Pot^{\leftarrow ?} \sqcap (X \stackrel{\frown}{\longrightarrow} X)$ and the solution: $Pot^{\leftarrow ?} \stackrel{\frown}{\longrightarrow} Pot^{\leftarrow ?} = Wlp$.

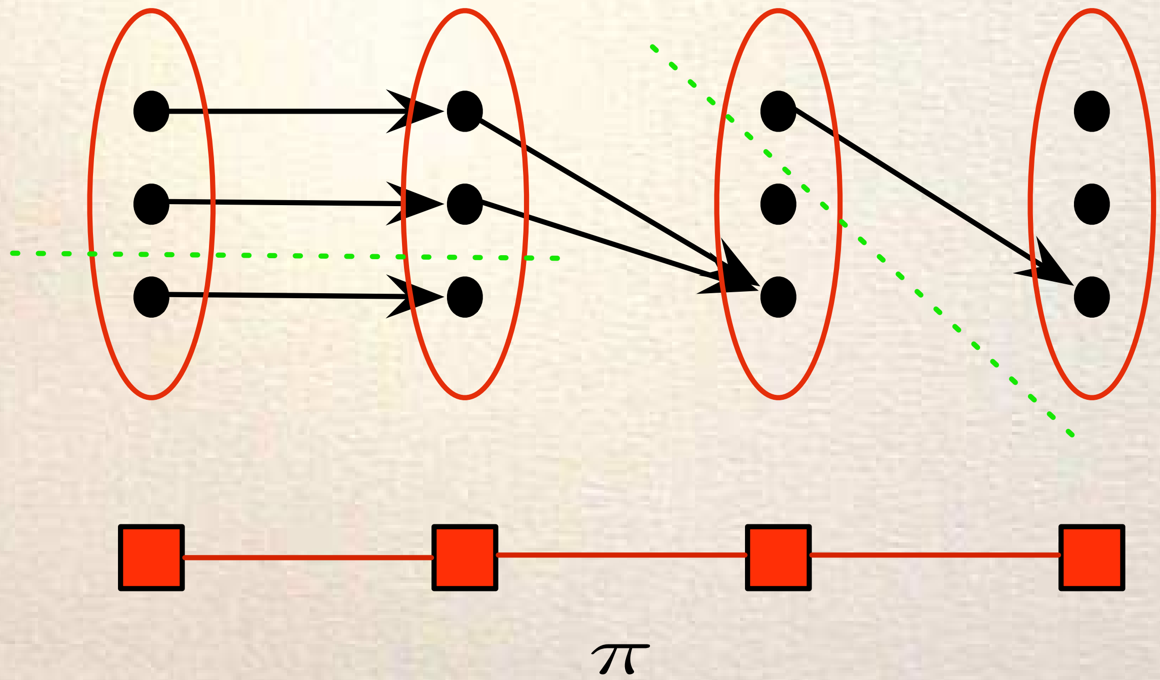


$\boxed{\Rightarrow \text{A COMPLETENESS PROBLEM}}$

[Giacobazzi & Mastroeni '05]

In Model Checking

Complete Abstract Model Checking: $M^A \models \Phi \iff M^C \models \Phi$



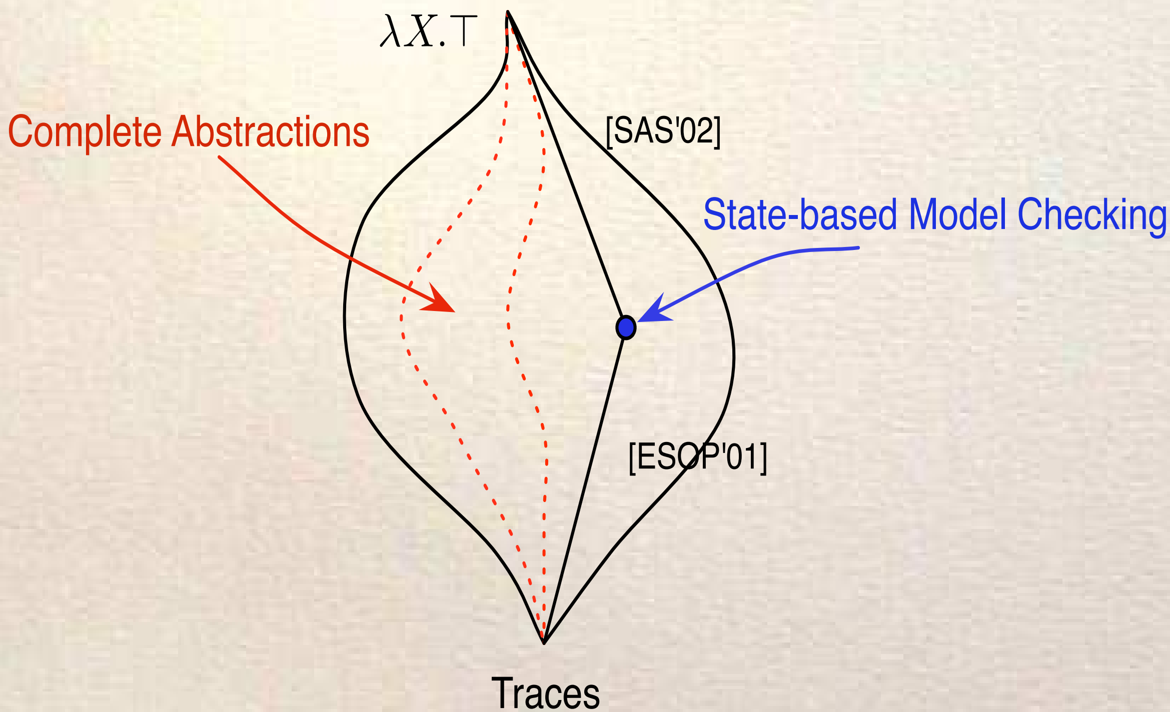
If π is spurious then the abstraction is incomplete for *post*

[Giacobazzi & Quintarelli '01, Ranzato & Tapparo '06, Cousot et al '07, Schmidt '08]

IN MODEL CHECKING

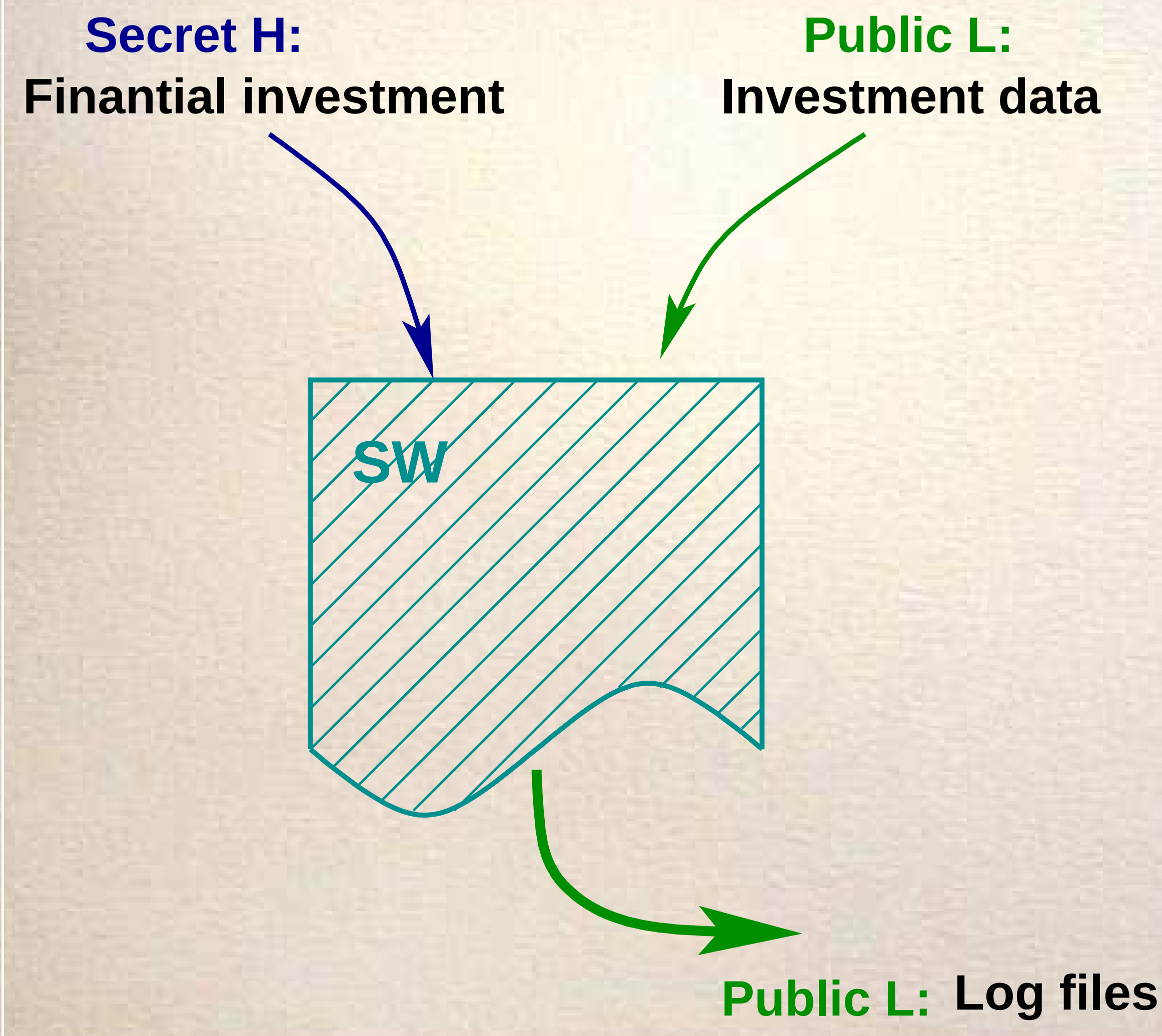
[Cousot & Cousot '00]

Let $\Phi \in \mu$-calculus: $[\![\Phi]\!]^{State} \subset \alpha^{State}([\![\Phi]\!]^{Trace})$

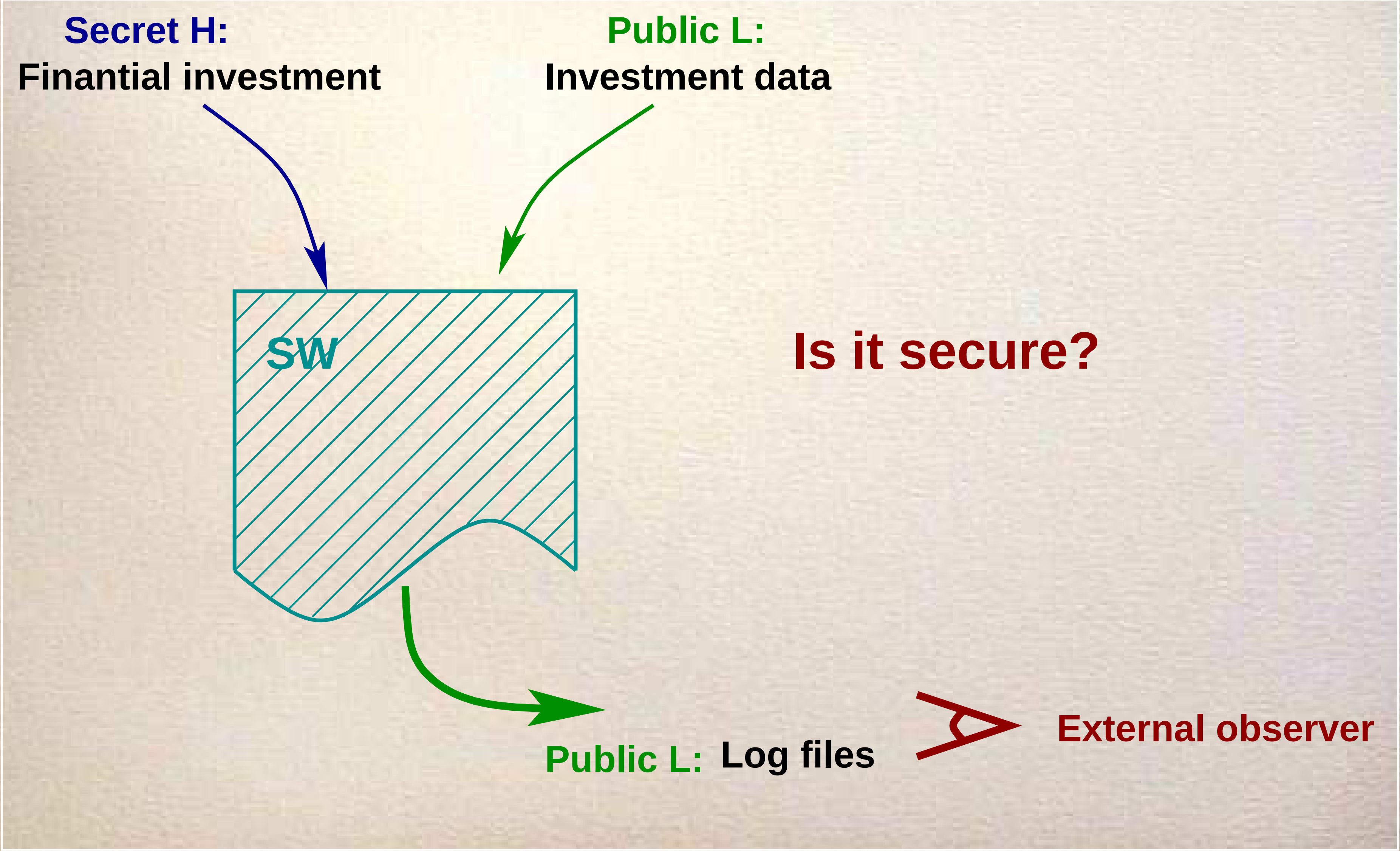


STATE-BASED MODEL CHECKING IS INTRINSICALLY INCOMPLETE FOR PROPERTIES OF TRACES!!

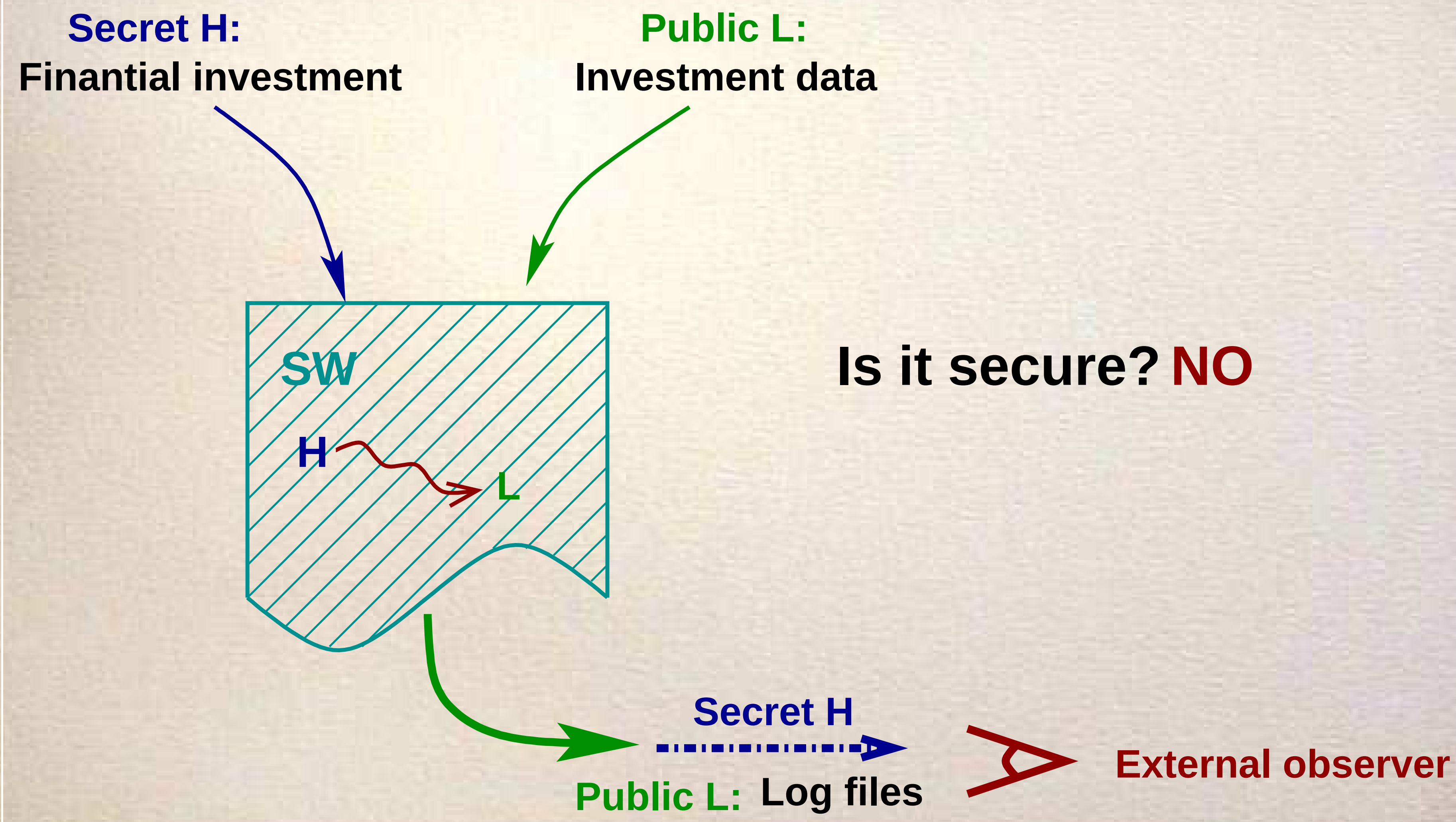
In Security: Non-Interference



In Security: Non-Interference

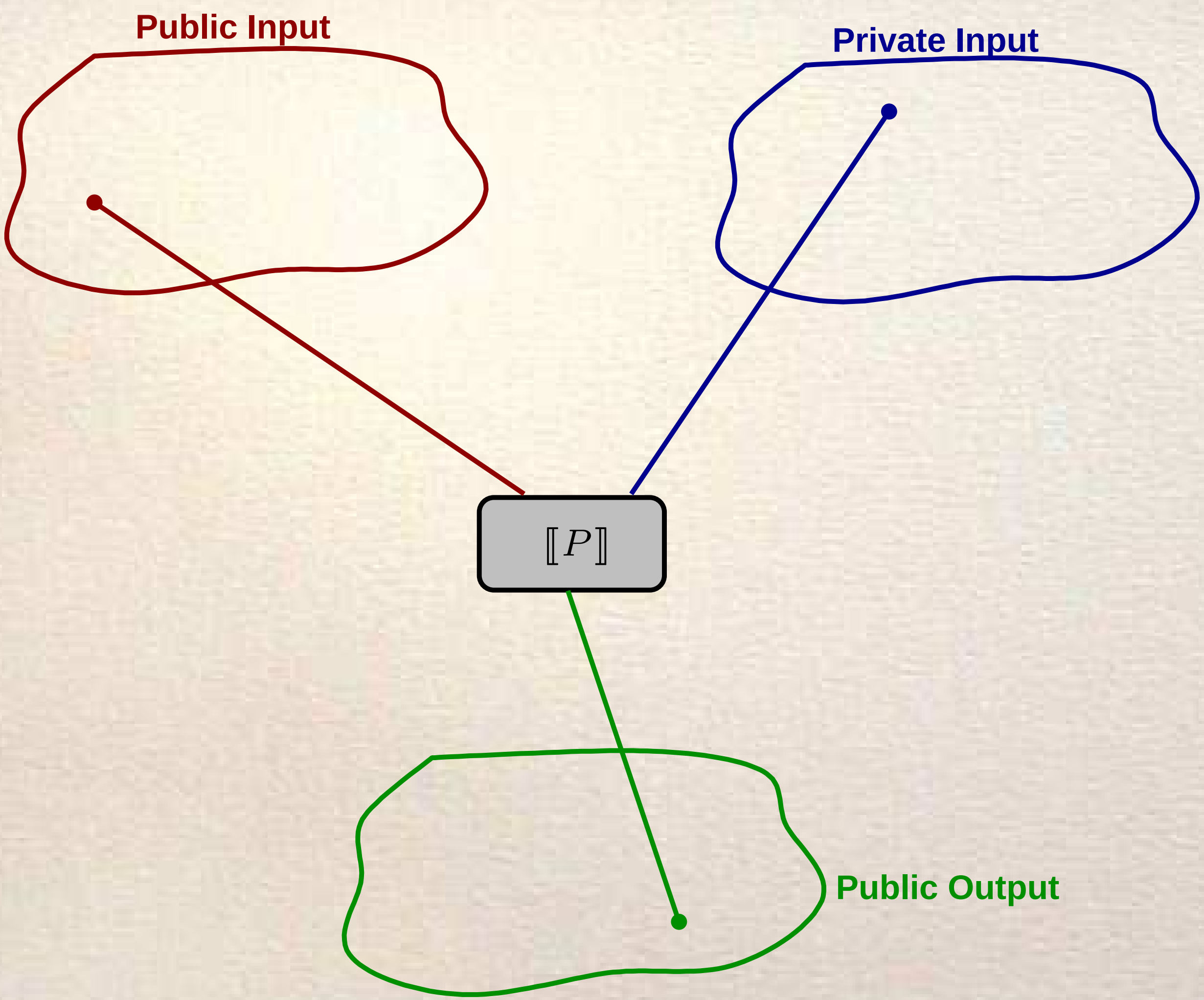


IN SECURITY: NON-INTERFERENCE



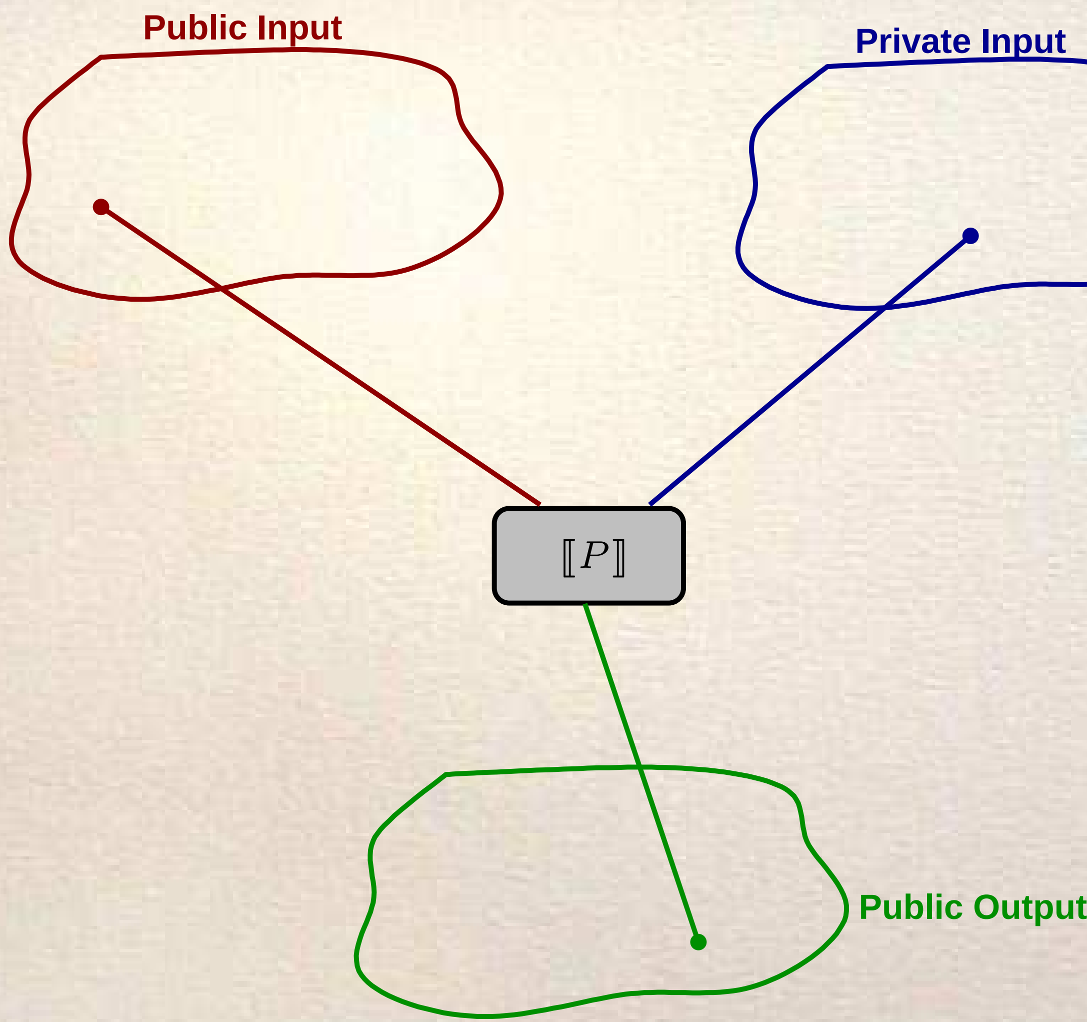
Is it secure? NO

STANDARD NON-INTERFERENCE



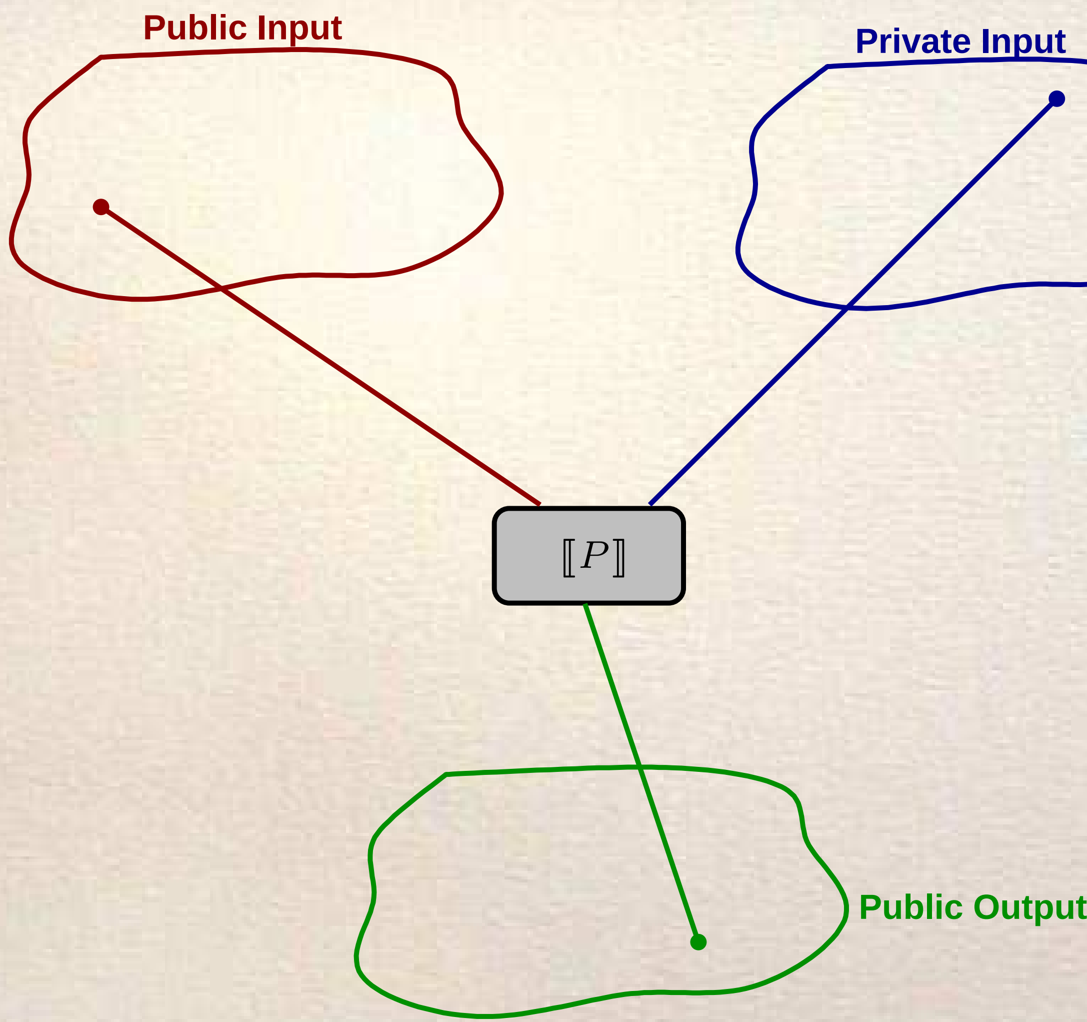
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard Non-Interference



