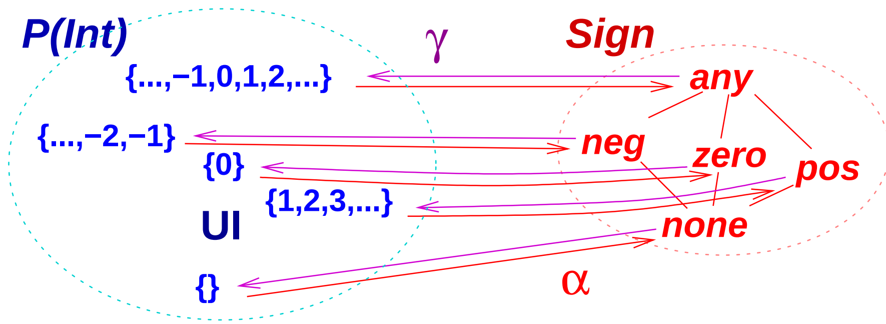
Underapproximating Predicate Transformers

David Schmidt

Kansas State University

www.cis.ksu.edu/~schmidt

Background

Given 

and $\mathrm{succ} : \mathrm{Int} \rightarrow \mathcal{P}(\mathrm{Int})$**,** $\mathrm{succ}(n) = \{n+1\}$**, let's validate** $\mathrm{succ}(0) \subseteq \{1,2,3,\cdots\}$ **within** Sign**:**

1. We approximate succ by $\mathrm{succ}^{\sharp}_{\mathrm{best}} = \alpha \circ \mathrm{succ}^{*} \circ \gamma$, and we approximate 0 by $\alpha\{0\} = \mathit{zero}$.
2. We approximate $\{1,2,3,\cdots\}$ by $\alpha\{1,2,3,\cdots\} = \mathit{pos}$ $(*)$
3. We check that $\mathrm{succ}^{\sharp}_{\mathrm{best}}(\mathit{zero}) \sqsubseteq_{\mathit{Sign}} \mathit{pos}$. (It does.)

$(*)$ Step 2 is sound only if the property, $S \subseteq \mathrm{Int}$, is *exact*: $S = \gamma(\alpha(S))$.

For example, $\alpha\{-2,0\} = \mathit{any}$, but $\gamma(\mathit{any}) \neq \{-2,0\}$. Therefore,

$\mathrm{succ}^{\sharp}_{\mathrm{best}}(\mathit{zero}) \sqsubseteq_{\mathit{Sign}} \mathit{any}$ *does not imply* $\mathrm{succ}(0) \in \{-2,0\}$.

A logic whose assertions are exact

For Galois connection, $(\mathcal{P}(C), \subseteq)\langle\alpha, \gamma\rangle(A, \sqsubseteq)$, define this logic:

$$\phi ::= a \mid \phi_1 \sqcap \phi_2 \text{ , where } a \in A$$

Each ϕ is interpreted as $[\![\phi]\!] = \gamma(\phi)$, so that $a \sqsubseteq \phi$ implies $\gamma(a) \subseteq [\![\phi]\!]$. That is, the sets, $\gamma(\phi)$, are exact.

This makes $f^\sharp_{best} : A \to A$ the strongest postcondition transformer for $f : C \to \mathcal{P}(C)$ in "logic" A:

$$f^*[\![\phi]\!] \subseteq [\![\phi']\!] \text{ iff } f^\sharp_{best}(\phi) \sqsubseteq \phi'$$

That is, $\{\phi\}\, f\, \{f^\sharp_{best}(\phi)\}$ is a sound and complete Hoare-triple for f [Cousot78] .

But such logics are rare

$$\phi ::= \mathrm{neg} \mid \mathrm{zero} \mid \mathrm{pos} \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$$

$$[\![\mathrm{neg}]\!] = \gamma(\mathrm{neg}) \qquad [\![\mathrm{zero}]\!] = \gamma(\mathrm{zero}) \qquad [\![\mathrm{pos}]\!] = \gamma(\mathrm{pos})$$

