# Properties and satisfaction

We have seen: at the semantic level:

- A *property* $\varphi$ is some *semantic set* (of states, streams, trees, ...)
- A *model* $M$ represents a set of properties
- *Conformance* ($\models$) essentially boils down to inclusion of semantic sets

$\Longrightarrow$ We may use a lattice $(\mathcal{P}, <, \sqcup, \sqcap, \bot, T)$ to represent this situation:

$$P_1 < P_2 \text{ represents } M \models \varphi \quad (\text{or } M \models M' \text{ or } \varphi \models \varphi')$$

An *Abstraction* $\alpha$ must define a property preserving mapping between concrete and abstract properties:

$$|\alpha(M)| < |\alpha(\varphi)| \text{ implies } |M| < |\varphi|$$

But: $M$ defines also a (set of) basic property transformations $F$ (*succ*, *pred*, ...) used to *compute* the semantics of $M$ or $\varphi$.

$\Longrightarrow$ as we want to *compute* $|M|$, $|\alpha(M)|$ ... by computing fixpoints of basic functions associated with $M$, $\alpha(M)$, ... we want to *preserve these functions* at the first place.

# Properties and satisfaction

We have seen: at the semantic level:

- A *property* $\varphi$ is some *semantic set* (of states, streams, trees, ...)
- A *model* $M$ represents a set of properties
- *Conformance* ($\models$) essentially boils down to inclusion of semantic sets

$\Longrightarrow$ We may use a lattice $(\mathcal{P}, <, \sqcup, \sqcap, \perp, T)$ to represent this situation:

$P_1 < P_2$ represents $M \models \varphi$ (or $M \models M'$ or $\varphi \models \varphi'$)

An *Abstraction* $\alpha$ must define a property preserving mapping between concrete and abstract properties:

$$|\alpha(M)| < |\alpha(\varphi)| \text{ implies } |M| < |\varphi|$$

But: $M$ defines also a (set of) basic property transformations $F$ (*succ*, *pred*, ...) used to *compute* the semantics of $M$ or $\varphi$.

$\Longrightarrow$ as we want to *compute* $|M|$, $|\alpha(M)|$ ... by computing fixpoints of basic functions associated with $M$, $\alpha(M)$, ... we want to *preserve these functions* at the first place.

# Properties and satisfaction

We have seen: at the semantic level:

- A *property* $\varphi$ is some *semantic set* (of states, streams, trees, ...)
- A *model* $M$ represents a set of properties
- *Conformance* ($\models$) essentially boils down to inclusion of semantic sets

$\Longrightarrow$ We may use a lattice $(\mathcal{P}, <, \sqcup, \sqcap, \bot, T)$ to represent this situation:

$$P_1 < P_2 \text{ represents } M \models \varphi \quad (\text{or } M \models M' \text{ or } \varphi \models \varphi')$$

An *Abstraction* $\alpha$ must define a property preserving mapping between concrete and abstract properties:

$$|\alpha(M)| < |\alpha(\varphi)| \text{ implies } |M| < |\varphi|$$

But: $M$ defines also a (set of) basic property transformations $F$ (*succ*, *pred*, ...) used to *compute* the semantics of $M$ or $\varphi$.

$\Longrightarrow$ as we want to *compute* $|M|$, $|\alpha(M)|$ ... by computing fixpoints of basic functions associated with $M$, $\alpha(M)$, ... we want to *preserve these functions* at the first place.

# Properties and satisfaction

We have seen: at the semantic level:

- A *property* $\varphi$ is some *semantic set* (of states, streams, trees, ...)
- A *model* $M$ represents a set of properties
- *Conformance* ($\models$) essentially boils down to inclusion of semantic sets

$\Longrightarrow$ We may use a lattice $(\mathcal{P}, <, \sqcup, \sqcap, \bot, T)$ to represent this situation:

$P_1 < P_2$ represents $M \models \varphi$ (or $M \models M'$ or $\varphi \models \varphi'$)

An *Abstraction* $\alpha$ must define a property preserving mapping between concrete and abstract properties:

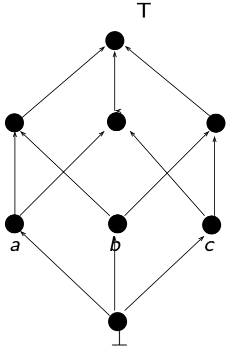
$$|\alpha(M)| < |\alpha(\varphi)| \text{ implies } |M| < |\varphi|$$

But: $M$ defines also a (set of) basic property transformations $F$ (*succ*, *pred*, ...) used to *compute* the semantics of $M$ or $\varphi$.

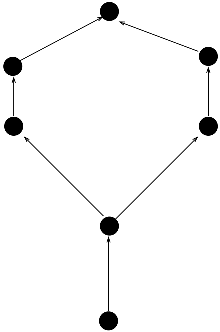
$\Longrightarrow$ as we want to *compute* $|M|$, $|\alpha(M)|$ ... by computing fixpoints of basic functions associated with $M$, $\alpha(M)$, ... we want to *preserve these functions* at the first place.