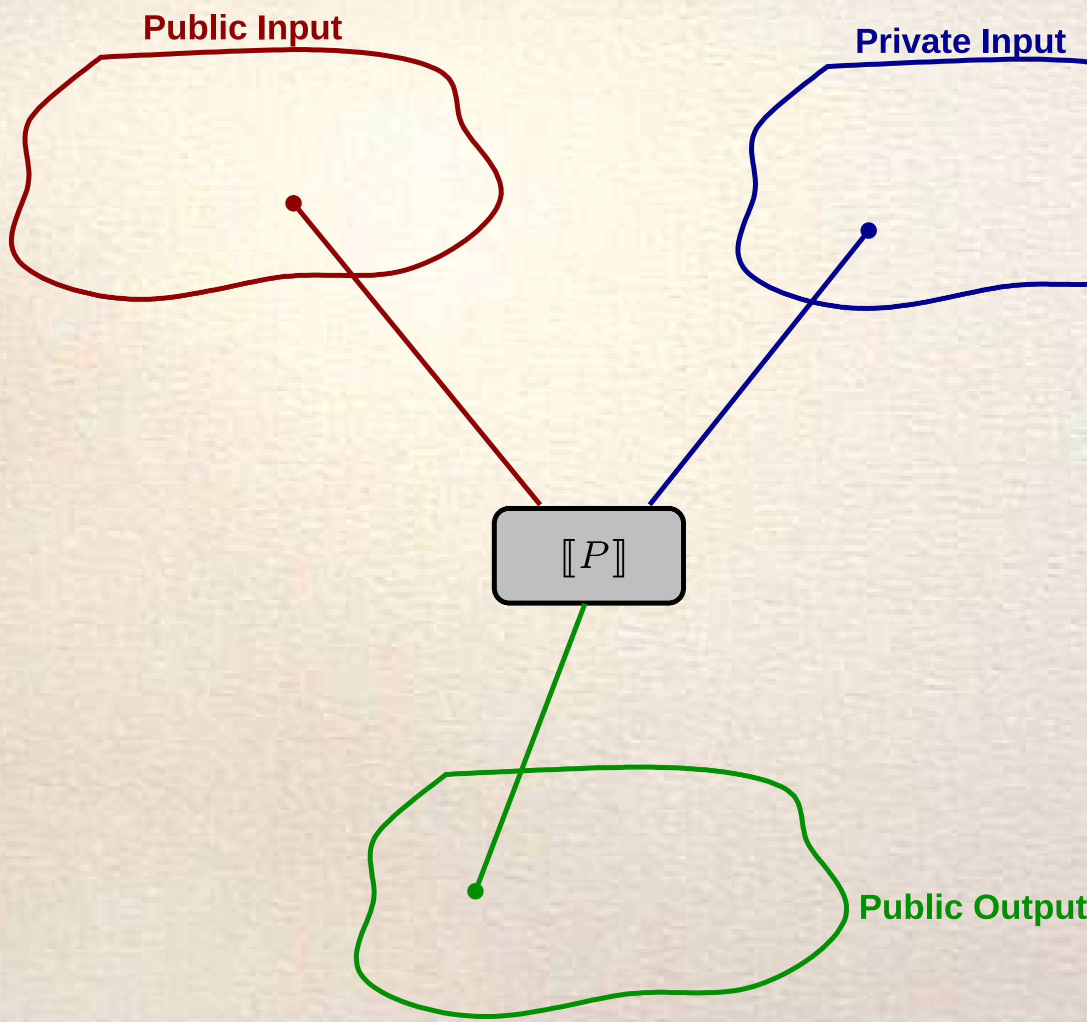
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

Standard Non-Interference



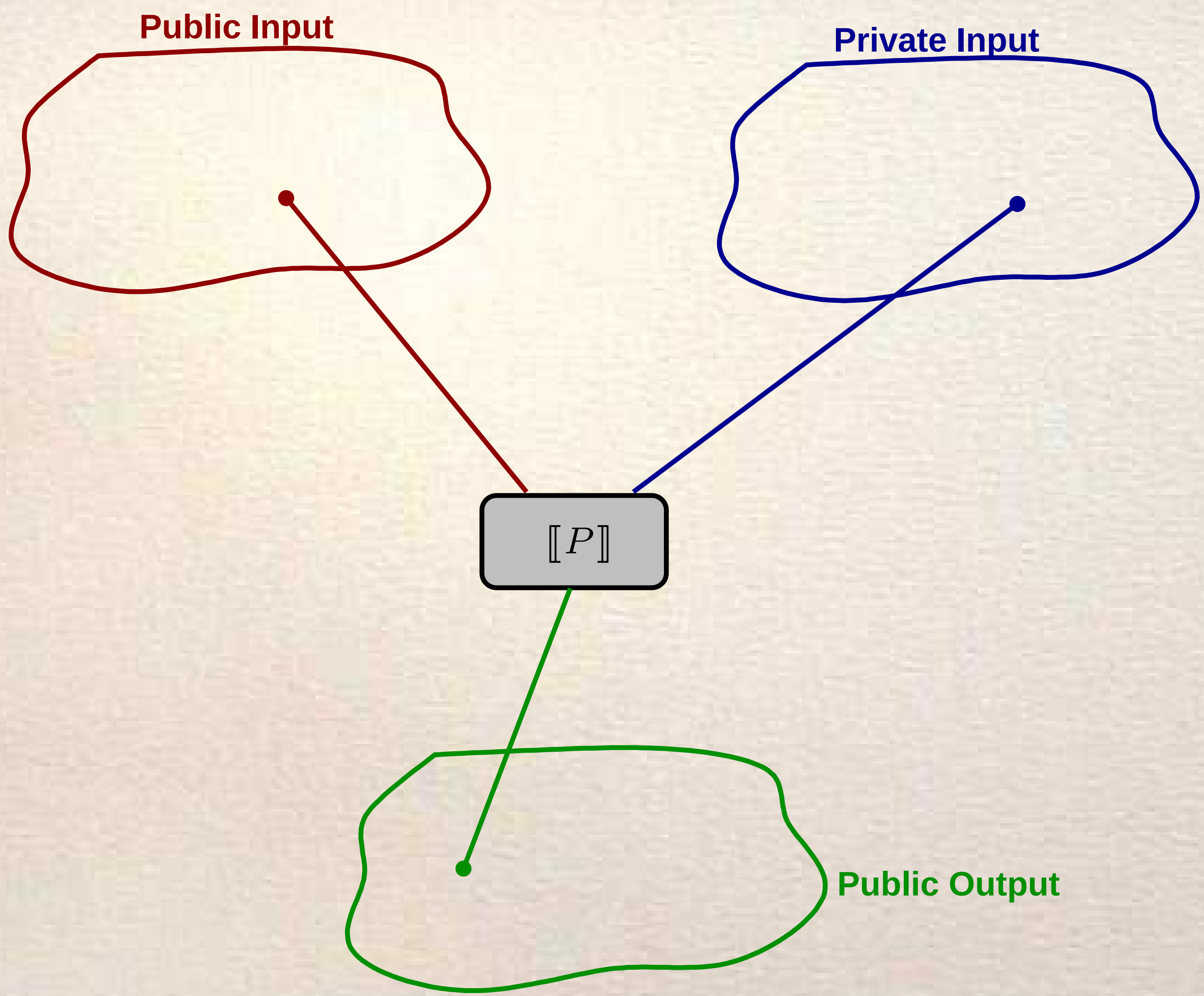
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

STANDARD NON-INTERFERENCE



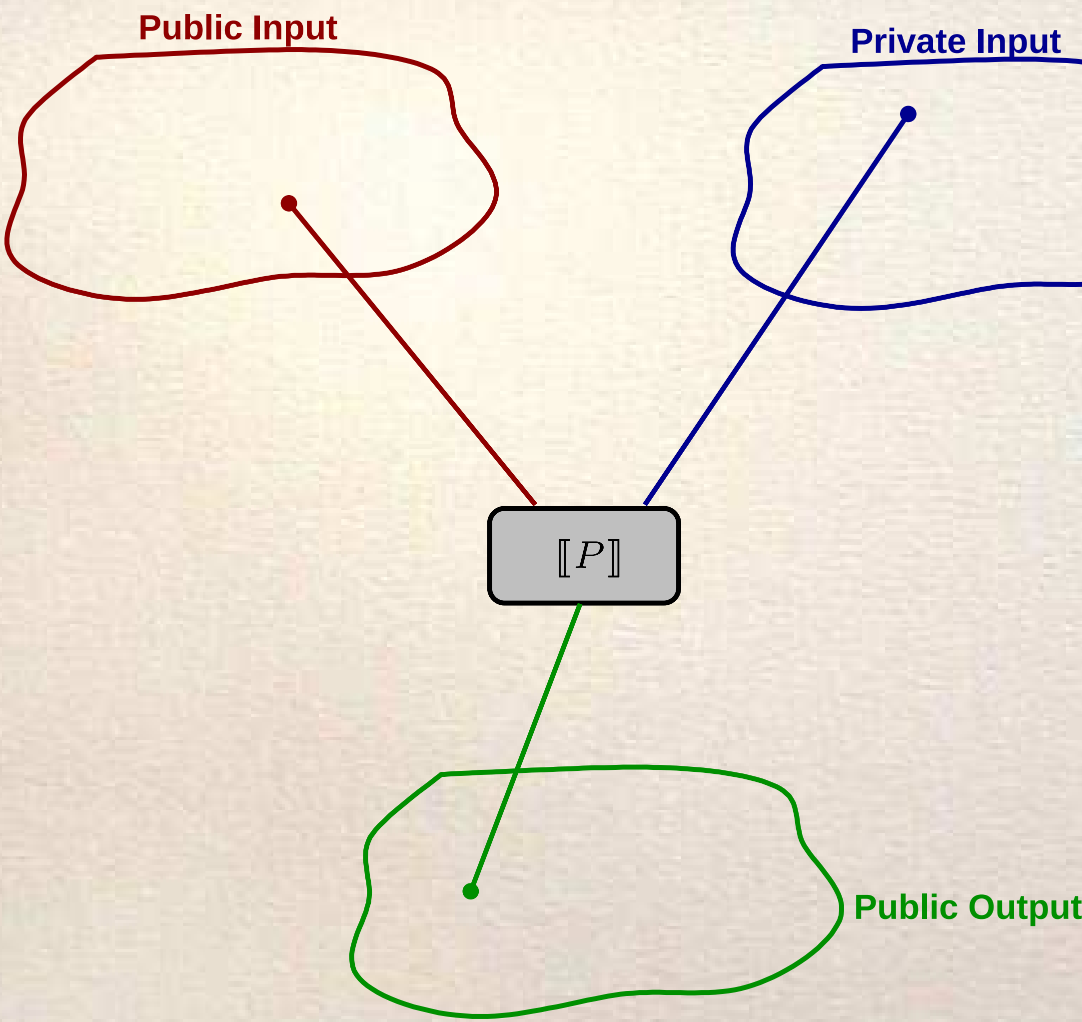
$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

STANDARD NON-INTERFERENCE



$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ \llbracket P \rrbracket(h_1, l)^{\mathsf{L}} = \llbracket P \rrbracket(h_2, l)^{\mathsf{L}}$$

STANDARD NON-INTERFERENCE



$$\forall l : \mathsf{L}, \forall h_1, h_2 : \mathsf{H}.\ [\![P]\!](h_1, l)^{\mathsf{L}} = [\![P]\!](h_2, l)^{\mathsf{L}}$$

NI: A COMPLETENESS PROBLEM

Recall that [Joshi & Leino'00]

$$P \text{ is } \textit{secure} \quad \text{iff} \quad \mathtt{HH}\,;\, P;\, \mathtt{HH} \doteq P\,;\, \mathtt{HH}$$

NI: A COMPLETENESS PROBLEM

Recall that [Joshi & Leino'00]

$$P \text{ is } \textit{secure} \quad \text{iff} \quad \mathsf{HH}\,;\,P;\,\mathsf{HH} \doteq P\,;\,\mathsf{HH}$$

Let $X = \langle X^{\mathsf{H}}, X^{\mathsf{L}}\rangle \Rightarrow \mathcal{H}(X) \stackrel{\text{def}}{=} \langle \top^{\mathsf{H}}, X^{\mathsf{L}}\rangle \in \mathit{uco}(\wp(\mathbb{V}))$

$$\begin{array}{ccc} \mathsf{HH}\,;\,P;\,\mathsf{HH} & \doteq & P\,;\,\mathsf{HH} \\ & \Downarrow & \\ \mathcal{H}\circ[\![P]\!]\circ\mathcal{H} & = & \mathcal{H}\circ[\![P]\!] \end{array}$$

NI: A COMPLETENESS PROBLEM

Recall that [Joshi & Leino'00]

$$P \text{ is } \textit{secure} \qquad \text{iff} \qquad \mathsf{HH}\,;\ P;\ \mathsf{HH} \doteq P\,;\ \mathsf{HH}$$

$$\text{Let } X = \langle X^{\mathsf{H}}, X^{\mathsf{L}} \rangle \Rightarrow \mathcal{H}(X) \stackrel{\text{def}}{=} \langle \top^{\mathsf{H}}, X^{\mathsf{L}} \rangle \in \mathit{uco}(\wp(\mathbb{V}))$$

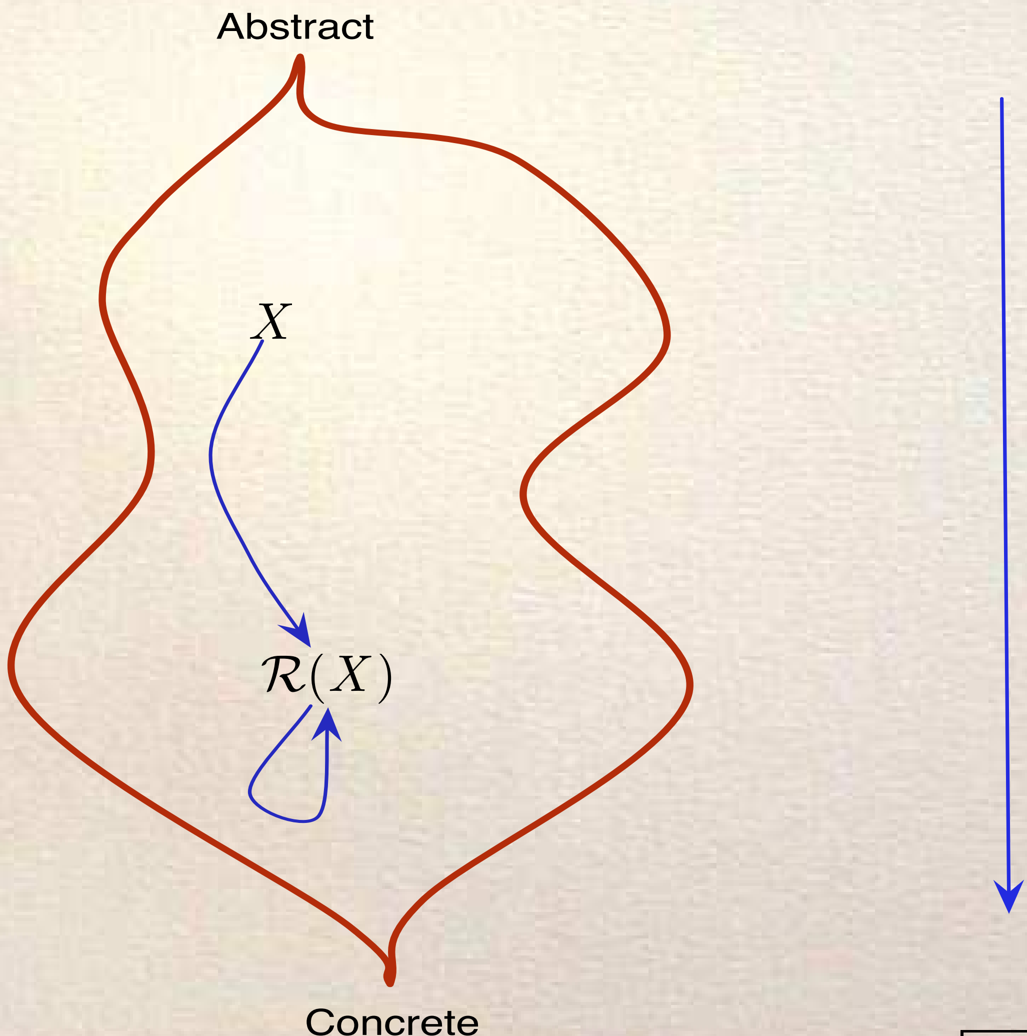
$$\begin{array}{ccc} \mathsf{HH}\,;\ P;\ \mathsf{HH} & \doteq & P\,;\ \mathsf{HH} \\ & \Downarrow & \\ \mathcal{H} \circ [\![P]\!] \circ \mathcal{H} & = & \mathcal{H} \circ [\![P]\!] \end{array}$$

$\boxed{\Rightarrow \text{A COMPLETENESS PROBLEM}}$

MAKING
ABSTRACT INTERPRETATIONS COMPLETE

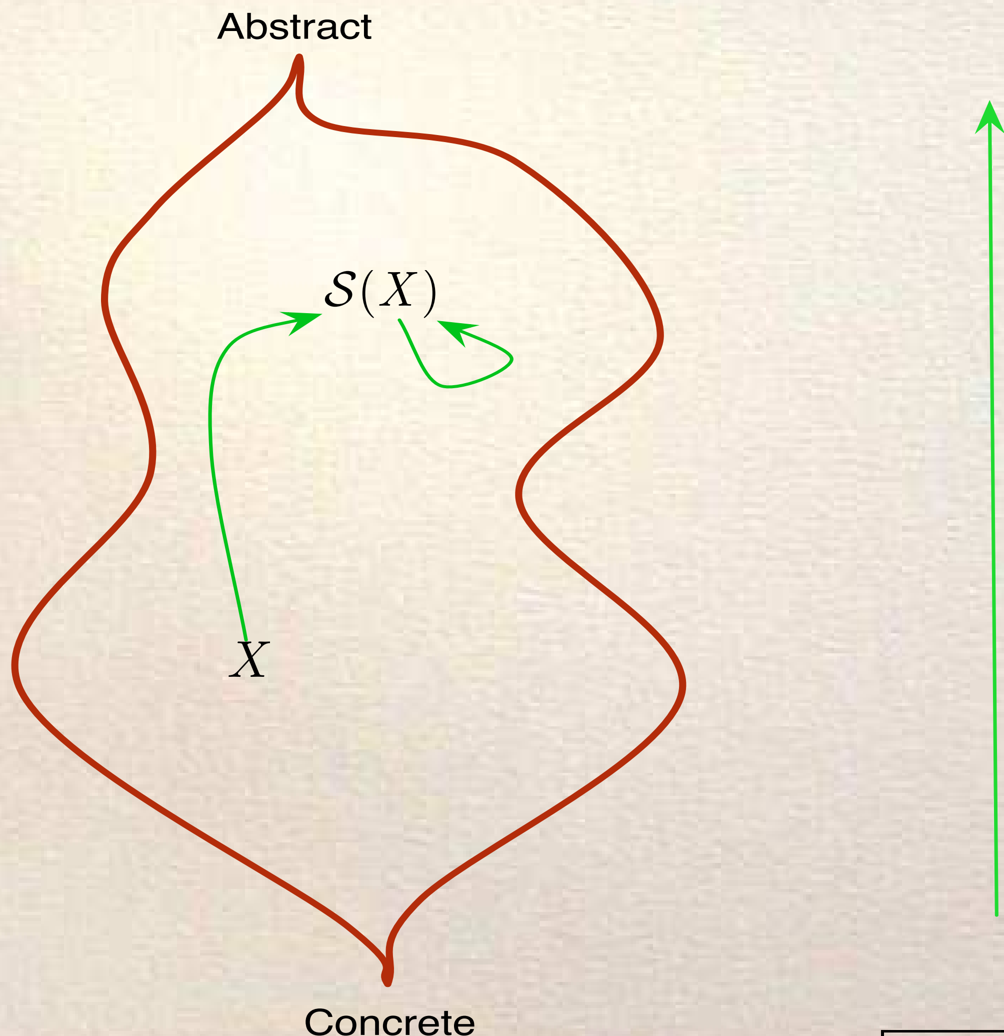
10 YEARS AFTER

THE GEOMETRY OF AI TRANSFORMERS



lco – REFINEMENT

THE GEOMETRY OF AI TRANSFORMERS



$\boxed{uco - \text{SIMPLIFICATION}}$

The Geometry of AI transformers

Can we use abstract interpretation for transforming abstract interpretations?

- Refinements: $X \subseteq \mathcal{R}(X)$ (improving precision – lower closure)
- Simplification: $\mathcal{S}(X) \subseteq X$ (reducing precision – upper closure)

[Janowitz '67]

$$(1)\ \eta \in uco(C) \Leftrightarrow \eta^+ \in lco(C) \Leftrightarrow \begin{cases} \eta \circ \eta^+ = \eta^+ \\ \eta^+ \circ \eta = \eta \end{cases}$$

$$(2)\ \eta \in uco(C) \Leftrightarrow \eta^- \in lco(C) \Leftrightarrow \begin{cases} \eta \circ \eta^- = \eta \\ \eta^- \circ \eta = \eta^- \end{cases}$$

THE GEOMETRY OF AI TRANSFORMERS

Can we use abstract interpretation for transforming abstract interpretations?

- Refinements: $X \subseteq \mathcal{R}(X)$ (improving precision – lower closure)
- Simplification: $\mathcal{S}(X) \subseteq X$ (reducing precision – upper closure)

[Janowitz '67]

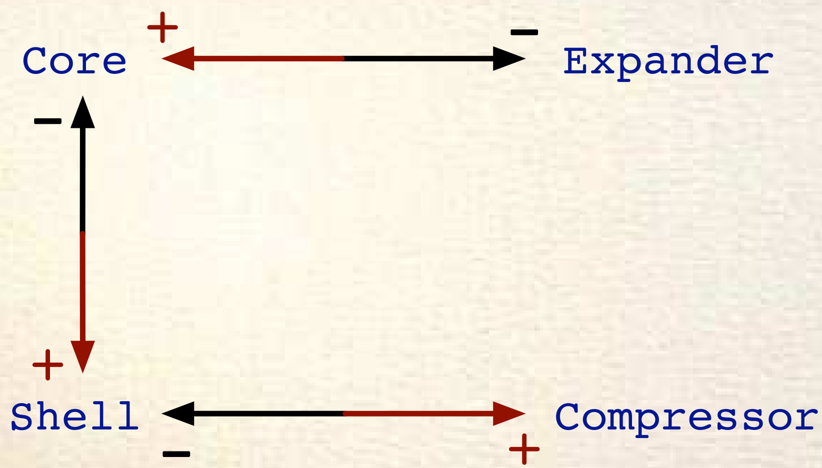
$$(1)\ \ \mathcal{S} \text{ simplification } \Leftrightarrow \mathcal{S}^{+} \text{refinement } \Leftrightarrow \begin{cases} \mathcal{S} \circ \mathcal{S}^{+} = \mathcal{S}^{+} \\ \mathcal{S}^{+} \circ \mathcal{S} = \mathcal{S} \end{cases}$$

Shell/Core of a given property

$$(2)\ \ \mathcal{S} \text{ simplification } \Leftrightarrow \mathcal{S}^{-} \text{refinement } \Leftrightarrow \begin{cases} \mathcal{S} \circ \mathcal{S}^{-} = \mathcal{S} \\ \mathcal{S}^{-} \circ \mathcal{S} = \mathcal{S}^{-} \end{cases}$$

Expander/Compressor for a given property

THE GEOMETRY OF DOMAIN TRANSFORMERS



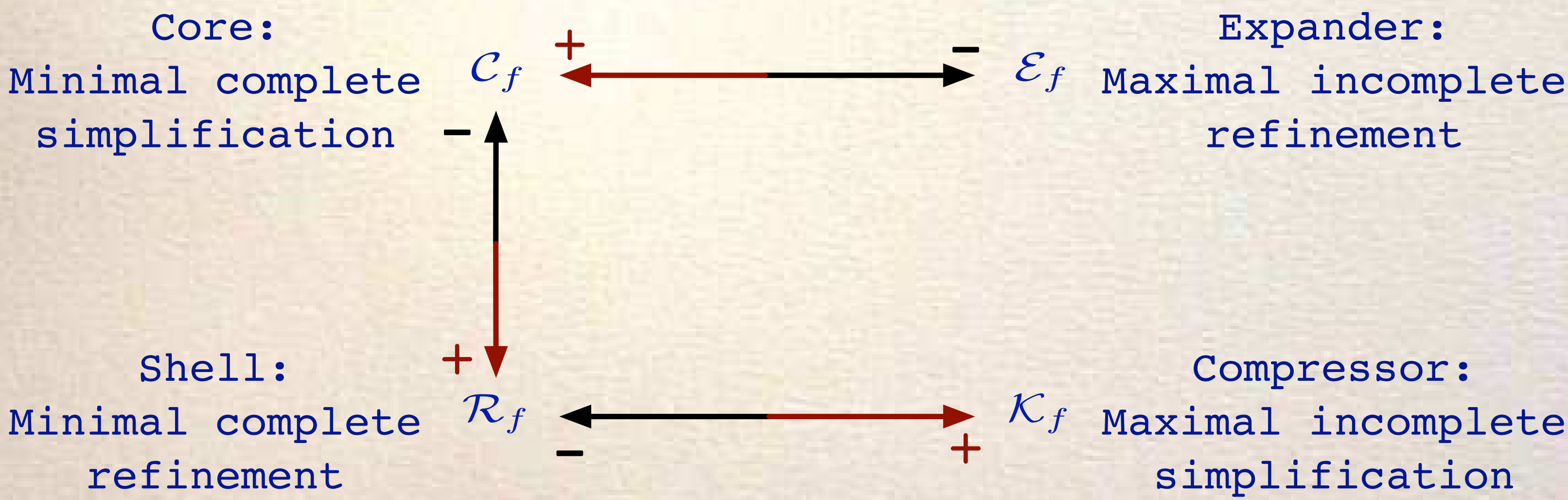
- Shell/Core minimally transform domains in order to achieve a given property

- Expander/Compressor maximally transform domains in order to achieve a given property

WHAT IS THE MEANING OF SHELL/CORE AND EXPANDER/COMPRESSOR FOR THE COMPLETENESS PROPERTY?

THE GEOMETRY OF DOMAIN TRANSFORMERS

Basic abstract domain transformers

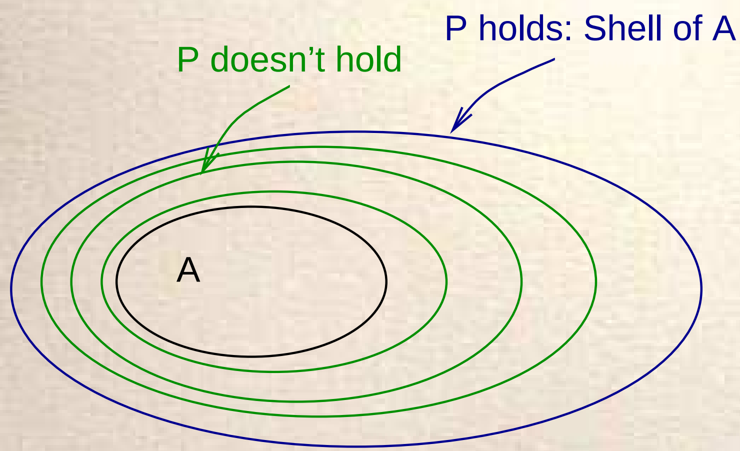


[Giacobazzi et al.'00]

[SAS'08]