$$[\![\phi_1 \wedge \phi_2]\!] = [\![\phi_1]\!] \cap [\![\phi_2]\!]$$

$$[\![\phi_1 \vee \phi_2]\!] = [\![\phi_1]\!] \cup [\![\phi_2]\!]$$

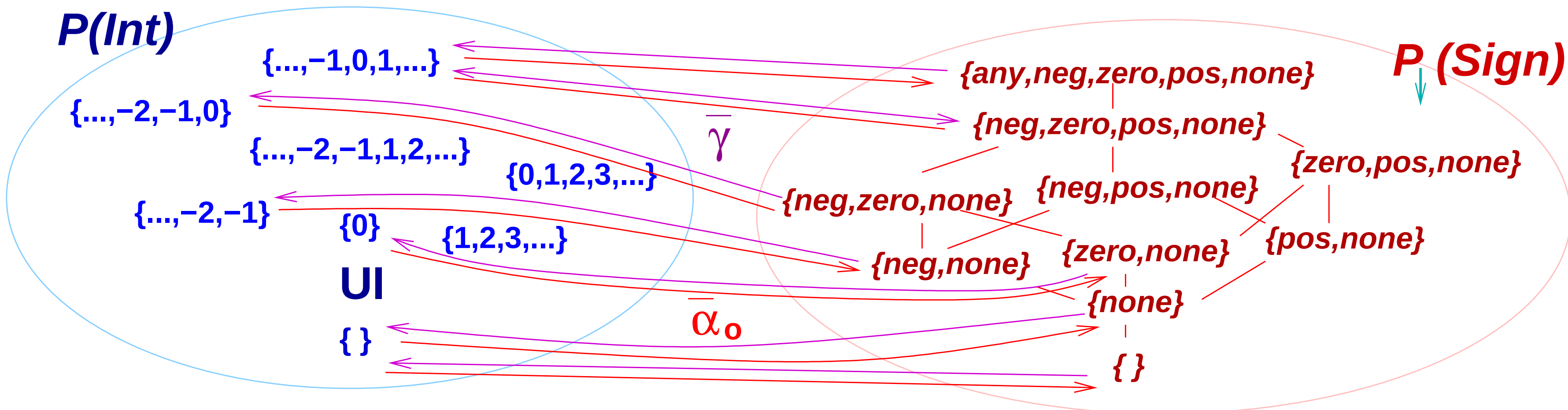
For $(\mathcal{P}(\mathrm{Int}), \subseteq)\langle\alpha, \gamma\rangle(\mathit{Sign}, \sqsubseteq)$, disjunction is not exact, e.g.,

$[\![\mathrm{neg} \vee \mathrm{zero}]\!] = \{\cdots, -2, -1, 0\} \subset \gamma(\alpha\{\cdots, -2, -1, 0\}) = \gamma(\mathrm{any}) = \mathrm{Int}$.

Therefore, we dare not approximate the assertion, $[\![\mathrm{neg} \vee \mathrm{zero}]\!]$, by $\alpha[\![\mathrm{neg} \vee \mathrm{zero}]\!] = \mathrm{any} \in \mathit{Sign}$, because it is an *overapproximation*

Sometimes, we can complete the abstract domain

We construct the *disjunctive completion* [Cousots79,Giacobazzi00] :



$$(\mathcal{P}(\mathrm{int}), \subseteq)\langle\overline{\alpha_o}, \overline{\gamma}\rangle(\mathcal{P}_{\downarrow}(\mathrm{Sign}), \subseteq)$$

$$\overline{\gamma}(T) = \cup_{a \in T}\gamma(a) \qquad \overline{\alpha_o}(S) = \downarrow\{\alpha\{c\} \mid c \in S\}$$

Downclosed sets are needed for monotonicity of key functions on the sets.

We interpret properties, $S \subseteq \mathrm{Int}$, as $\overline{\alpha_o}(S) \in \mathcal{P}_{\downarrow}(A)$ and functions, $f : \mathrm{Int} \to \mathcal{P}(\mathrm{Int})$, as $f^{\sharp}_{best} = (\overline{\alpha_o} \circ f^* \circ \gamma) \in A \to \mathcal{P}_{\downarrow}(A)$.

Now, all assertions are exact: $\phi ::= neg \mid zero \mid pos \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$

E.g., $\overline{\alpha_o}[\![neg \vee zero]\!] = \downarrow\{neg, zero\} = \{neg, zero, none\}$.