# Preliminaries: Galois connexions

... monotonic mappings between property lattices

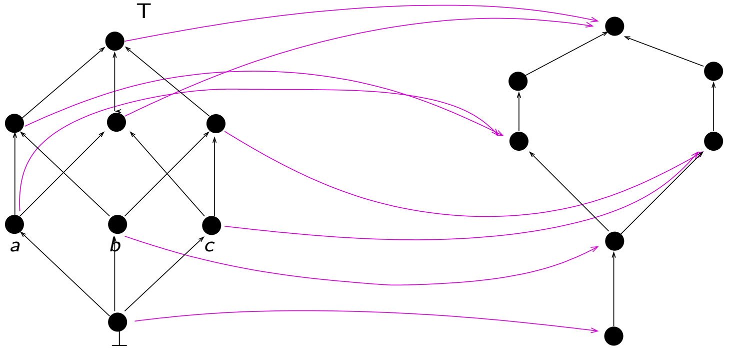



Disjunctions of $a, b, c$



# Preliminaries: Galois connexions

... monotonic mappings between property lattices



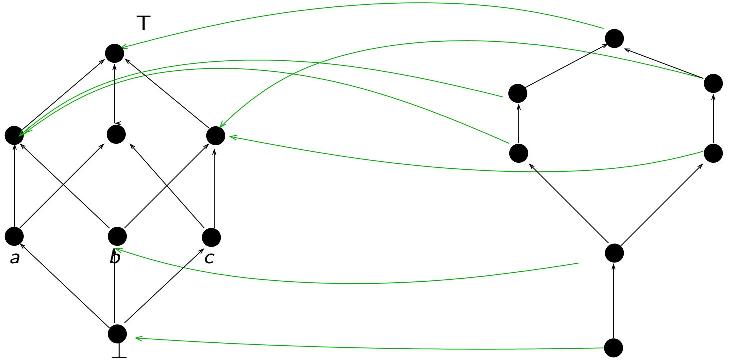

Disjunctions of $a, b, c$

$\alpha$**: distributes over** $\sqcup$

$\alpha$: "is represented by" (abstraction)

# Preliminaries: Galois connexions

... monotonic mappings between property lattices



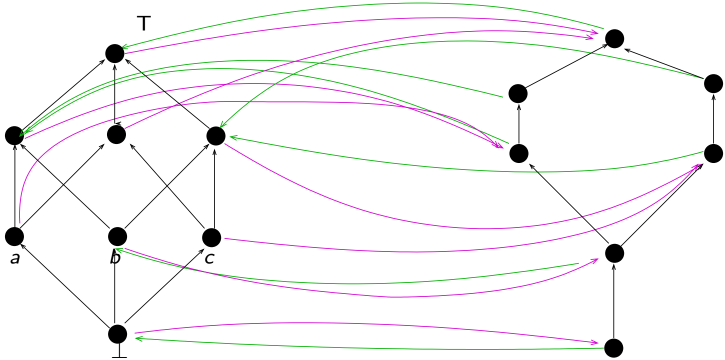

Disjunctions of $a, b, c$

$\gamma$: **distributes over** $\sqcap$

$\gamma$ : "represents" (concretisation)

# Preliminaries: Galois connexions

... monotonic mappings between property lattices




Disjunctions of $a, b, c$

$\alpha$: **distributes over $\sqcup$**

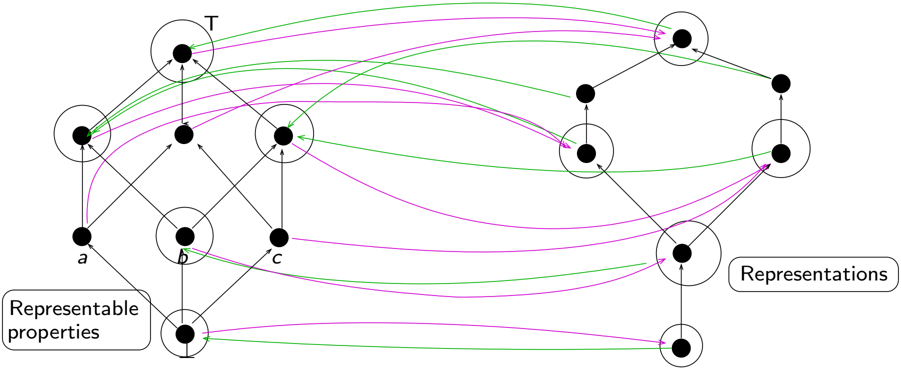
$\gamma$: **distributes over $\sqcap$**

$Id < \alpha \circ \gamma \quad \alpha = \alpha \circ \gamma \circ \alpha$

$\gamma \circ \alpha <^{A} Id \quad \gamma = \gamma \circ \alpha \circ \gamma$

# Preliminaries: Galois connexions

... monotonic mappings between property lattices



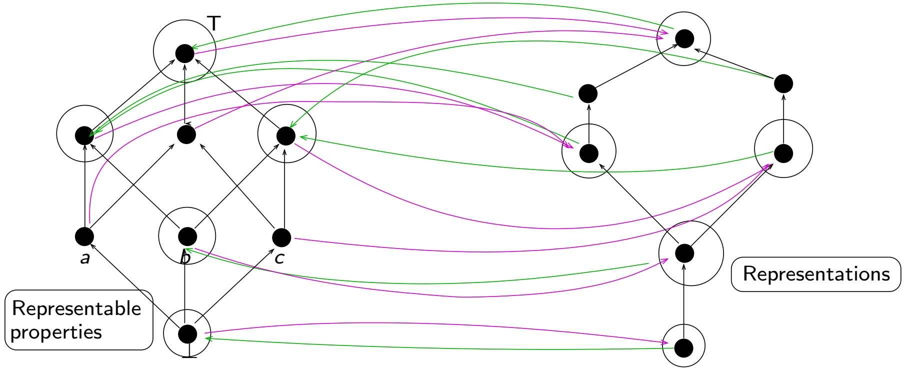

Disjunctions of $a, b, c$

$\alpha$: **distributes over $\sqcup$** $\quad Id < \alpha \circ \gamma \quad \alpha = \alpha \circ \gamma \circ \alpha$