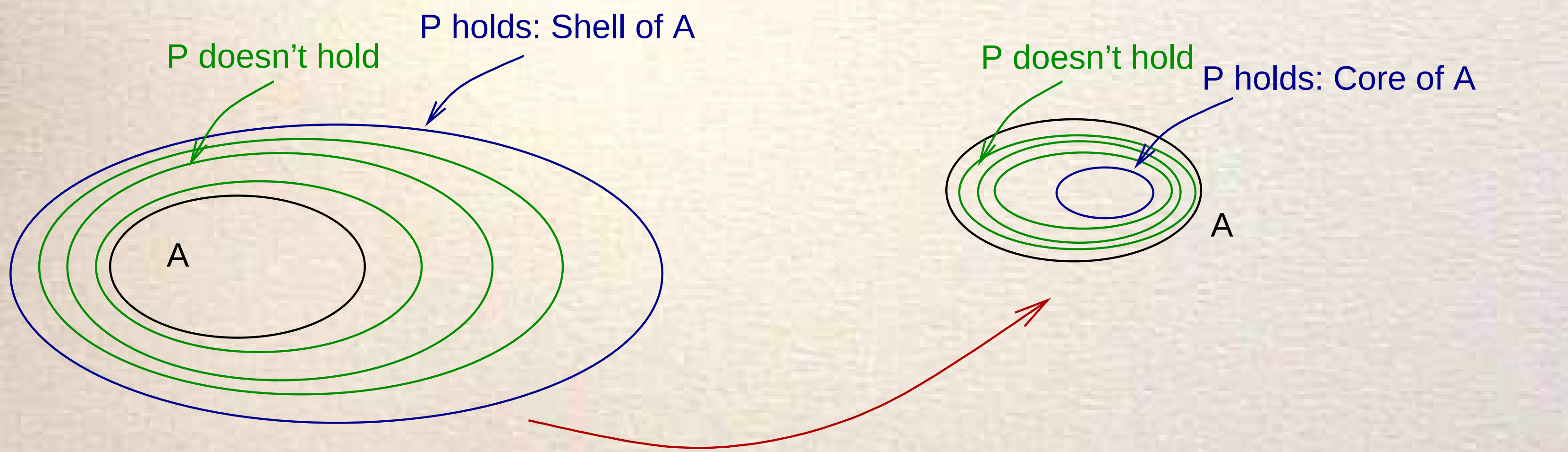
SHELL/CORE

Let P be completeness

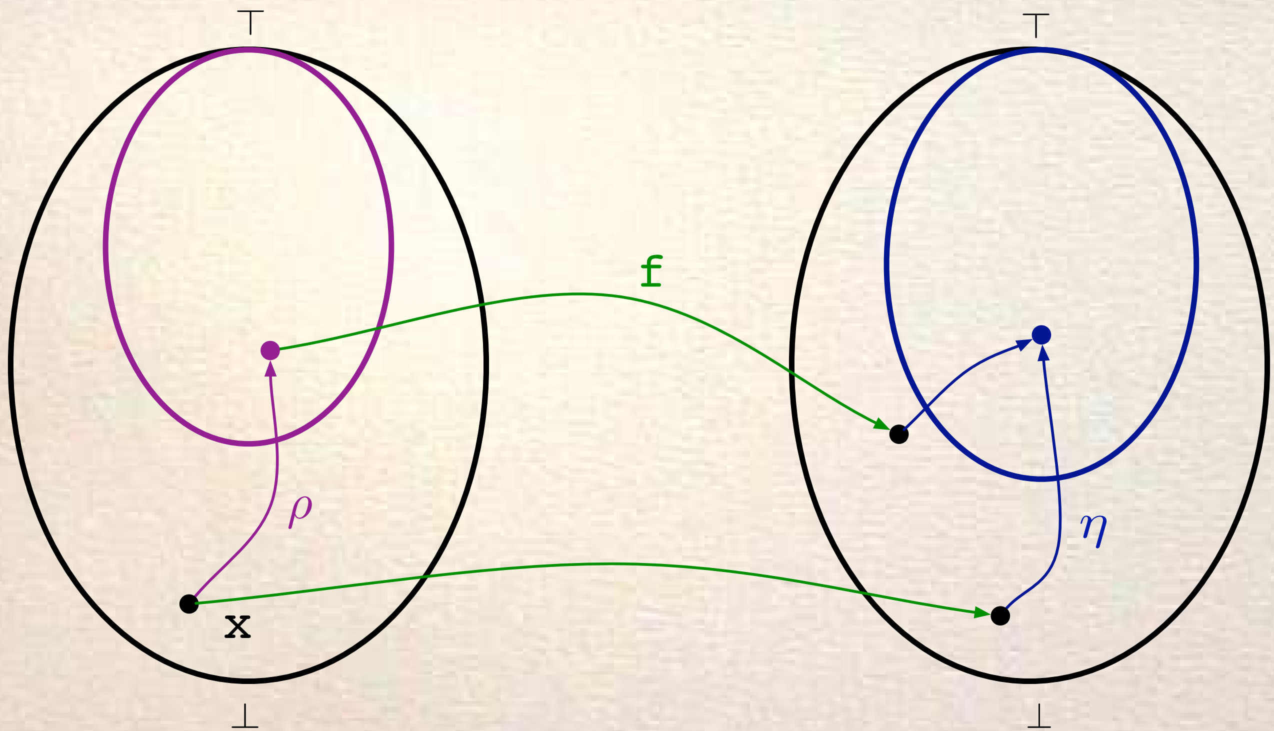


SHELL/CORE

Let P be completeness

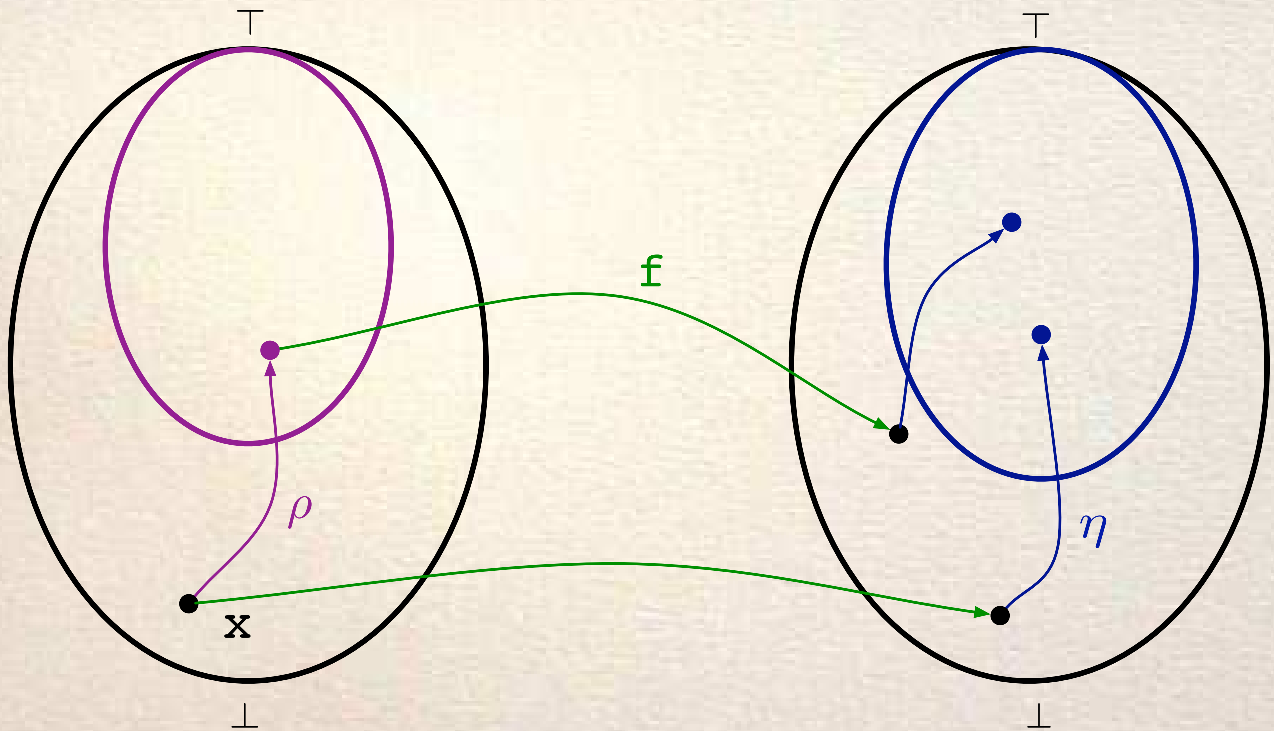


DOMAIN COMPLETENESS: SHELL/CORE



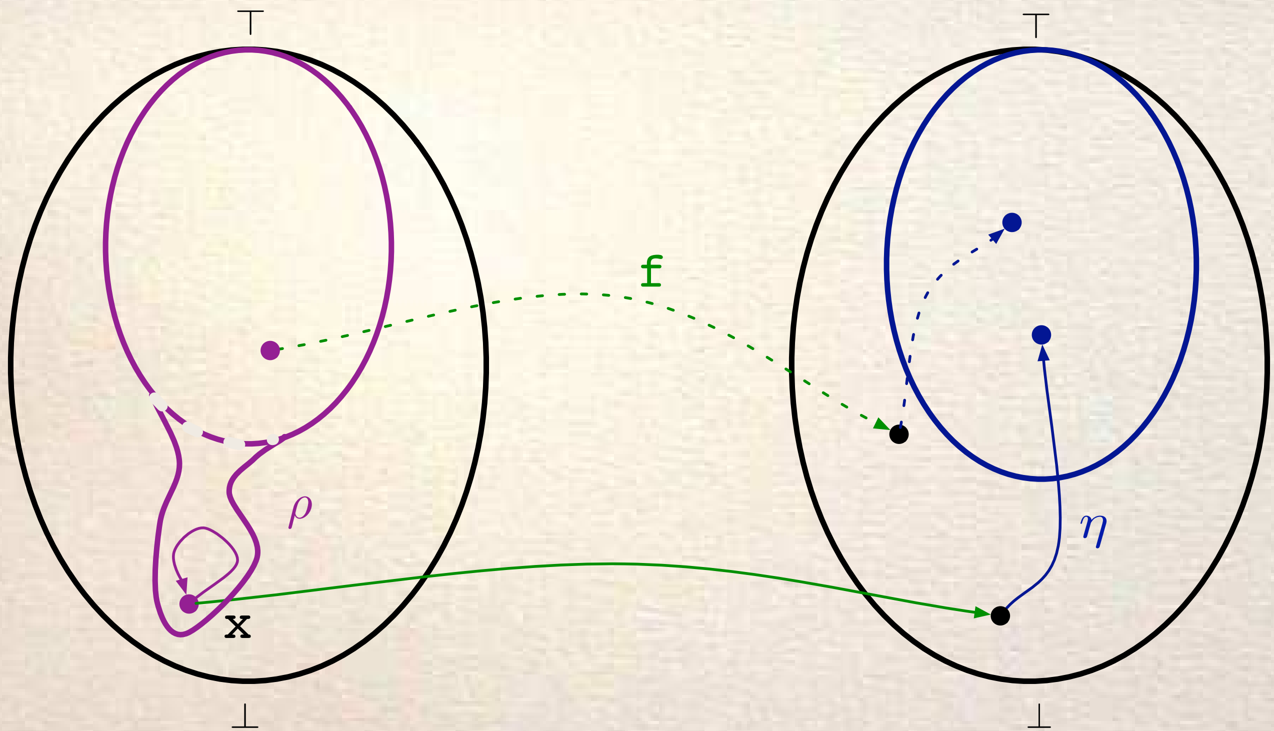
BACKWARD COMPLETENESS: $\eta \circ f \circ \rho = \eta \circ f$

DOMAIN COMPLETENESS: SHELL/CORE



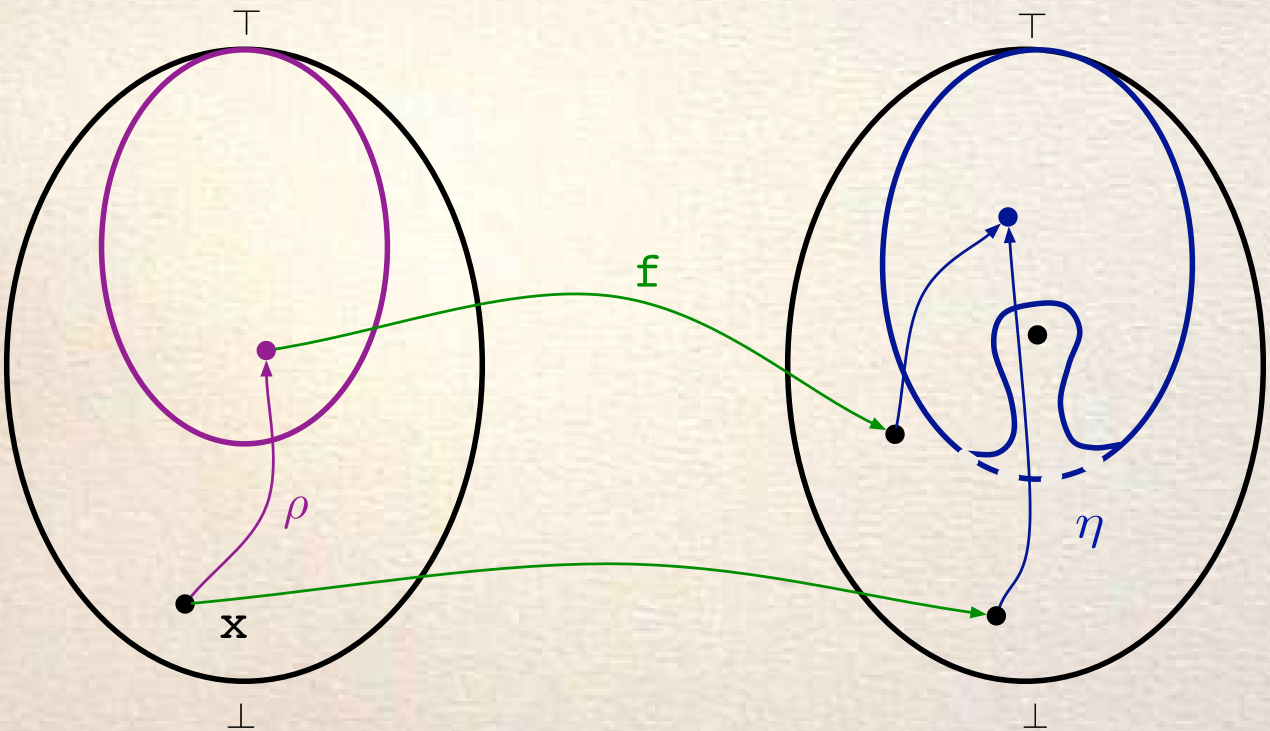
BACKWARD IN-COMPLETENESS: $\eta \circ f \circ \rho \geq \eta \circ f$

DOMAIN COMPLETENESS: SHELL/CORE



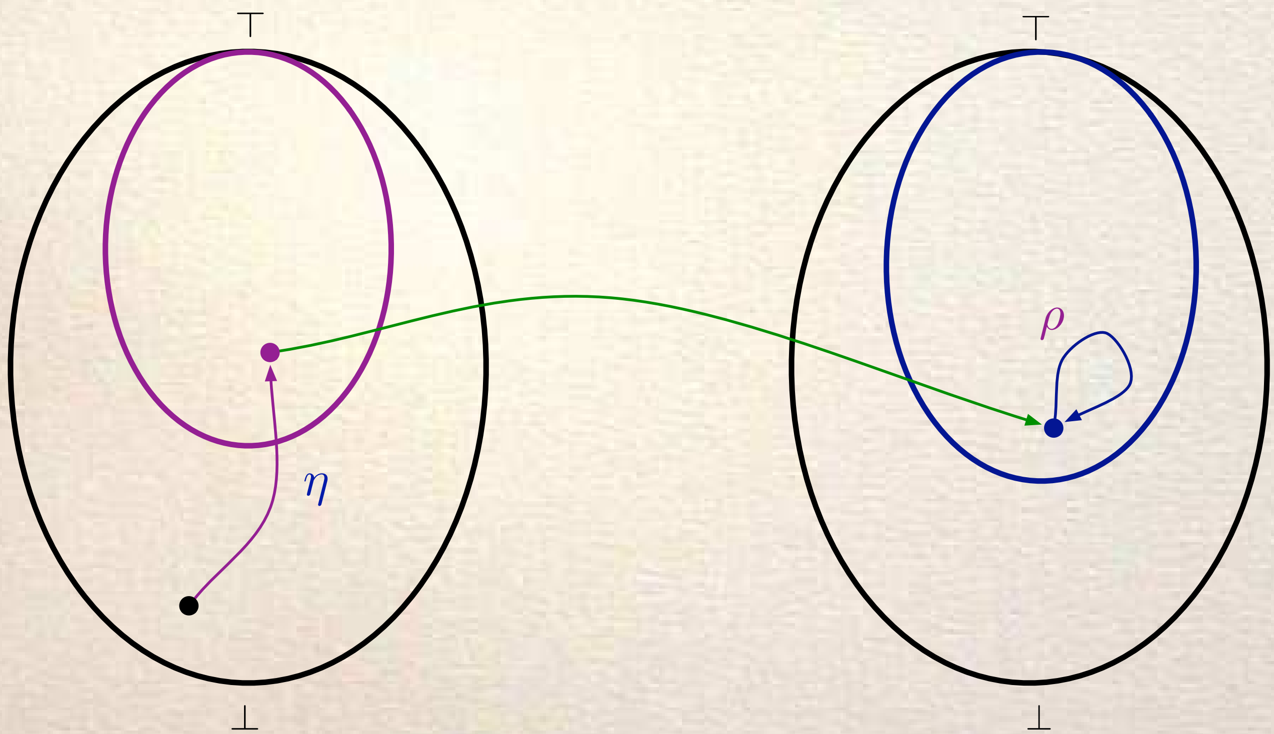
Making BACKWARD COMPLETE: Refining input domains [GRS'00]

Domain Completeness: Shell/Core



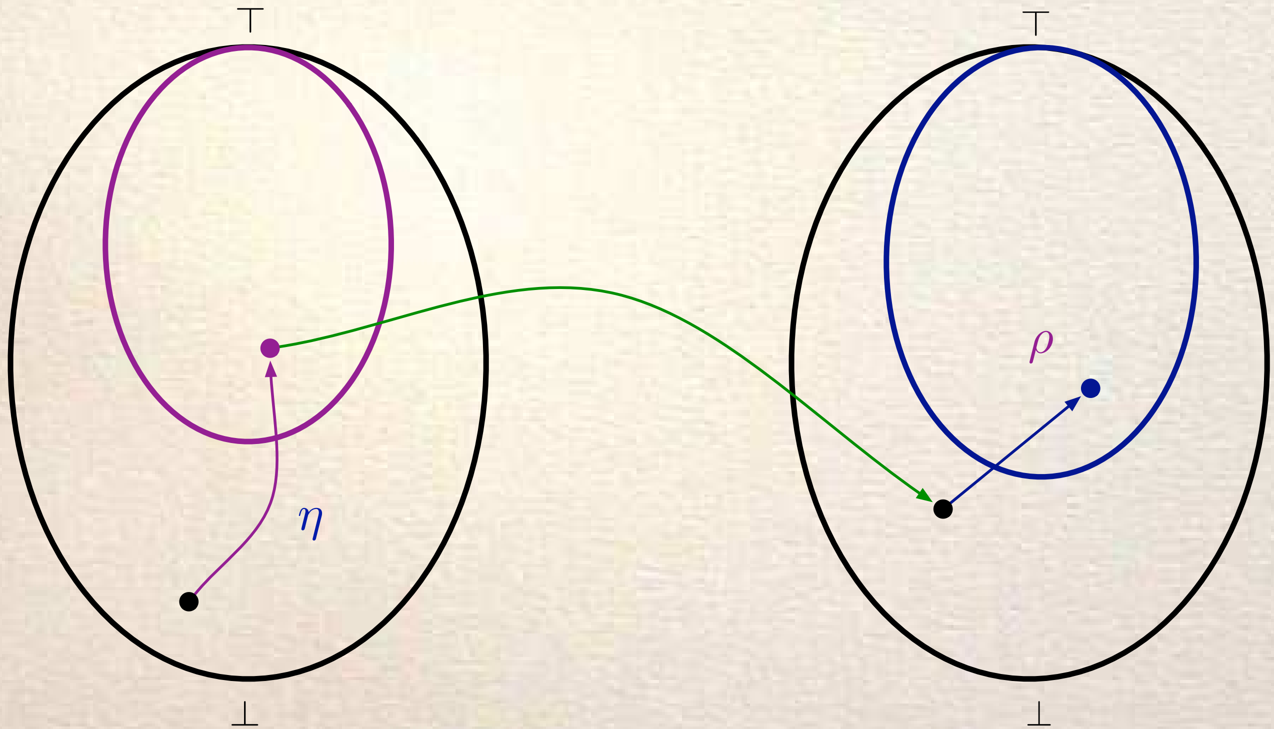
Making BACKWARD COMPLETE: Simplifying output domains [GRS'00]

DOMAIN COMPLETENESS: SHELL/CORE



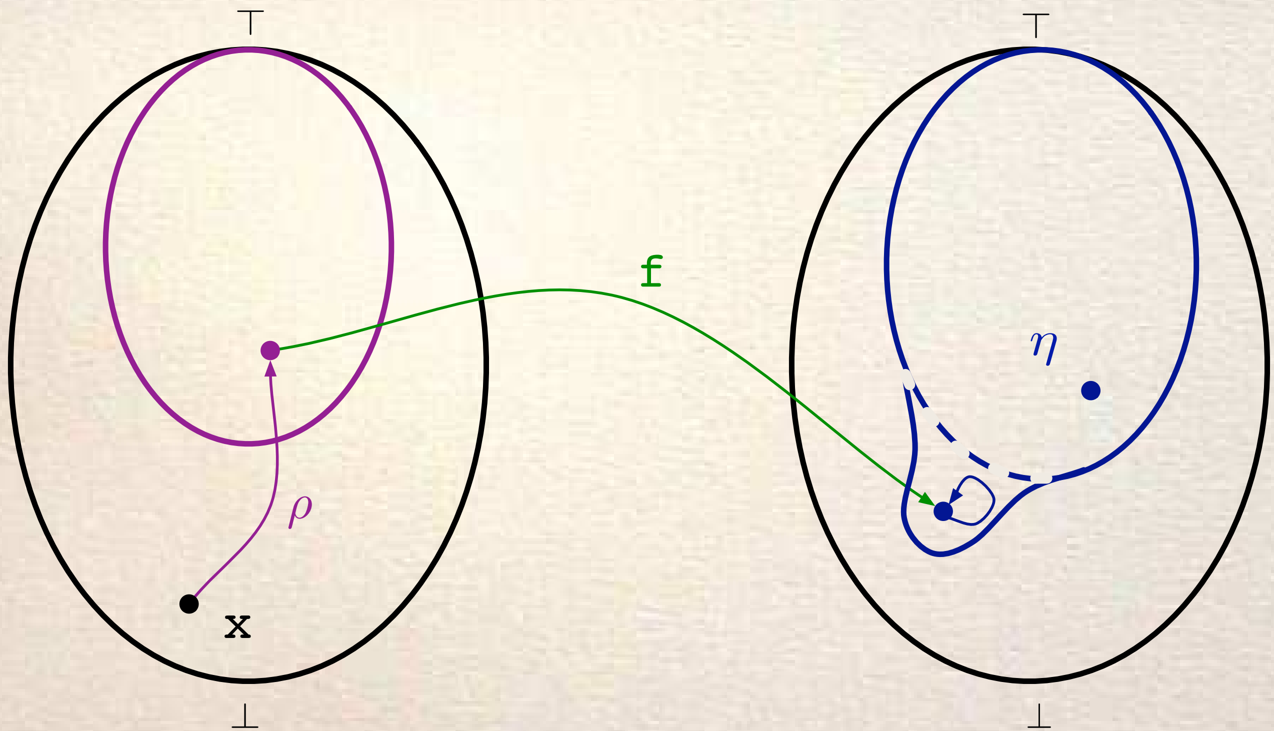
FORWARD COMPLETENESS: $\eta \circ f \circ \rho = f \circ \rho$

DOMAIN COMPLETENESS: SHELL/CORE



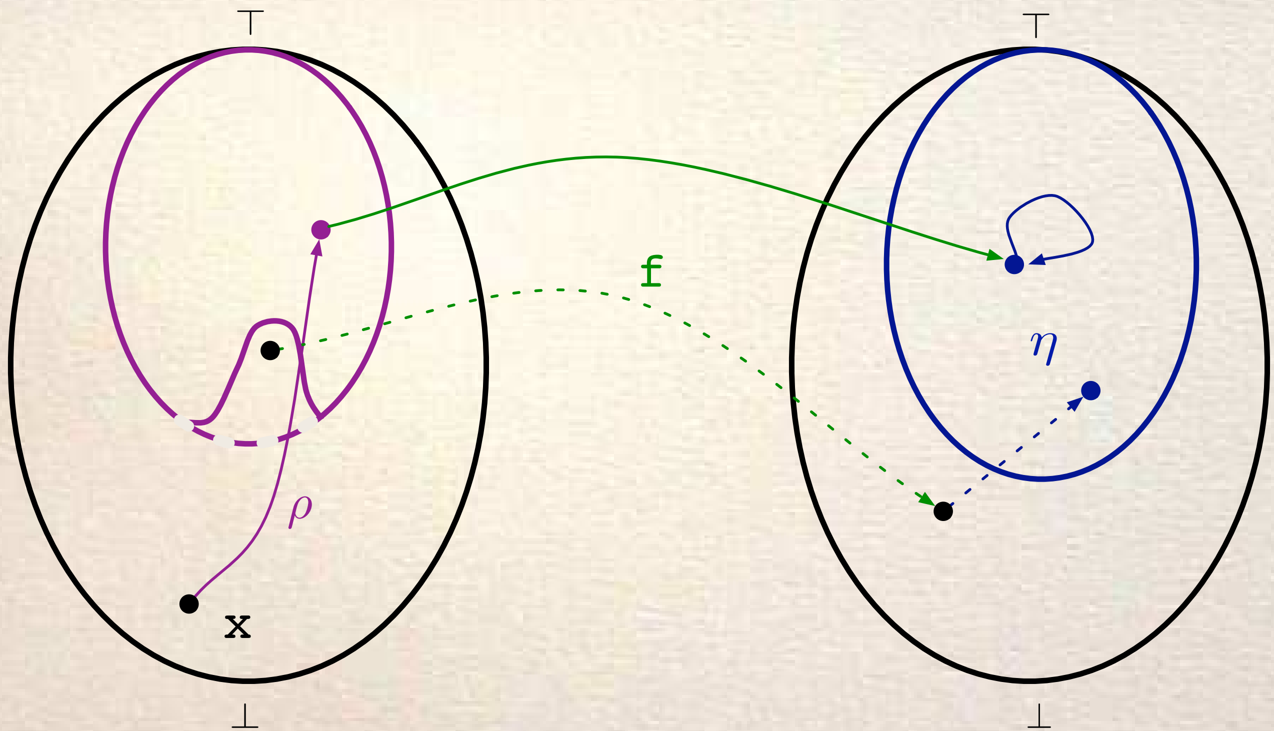
FORWARD IN-COMPLETENESS: $\eta \circ f \circ \rho \geq f \circ \rho$

DOMAIN COMPLETENESS: SHELL/CORE



Making FORWARD COMPLETE: Refining output domains [GQ'01]

DOMAIN COMPLETENESS: SHELL/CORE



Making FORWARD COMPLETE: Simplifying input domains [GQ'01]

BACKWARD VS FORWARD

- A domain is *backward complete* wrt f iff it is *forward complete* wrt $f^+ = \lambda X.\bigcup\left\{ Y \,\middle|\, f(Y) \subseteq X \right\}$;
- A (not trivial) partition is *backward stable* wrt f iff it is *forward stable* wrt $f^{-1} = \lambda X.\left\{ y \,\middle|\, f(y) \in X \right\}$;
- If f is injective, a (not trivial) partition is *forward stable* wrt f iff it is *backward stable* wrt f^{-1};

Backward vs Forward

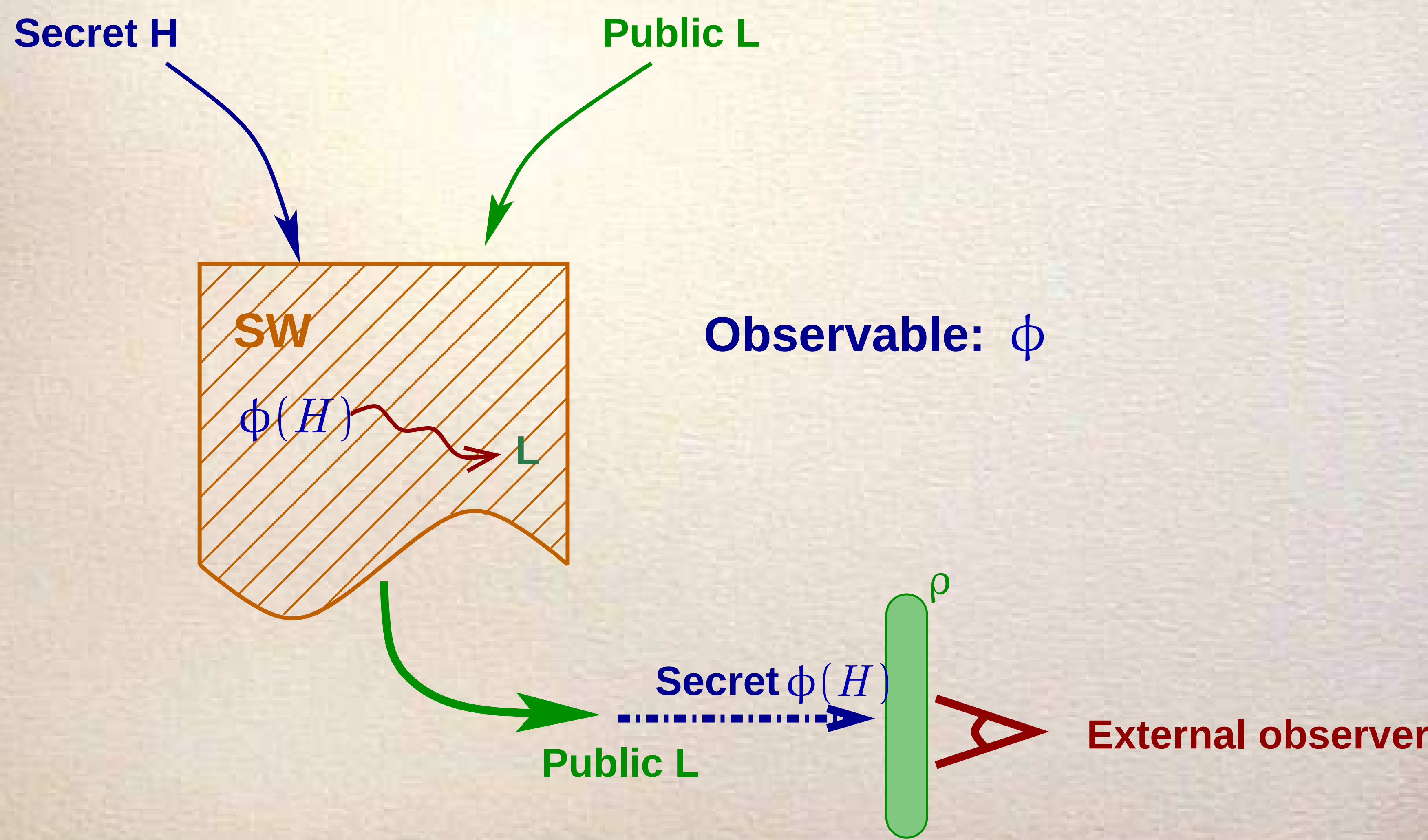
- A domain is *backward complete* wrt f iff it is *forward complete* wrt $f^{+} = \lambda X. \bigcup \left\{ Y \,\middle|\, f(Y) \subseteq X \right\}$;

- A (not trivial) partition is *backward stable* wrt f iff it is *forward stable* wrt $f^{-1} = \lambda X. \left\{ y \,\middle|\, f(y) \in X \right\}$;

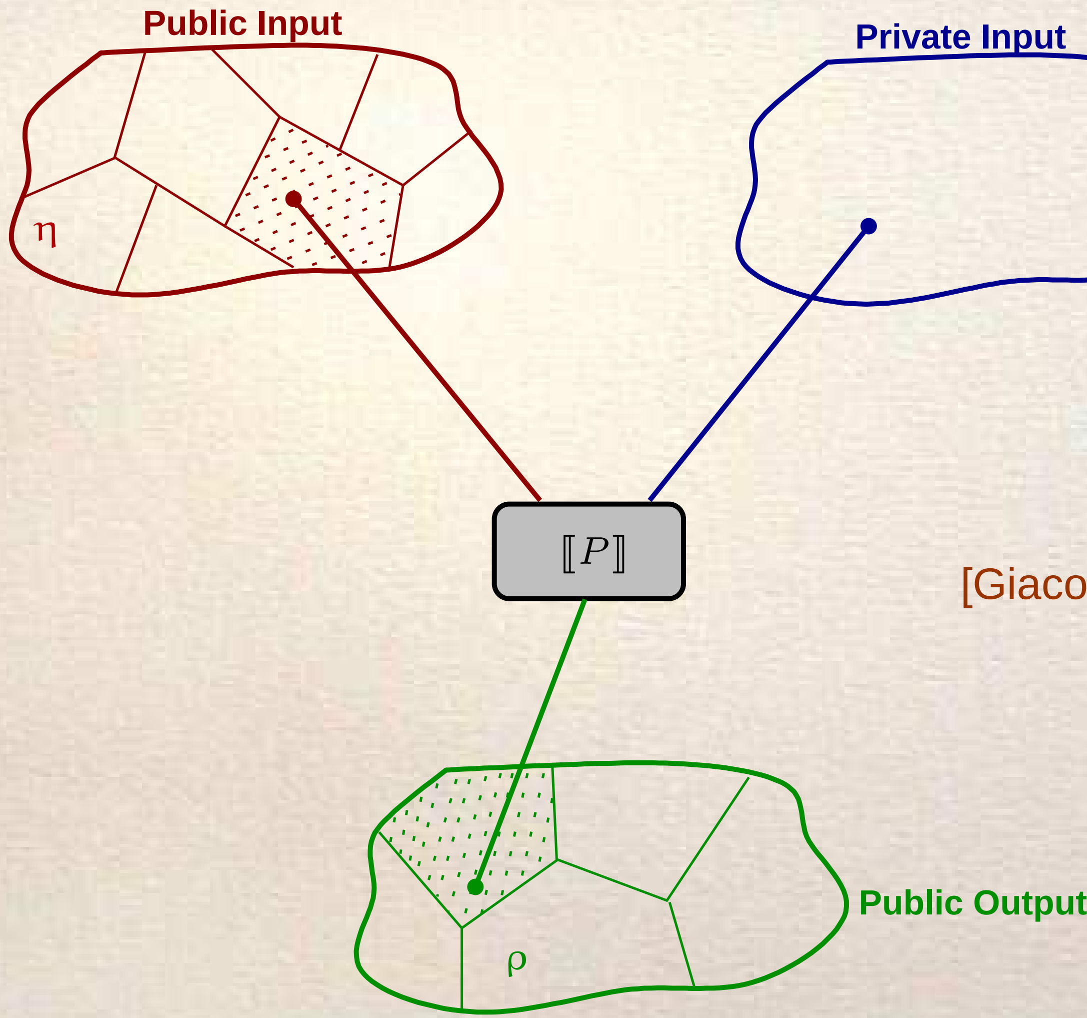
- If f is injective, a (not trivial) partition is *forward stable* wrt f iff it is *backward stable* wrt f^{-1};

A backward problem can always be transformed in a forward one, but the viceversa is not always possible!