Sometimes, the completion is too expensive

For $succ : \mathrm{Int} \rightarrow \mathcal{P}(\mathrm{Int})$, define the precondition assertion $[succ]\phi$ as

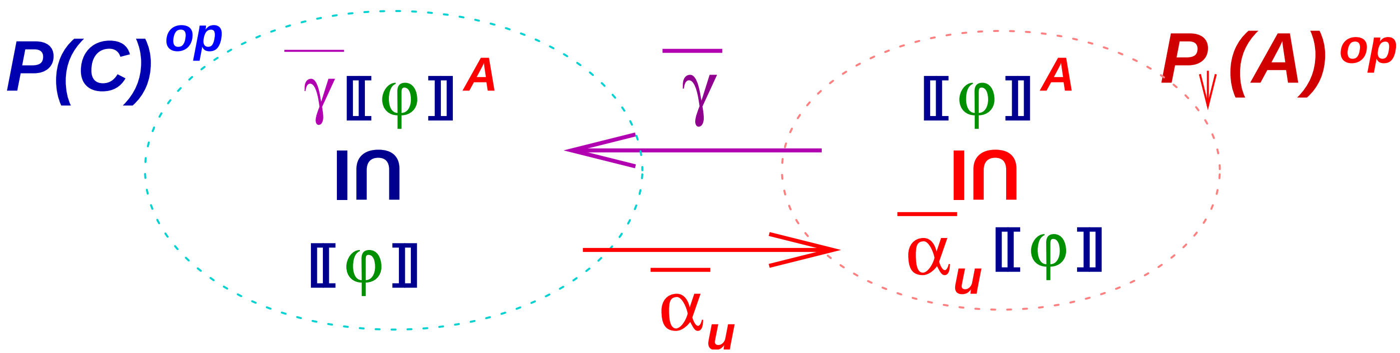
$$[\![[succ]\phi]\!] = \{n \mid succ(n) \subseteq [\![\phi]\!]\}$$

Because $zero \in Sign$, the completion of $Sign$ with respect to $[succ]zero$ *adds each and every negative integer,* $-1, -2, \cdots$ to the abstract domain. (because we must make $[succ]zero$ exact, and then make $[succ][succ]zero$ exact, etc.)

As an alternative, we *underapproximate* nonexact assertions.

How do we underapproximate $[\![\cdot]\!] : \mathcal{L} \to \mathcal{P}(C)$?

Lift the original Galois connection, $\mathcal{P}(C)\langle\alpha,\gamma\rangle A$, to [Cousots00] :



The best abstraction of $[\![\phi]\!]$ is merely

$$[\![\phi]\!]^A = \overline{\alpha_u}[\![\phi]\!],$$

because $[\![\phi]\!] \supseteq \overline{\gamma}(\overline{\alpha_u}[\![\phi]\!])$.

Example: for $[\![\phi_1 \vee \phi_2]\!] = [\![\phi_1]\!] \cup [\![\phi_2]\!]$, we have

$$\begin{aligned}[\![\phi_1 \vee \phi_2]\!]^{Sign} &= \overline{\alpha_u}[\![\phi_1 \vee \phi_2]\!] \\ &= \{a \in Sign \mid \gamma(a) \subseteq [\![\phi_1]\!] \cup [\![\phi_2]\!]\}.\end{aligned}$$

But this is not defined inductively on $[\![\phi]\!]^A$.

Define the abstract logic inductively

For assertion, $\mathrm{op}_g(\phi_i)_{i<k}$, interpreted as

$$[\![\mathrm{op}_g(\phi_i)_{i<k}]\!] = g([\![\phi_i]\!])_{i<k}, \quad \text{where } g : \mathcal{P}(C)^k \to \mathcal{P}(C),$$

interpret it abstractly as

$$[\![\mathrm{op}_g(\phi_i)_{i<k}]\!]^{A}_{ind} = (\overline{\alpha_u} \circ g \circ \overline{\gamma}^k)([\![\phi_i]\!]^{A}_{ind})_{i<k}$$

We have $\overline{\alpha_u}[\![\phi]\!] \supseteq [\![\phi]\!]^{A}_{ind}$, and when ϕ is exact, $\supseteq$ becomes $=$.

Example: $[\![\phi_1 \vee \phi_2]\!] = [\![\phi_1]\!] \cup [\![\phi_2]\!]$ abstracts to

$$[\![\phi_1 \vee \phi_2]\!]^{Sign}_{ind} = (\overline{\alpha_u} \circ \cup \circ \overline{\gamma}^2)([\![\phi_1]\!]^{Sign}_{ind}, [\![\phi_2]\!]^{Sign}_{ind}).$$

Can we eliminate concrete $\cup$ *from* $[\![\phi_1 \vee \phi_2]\!]^{Sign}_{ind}$*?* Try this:

$$[\![\phi_1 \vee \phi_2]\!]^{Sign} = [\![\phi_1]\!]^{Sign} \cup_{\mathcal{P}_\downarrow(Sign)} [\![\phi_2]\!]^{Sign}.$$