$\gamma$: **distributes over $\sqcap$** $\quad \gamma \circ \alpha <^{A} Id \quad \gamma = \gamma \circ \alpha \circ \gamma$

# Preliminaries: Galois connexions

… monotonic mappings between property lattices




Disjunctions of $a, b, c$

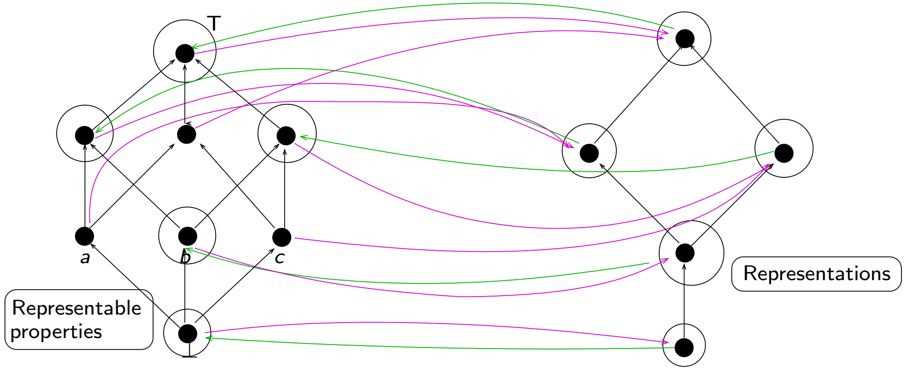
$\alpha$: **distributes over** $\sqcup$ $\quad$ $Id < \alpha \circ \gamma \quad \alpha = \alpha \circ \gamma \circ \alpha$

$\gamma$: **distributes over** $\sqcap$ $\quad$ $\gamma \circ \alpha <^A Id \quad \gamma = \gamma \circ \alpha \circ \gamma$

$$\gamma(x) = \sqcup_{\alpha(x') <^A x} x'$$

# Preliminaries: Galois connexions

... monotonic mappings between property lattices




Disjunctions of $a, b, c$

$\alpha$: **distributes over $\sqcup$**

$Id < \alpha \circ \gamma \quad \alpha = \alpha \circ \gamma \circ \alpha$

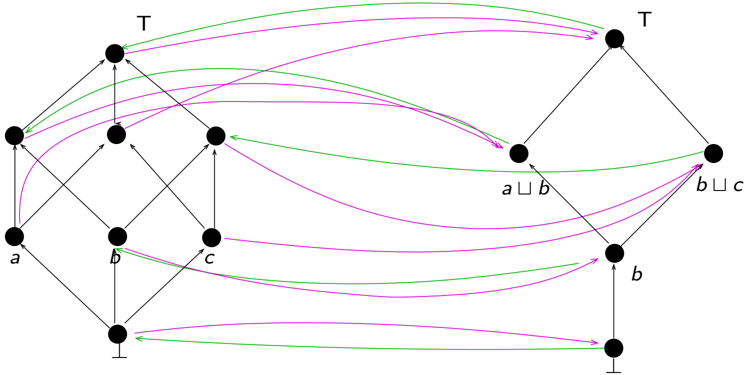
$\gamma$: **distributes over $\sqcap$**

$\gamma \circ \alpha <^{A} Id \quad \gamma = \gamma \circ \alpha \circ \gamma$

$\gamma(x) = \sqcup_{\alpha(x') <^{A} x} x'$

# Preliminaries: Galois connexions

... monotonic mappings between property lattices




Disjunctions of $a, b, c$

Abstract property lattice

$\alpha$: **distributes over $\sqcup$**

$\gamma$: **distributes over $\sqcap$**

$Id < \alpha \circ \gamma \quad \alpha = \alpha \circ \gamma \circ \alpha$

$\gamma \circ \alpha <^A Id \quad \gamma = \gamma \circ \alpha \circ \gamma$

$\gamma(x) = \sqcup_{\alpha(x')<^A x} x'$

# Preliminaries: Galois connexions

Let $(L, <, \sqcup, \sqcap, \bot, \top)$, $(L^A, <^A, \sqcup^A, \sqcap^A, \bot^A, \top^A)$ be (property) lattices and $\alpha : L \mapsto L^A$, $\gamma : L^A \mapsto L$ strict monotonic functions.

$(\alpha, \gamma)$ is a *Galois connexion* from $L$ to $L^A$ if

- $Id < \alpha \circ \gamma$ — $\alpha \circ \gamma \circ \alpha = \alpha$ ($\alpha \circ \gamma$ is an extensive closure)
- $\gamma \circ \alpha <^A Id$ — $\gamma \circ \alpha \circ \gamma = \gamma$ ($\gamma \circ \alpha$ is a reductive closure)

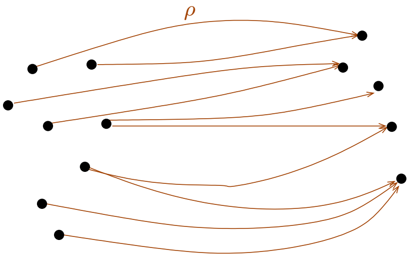
That is, we also have

- $\alpha$ distributes over $\sqcup$ and $\gamma$ distributes over $\sqcap$ (no loss of precision)
- $\alpha$ and $\gamma$ are each others inverse on the set of *closed* elements $\{\mathrm{Q} \in L \mid \mathrm{Q} \in img(\alpha \circ \gamma)\}$, $\{\mathrm{Q}^A \in L^A \mid \mathrm{Q}^A \in img(\gamma \circ \alpha)\}$. Closed elements of $L$ are properties *representable* in $L^A$.