NEW PERSPECTIVES IN LANGUAGE-BASED SECURITY



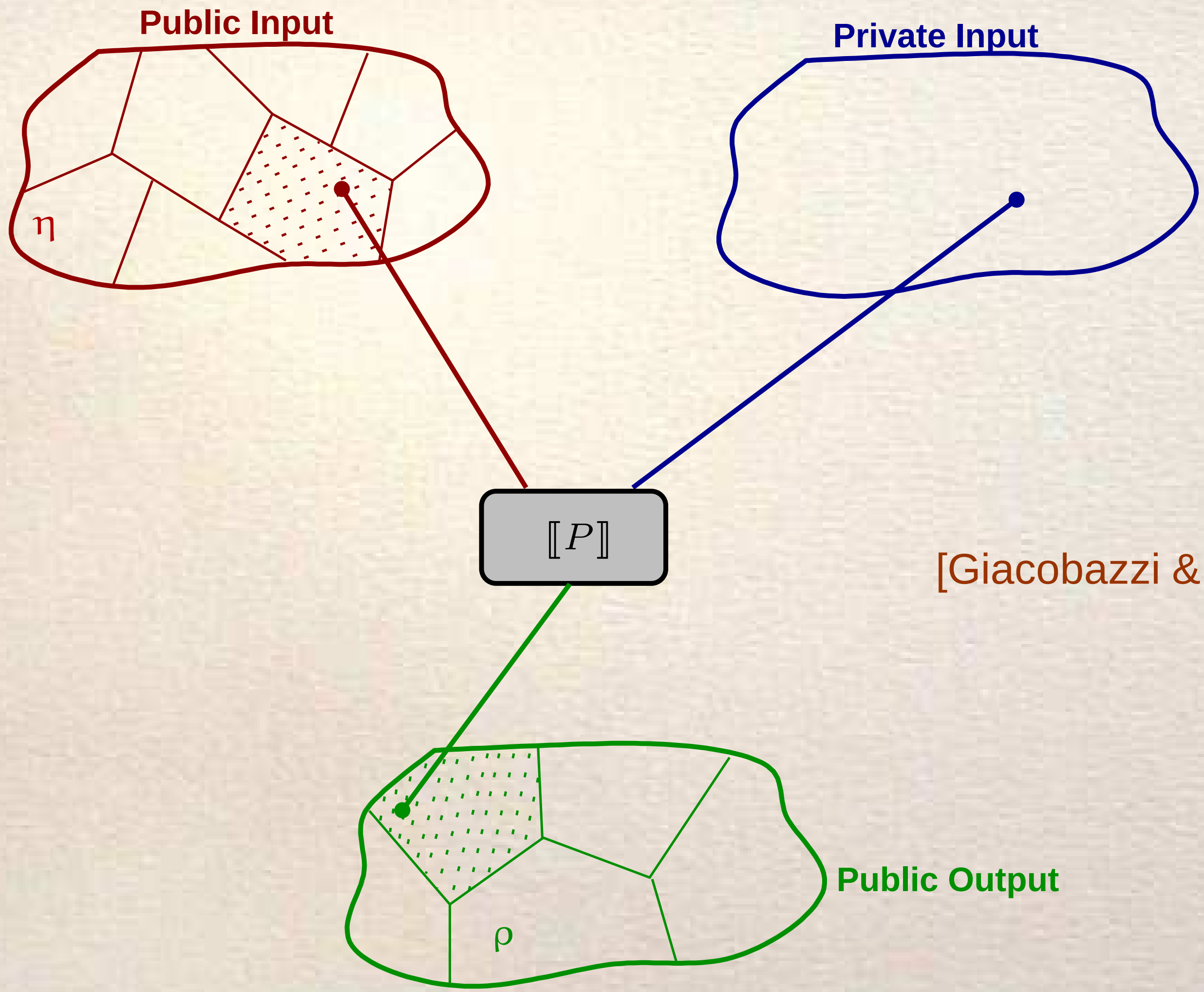
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})):\ [\eta]P(\rho):\ \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(h_2, l_2)^{\mathsf{L}})$$

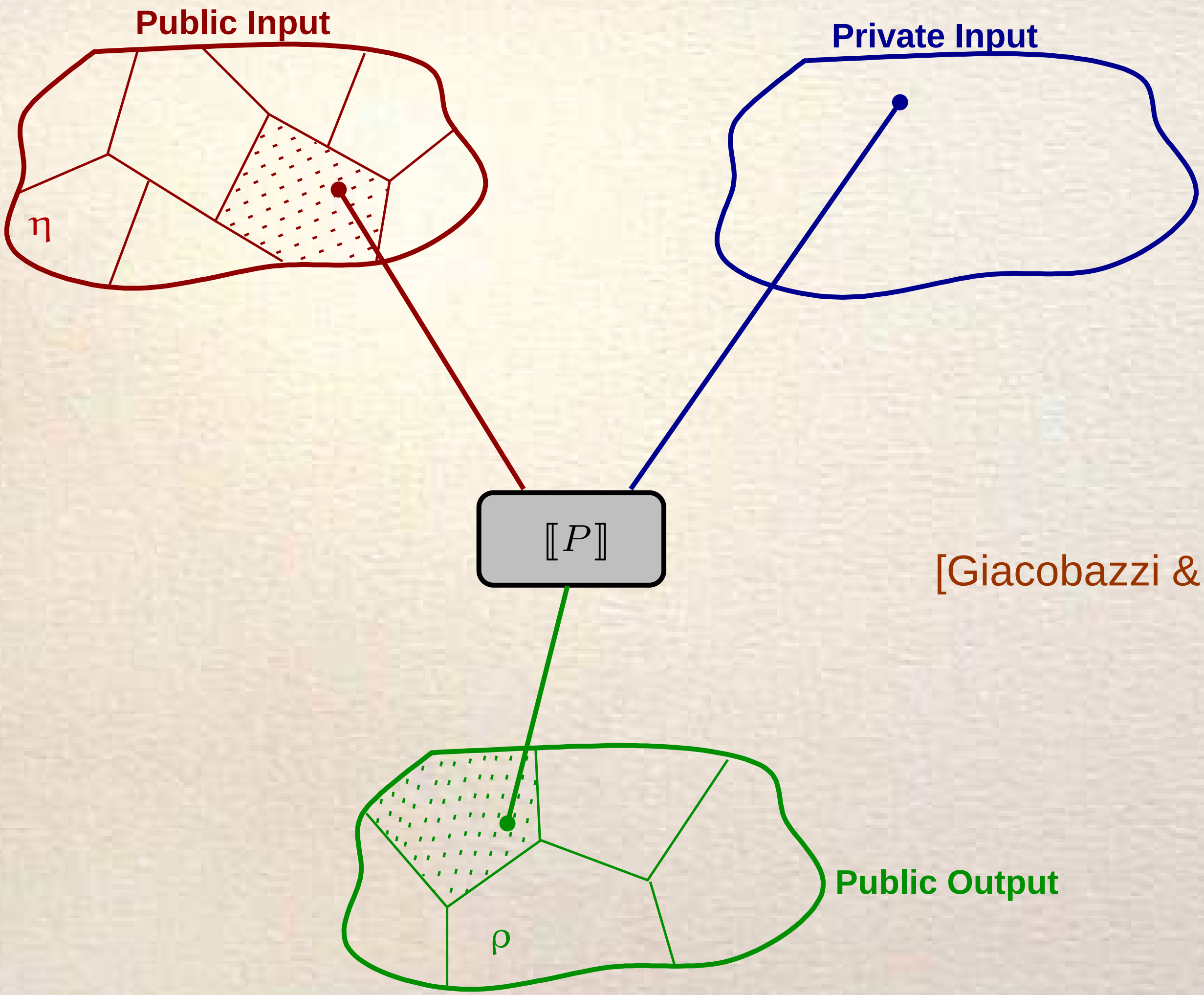
Abstract Non-Interference (Narrow)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}}))$: $[\eta]P(\rho)$: $\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, l_1)^{\mathsf{L}}) = \rho([\![P]\!](h_2, l_2)^{\mathsf{L}})$

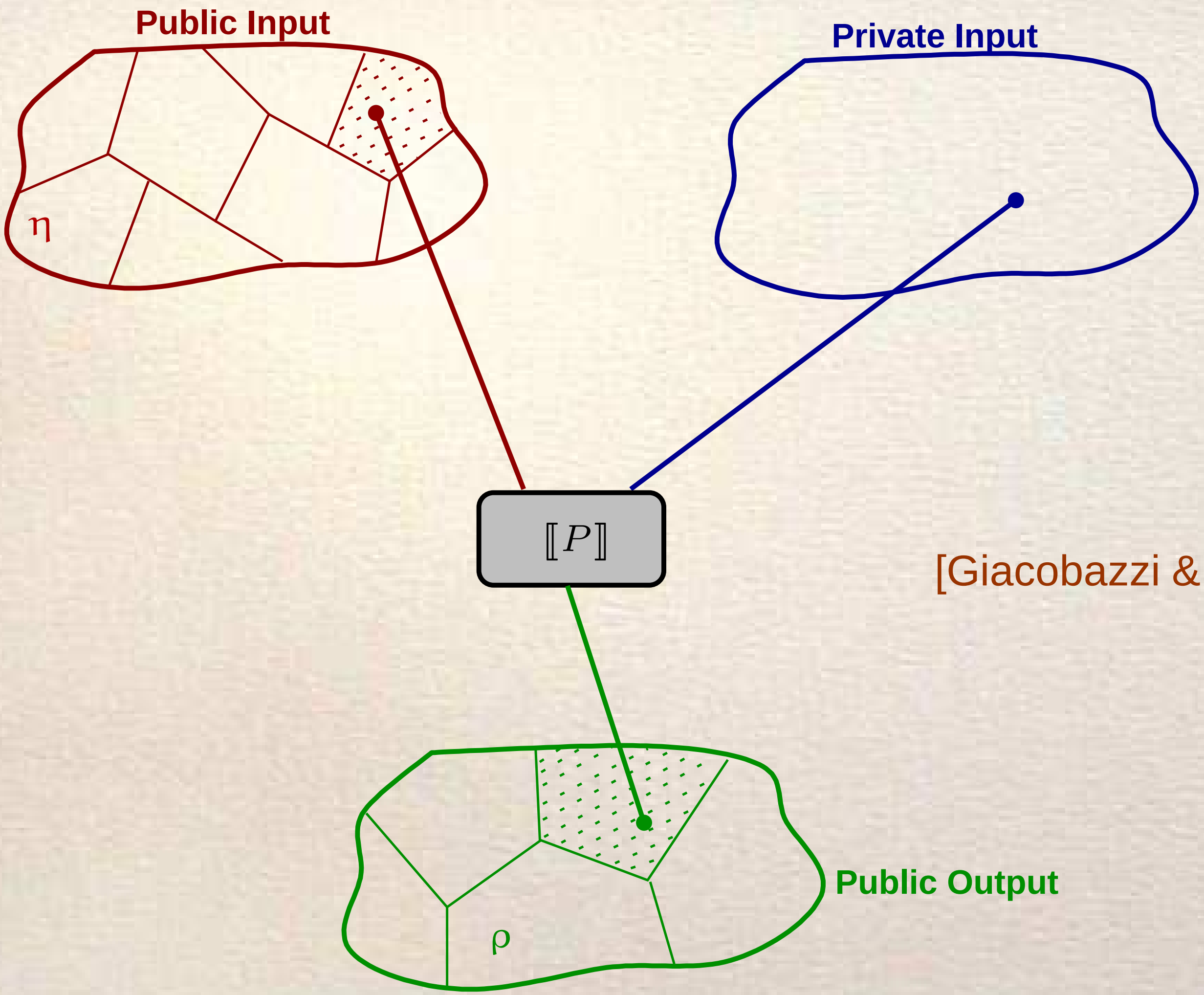
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}}))$: $[\eta]P(\rho)$: $\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, l_1)^{\mathsf{L}}) = \rho([\![P]\!](h_2, l_2)^{\mathsf{L}})$

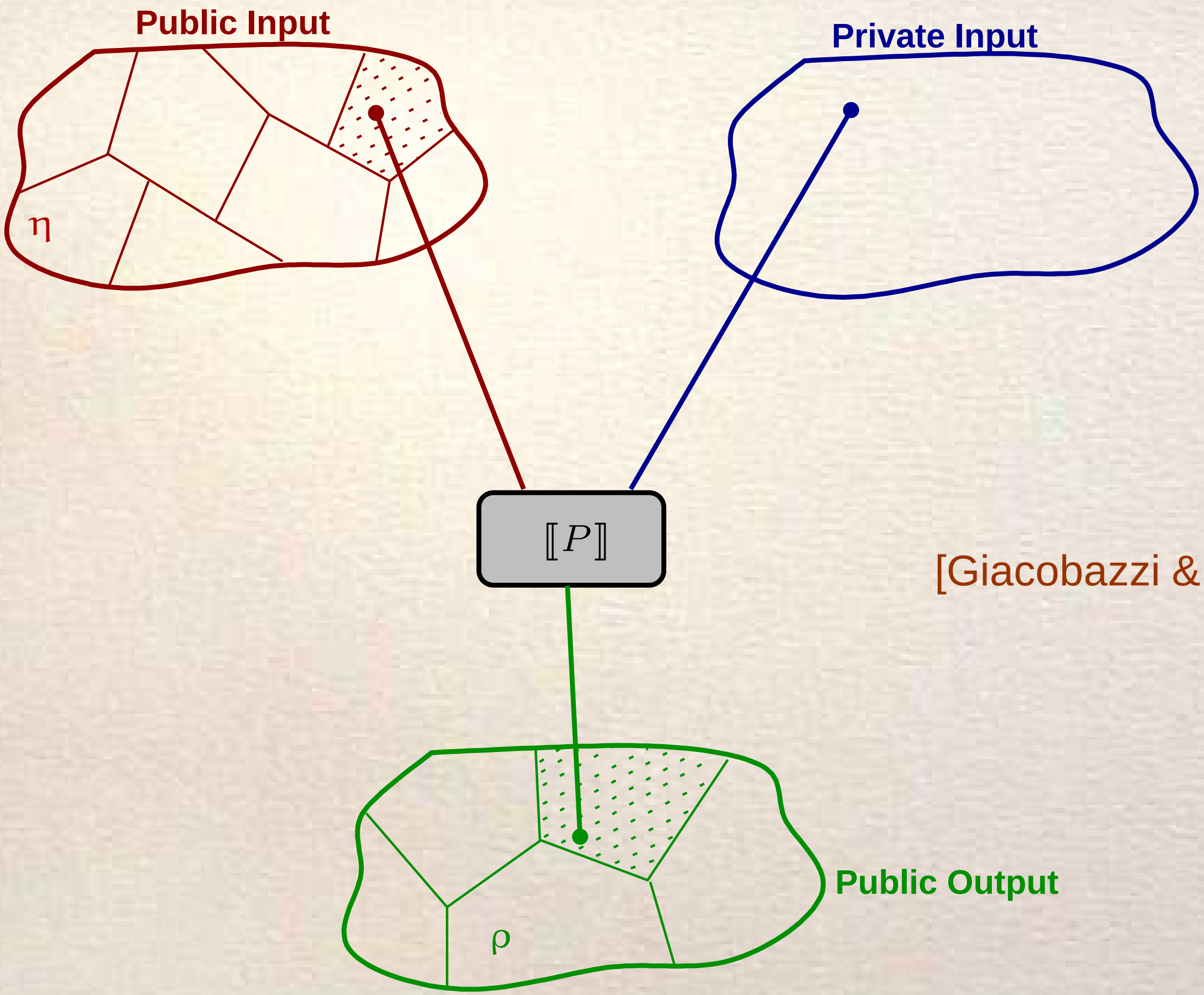
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}}))$: $[\eta]P(\rho)$: $\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, l_1)^{\mathsf{L}}) = \rho([\![P]\!](h_2, l_2)^{\mathsf{L}})$

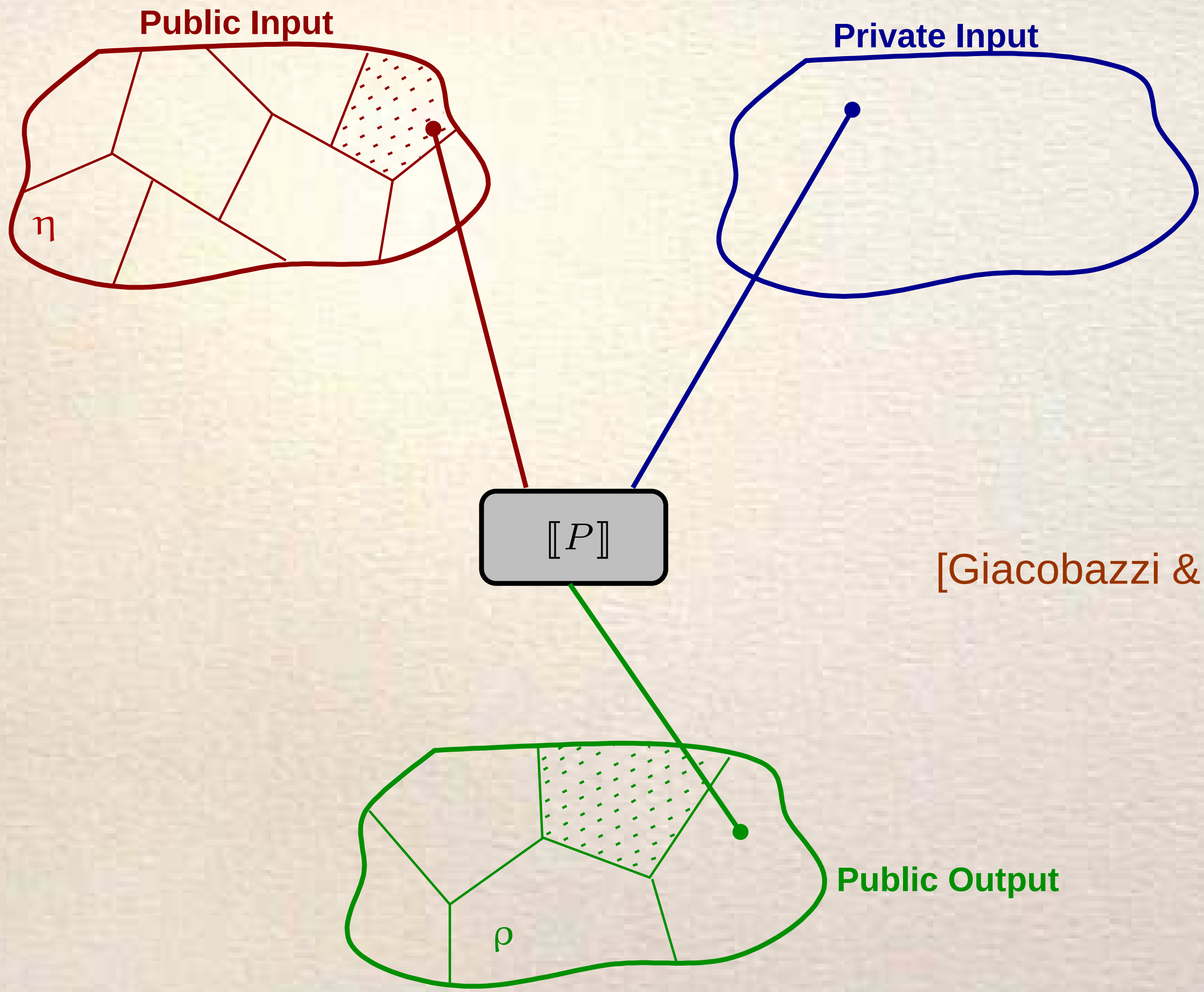
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}}))\colon\ [\eta]P(\rho)\colon\ \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P\rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket P\rrbracket(h_2, l_2)^{\mathsf{L}})$$

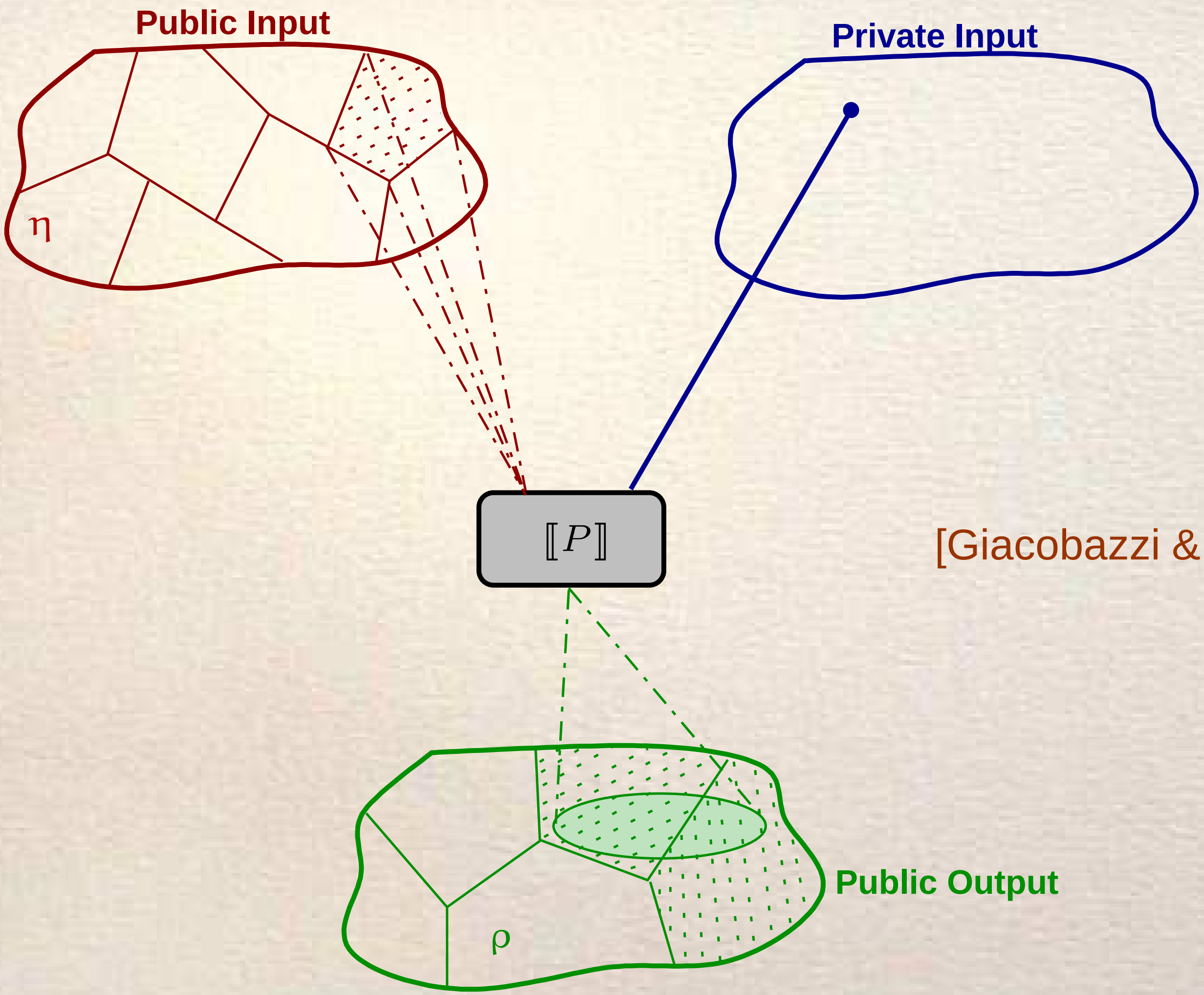
ABSTRACT NON-INTERFERENCE (NARROW)



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})) \colon [\eta]P(\rho) \colon \eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(h_1, l_1)^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(h_2, l_2)^{\mathsf{L}})$$

ABSTRACT NON-INTERFERENCE (ANI)

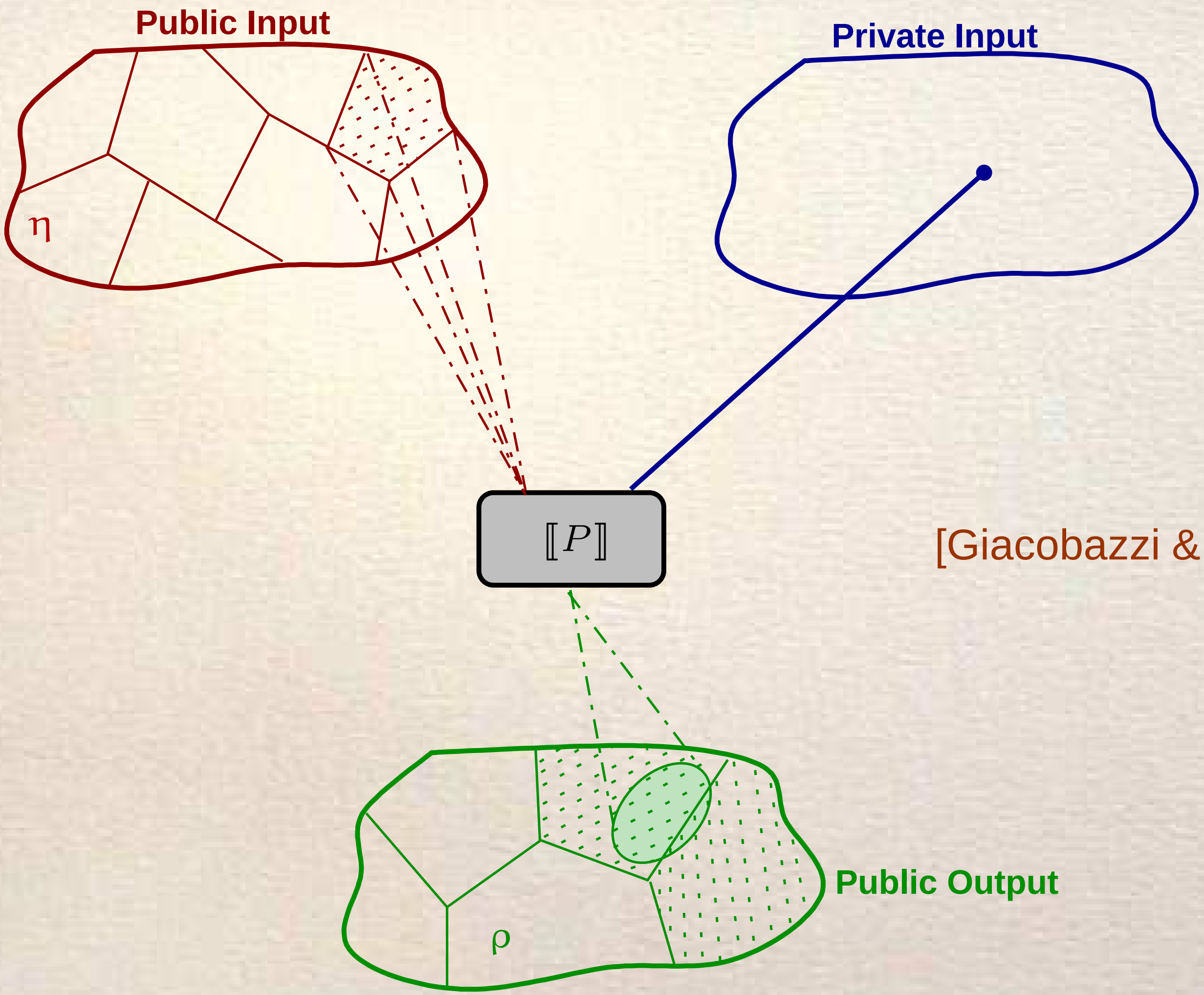


[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})):\ (\eta)P(\rho):$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

ABSTRACT NON-INTERFERENCE (ANI)