But $\cup_{\mathcal{P}_\downarrow(Sign)} \neq (\overline{\alpha_u} \circ \cup \circ \overline{\gamma}^2)$ — we lose precision:

$any \in [\![neg \vee zero \vee pos]\!]^{Sign}_{ind}$, yet $any \notin [\![neg]\!]^{Sign} \cup [\![zero]\!]^{Sign} \cup [\![pos]\!]^{Sign}$

A more difficult example — *preconditions*: for $f : C \to \mathcal{P}(C)$,

$$[\![[f]\phi]\!] = \widetilde{pre}_f [\![\phi]\!],$$

$$\text{where } \widetilde{pre}_f(S) = \{c \mid f(c) \subseteq S\},$$

we have

$$\begin{aligned} [\![[f]\phi]\!]^A_{ind} &= (\overline{\alpha_u} \circ \widetilde{pre}_f \circ \overline{\gamma}) [\![\phi]\!]^A_{ind} \\ &= \{a \mid f^*[\gamma(a)] \subseteq \overline{\gamma} [\![\phi]\!]^A_{ind}\}. \end{aligned}$$

Is this finitely computable? Can it be expressed compositionally as

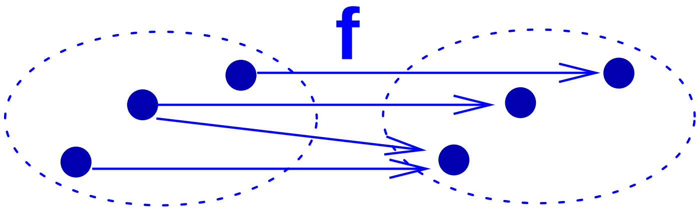
$$[\![[f]\phi]\!]^A = \widetilde{pre}_{f^\sharp} [\![\phi]\!]^A$$

for some $f^\sharp : A \to \mathcal{P}(A)$? Do we lose precision?

This is the topic of the paper in the SAS'06 proceedings.

Defining sound underapproximations of predicate transformers used in dynamic and temporal logic

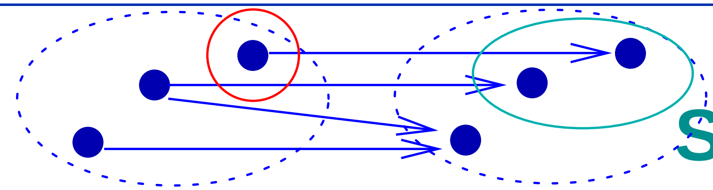
For nondeterministic state-transition function, $f : C \rightarrow \mathcal{P}(C)$,



, and property $S \subseteq C$, we have

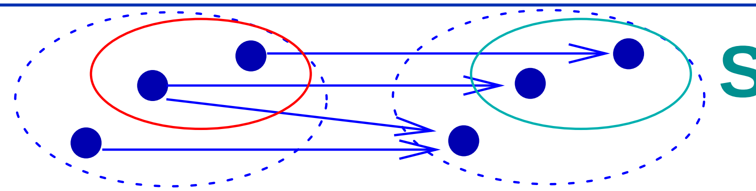
$\widetilde{\mathrm{pre}}_f(S) = \{c \mid f(c) \subseteq S\}$

"forall precondition": transit only into S



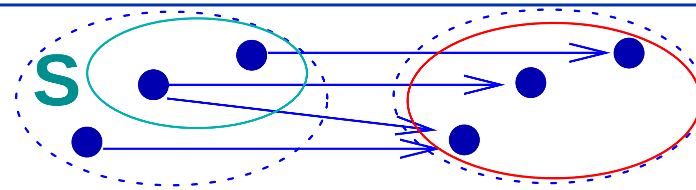
$\mathrm{pre}_f(S) = \{c \mid f(c) \cap S \neq \emptyset\}$

"exists precondition": transit to S



$\mathrm{post}_f(S) = f^*(S)$

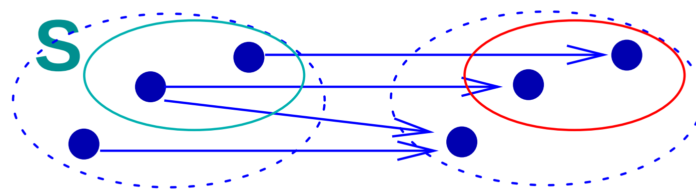
"exists postcondition": are reached by S