- for *Boolean lattices*, $\alpha$, $\gamma$ have duals $\widetilde{\alpha} = \neg\alpha\neg$, $\widetilde{\gamma} = \neg\gamma\neg$
- $(\widetilde{\alpha}, \widetilde{\gamma})$ is a Galois connexion from $\widetilde{L}$ to $\widetilde{L^A}$ (lattices for $>$ and $>^A$), and $(\widetilde{\gamma}, \widetilde{\alpha})$ from $L^A$ to $L$.

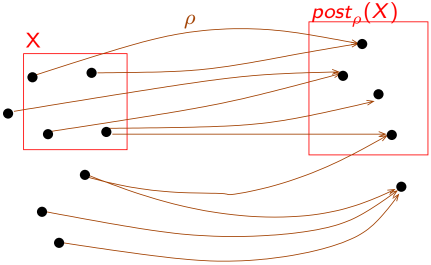
# Preliminaries on property transformers

Relation $\rho$ relates semantic "items". A *property* is a set of items (states, sequences, ...).




Binary relation $\rho$ defines 4 basic functions on sets (property transformers):

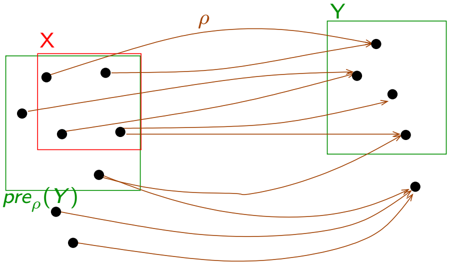
# Preliminaries on property transformers




$\rho$ defines 4 property transformers:

- $post_\rho(X) = \{q' \mid \exists q \in X \wedge q \rightarrow_\rho q'\}$ (post-condition)
- $post_\rho$ monotonic, distributes over $\sqcup$

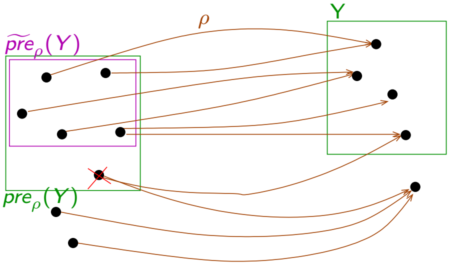
# Preliminaries on property transformers




$\rho$ defines 4 property transformers:

- $post_\rho(X) = \{q' \mid \exists q \in X \wedge q \rightarrow_\rho q'\}$ (post-condition)
- $pre_\rho(Y) = post_{\rho^{-1}}(Y)$ (predecessors)

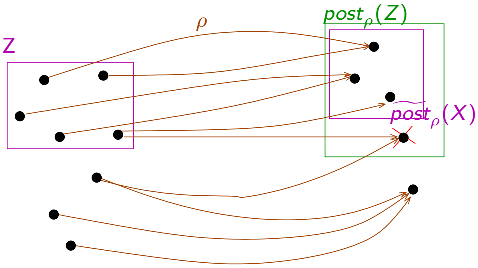
# Preliminaries on property transformers




$\rho$ defines 4 property transformers:

- $\widetilde{pre}_\rho(Y) = \{q \mid \forall q \rightarrow_\rho q' \implies q' \in Y\}$ (weakest precondition)
- $\widetilde{pre}_\rho$ monotonic, distributes over $\sqcap$
- if $\rho$ total on $Q$: $\widetilde{pre}_\rho \implies pre_\rho$
- $post_\rho \circ \widetilde{pre}_\rho$ an upper closure
- $(post_\rho, \widetilde{pre}_\rho)$, a Galois connexion (from left to right)

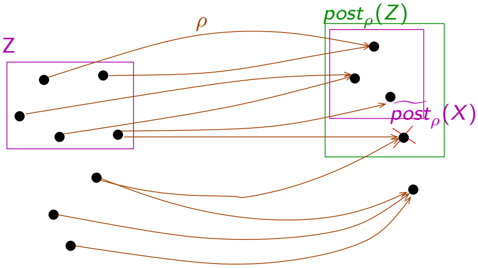
# Preliminaries on property transformers




$\rho$ defines 4 property transformers:

- $\widetilde{post}_\rho(X) = \widetilde{pre}_{\rho^{-1}}(X)$
- $(pre_\rho, \widetilde{post}_\rho)$ is a Galois connexion (from right to left)

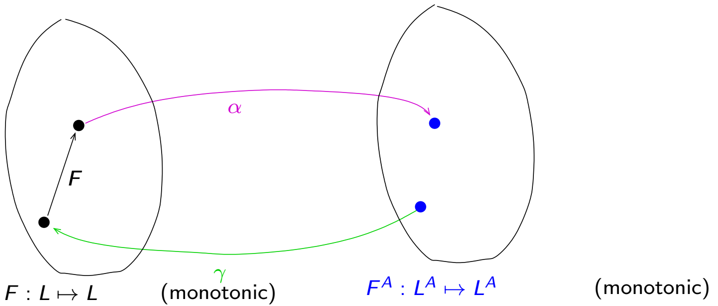
# Preliminaries on property transformers