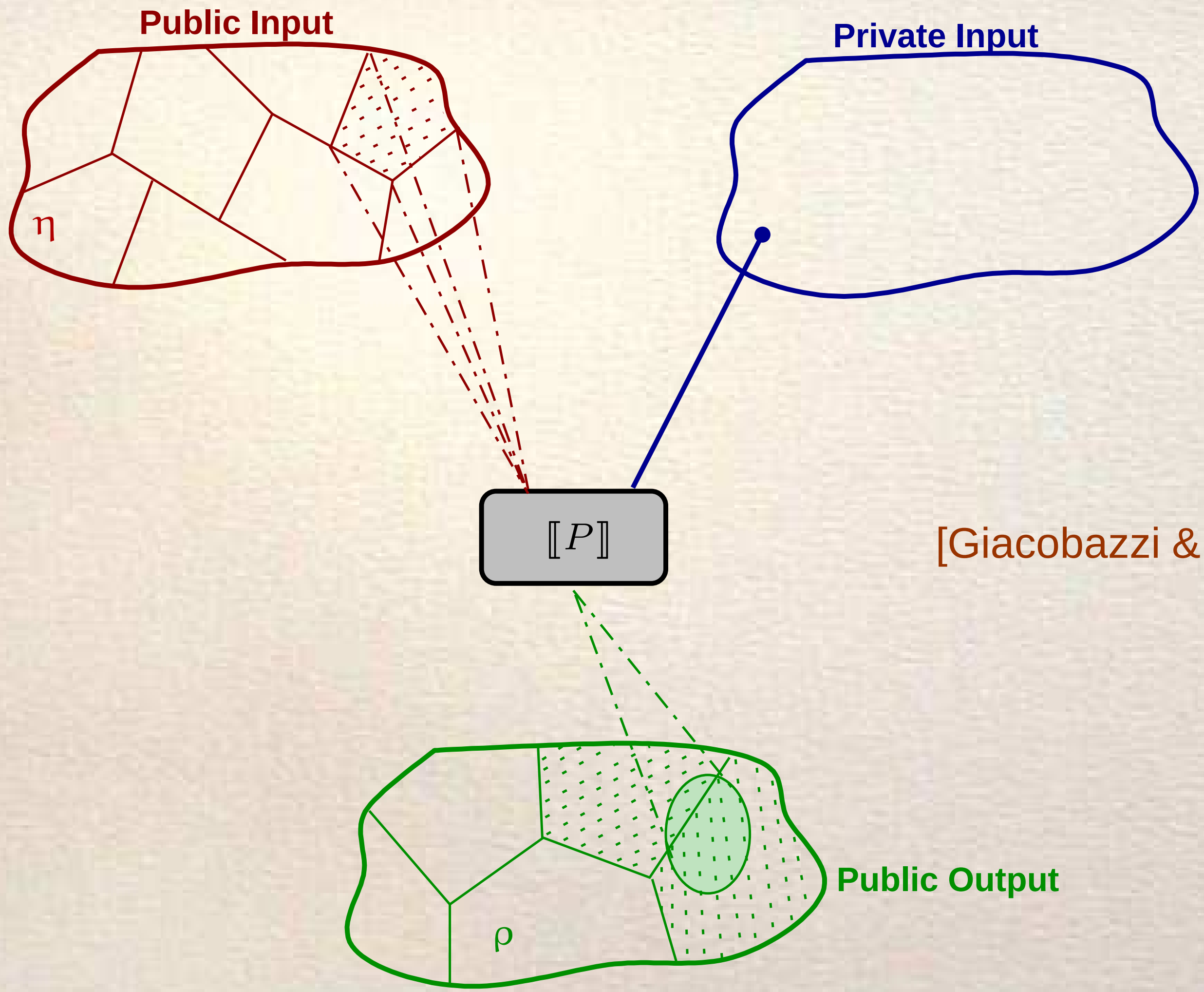


[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)P(\rho) \colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

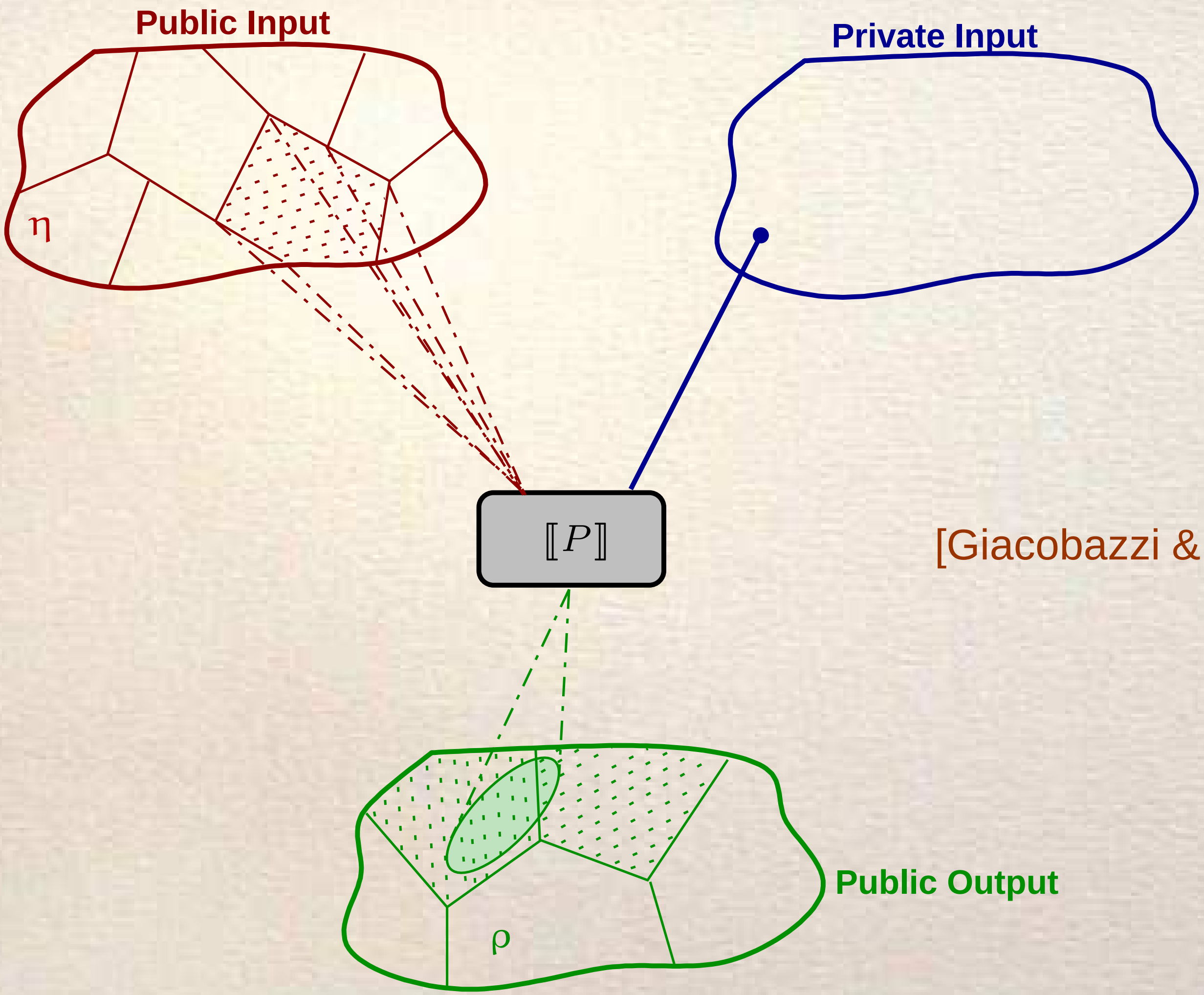
ABSTRACT NON-INTERFERENCE (ANI)



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)P(\rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

ABSTRACT NON-INTERFERENCE (ANI)

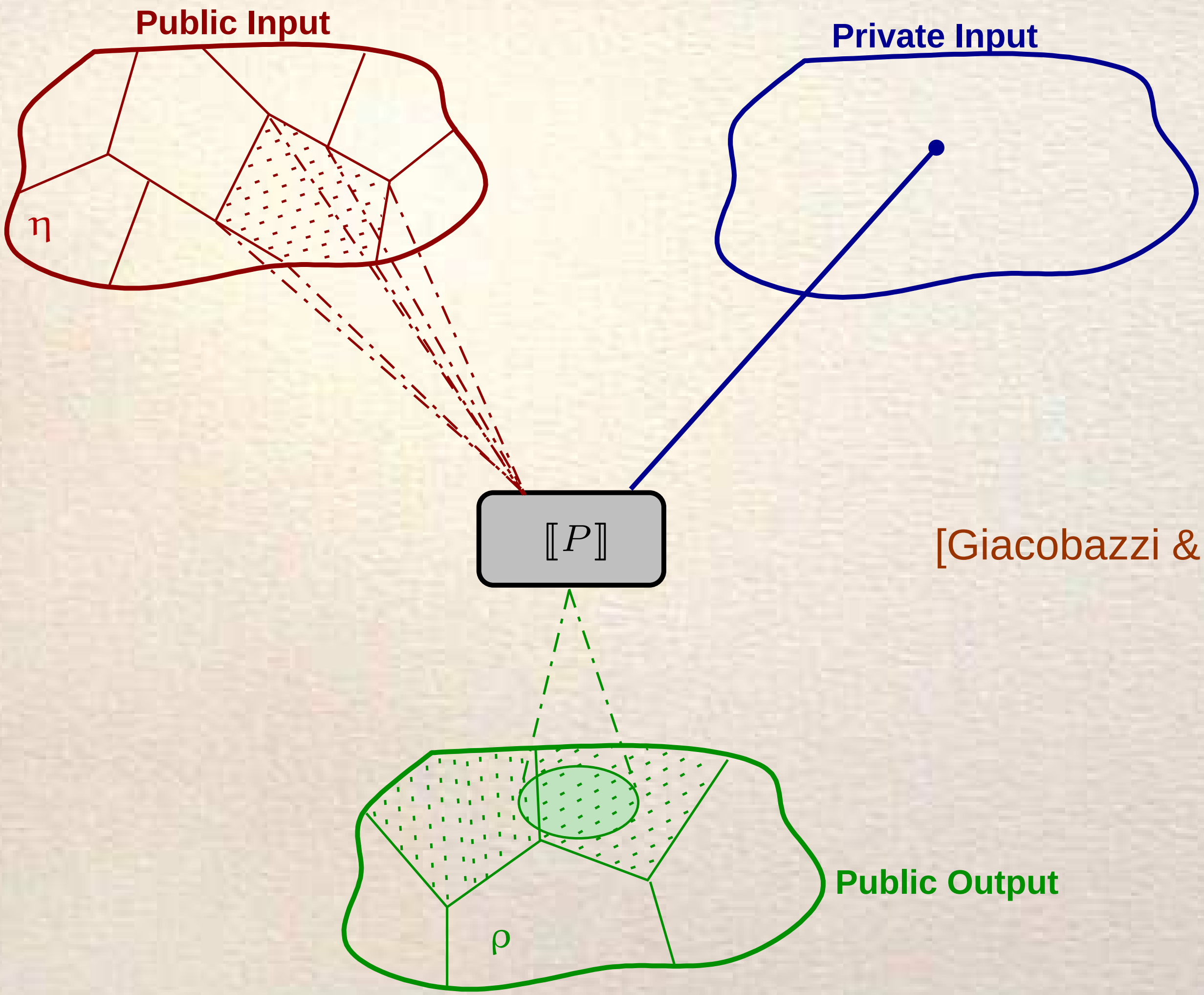


[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})) \text{: } (\eta)P(\rho)\text{:}$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

ABSTRACT NON-INTERFERENCE (ANI)



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})) \colon (\eta)P(\rho) \colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

EXAMPLES

EXAMPLE I:

$$\textbf{while } h \textbf{ do } (l := l + 2;\ h := h - 1).$$

$$\boxed{\text{Standard Non-Interference} \equiv [id]P(id)}$$

$$h = 0,\ l = 1 \rightsquigarrow l = 1$$
$$h = 1,\ l = 1 \rightsquigarrow l = 3$$
$$h = n,\ l = 1 \rightsquigarrow l = 1 + 2n$$

EXAMPLES

EXAMPLE I:

$$\textbf{while } h \textbf{ do } (l := l + 2;\ h := h - 1).$$

$$\boxed{\text{Standard Non-Interference} \equiv [id]P(id)}$$

$$h = 0,\ l = 1 \ \rightsquigarrow\ l = 1$$
$$h = 1,\ l = 1 \ \rightsquigarrow\ l = 3$$
$$h = n,\ l = 1 \ \rightsquigarrow\ l = 1 + 2n$$

$$\Downarrow$$

$$\boxed{[id]P(Par)}$$

$$h = 0,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{odd}$$
$$h = 1,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{odd}$$
$$h = n,\ l = 1 \ \rightsquigarrow\ Par(l) = \text{odd}$$

Examples

Example II:

$$P = \quad l := 2 * l * h^2.$$

$$\boxed{[Par]P(Sign)}$$

$$h = 1,\ l = 4\ (Par(4) = \text{even}) \ \rightsquigarrow\ Sign(l) = +$$
$$h = 1,\ l = -4\ (Par(-4) = \text{even}) \ \rightsquigarrow\ Sign(l) = -$$

$$\boxed{\text{Deceptive Flow}}$$

EXAMPLES

EXAMPLE II:

$$P = \quad l := 2 * l * h^2.$$

$$\boxed{[Par]P(Sign)}$$

$$h = 1,\ l = 4\ (Par(4) = \text{even}) \leadsto Sign(l) = +$$
$$h = 1,\ l = -4\ (Par(-4) = \text{even}) \leadsto Sign(l) = -$$

$$\boxed{\text{DECEPTIVE FLOW}}$$
$$\Downarrow$$
$$\boxed{(Par)P(Sign)}$$

$$h = -3,\ Par(l) = \text{even} \leadsto Sign(l) = \text{I don't know}$$
$$h = 1,\ Par(l) = \text{even} \leadsto Sign(l) = \text{I don't know}$$

Examples

Example III:

$$P = \quad l := l * h^2.$$

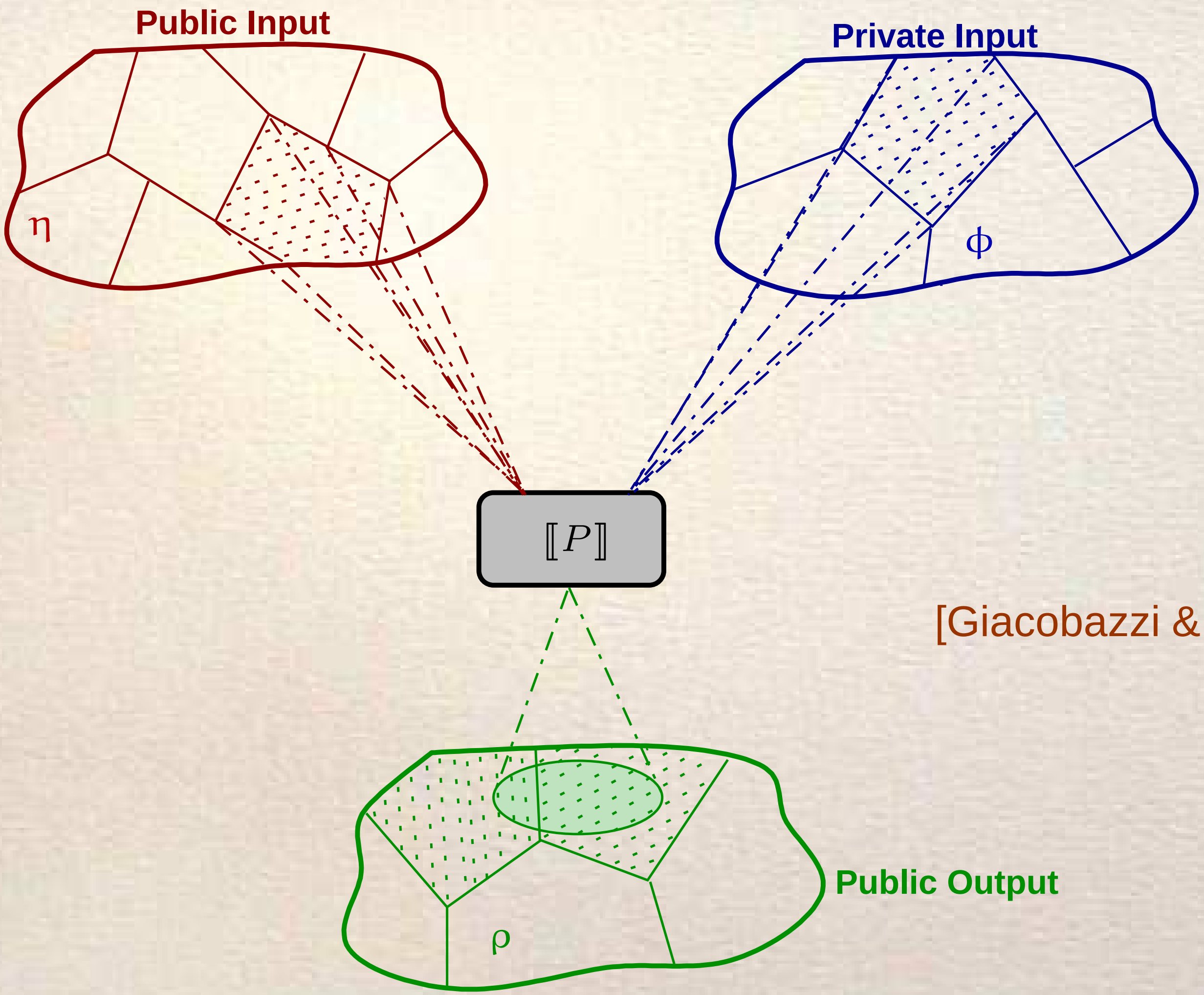
$$\boxed{(id)\,P\,(Par)}$$

$h = 2,\ l = 1 \ \leadsto\ Par(l) = \text{even}$

$h = 3,\ l = 1 \ \leadsto\ Par(l) = \text{odd}$

$h = n,\ l = 1 \ \leadsto\ Par(l) = Par(n)$

DECLASSIFIED ANI VIA BLOCKING

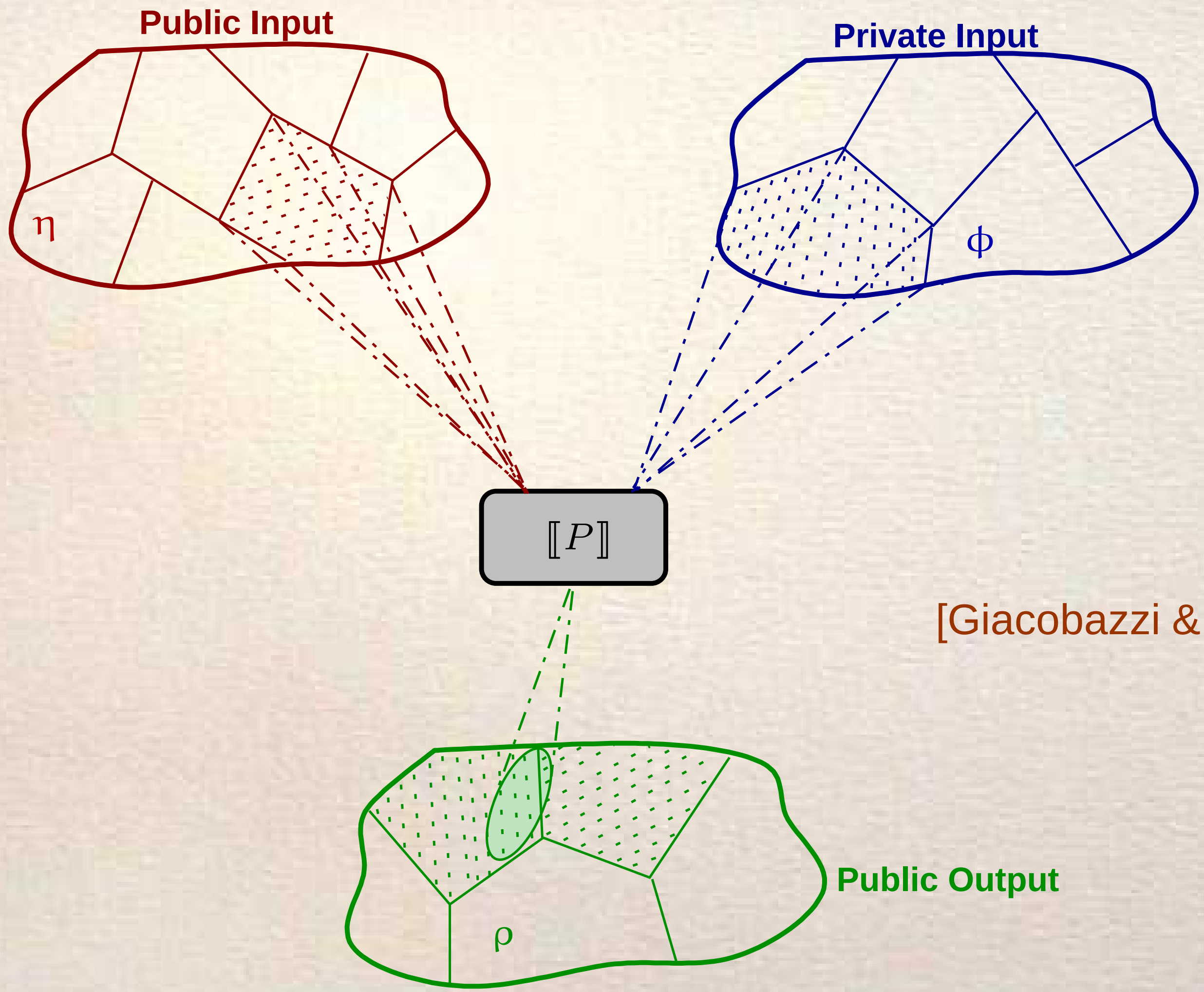


[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in uco(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow\!\!\| \rho)\colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

DECLASSIFIED ANI VIA BLOCKING

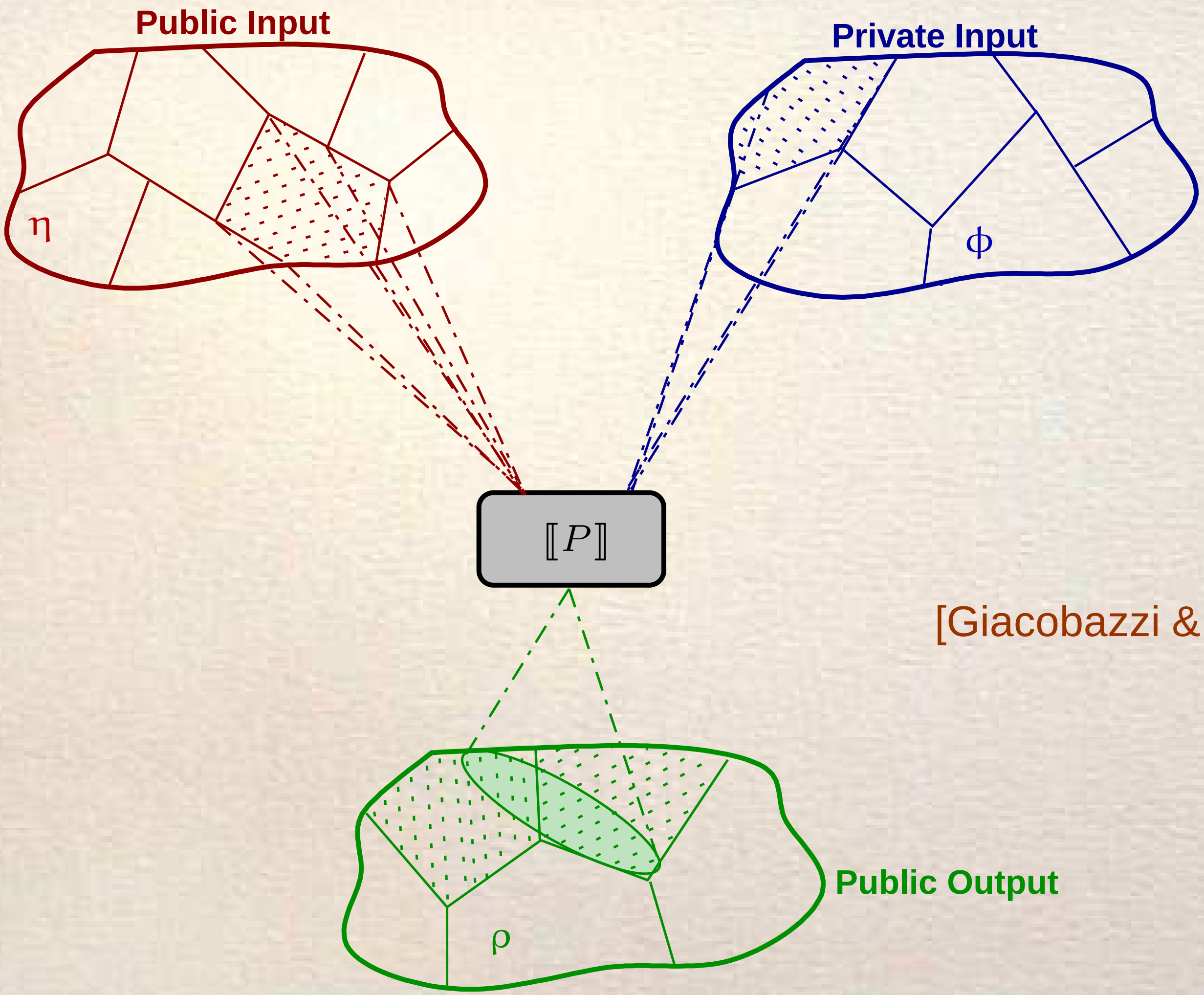


[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in uco(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow\!\!\Vert \rho) \colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

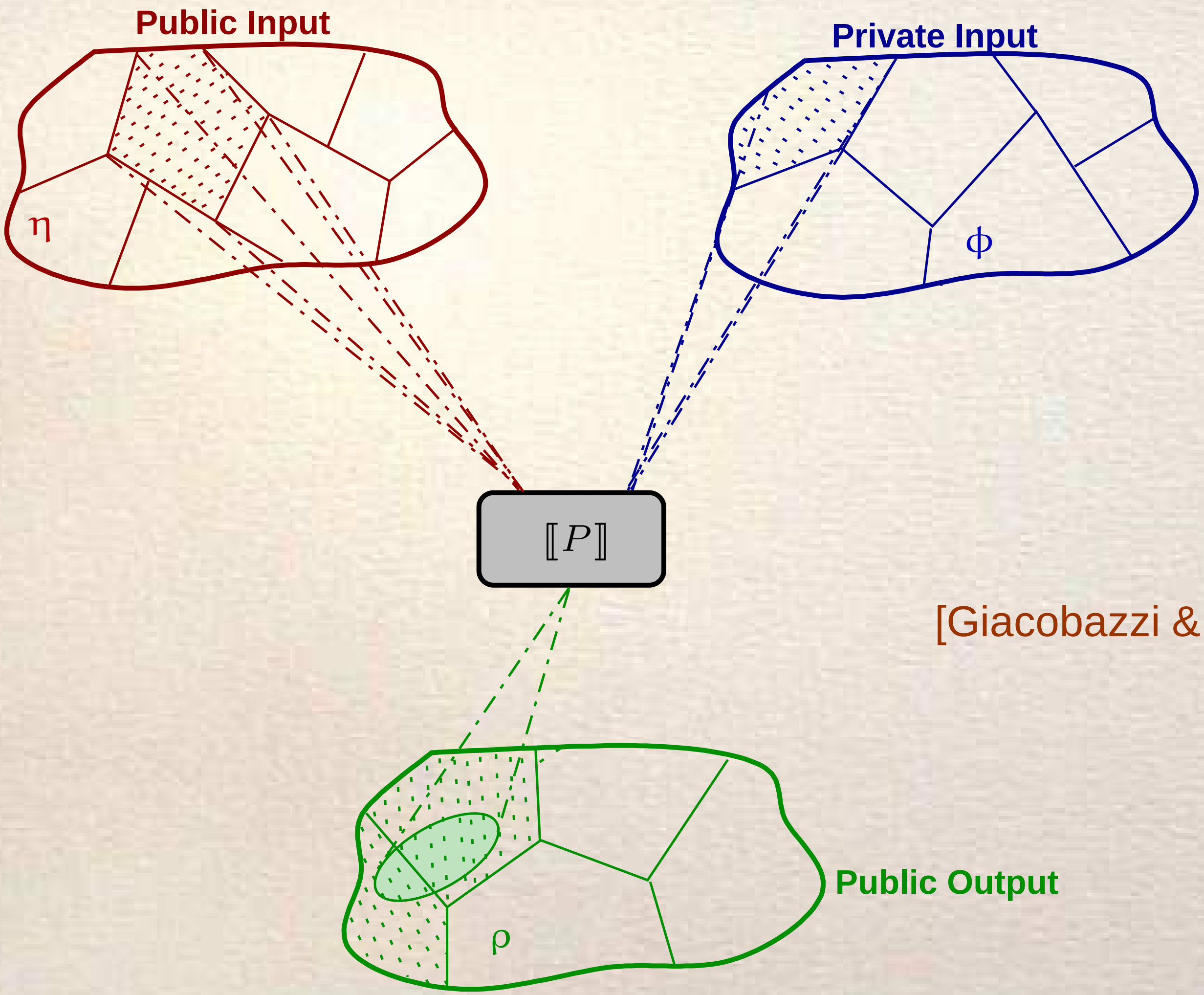
DECLASSIFIED ANI VIA BLOCKING



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in uco(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow\!\!\Vert \rho)\colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho(\llbracket P \rrbracket(\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho(\llbracket P \rrbracket(\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