$\widetilde{\mathrm{post}}_f(S)$

$= \{d \mid \forall c \in C, d \in f(c) \Rightarrow c \in S\}$

"forall postcondition": are reached only by S



$\widetilde{\mathrm{pre}}, \mathrm{post}$ are used for validation; $\mathrm{pre}, \widetilde{\mathrm{post}}$ are used for code improvement

The transformers interpret this logic

$$\phi ::= a \mid \cdots \mid [f]\phi \mid \langle f\rangle\phi \mid \phi\overline{[f]} \mid \phi\overline{\langle f\rangle}$$

as follows:

$$[\![[f]\phi]\!] = \widetilde{pre}_f[\![\phi]\!] \qquad [\![\phi\overline{[f]}]\!] = \widetilde{post}_f[\![\phi]\!]$$

$$[\![\langle f\rangle\phi]\!] = pre_f[\![\phi]\!] \qquad [\![\phi\overline{\langle f\rangle}]\!] = post_f[\![\phi]\!]$$

Although these are "single-step" assertions, we use recursion to define interesting properties, like those in *CTL*:

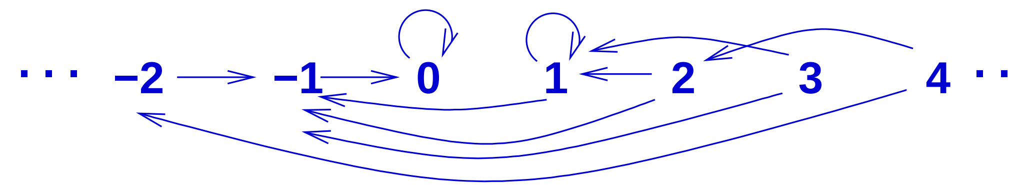
$AG_f\phi \equiv \nu Z.\phi \wedge [f]Z$ for all f-transition sequences, ϕ holds

$EF_f\phi \equiv \mu Z.\phi \vee \langle f\rangle Z$ there exists an f-transition sequence leading to ϕ

$\phi\overline{EF}_f \equiv \mu Z.\phi \vee Z\overline{\langle f\rangle}$ there exists an f-transition sequence from ϕ to here

Example: ***Transition function*** $\mathrm{h} : \mathrm{Int} \to \mathcal{P}(\mathrm{int})$

```
let h(n) = if neg(n) :
               n:= n+1
           else truncate(sqrt(n))
in loopforever h
```



Some properties of h:

$[\![[\mathrm{h}]\mathrm{neg}]\!] = \widetilde{\mathrm{pre}}_{\mathrm{h}}\{\cdots, -2, -1\} = \{\cdots, -3, -2\}$ transit only into negatives

$[\![\langle \mathrm{h} \rangle \mathrm{neg}]\!] = \mathrm{pre}_{\mathrm{h}}\{\cdots, -2, -1\} = \{\cdots, -3, -2, 1, 2, 3, \cdots\}$ transit to a negative

$[\![\mathrm{neg}\overline{\langle \mathrm{h} \rangle}]\!] = \mathrm{post}_{\mathrm{h}}\{\cdots, -2, -1\} = \{\cdots, -2, -1, 0\}$ are reached by negatives

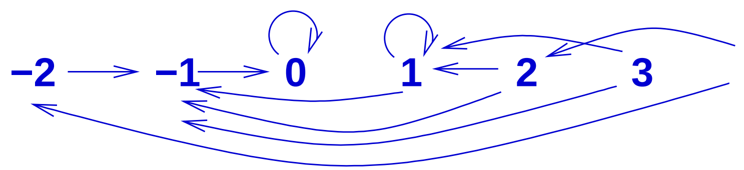
$[\![\mathrm{neg}\overline{[\mathrm{h}]}]\!] = \widetilde{\mathrm{post}}_{\mathrm{h}}\{\cdots, -2, -1\} = \{\}$ are reached only by negatives

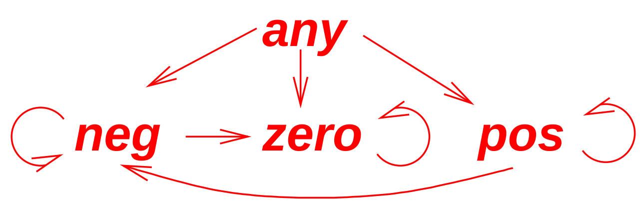
Underapproximating $\widetilde{\mathsf{pre}}_f(S) = \{c \mid f(c) \subseteq S\}$

Theorem: $(\overline{\alpha_u} \circ \widetilde{\mathsf{pre}}_f \circ \overline{\gamma}) = \widetilde{\mathsf{pre}}_{f^\sharp_{best}}$, where $f^\sharp_{best} = \overline{\alpha_o} \circ f^* \circ \gamma$.