Furthermore:

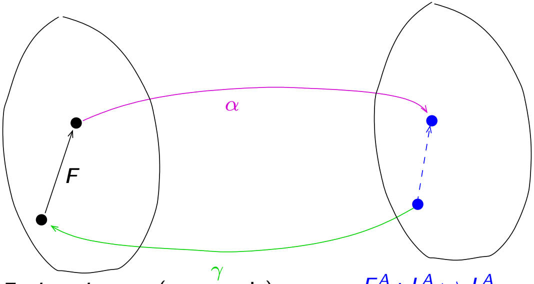
- $(\widetilde{post}_\rho, pre_\rho)$, $(\widetilde{pre}_\rho, post_\rho)$: connexions between dual lattices

# Property preservation with Galois connexions



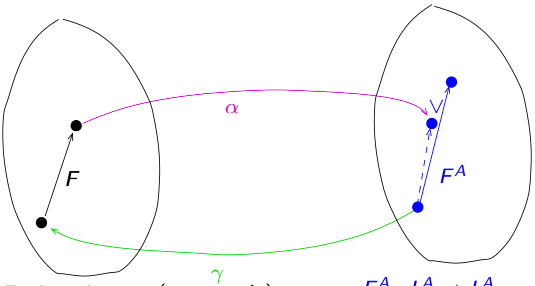

Remind that elements of the lattice are "properties" (sets of items)

# Property preservation with Galois connexions




$F : L \mapsto L$ (monotonic) $F^A : L^A \mapsto L^A$ (monotonic)

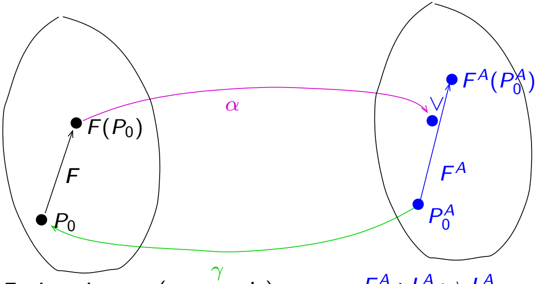
# Property preservation with Galois connexions




$F : L \mapsto L$ (monotonic) $F^A : L^A \mapsto L^A$ (monotonic)

$$\gamma \circ F \circ \alpha <^A F^A \;\Leftrightarrow\; (\alpha\circ)$$
$$F \circ \alpha <^A \alpha \circ F^A \;\Leftrightarrow\; (\circ\gamma)$$
$$F < \alpha \circ F^A \circ \gamma \;\Leftrightarrow\; (\gamma\circ)$$
$$\gamma \circ F < F^A \circ \gamma$$

# Property preservation with Galois connexions

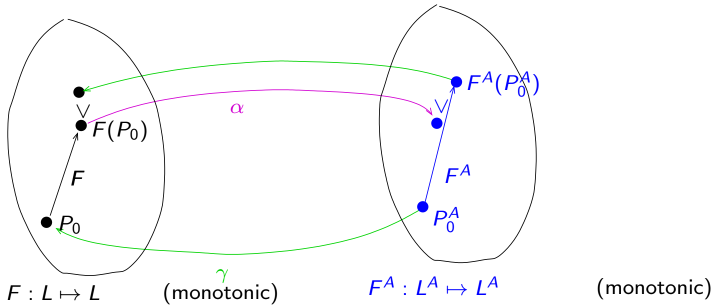



$F : L \mapsto L$ (monotonic) $\quad$ $F^A : L^A \mapsto L^A$ (monotonic)

$F$, $F^A$: obtained from $F_i$ (resp. $F_i^A$) using $\circ$, $\sqcup$, $\sqcap$ and fix-point operators.

*Typically*: *reach*, the least fix-point of the successor function ($post_{\rightarrow}$) for calculating set of *reachable states* from the initial states

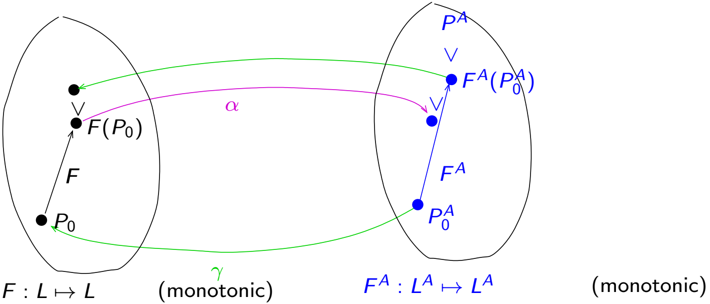
# Property preservation with Galois connexions




$F$, $F^A$: obtained from $F_i$ (resp. $F_i^A$) using $\circ$, $\sqcup$, $\sqcap$ and fix-point operators.

$$\boxed{F(P_0) < \gamma(F^A(P_0^A))}$$

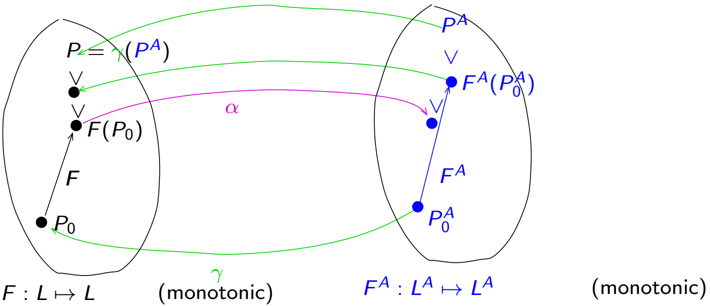
# Property preservation with Galois connexions