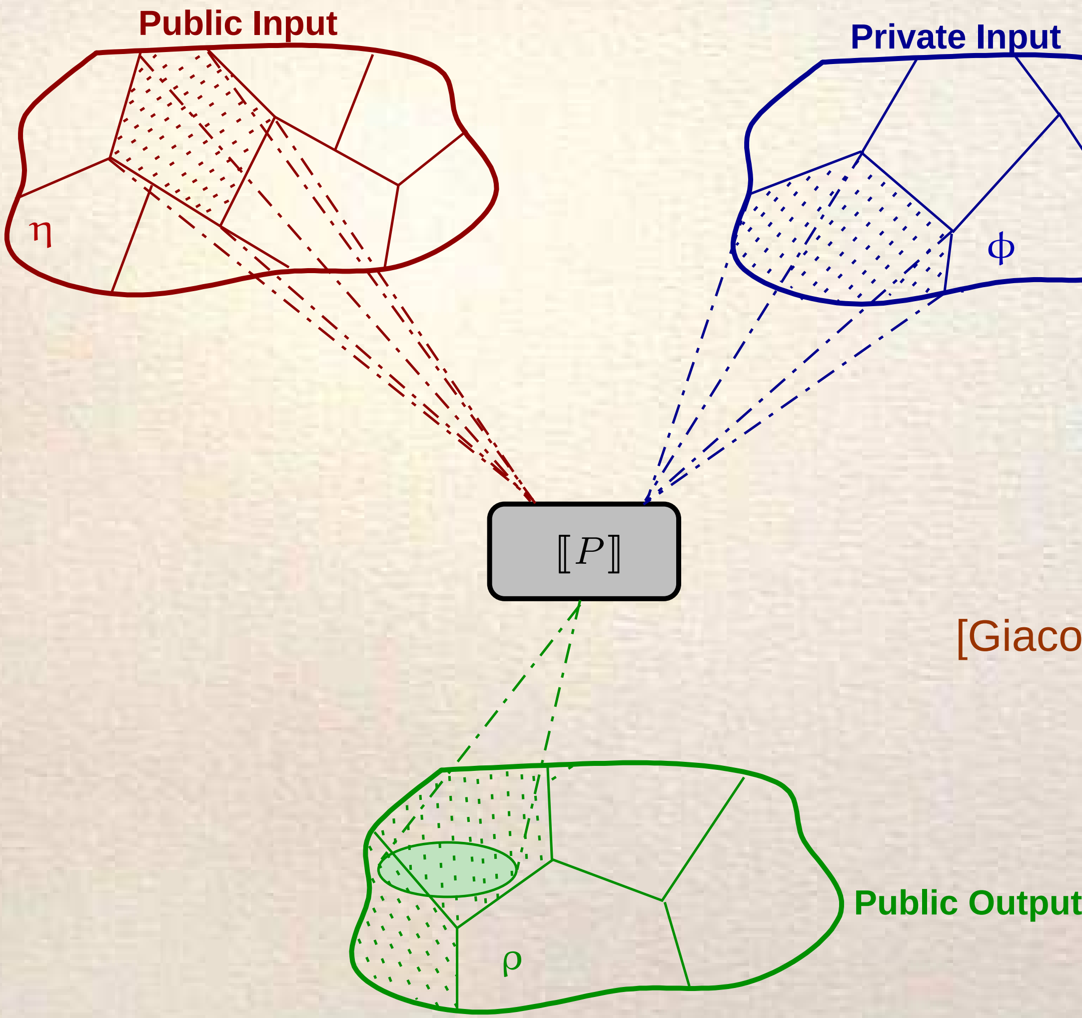
DECLASSIFIED ANI VIA BLOCKING



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in uco(\wp(\mathbb{V}^{\mathsf{H}})): (\eta)P(\phi \rightsquigarrow\!\!\| \rho):$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

DECLASSIFIED ANI VIA BLOCKING

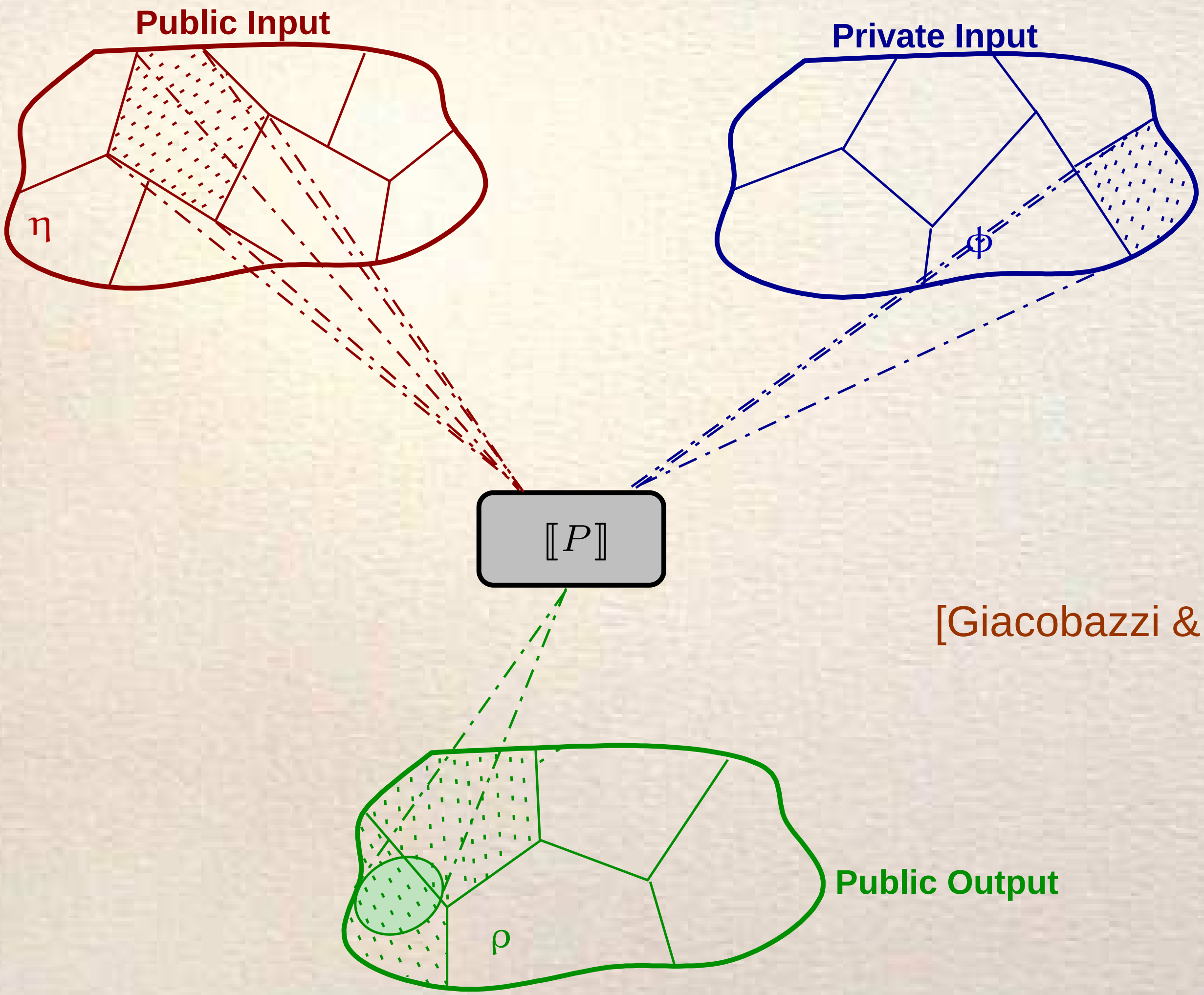


[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in uco(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow\!\!\| \rho) \colon$$

$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

DECLASSIFIED ANI VIA BLOCKING



[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in uco(\wp(\mathbb{V}^{\mathsf{H}})) \colon (\eta)P(\phi \rightsquigarrow\!\!\| \rho) \colon$$
$$\eta(l_1) = \eta(l_2) \Rightarrow \rho([\![P]\!](\phi(h_1), \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](\phi(h_2), \eta(l_2))^{\mathsf{L}})$$

Example

EXAMPLE:

$$P = \quad l := l * h^2.$$

$$\boxed{(id)P(Par)}$$

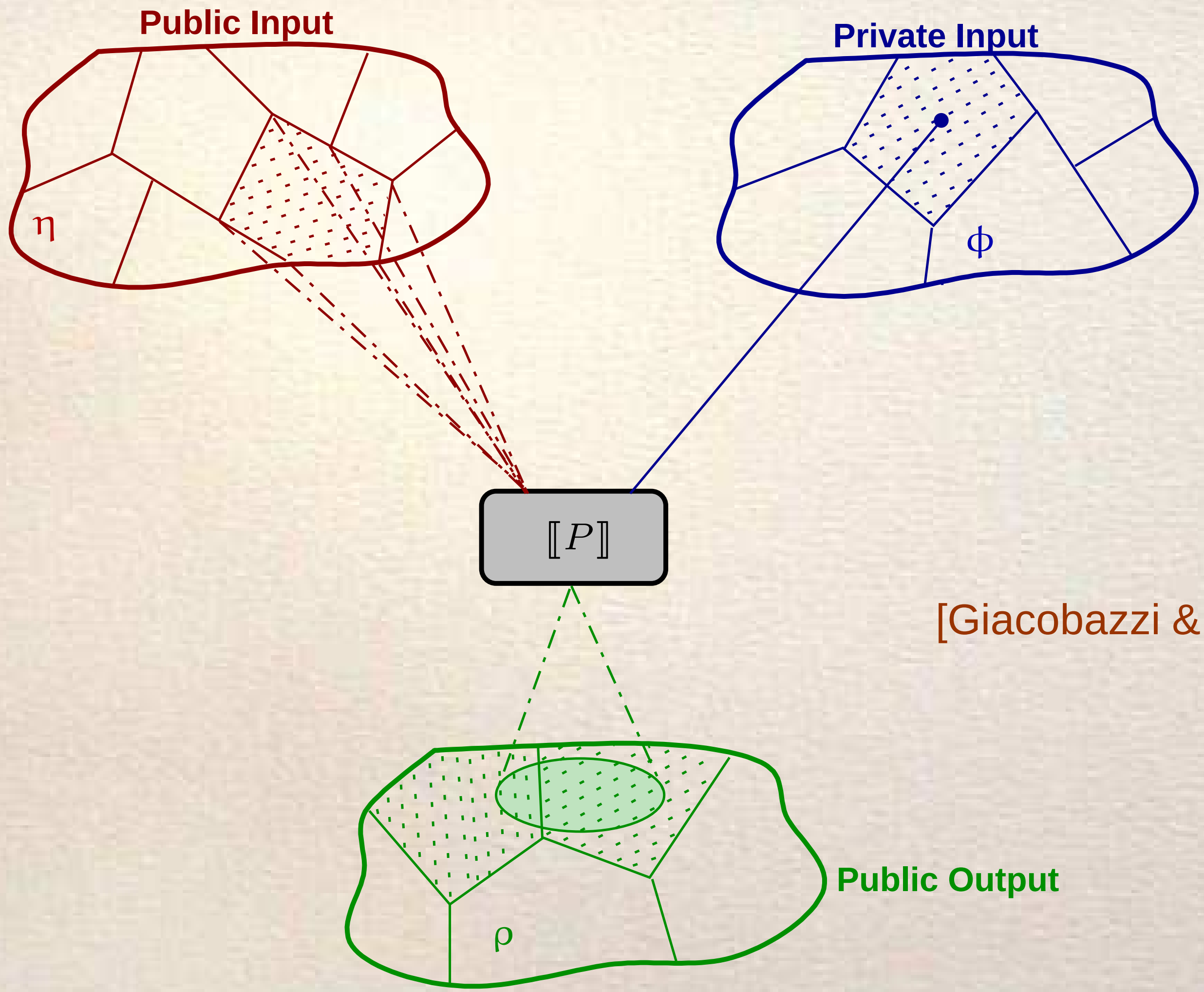
$$h = 2,\ l = 1 \rightsquigarrow Par(l) = \text{even}$$
$$h = 3,\ l = 1 \rightsquigarrow Par(l) = \text{odd}$$
$$h = n,\ l = 1 \rightsquigarrow Par(n) = Par(n)$$

$$\Downarrow$$

$$\boxed{(id)P(Sign \rightsquigarrow\!\!\| Par)}$$

$$Sign(h) = +,\ l = 1 \rightsquigarrow Par(l) = \text{I don't know}$$
$$Sign(h) = -,\ l = 1 \rightsquigarrow Par(l) = \text{I don't know}$$

DECLASSIFIED ANI (VIA ALLOWING)

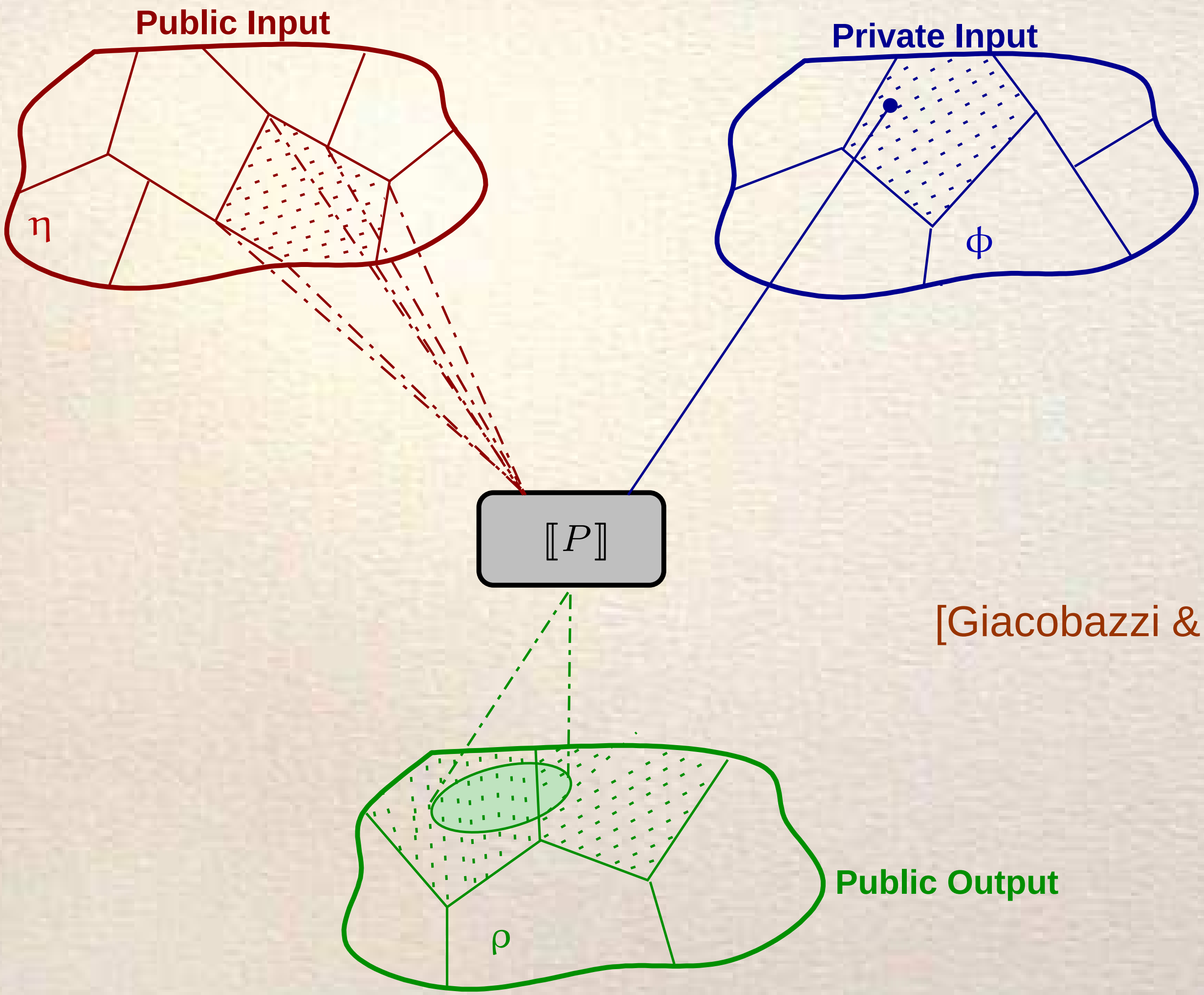


[Giacobazzi & Mastroeni '04]

$$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in uco(\wp(\mathbb{V}^{\mathsf{H}})) \text{: } (\eta)P(\phi \Rightarrow \rho)\text{:}$$

$$\eta(l_1) = \eta(l_2) \text{ and } \phi(h_1) = \phi(h_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$$

DECLASSIFIED ANI (VIA ALLOWING)

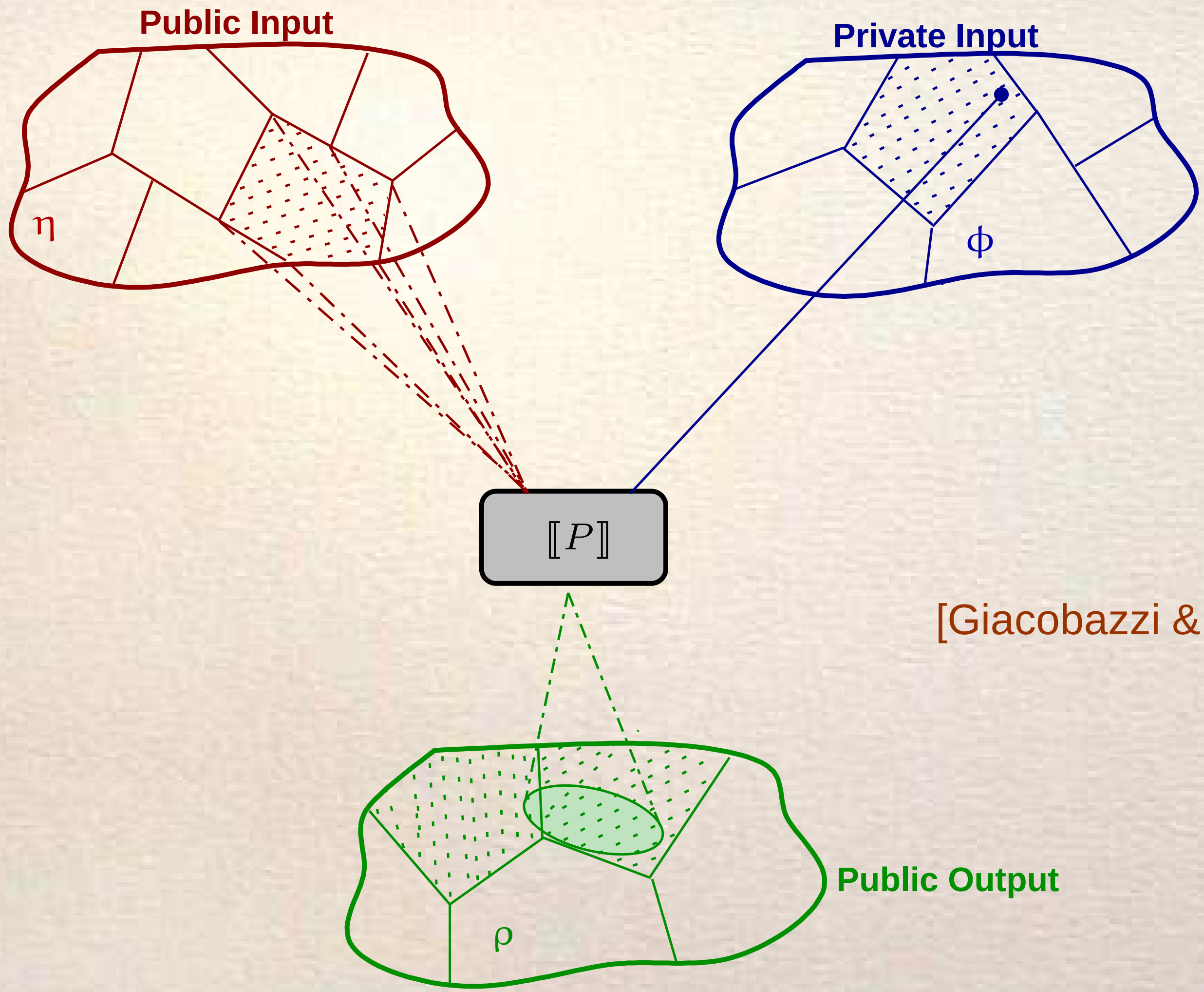


[Giacobazzi & Mastroeni '04]

$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in uco(\wp(\mathbb{V}^{\mathsf{H}}))$: $(\eta)P(\phi \Rightarrow \rho)$:

$\eta(l_1) = \eta(l_2)$ and $\phi(h_1) = \phi(h_2) \Rightarrow \rho(⟦P⟧(h_1, \eta(l_1))^{\mathsf{L}}) = \rho(⟦P⟧(h_2, \eta(l_2))^{\mathsf{L}})$

DECLASSIFIED ANI (VIA ALLOWING)



[Giacobazzi & Mastroeni '04]

$\rho, \eta \in uco(\wp(\mathbb{V}^{\mathsf{L}})), \phi \in uco(\wp(\mathbb{V}^{\mathsf{H}}))$: $(\eta)P(\phi \Rightarrow \rho)$:

$\eta(l_1) = \eta(l_2)$ and $\phi(h_1) = \phi(h_2) \Rightarrow \rho([\![P]\!](h_1, \eta(l_1))^{\mathsf{L}}) = \rho([\![P]\!](h_2, \eta(l_2))^{\mathsf{L}})$

Observer vs Observable

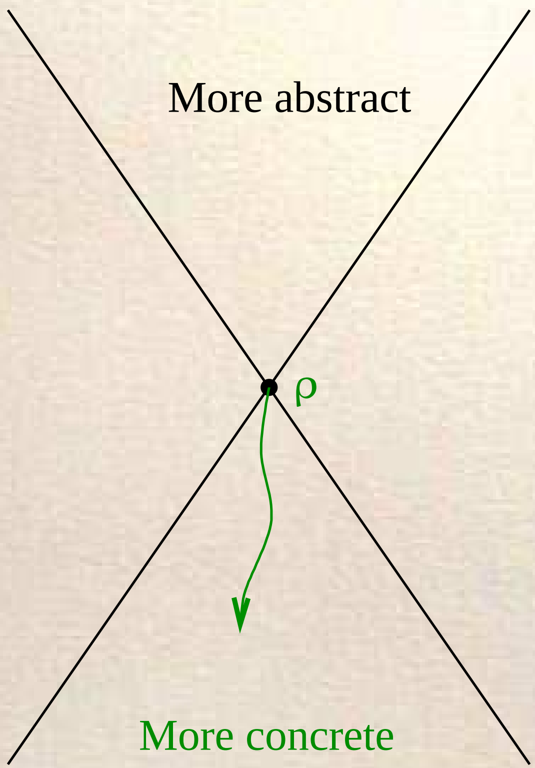
Modelling Attackers as Domain Transformers

Consider $\models (\eta)P(\phi \rightsquigarrow\!\!\rrbracket \rho)$: *In order to preserve non-interference...*

Observer vs Observable

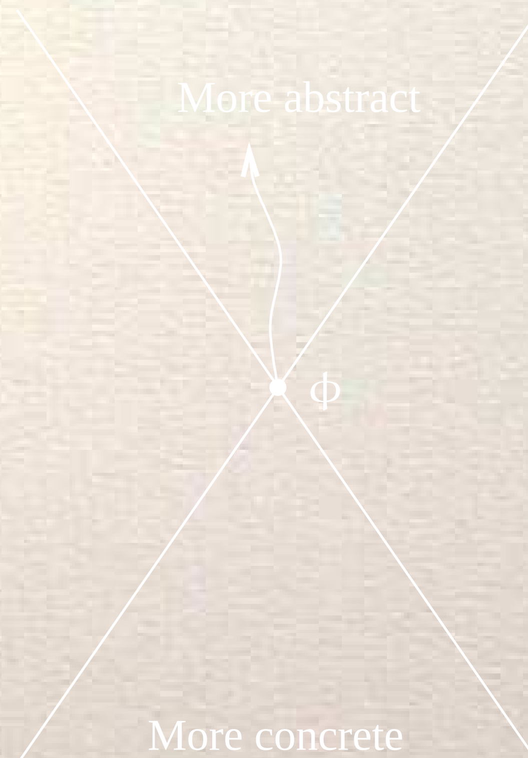
Modelling Attackers as Domain Transformers

Consider $\models (\eta) P(\phi \rightsquigarrow [\![\rho)$: *In order to preserve non-interference...*



$uco(\wp(\mathbb{V}^{\mathsf{L}}))$

AND

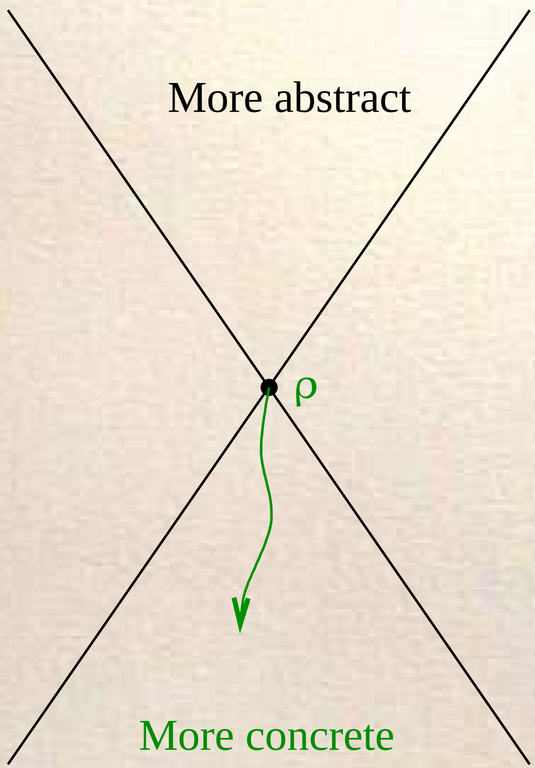


$uco(\wp(\mathbb{V}^{\mathsf{H}}))$

Observer vs Observable

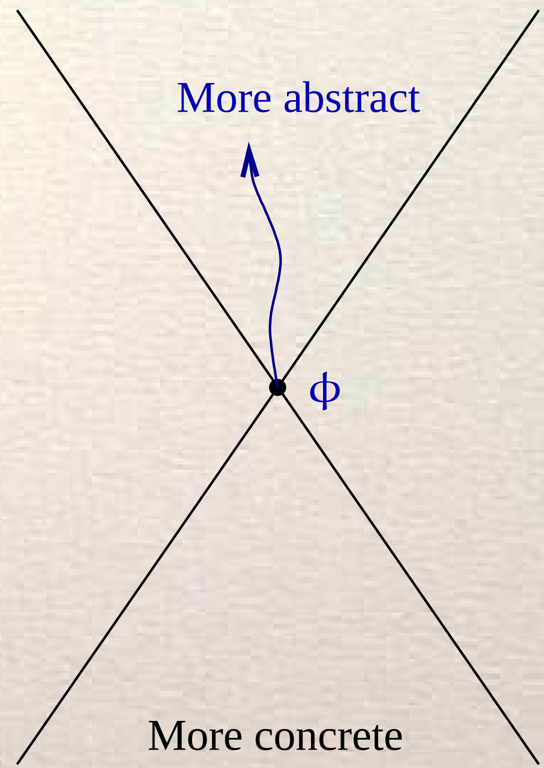
Modelling Attackers as Domain Transformers

Consider $\models (\eta) P(\phi \rightsquigarrow\!\!\rrbracket \rho)$: *In order to preserve non-interference...*



$uco(\wp(\mathbb{V}^{\mathsf{L}}))$

And



$uco(\wp(\mathbb{V}^{\mathsf{H}}))$

ANI AS COMPLETENESS

Let $\rho \in uco(\wp(\mathbb{V}^{\mathsf{L}})) \Rightarrow \mathcal{H}_\rho(X) \stackrel{\text{def}}{=} \langle \top^{\mathsf{H}}, \rho(X^{\mathsf{L}}) \rangle \in uco(\wp(\mathbb{V}))$

- *Narrow abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!] \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]$;
- *Abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi} \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi}$

ANI AS COMPLETENESS

$$\text{Let } \rho \in uco(\wp(\mathbb{V}^{\mathsf{L}})) \Rightarrow \mathcal{H}_\rho(X) \stackrel{\text{def}}{=} \langle \top^{\mathsf{H}}, \rho(X^{\mathsf{L}}) \rangle \in uco(\wp(\mathbb{V}))$$

- *Narrow abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!] \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]$;
- *Abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi} \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi}$

$$\Downarrow$$

- PUBLIC OBSERVER AS COMPLETENESS CORE:
  $(\eta)P(\phi \rightsquigarrow\!\!\rrbracket \mathcal{C}^{\mathcal{H}_\eta}_{[\![P]\!]^{\eta,\phi}}(\mathcal{H}))$

ANI AS COMPLETENESS

Let $\rho \in uco(\wp(\mathbb{V}^{\mathsf{L}})) \Rightarrow \mathcal{H}_\rho(X) \stackrel{\mathsf{def}}{=} \langle \top^{\mathsf{H}}, \rho(X^{\mathsf{L}}) \rangle \in uco(\wp(\mathbb{V}))$

- *Narrow abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!] \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]$;
- *Abstract non-interference:* $\mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi} \circ \mathcal{H}_\eta = \mathcal{H}_\rho \circ [\![P]\!]^{\eta,\phi}$

$$\Downarrow$$

- PUBLIC OBSERVER AS FORWARD COMPLETENESS CORE:
  $(\eta)P(\phi \rightsquigarrow\!\!\!]\, \mathcal{C}^{\mathcal{H}_\eta}_{[\![P]\!]^{\eta,\phi}}(\mathcal{H}))$

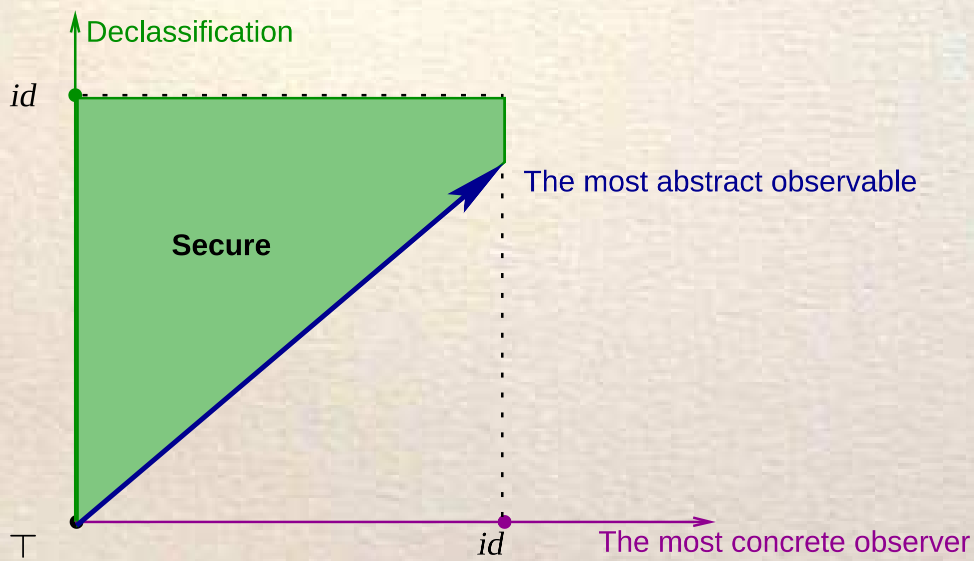
Strongest harmless attacker

- PRIVATE OBSERVABLE AS FORWARD COMPLETENESS SHELL:
  $(\eta)P(\mathcal{R}^{\mathcal{H}_\rho}_{[\![P]\!]^{\eta,id}}(\mathcal{H}_\eta) \Rightarrow \rho)$

Maximal information released

ANI AS COMPLETENESS

- ADJOINING ATTACKERS AND DECLASSIFICATION BY COMPLETENESS



DECLASSIFICATION

[Banerjee, Giacobazzi and Mastroeni ’07]

- By exploiting the strong relation between completeness and non-iterference we can obtain the following results:
  - Model declassification as a forward completeness problem for the weakest precondition semantics;
  - Derive counterexamples to a given declassification policy;
  - Refine a given declassification policy (Shell);

DNI: A COMPLETENESS PROBLEM

Let $\mathcal{H}^{\phi}$ the abstract domain declassifying the property ϕ of the private *input*:

$$\boxed{\mathcal{H}\circ[\![P]\!]\circ\mathcal{H}^{\phi} = \mathcal{H}\circ[\![P]\!] \ \Leftrightarrow\ \mathcal{H}^{\phi}\circ Wlp_P\circ\mathcal{H} = Wlp_P\circ\mathcal{H}}$$

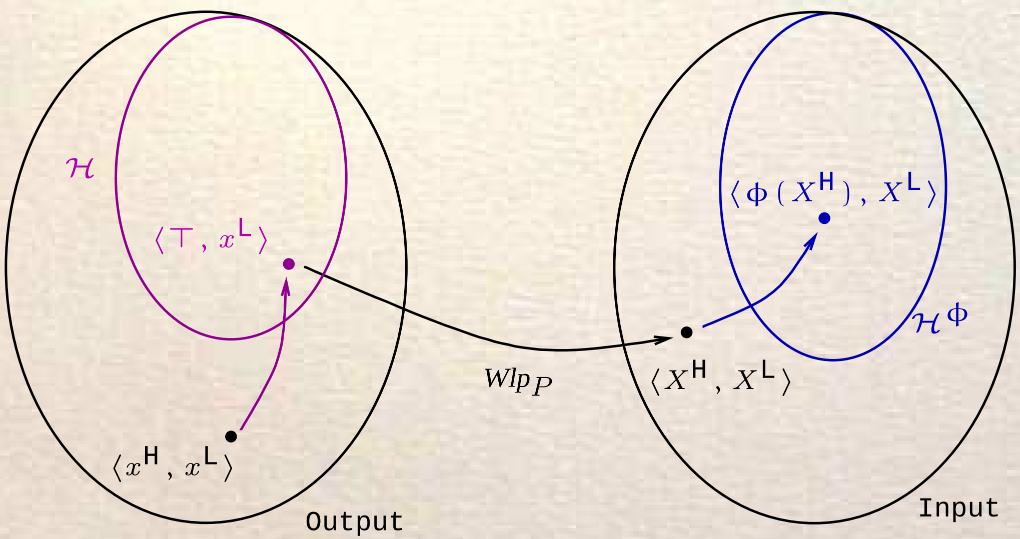
$$\Downarrow$$

To release ϕ *means* to distinguish between elements in ϕ!