Intuition: $f^\sharp$'s preimage overapproxes f's, and $[\![\phi]\!]^A$ underapproxes $[\![\phi]\!]$.

$$[\![[f]\phi]\!]^A_{ind} = (\overline{\alpha_u} \circ \widetilde{\mathsf{pre}}_f \circ \overline{\gamma})[\![\phi]\!]^A_{ind} = \widetilde{\mathsf{pre}}_{f^\sharp_{best}}[\![\phi]\!]^A_{ind}$$

Example: $h = \cdots$  $\cdots$

$h^\sharp_{best} =$ 

What must transit to zero ? $[\![[h]zero]\!] = \{-1, 0\}$

The approximation is $[\![[h]zero]\!]^{Sign}_{ind} = \downarrow\{zero\}$

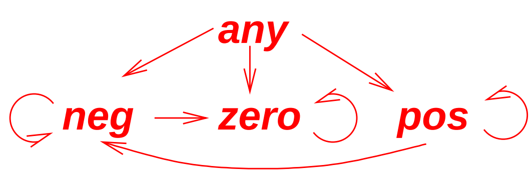
The abstraction of $\widetilde{\mathsf{pre}}_h$ is the best we can do, but it loses precision.

Underapproximating $\mathrm{pre}_f(S) = \{c \mid f(c) \cap S \neq \emptyset\}$

$$[\![\langle f\rangle\phi]\!]^{A}_{ind} = (\overline{\alpha_u} \circ \mathrm{pre}_f \circ \overline{\gamma})[\![\phi]\!]^{A}_{ind}$$

But, for $f^\sharp : A \to \mathcal{P}_\downarrow(A)$, $\mathrm{pre}_{f^\sharp}$ can be *unsound* ! Intuition: $h^\sharp$ overestimates h's preimage, so there can be “false transitions.”

Example: $[\![\langle h\rangle neg]\!] = \mathrm{pre}_h[\![neg]\!] = \{\cdots, -3, -2, 1, 2, 3\}$ transit to negatives.

But $h^\sharp_{best} =$ 

, and

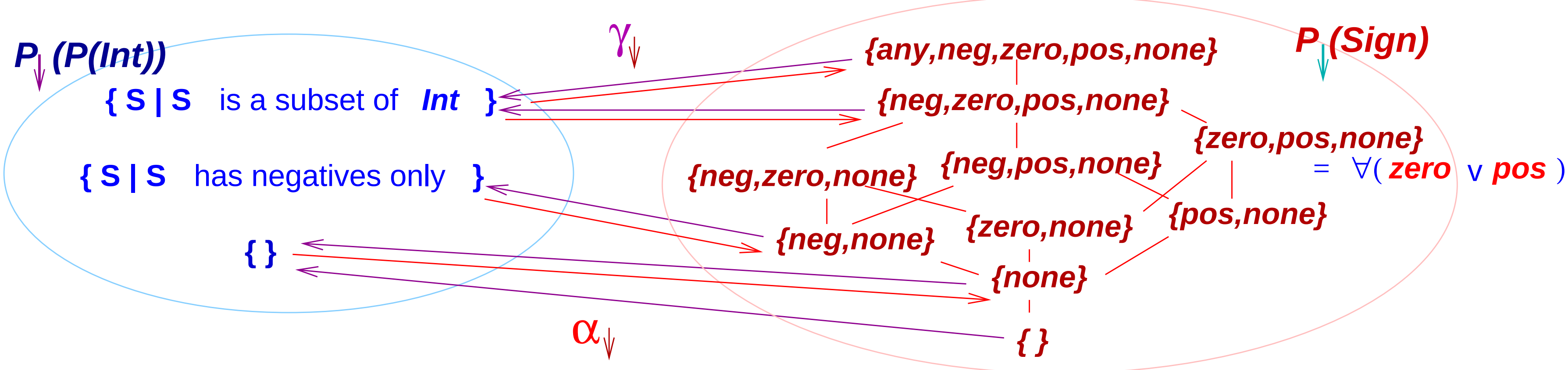
$\mathrm{pre}_{h^\sharp_{best}}[\![neg]\!] = \{neg, pos, any\}$ and $\overline{\gamma}\{neg, pos, any\} = \mathrm{Int}$!