$P = \gamma(P^A)$ — an invariance property to hold, then

$$F^A(P_0^A) <^A P^A \text{ implies } F(P_0) < P$$

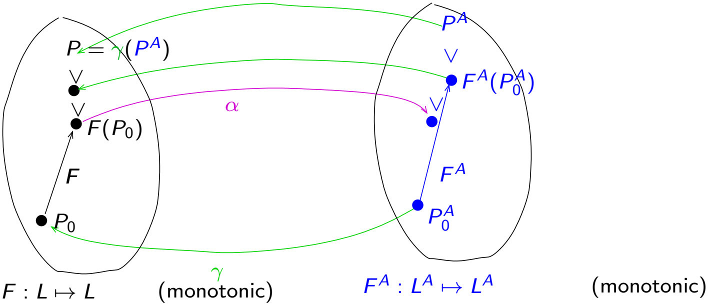
# Property preservation with Galois connexions




$P = \gamma(P^A)$ — an invariance property to hold, then

$$\boxed{F^A(P_0^A) <^A P^A \text{ implies } F(P_0) < P}$$

# Property preservation with Galois connexions



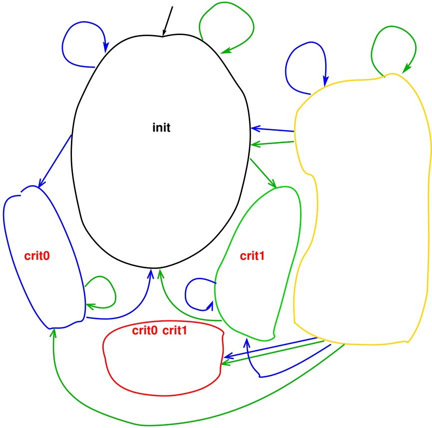

$P = \gamma(P^A)$ — an invariance property to hold, then

$$F^A(P_0^A) <^A P^A \text{ implies } F(P_0) < P$$

$$M^A \models \varphi^A \text{ implies } M \models \varphi$$

# Example: Abstract Peterson

$\alpha$: (1) group *states* to 5 abstract ones (black, green, blue, red, yellow),
(2) draw a (green / blue) *transition* between abstract states if there is one between a corresponding pair of concrete ones




$\alpha(|M|)$ satisfies property (1) *mutual exclusion*.

A typical $\alpha$ which does satisfy

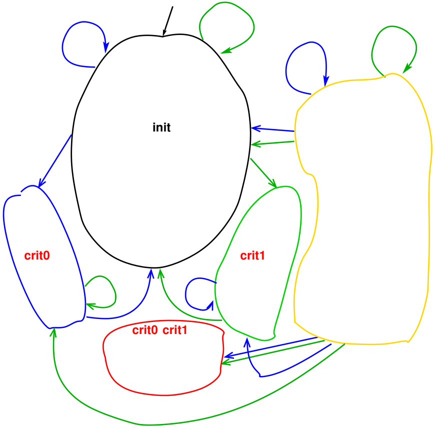
$$\gamma \circ post_{\rightarrow} \circ \alpha <^{A} post_{\rightarrow^{A}}$$

and there fore also

$$reach(init) < \gamma(reach^{A}(init^{A}))$$

# Example: Abstract Peterson

$\alpha$: (1) group *states* to 5 abstract ones (black, green, blue, red, yellow),
(2) draw a (green / blue) *transition* between abstract states if there is one between a corresponding pair of concrete ones




$\alpha(|M|)$ satisfies property (1) *mutual exclusion*.

A typical $\alpha$ which does satisfy

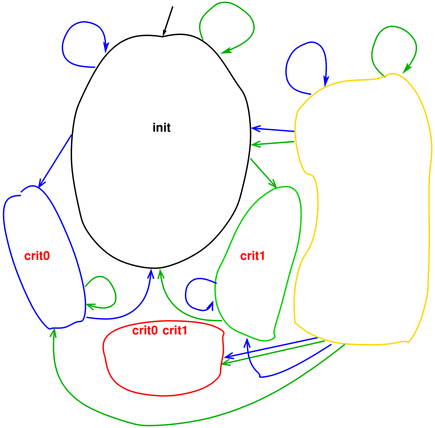
$$\gamma \circ post_{\rightarrow} \circ \alpha <^{A} post_{\rightarrow^{A}}$$

and there fore also

$$reach(init) < \gamma(reach^{A}(init^{A}))$$

# Example: Abstract Peterson

$\alpha$: (1) group *states* to 5 abstract ones (black, green, blue, red, yellow),
(2) draw a (green / blue) *transition* between abstract states if there is one between a corresponding pair of concrete ones




$\alpha(|M|)$ satisfies property (1) *mutual exclusion*.

A typical $\alpha$ which does satisfy

$$\gamma \circ post_{\rightarrow} \circ \alpha <^{A} post_{\rightarrow^{A}}$$

and there fore also

$$reach(init) < \gamma(reach^{A}(init^{A}))$$

# Property preservation ... continued

To combine model-checking and abstraction, we are interested in

- proving properties of the form $init < F$ where $F$ represents a requirement $\varphi$ obtained as a fix-point, and $init$ the initial states,
- computing fix-points on the (smaller) abstract lattice: we need *under approximations* of $F$.