DNI: A COMPLETENESS PROBLEM

Let $\mathcal{H}^{\phi}$ the abstract domain declassifying the property ϕ of the private *input*:

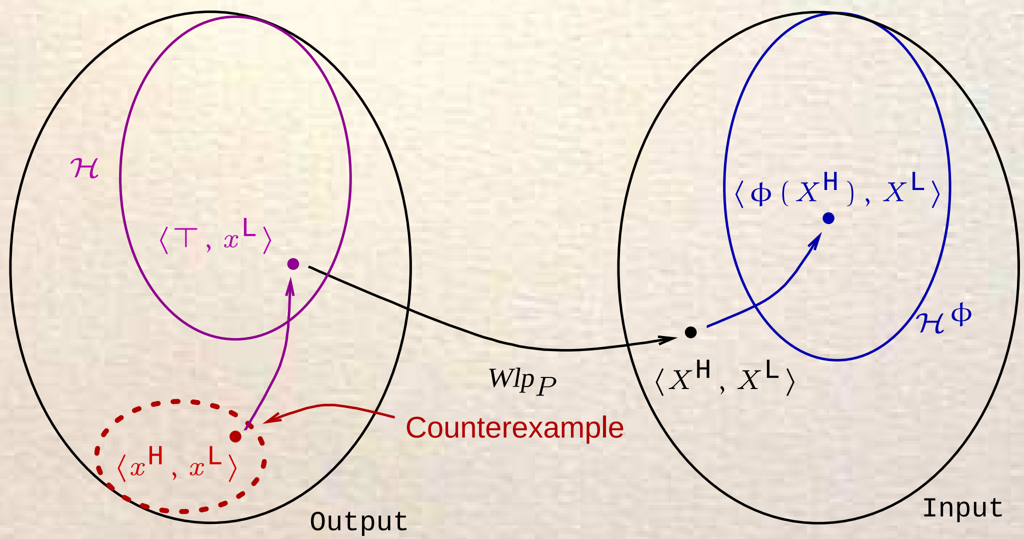
$$\boxed{\mathcal{H}\circ[\![P]\!]\circ\mathcal{H}^{\phi} = \mathcal{H}\circ[\![P]\!] \;\Leftrightarrow\; \mathcal{H}^{\phi}\circ Wlp_P\circ\mathcal{H} = Wlp_P\circ\mathcal{H}}$$



DNI: A completeness problem

Let $\mathcal{H}^{\phi}$ the abstract domain declassifying the property ϕ of the private *input*:

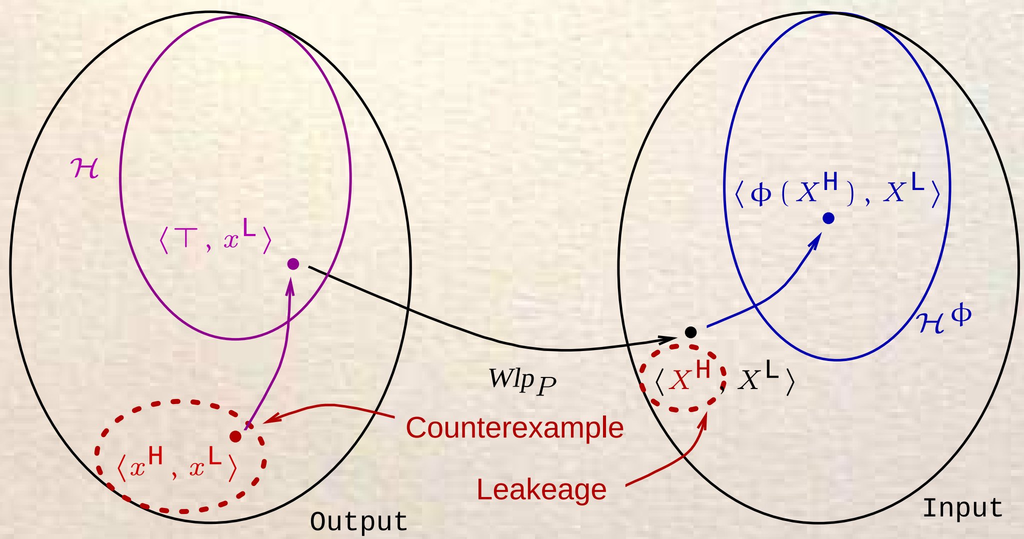
$$\boxed{\mathcal{H}\circ[\![P]\!]\circ\mathcal{H}^{\phi}=\mathcal{H}\circ[\![P]\!] \;\Leftrightarrow\; \mathcal{H}^{\phi}\circ Wlp_P\circ\mathcal{H}=Wlp_P\circ\mathcal{H}}$$



DNI: A COMPLETENESS PROBLEM

Let $\mathcal{H}^{\phi}$ the abstract domain declassifying the property ϕ of the private *input*:

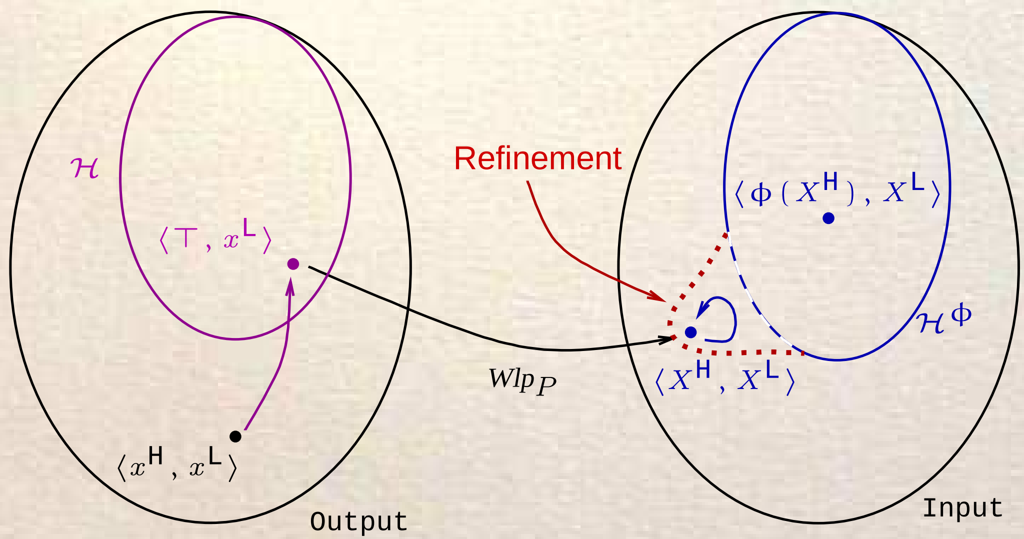
$$\boxed{\mathcal{H}\circ[\![P]\!]\circ\mathcal{H}^{\phi} = \mathcal{H}\circ[\![P]\!] \Leftrightarrow \mathcal{H}^{\phi}\circ Wlp_P\circ\mathcal{H} = Wlp_P\circ\mathcal{H}}$$



DNI: A COMPLETENESS PROBLEM

Let $\mathcal{H}^{\phi}$ the abstract domain declassifying the property ϕ of the private *input*:

$$\boxed{\mathcal{H} \circ [\![P]\!] \circ \mathcal{H}^{\phi} = \mathcal{H} \circ [\![P]\!] \;\Leftrightarrow\; \mathcal{H}^{\phi} \circ Wlp_P \circ \mathcal{H} = Wlp_P \circ \mathcal{H}}$$



SHELL: THE MAXIMAL RELEASED INFORMATION

Consider $\rho =$Parity$\stackrel{\text{def}}{=}\{\top, \mathit{Even}, \mathit{Odd}, \varnothing\}$, as the information observed by the attacker.

$$P = \Big[\qquad l := l * h^2;$$

Shell: The maximal released information

Consider $\rho = \text{Parity} \stackrel{\text{def}}{=} \{\top, \mathit{Even}, \mathit{Odd}, \varnothing\}$, as the information observed by the attacker.

$$\begin{array}{ll} & (l \in \mathit{Even} \;\vee\; (l \in \mathit{Odd},\; h \in \mathit{Even})) \\ l := l * h^2; & \\ & (l \in \mathit{Even}) \end{array} \qquad \text{OR} \qquad \begin{array}{ll} & (l \in \mathit{Odd} \;\wedge\; h \in \mathit{Odd}) \\ l := l * h^2; & \\ & (l \in \mathit{Odd}) \end{array}$$

Let $l = 3$, $h = 2 \in \mathit{Even}$:

$$\mathcal{H}_{Par}[\![P]\!](\langle 2, 3\rangle) = \langle \top, \mathit{Even}\rangle \neq \langle \top, \top\rangle = \mathcal{H}_{Par}[\![P]\!](\langle \top, 3\rangle) = \mathcal{H}_{Par}[\![P]\!](\mathcal{H}(\langle 2, 3\rangle))$$

SHELL: THE MAXIMAL RELEASED INFORMATION

Consider $\rho = \text{Parity} \stackrel{\text{def}}{=} \{\top, \mathit{Even}, \mathit{Odd}, \varnothing\}$, as the information observed by the attacker.

$$
\begin{array}{lll}
\quad (l \in \mathit{Even} \ \vee \ (l \in \mathit{Odd},\ h \in \mathit{Even})) & & \quad (l \in \mathit{Odd} \ \wedge \ h \in \mathit{Odd}) \\
l := l * h^2; & \text{OR} & l := l * h^2; \\
\quad (l \in \mathit{Even}) & & \quad (l \in \mathit{Odd})
\end{array}
$$

Let $l = 3$, $h = 2 \in \mathit{Even}$:

$$\mathcal{H}_{Par}[\![P]\!](\langle 2, 3\rangle) = \langle \top, \mathit{Even}\rangle \neq \langle \top, \top\rangle = \mathcal{H}_{Par}[\![P]\!](\langle \top, 3\rangle) = \mathcal{H}_{Par}[\![P]\!](\mathcal{H}(\langle 2, 3\rangle))$$

WE RELEASE SOMETHING ABOUT THE PRIVATE INPUT!

Shell: The maximal released information

Consider $\rho = \text{Parity} \stackrel{\text{def}}{=} \{\top, \mathit{Even}, \mathit{Odd}, \varnothing\}$, as the information observed by the attacker.

$$\begin{array}{lll} (l \in \mathit{Even} \vee (l \in \mathit{Odd},\ h \in \mathit{Even})) & & (l \in \mathit{Odd} \wedge h \in \mathit{Odd}) \\ l := l * h^2; & \textsc{Or} & l := l * h^2; \\ (l \in \mathit{Even}) & & (l \in \mathit{Odd}) \end{array}$$

Let us compute the shell of the input domain $\mathcal{H}$:

$$\mathcal{H}' \stackrel{\text{def}}{=} \mathcal{R}^{\mathcal{H}_{Par}}_{[\![P]\!]}(\mathcal{H}) = \mathcal{H} \sqcap (\langle \top, \mathit{Even} \rangle \cup \langle \mathit{Even}, \mathit{Odd} \rangle, \langle \mathit{Odd}, \mathit{Odd} \rangle, \langle \mathit{Odd}, \mathit{Even} \rangle)$$

Shell: The maximal released information

Consider $\rho =$ Parity $\stackrel{\text{def}}{=} \{\top, \mathit{Even}, \mathit{Odd}, \varnothing\}$, as the information observed by the attacker.

$$\begin{array}{lcl} \quad (l \in \mathit{Even} \ \vee \ (l \in \mathit{Odd},\ h \in \mathit{Even})) & & \quad (l \in \mathit{Odd} \ \wedge \ h \in \mathit{Odd}) \\ l := l * h^2; & \text{OR} & l := l * h^2; \\ \quad (l \in \mathit{Even}) & & \quad (l \in \mathit{Odd}) \end{array}$$

Let us compute the shell of the input domain $\mathcal{H}$:

$$\mathcal{H}' \stackrel{\text{def}}{=} \mathcal{R}^{\mathcal{H}_{Par}}_{[\![P]\!]}(\mathcal{H}) = \mathcal{H} \sqcap (\langle \top, \mathit{Even} \rangle \cup \langle \mathit{Even}, \mathit{Odd} \rangle, \langle \mathit{Odd}, \mathit{Odd} \rangle, \langle \mathit{Odd}, \mathit{Even} \rangle)$$

Hence (NB: By reduced product in $\mathcal{H}'$ we have the elements $\langle \mathit{Even}, l \rangle$)

Let $l = 3$, $h = 2 \in \mathit{Even}$:

$$\mathcal{H}_{Par}[\![P]\!](\langle 2, 3 \rangle) = \langle \top, \mathit{Even} \rangle = \mathcal{H}_{Par}[\![P]\!](\langle \mathit{Even}, 3 \rangle) = \mathcal{H}_{Par}[\![P]\!](\mathcal{H}'(\langle 2, 3 \rangle))$$

CORE: THE MOST POWERFUL ATTACKER

$$P = \Big[\quad \textbf{while } (h \neq 0) \textbf{ do } (h := 0; l := 2l) \textbf{ endw}$$

CORE: THE MOST POWERFUL ATTACKER

$((l \in Even, h = 0) \ \vee \ (h \neq 0))$

while $(h \neq 0)$ **do** $(h := 0; l := 2l)$ **endw**;

$(l \in Even)$

OR

$(h = 0)$

while $(h \neq 0)$ **do** $(h := 0; l := 2l)$ **endw**

$(l \in Odd)$

Let $l = 5$, $h = 3$:

$$\mathcal{H}[\![P]\!](\langle 3, 5\rangle) = \langle \top, 10\rangle \neq \langle \top, \top\rangle = \mathcal{H}[\![P]\!](\langle \top, 5\rangle) = \mathcal{H}[\![P]\!](\mathcal{H}(\langle 3, 5\rangle))$$

CORE: THE MOST POWERFUL ATTACKER

$((l \in \mathit{Even}, h = 0) \ \vee \ (h \neq 0))$
while $(h \neq 0)$ **do** $(h := 0; l := 2l)$ **endw**;
$(l \in \mathit{Even})$

OR

$(h = 0)$
while $(h \neq 0)$ **do** $(h := 0; l := 2l)$ **endw**
$(l \in \mathit{Odd})$

Let $l = 5$, $h = 3$:

$$\mathcal{H}[\![P]\!](\langle 3, 5\rangle) = \langle \top, 10\rangle \neq \langle \top, \top\rangle = \mathcal{H}[\![P]\!](\langle \top, 5\rangle) = \mathcal{H}[\![P]\!](\mathcal{H}(\langle 3, 5\rangle))$$

WE RELEASE SOMETHING ABOUT THE PRIVATE INPUT!

CORE: THE MOST POWERFUL ATTACKER

$$\begin{array}{lcl} ((l \in \mathit{Even}, h = 0) \ \vee \ (h \neq 0)) & & (h = 0) \\ \textbf{while } (h \neq 0) \textbf{ do } (h := 0; l := 2l) \textbf{ endw}; & \text{OR} & \textbf{while } (h \neq 0) \textbf{ do } (h := 0; l := 2l) \textbf{ endw} \\ (l \in \mathit{Even}) & & (l \in \mathit{Odd}) \end{array}$$

Let us compute the core of the output domain $\mathcal{H}$:

$$\mathcal{H}' \stackrel{\text{def}}{=} \mathcal{C}^{\mathcal{H}}_{[\![P]\!]}(\mathcal{H}) = \left\{ \langle \top, L \rangle \;\middle|\; \forall l \in \top.\, l \in L \Leftrightarrow 2l \in L \right\} = \curlyvee \left(\left\{ n\{2\}^{\mathbb{N}} \;\middle|\; n \in \mathit{Odd} \right\} \right)$$

Core: The most powerful attacker

$$\begin{array}{ll} ((l \in Even, h = 0) \ \vee \ (h \neq 0)) & (h = 0) \\ \textbf{while } (h \neq 0) \textbf{ do } (h := 0; l := 2l) \textbf{ endw}; \quad \text{OR} & \textbf{while } (h \neq 0) \textbf{ do } (h := 0; l := 2l) \textbf{ endw} \\ (l \in Even) & (l \in Odd) \end{array}$$

Let us compute the core of the output domain $\mathcal{H}$:

$$\mathcal{H}' \stackrel{\text{def}}{=} \mathcal{C}^{\mathcal{H}}_{[\![P]\!]}(\mathcal{H}) = \left\{ \langle \top, L \rangle \ \middle| \ \forall l \in \top.\, l \in L \Leftrightarrow 2l \in L \ \right\} = \Upsilon\left(\left\{ \ n\{2\}^{\mathbb{N}} \ \middle| \ n \in Odd \ \right\}\right)$$

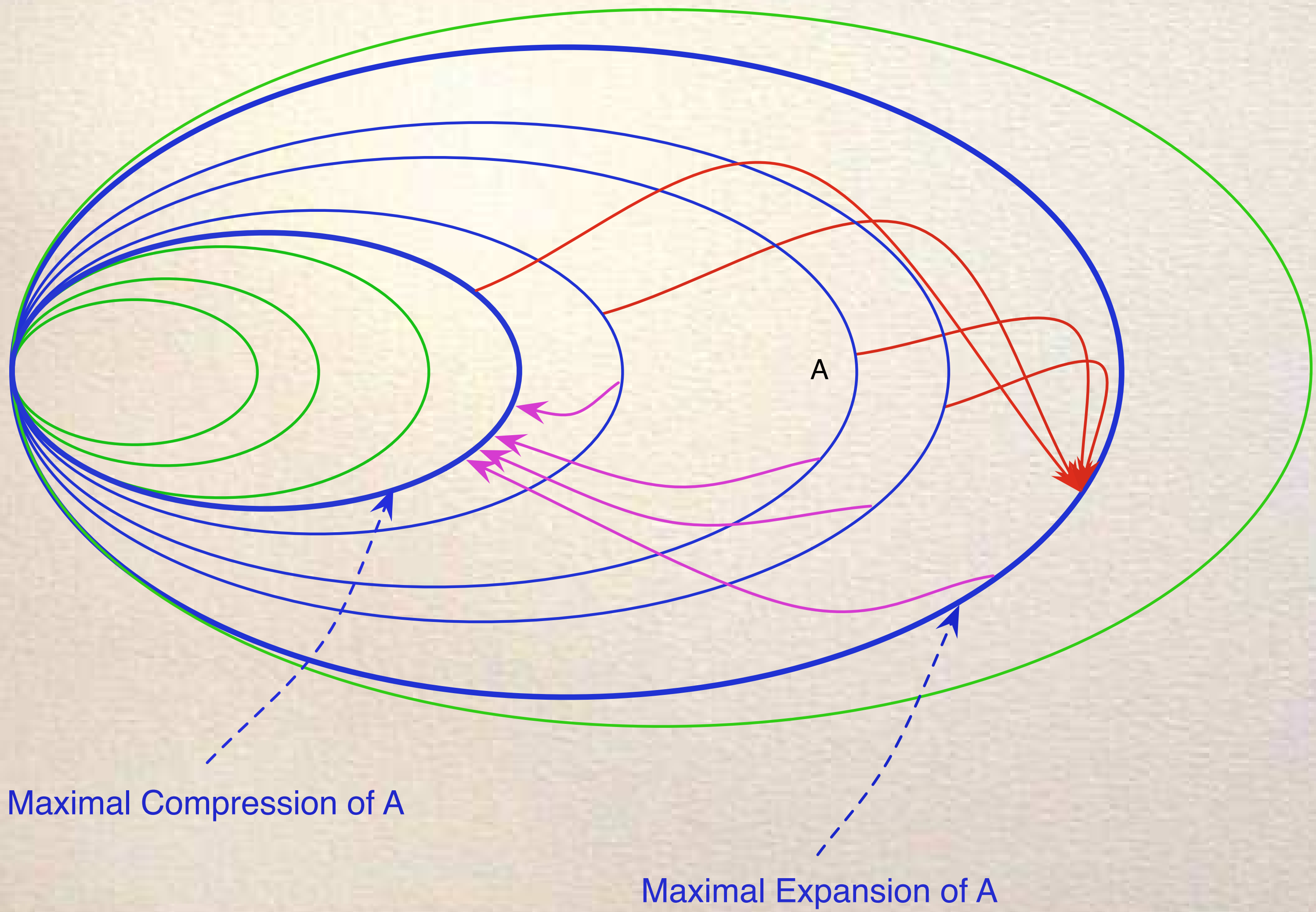
Hence

Let $l = 5$, $h = 3 \in Even$:

$$\mathcal{H}'[\![P]\!](\langle 3, 5 \rangle) = \mathcal{H}'(\langle \top, 10 \rangle) = \langle \top, 5\{2\}^{\mathbb{N}} \rangle = \mathcal{H}'(\{5, 10\}) = \mathcal{H}'[\![P]\!](\langle \top, 5 \rangle) = \mathcal{H}'[\![P]\!](\mathcal{H}(\langle 3, 5 \rangle))$$

CAN WE EXPAND AND COMPRESS DOMAINS?

THE GEOMETRY OF DOMAIN TRANSFORMERS



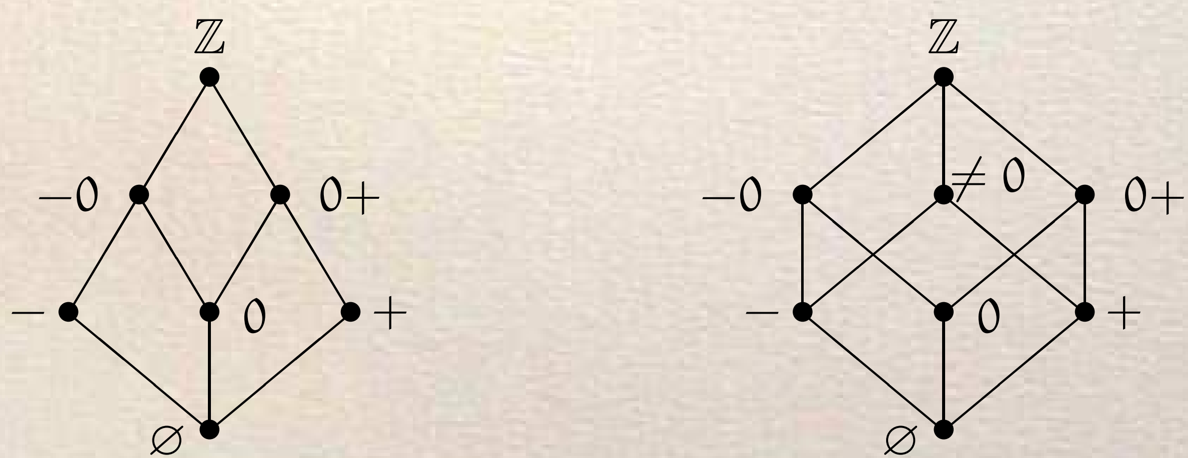
THE GEOMETRY OF DOMAIN TRANSFORMERS

DISJUNCTIVE COMPLETION

- Refinement: Forward Completeness for disjunction

$$\mathcal{R}(X) = \left\{ \bigvee Y \;\middle|\; Y \subseteq X \right\} \qquad \text{one step}$$

The least $X = \curlyvee(A)$: $X = A \sqcap \mathcal{R}(X)$ Disjunctive Completion

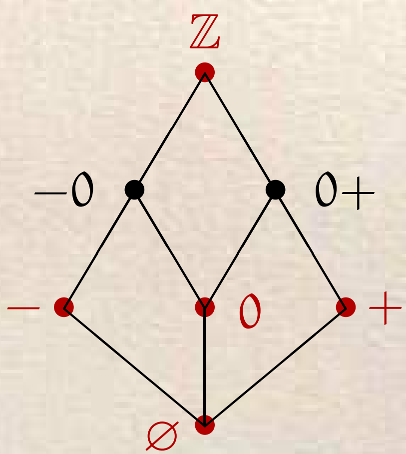


Sign $\qquad\qquad \curlyvee(\mathit{Sign})$

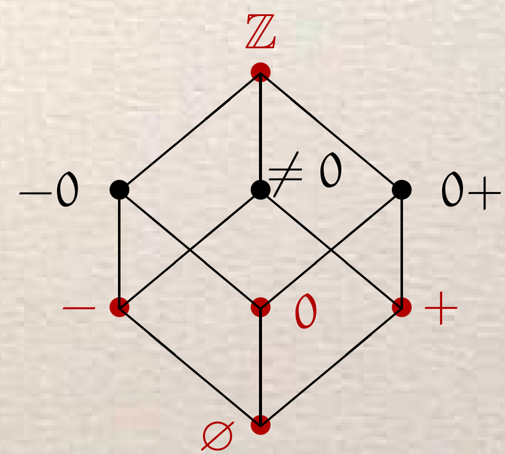
THE GEOMETRY OF DOMAIN TRANSFORMERS

DISJUNCTIVE COMPLETION

- Compressor: The domain of Join-Irreducible elements of X

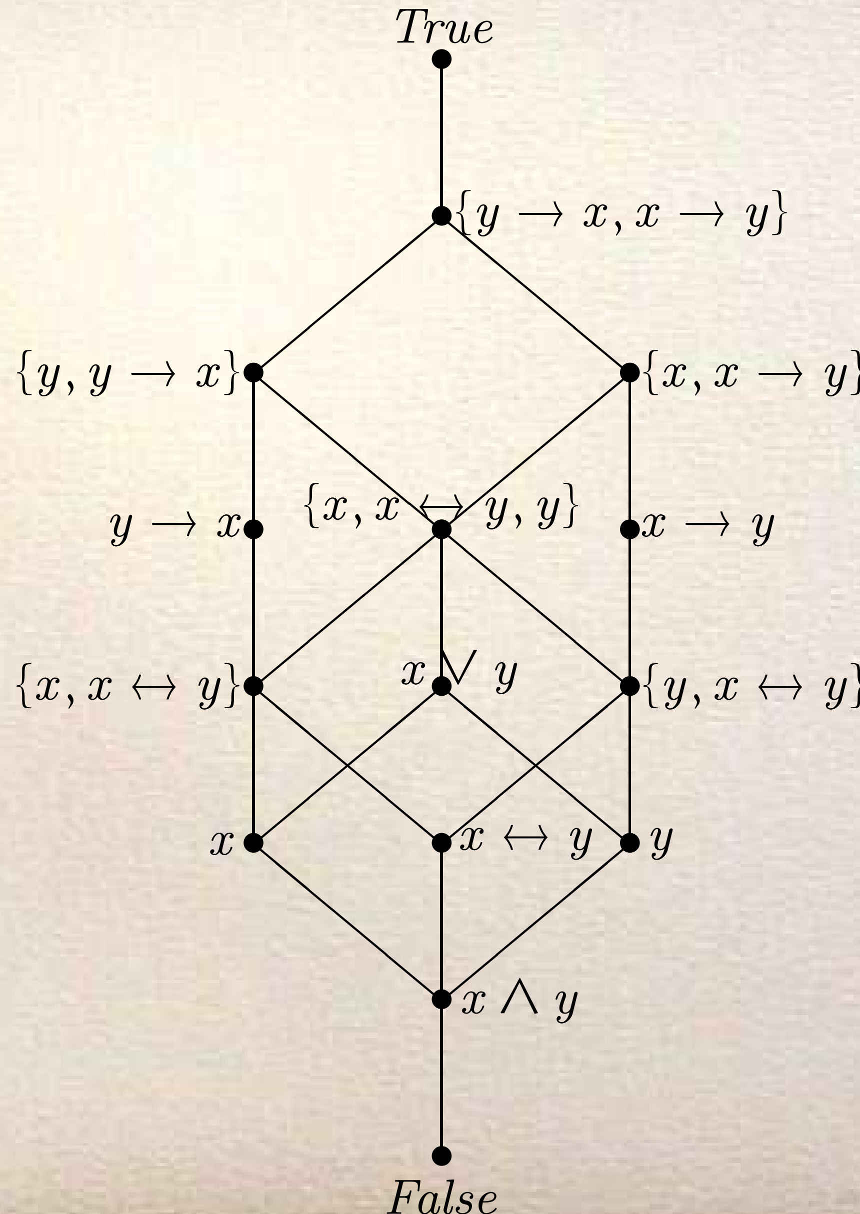


Sign

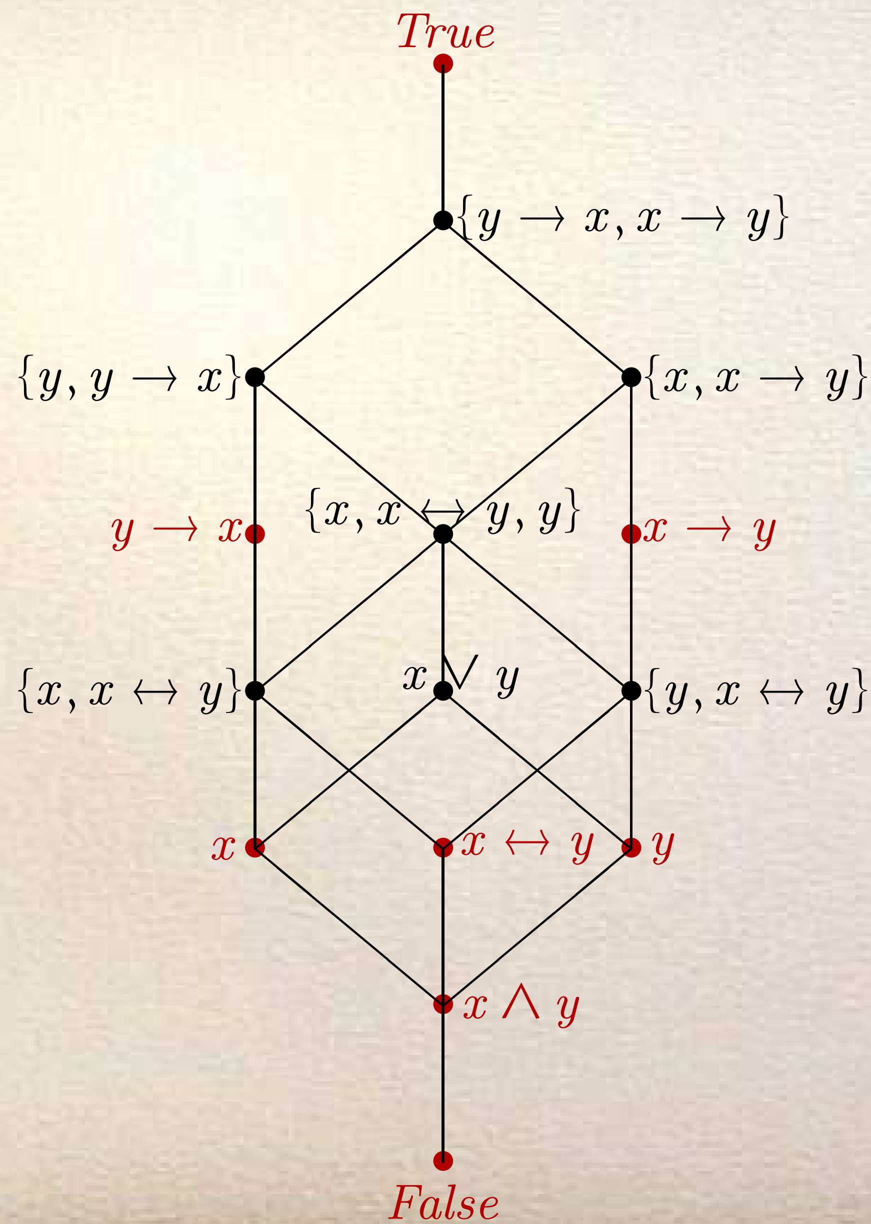


$\curlyvee(Sign)$

THE GEOMETRY OF DOMAIN TRANSFORMERS



THE GEOMETRY OF DOMAIN TRANSFORMERS



THE EXPANDER IN ANI

Let $l := 2h$ and $\mathcal{E}(X) = \bigsqcap \left\{ \, Y \, \middle| \, \mathcal{C}(X) = \mathcal{C}(Y) \, \right\}$.