Computational approximation with downclosed sets is incorrect *for* pre*:*

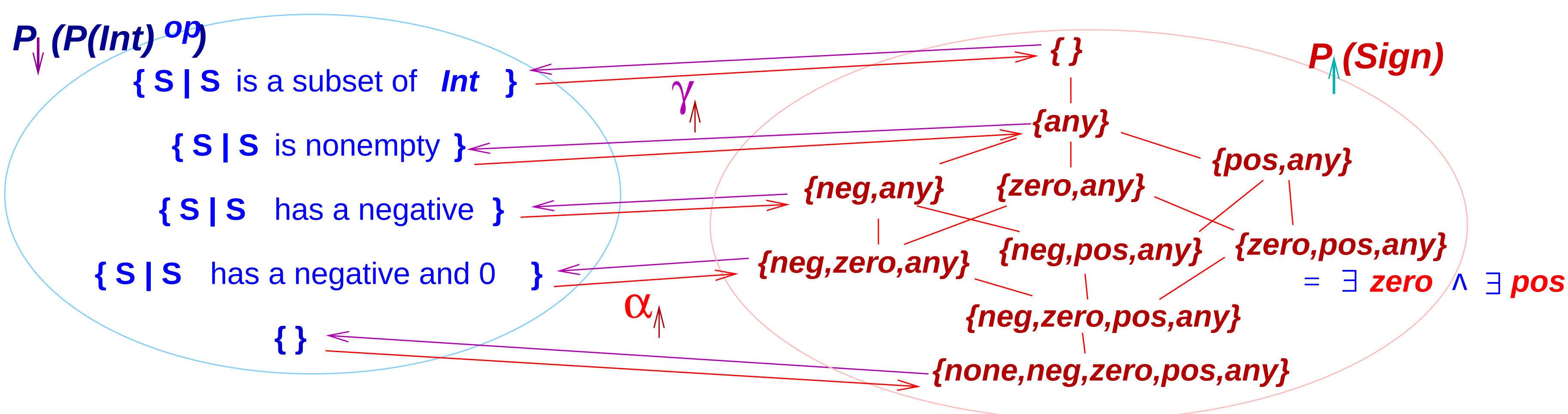
Theorem: For every $f^\sharp : A \to \mathcal{P}_\downarrow(A)$ and $T \in \mathcal{P}_\downarrow(A)$, $\mathrm{pre}_{f^\sharp}(T) \in \mathcal{P}_\uparrow(A)$!

Under*approximate* $f : C \to \mathcal{P}(C)$ ***by*** $f^{\flat} : A \to \mathcal{P}_{\uparrow}(A)$

Down-closed-set interpretation: $\downarrow\{zero, pos\}$ asserts $\forall\{zero, pos\} \equiv \forall(zero \vee pos)$ — all outputs are zero or positive :



Up-closed-set interpretation: $\uparrow\{zero, pos\}$ asserts $\exists\{zero, pos\}$ $\equiv \exists zero \wedge \exists pos$ — there exist 0 and a positive in the output:



Underapproximating $\mathrm{pre}_f(S) = \{c \mid f(c) \cap S \neq \emptyset\}$

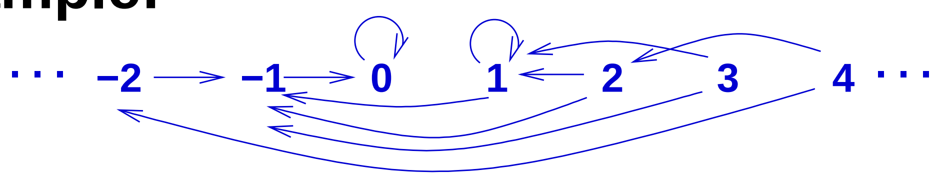
Use $\mathcal{P}_{\uparrow}(A)$ to define $f^{\flat}_{\mathrm{best}} : A \to \mathcal{P}_{\uparrow}(A)$ as

$$\begin{aligned} f^{\flat}_{\mathrm{best}}(a) &= (\alpha_{\uparrow} \circ (\{\!|\cdot|\!\} \circ f^{*}) \circ \gamma)(a) \\ &= \{a' \mid \forall c \in \gamma(a), f(c) \cap \gamma(a') \neq \emptyset\} \end{aligned}$$

and define $[\![\langle f \rangle \phi]\!]^{A} = \mathrm{pre}_{f^{\flat}_{\mathrm{best}}} [\![\phi]\!]^{A}$

Proposition: *(soundness)* $\mathrm{pre}_{f^{\flat}_{\mathrm{best}}}(T) \subseteq (\overline{\alpha_u} \circ \mathrm{pre}_f \circ \overline{\gamma})(T)$.