Consider $(\widetilde{\alpha}, \widetilde{\gamma})$, the dual of $(\alpha, \gamma)$ between dual lattices.

- if $F$ on $L$ obtained from $F_i$ using $\circ$, $\vee$, $\wedge$ and fix-point operators, and analogously for $F^A$
- if $\widetilde{\gamma} \circ F_i \circ \widetilde{\alpha} >^A F_i^A$ (which is equivalent to $\gamma \circ \widetilde{F_i} \circ \alpha <^A \widetilde{F_i^A}$ )
- if $(P_1, ...)$ with $P_i \in L$, and $P_i^A = \widetilde{\alpha}(P_i)$

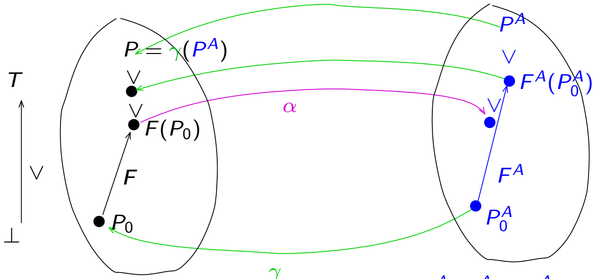
Then $F(P_1, ...) > \widetilde{\gamma}(F_A(P_1^A, ...))$: $init^A <^A F^A(P_1^A, ...)$ is an *under approximation* of $F(P_1, ...)$. If $\widetilde{\gamma}(init^A) < init$

Preservation of verification results from $L^A$ to $L$:

# Property preservation ... continued

To combine model-checking and abstraction, we are interested in

- proving properties of the form *init* $< F$ where $F$ represents a requirement $\varphi$ obtained as a fix-point, and *init* the initial states,
- computing fix-points on the (smaller) abstract lattice: we need *under approximations* of $F$.




$F : L \mapsto L$ (monotonic) $F^A : L^A \mapsto L^A$ (monotonic)

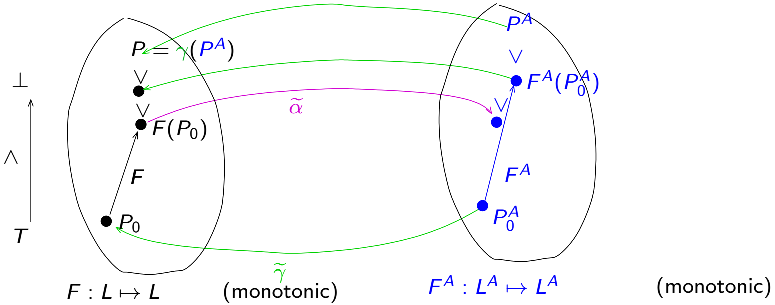
Consider $(\widetilde{\alpha}, \widetilde{\gamma})$, the dual of $(\alpha, \gamma)$ between dual lattices.

- if $F$ on $L$ obtained from $F_i$ using $\circ$, $\vee$, $\wedge$ and fix-point operators, and

# Property preservation ... continued

To combine model-checking and abstraction, we are interested in

- proving properties of the form *init* $<$ $F$ where $F$ represents a requirement $\varphi$ obtained as a fix-point, and *init* the initial states,
- computing fix-points on the (smaller) abstract lattice: we need *under approximations* of $F$.




Consider $(\widetilde{\alpha}, \widetilde{\gamma})$, the dual of $(\alpha, \gamma)$ between dual lattices.

- if $F$ on $L$ obtained from $F_i$ using $\circ$, $\vee$, $\wedge$ and fix-point operators, and

# Property preservation ... continued

Consider $(\widetilde{\alpha}, \widetilde{\gamma})$, the dual of $(\alpha, \gamma)$ between dual lattices.

- if $F$ on $L$ obtained from $F_i$ using $\circ$, $\vee$, $\wedge$ and fix-point operators, and analogously for $F^A$
- if $\widetilde{\gamma} \circ F_i \circ \widetilde{\alpha} >^A F_i^A$ (which is equivalent to $\gamma \circ \widetilde{F_i} \circ \alpha <^A \widetilde{F_i^A}$ )
- if $(P_1, ...)$ with $P_i \in L$, and $P_i^A = \widetilde{\alpha}(P_i)$

Then $F(P_1, ...) > \widetilde{\gamma}(F_A(P_1^A, ...))$: $init^A <^A F^A(P_1^A, ...)$ is an *under approximation* of $F(P_1, ...)$. If $\widetilde{\gamma}(init^A) < init$

Preservation of verification results from $L^A$ to $L$:

$$init^A <^A F^A(P_1^A, ...) \text{ implies } init < F(P_1, ...).$$

# Property preservation ... continued

Consider $(\widetilde{\alpha}, \widetilde{\gamma})$, the dual of $(\alpha, \gamma)$ between dual lattices.