- The most powerful harmless attacker for P is: $\mathcal{H}' = \curlyvee(\{Even, \{1\}, \{3\}, \ldots\})$

- Suppose the initial observer is $\rho = \{\top, Even \smallsetminus \{0\}, \{0\}, Odd, \varnothing\}$, then the most powerful harmless attacker more abstract than ρ is $Par = \mathcal{H}' \sqcup \rho$.

- The expander provides the most powerful attacker such that the <u>harmless</u> simplification is Par: $\curlyvee(\{Odd, \{0\}, \{2\}, \{4\}, \ldots\})$;

- WE OBTAIN THE MOST POWERFUL <u>MALICIOUS</u> ATTACKER, I.E., THE ONE THAT IS ABLE TO EXPLOIT AS MUCH AS POSSIBLE THE FAILURE OF NON-INTERFERENCE!

- Any more abstract (less powerful) attacker has to confuse some even inputs, for instance if it confuses $l = 0$ with $l = 2$ then it can not distinguish when $h = 0$ and $h = 1$.

THE COMPRESSOR IN ANI

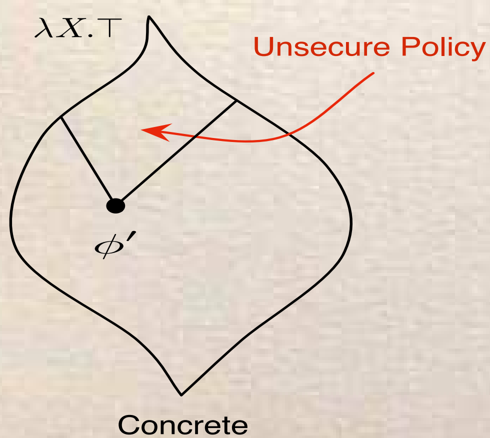
Let **if** $h = 0$ **then** $l := 0$ **else** $l := |l|(h/|h|)$ and $\mathcal{E}(X) = \bigsqcup\left\{ Y \;\middle|\; \mathcal{R}(X) = \mathcal{R}(Y) \right\}$.

- Suppose we let to flow $\phi = \{\top, \geq 0, < 0, \varnothing\}$;
- The maximal information released by P, is the shell of ϕ:
  $\phi' = \{\top, \geq 0, \neq 0, \leq 0, < 0, > 0, 0, \varnothing\}$
- THE COMPRESSOR PROVIDES THE MOST ABSTRACT DECLASSIFICATION POLICY WHICH CANNOT CAPTURE WHAT IS RELEASED BY AN ATTACKER
- The compressor is $\lambda X.\, \top$
- This means that each policy between ϕ' and $\lambda X.\, \top$ is not able to protect the program.

THE COMPRESSOR IN ANI

Let **if** $h = 0$ **then** $l := 0$ **else** $l := |l|(h/|h|)$ and $\mathcal{E}(X) = \bigsqcup \left\{ Y \;\middle|\; \mathcal{R}(X) = \mathcal{R}(Y) \right\}$.

- Suppose we let to flow $\phi = \{\top, \geq 0, < 0, \varnothing\}$;
- The maximal information released by P, is the shell of ϕ:
  $\phi' = \{\top, \geq 0, \neq 0, \leq 0, < 0, > 0, 0, \varnothing\}$
- THE COMPRESSOR PROVIDES THE MOST ABSTRACT DECLASSIFICATION POLICY WHICH CANNOT CAPTURE WHAT IS RELEASED BY AN ATTACKER



Can we make completeness by transforming semantics?

THE GEOMETRY OF SEMANTICS TRANSFORMERS

MAKING SEMANTICS COMPLETE (FROM ABOVE AND BELOW):

$$\mathbb{F}^{\uparrow}_{\eta,\rho}(f) = \bigsqcap\{h : C \longrightarrow C \mid f \sqsubseteq h,\ \rho \circ h \circ \eta = h \circ \eta\}$$
$$\mathbb{F}^{\downarrow}_{\eta,\rho}(f) = \bigsqcup\{h : C \longrightarrow C \mid f \sqsupseteq h,\ \rho \circ h \circ \eta = h \circ \eta\}$$

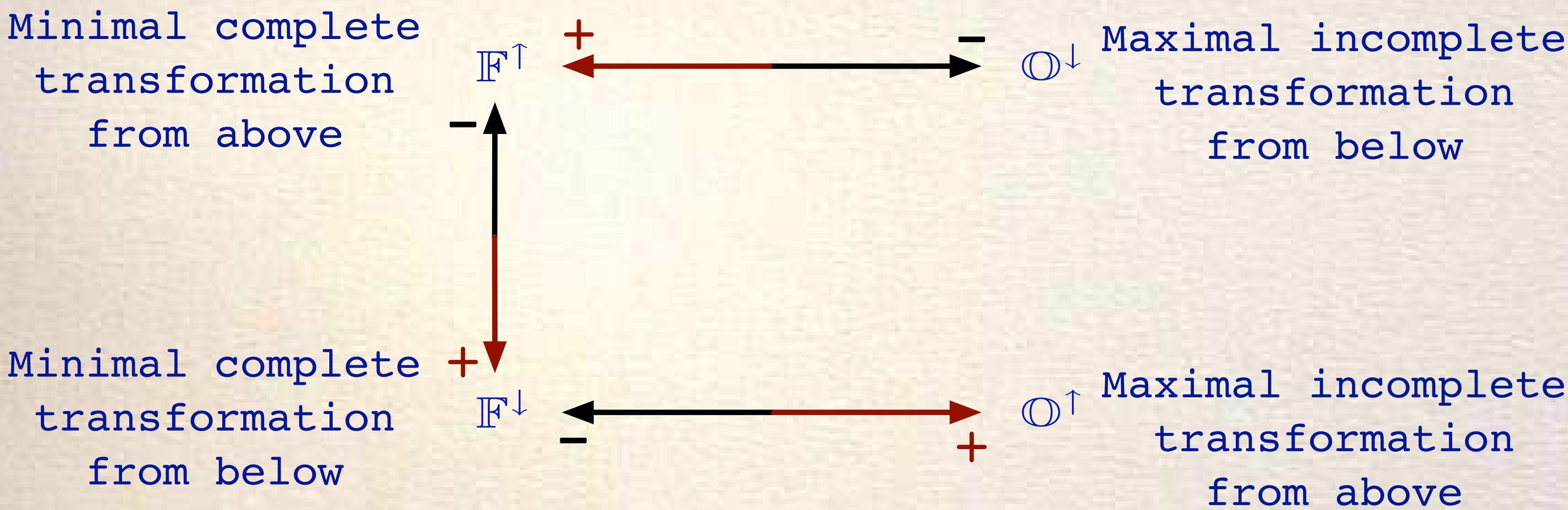
$\mathbb{F}^{\uparrow}_{\eta,\rho}(f)$ and $\mathbb{F}^{\downarrow}_{\eta,\rho}(f)$ are (Forward) complete

MAKING SEMANTICS MAXIMALLY IN-COMPLETE (FROM ABOVE AND BELOW):

$$\mathbb{O}^{\uparrow}_{\eta,\rho}(f) = \bigsqcup\{g : C \longrightarrow C \mid \mathbb{F}^{\downarrow}_{\eta,\rho}(g) = \mathbb{F}^{\downarrow}_{\eta,\rho}(f)\}$$
$$\mathbb{O}^{\downarrow}_{\eta,\rho}(f) = \bigsqcap\{g : C \longrightarrow C \mid \mathbb{F}^{\uparrow}_{\eta,\rho}(g) = \mathbb{F}^{\uparrow}_{\eta,\rho}(f)\}$$

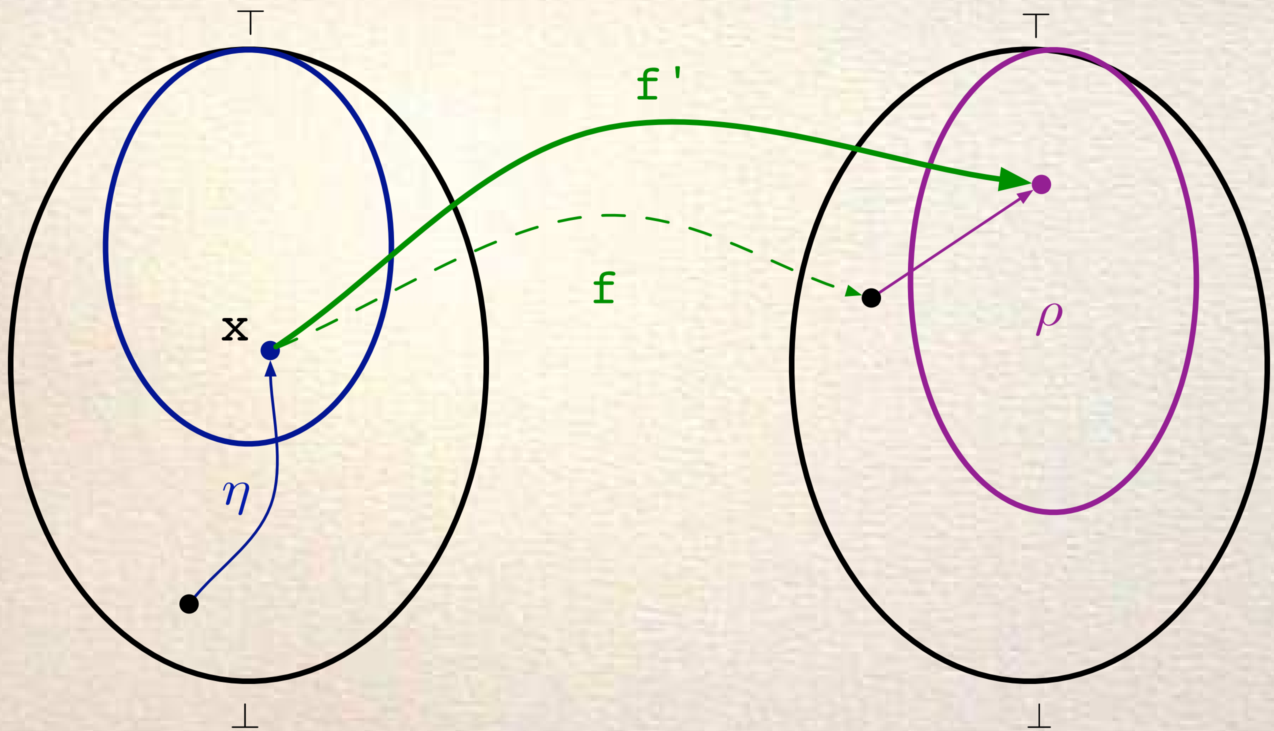
$\mathbb{O}^{\uparrow}_{\eta,\rho}(f)$ and $\mathbb{O}^{\downarrow}_{\eta,\rho}(f)$ are generally in-complete

THE GEOMETRY OF SEMANTICS TRANSFORMERS



$(\mathbb{F}^{\uparrow})^{+} = \mathbb{F}^{\downarrow}$ and $(\mathbb{F}^{\uparrow})^{-} = \mathbb{O}^{\downarrow}$

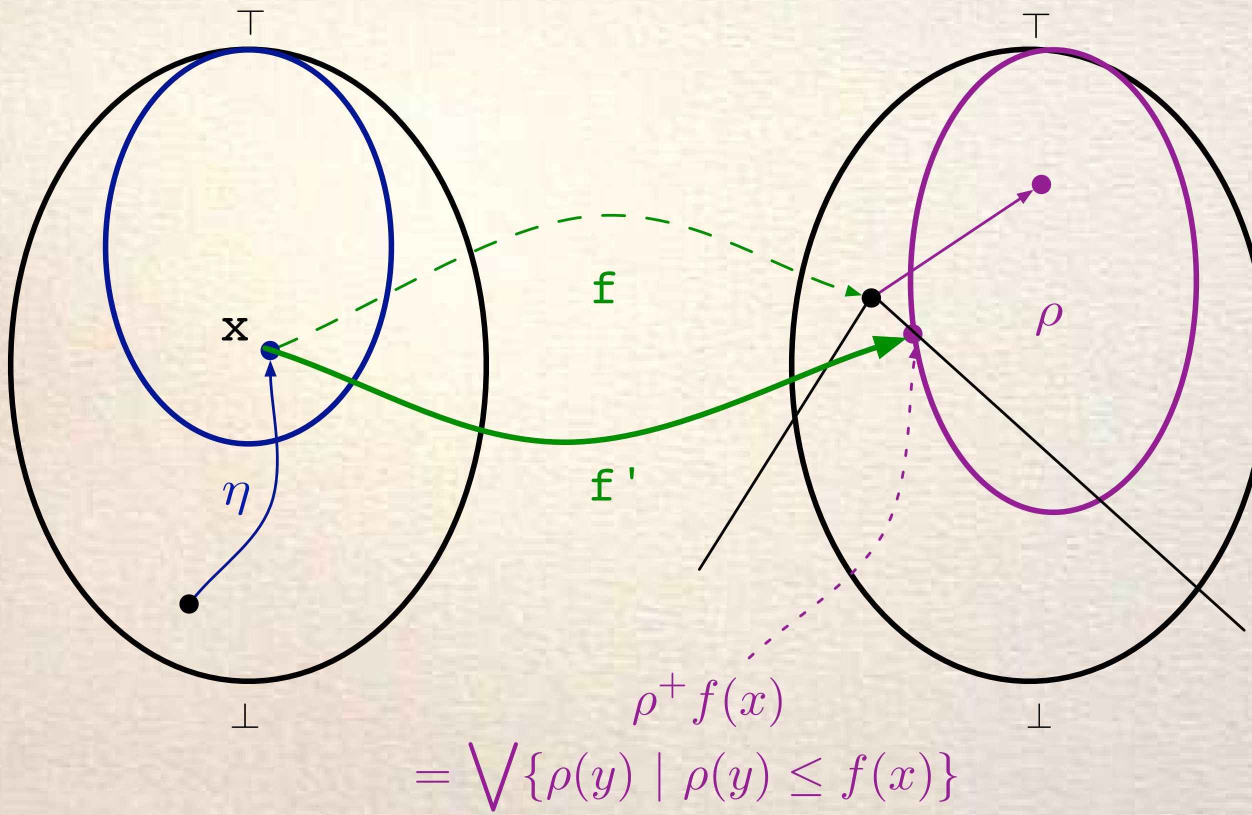
THE GEOMETRY OF SEMANTICS TRANSFORMERS



Making FORWARD COMPLETENESS: Transforming the semantics upwards

$$\mathbb{F}^{\uparrow}_{\eta,\rho} = \lambda f.\lambda x. \begin{cases} \rho \circ f(x) & \text{if } x \in \eta(C) \\ f(x) & \text{otherwise} \end{cases}$$

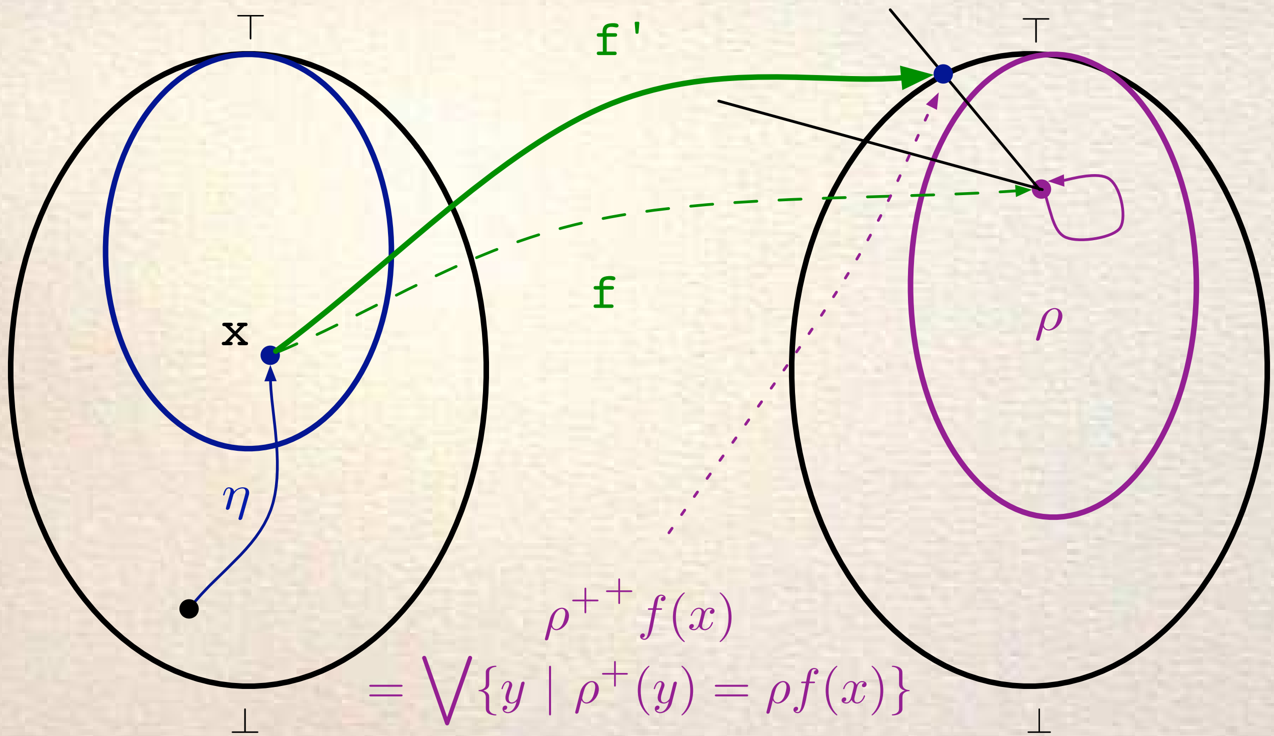
The Geometry of Semantics Transformers



Making FORWARD COMPLETENESS: Transforming the semantics downwards

$$\mathbb{F}^{\downarrow}_{\eta,\rho} = \lambda f.\lambda x. \begin{cases} \rho^{+} \circ f(x) & \text{if } x \in \eta(C) \\ f(x) & \text{otherwise} \end{cases}$$

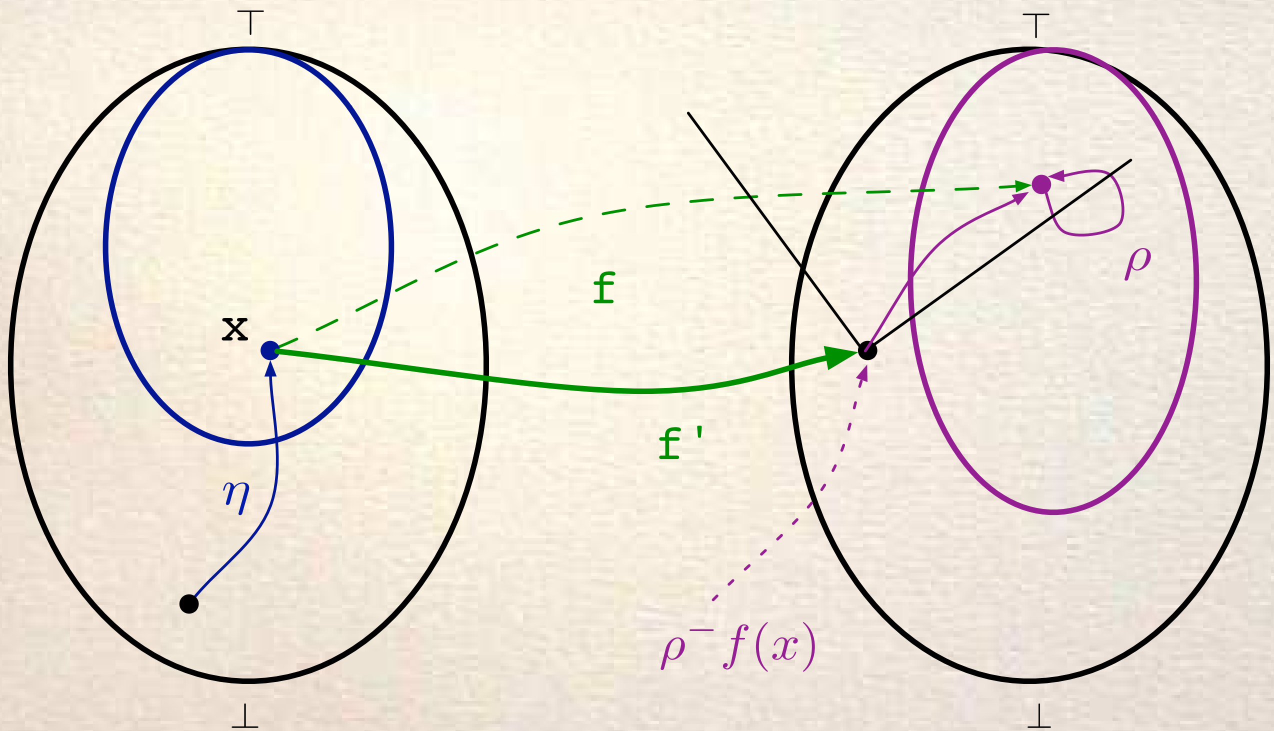
The Geometry of Semantics Transformers



Making FORWARD IN-COMPLETENESS: Transforming the semantics upwards

$$\mathbb{O}^{\uparrow}_{\eta,\rho}(f)(x) = \begin{cases} (\rho^{+})^{+}(f(x)) = \bigvee \left\{ y \;\middle|\; \rho^{+}(y) = \rho^{+}(f(x)) \right\} & \text{if } x \in \eta \\ f(x) & \text{otherwise} \end{cases}$$

The Geometry of Semantics Transformers



Making FORWARD IN-COMPLETENESS: Transforming the semantics downwards

$$\mathbb{O}^{\downarrow}_{\eta,\rho}(f)(x) = \begin{cases} \rho^{-}(f(x)) = \bigwedge \left\{ y \;\middle|\; \rho(y) = \rho(f(x)) \right\} & \text{if } x \in \eta \\ f(x) & \text{otherwise} \end{cases}$$

MAKING SEMANTICS COMPLETE: AN EXAMPLE

$$\textbf{while } (h > 0) \textbf{ do } (h := h - 1; l := h) \textbf{ endw}$$

Making semantics complete: An Example

$(h > 0) \;\vee\; (l = 0)$

while $(h > 0)$ **do** $(h := h - 1; l := h)$ **endw**;

$(l = 0)$

Or

$(h = 0)$

while $(h > 0)$ **do** $(h := h - 1; l := h)$ **endw**

$(l \neq 0)$

Let $l = 5$, $h_1 = 3$, $h_2 = 0$:

$\mathcal{H}[\![P]\!](\langle 3, 5\rangle) = \langle \top, 0\rangle \neq \langle \top, 5\rangle = \mathcal{H}[\![P]\!](\langle 0, 5\rangle)$

MAKING SEMANTICS COMPLETE: AN EXAMPLE

$$(h \geq 0)$$

while $(h > 0)$ **do** $(h := h - 1; l := h)$ **endw**;

$$(l = 0)$$

OR

$$(h = 0)$$

while $(h > 0)$ **do** $(h := h - 1; l := h)$ **endw**

$$(l \neq 0)$$

Let $l = 5$, $h_1 = 3$, $h_2 = 0$:

$$\mathcal{H}[\![P]\!](\langle 3, 5\rangle) = \langle \top, 0\rangle \neq \langle \top, 5\rangle = \mathcal{H}[\![P]\!](\langle 0, 5\rangle)$$

WE RELEASE SOMETHING (THE EQUALITY WITH 0) ABOUT THE PRIVATE INPUT!

MAKING SEMANTICS COMPLETE: AN EXAMPLE

$$(h \geq 0)$$
while $(h > 0)$ **do** $(h := h - 1; l := h)$ **endw**;
$$(l = 0)$$

OR

$$(h = 0)$$
while $(h > 0)$ **do** $(h := h - 1; l := h)$ **endw**
$$(l \neq 0)$$

The upward transformation inducing completeness of Wlp_P is:

$$\mathbb{F}^{\uparrow}(Wlp_P) : \{l = 0 \mapsto h \in \mathbb{Z} \text{ and } l \neq 0 \mapsto h \in \mathbb{Z}\}$$

MAKING SEMANTICS COMPLETE: AN EXAMPLE

$$(h \geq 0)$$

while $(h > 0)$ **do** $(h := h - 1; l := h)$ **endw**;

$$(l = 0)$$

OR

$$(h = 0)$$

while $(h > 0)$ **do** $(h := h - 1; l := h)$ **endw**

$$(l \neq 0)$$

The upward transformation inducing completeness of Wlp_P is:

$$\mathbb{F}^{\uparrow}(Wlp_P) : \{l = 0 \mapsto \ h \in \mathbb{Z} \text{ and } l \neq 0 \mapsto h \in \mathbb{Z}\}$$

This is, for example, the semantics of the program

$$Q : \quad l_1 := l;\ P;\ l := l_1$$

DISCUSSION

- Encoding AI problems as completeness problems:
  - Systematic transformations for optimal models
  - Better understanding of the limits of abstractions
- Adequacy of the theory
  - Abstract interpretation is perfectly adequate to reason about itself
  - A calculational design of domain and code transformations can be done in abstract interpretation
  - Completeness is a driving force for understanding domain and code transformers
  - From semantics transformers to code transformations (and deformations) by AI [Cousot & Cousot '02]

Future directions

- Code obfuscation and sw watermarking
  - Completeness corresponds to maximal precision
  - Obfuscating P corresponds to make P maximally incomplete against a given attack ($\mathbb{O}$?)
  - Watermarks and fingerprints can be hidden in completeness holes
- Language-based security
  - $\mathbb{F}$ provides code protection against information release!
  - Can we design a monitor M such that $\mathbb{F}(\llbracket P \rrbracket) = \llbracket M; P \rrbracket$?
  - Models for active attackers as code transformations (code deformations)... and the corresponding completeness problem?
- Abstract Model Checking
  - Isolate temporal sub-logics which are complete for a given abstract system to analyse.

MANY THANKS!!