- if $F$ on $L$ obtained from $F_i$ using $\circ$, $\vee$, $\wedge$ and fix-point operators, and analogously for $F^A$
- if $\widetilde{\gamma} \circ F_i \circ \widetilde{\alpha} >^A F_i^A$ (which is equivalent to $\gamma \circ \widetilde{F_i} \circ \alpha <^A \widetilde{F_i^A}$ )
- if $(P_1, ...)$ with $P_i \in L$, and $P_i^A = \widetilde{\alpha}(P_i)$

Then $F(P_1, ...) > \widetilde{\gamma}(F_A(P_1^A, ...))$: $init^A <^A F^A(P_1^A, ...)$ is an *under approximation* of $F(P_1, ...)$. If $\widetilde{\gamma}(init^A) < init$

Preservation of verification results from $L^A$ to $L$:

$$init^A <^A F^A(P_1^A, ...) \text{ implies } init < F(P_1, ...).$$

# Property preservation ... continued

Consider $(\widetilde{\alpha}, \widetilde{\gamma})$, the dual of $(\alpha, \gamma)$ between dual lattices.

- if $F$ on $L$ obtained from $F_i$ using $\circ$, $\vee$, $\wedge$ and fix-point operators, and analogously for $F^A$
- if $\widetilde{\gamma} \circ F_i \circ \widetilde{\alpha} >^A F_i^A$ (which is equivalent to $\gamma \circ \widetilde{F_i} \circ \alpha <^A \widetilde{F_i^A}$ )
- if $(P_1, ...)$ with $P_i \in L$, and $P_i^A = \widetilde{\alpha}(P_i)$

Then $F(P_1, ...) > \widetilde{\gamma}(F_A(P_1^A, ...))$: $init^A <^A F^A(P_1^A, ...)$ is an *under approximation* of $F(P_1, ...)$. If $\widetilde{\gamma}(init^A) < init$

Preservation of verification results from $L^A$ to $L$:

$$init^A <^A F^A(P_1^A, ...) \text{ implies } init < F(P_1, ...).$$

# Property preservation ... continued

*Strong property preservation*: allows to preserve both satisfaction and non satisfaction: $F^A$ must both over- and under- approximate $F$, in the following sense. Assume:

**(1)** For $(\alpha, \gamma)$ from $L$ to $L^A$ and $(\alpha', \gamma')$ from $L^A$ to $L$, *init*, $P$ are representable (closed) for both connexions.

**(2)** $\gamma \circ F \circ \alpha <^A F^A$ and $\gamma' \circ F^A \circ \alpha' < F$ on representable properties.

Then, we have strong preservation of verification results:

$$F^A(\alpha(init)) < \alpha(P) \text{ implies } F(init) < P$$

and

$$F(init) < P \text{ implies } \gamma'(init) <^A \gamma'(P)$$

A particular case is $(\alpha', \gamma') = (\widetilde{\gamma}, \widetilde{\alpha})$.

Strong property preservation is interesting, but generally hard to achieve ... and composition is more difficult.

# Property preservation ... continued

*Strong property preservation*: allows to preserve both satisfaction and non satisfaction: $F^A$ must both over- and under- approximate $F$, in the following sense. Assume:

**(1)** For $(\alpha, \gamma)$ from $L$ to $L^A$ and $(\alpha', \gamma')$ from $L^A$ to $L$, $init$, $P$ are representable (closed) for both connexions.

**(2)** $\gamma \circ F \circ \alpha <^A F^A$ and $\gamma' \circ F^A \circ \alpha' < F$ on representable properties.

Then, we have strong preservation of verification results:

$$F^A(\alpha(init)) < \alpha(P) \text{ implies } F(init) < P$$
and
$$F(init) < P \text{ implies } \gamma'(init) <^A \gamma'(P)$$

A particular case is $(\alpha', \gamma') = (\widetilde{\gamma}, \widetilde{\alpha})$.

Strong property preservation is interesting, but generally hard to achieve ... and composition is more difficult.

# Property preservation ... continued

*Strong property preservation*: allows to preserve both satisfaction and non satisfaction: $F^A$ must both over- and under- approximate $F$, in the following sense. Assume:

**(1)** For $(\alpha, \gamma)$ from $L$ to $L^A$ and $(\alpha', \gamma')$ from $L^A$ to $L$, *init*, $P$ are representable (closed) for both connexions.

**(2)** $\gamma \circ F \circ \alpha <^A F^A$ and $\gamma' \circ F^A \circ \alpha' < F$ on representable properties.

Then, we have strong preservation of verification results:

$$F^A(\alpha(init)) < \alpha(P) \text{ implies } F(init) < P$$

and

$$F(init) < P \text{ implies } \gamma'(init) <^A \gamma'(P)$$

A particular case is $(\alpha', \gamma') = (\widetilde{\gamma}, \widetilde{\alpha})$.

Strong property preservation is interesting, but generally hard to achieve ... and composition is more difficult.

# Why ist is not sufficient to require equality

Why do we not just require

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

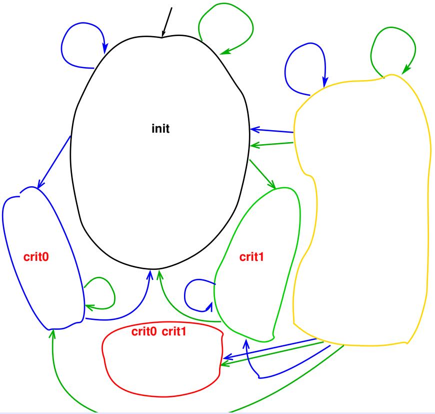
that is, that $F^A$ is exact ?

# Why ist is not sufficient to require equality

Why do we not just require

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

that is, that $F^A$ is exact ?



# Why ist is not sufficient to require equality

Why do we not just require

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

that is, that $F^A$ is exact ?