Example:

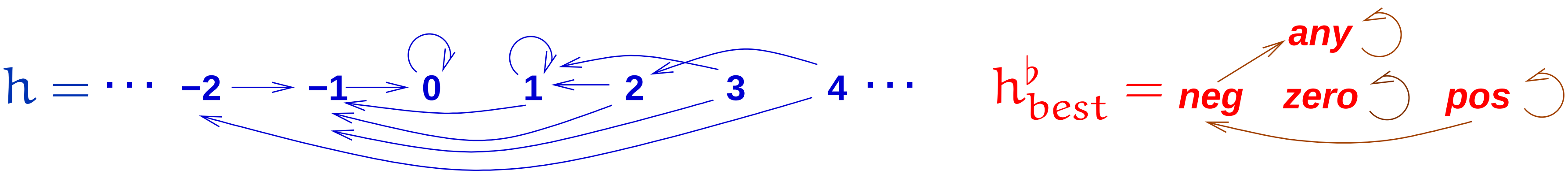
$h =$ 

$h^{\flat}_{\mathrm{best}} =$ 

We have $[\![\langle h \rangle(\mathit{neg} \vee \mathit{zero} \vee \mathit{pos})]\!] = \mathrm{pre}_h(\mathrm{Int}) = \mathrm{Int}$ and

$[\![\langle h \rangle(\mathit{neg} \vee \mathit{zero} \vee \mathit{pos})]\!]^{A} = \mathrm{pre}_{h^{\flat}_{\mathrm{best}}} \downarrow\{\mathit{neg}, \mathit{zero}, \mathit{pos}\} = \downarrow\{\mathit{zero}, \mathit{pos}\}$.

Improving precision with **focus**



For $\mathrm{pre}_h[\![\mathrm{neg} \vee zero \vee \mathrm{pos}]\!] = \mathrm{Int}$,

we lose precision: $\mathrm{pre}_{f^\flat_{best}}[\![\mathrm{neg} \vee zero \vee \mathrm{pos}]\!]^A = \downarrow\{zero, \mathrm{pos}\}$.

But $(\overline{\alpha_u} \circ \mathrm{pre}_f \circ \overline{\gamma})[\![\mathrm{neg} \vee zero \vee \mathrm{pos}]\!]^A_{ind} = \downarrow \mathrm{any} = Sign$!

Many analysis tools (e.g., TVLA [SagivRepsWilhelm02]) use a cases analysis, called focus*, to recover lost precision:*

$f^\flat_{best}(\mathrm{neg}) = \{\mathrm{any}\}$

$f^\flat_{best}(\mathrm{any}) = \{\mathrm{any}\}$

But any decomposes to the cases, neg, zero, pos. For each case, p, $p \in [\![\mathrm{neg} \vee zero \vee \mathrm{pos}]\!]^A$.

Theorem: When $\gamma : A \rightarrow \mathcal{P}(A)$ preserves joins, then $pre^{focus}_{f^\flat_{best}} = (\overline{\alpha_u} \circ \mathrm{pre}_f \circ \overline{\gamma})$.

Underapproximating post and $\widetilde{\text{post}}$

$$\text{post}_f(S) = f^*(S)$$
$$\widetilde{\text{post}}_f(S) = \{d \mid \forall c \in C, d \in f(c) \Rightarrow c \in S\}$$

Proposition: Let $f : D \rightarrow \mathcal{P}_\delta(D)$, where $\delta \in \{\downarrow, \uparrow\}$. Let $\tilde{\downarrow} = \uparrow$ and $\tilde{\uparrow} = \downarrow$. Then, for all $S \in \mathcal{P}(D)$,

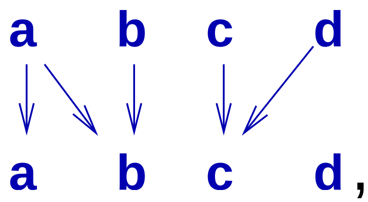
- $\widetilde{\text{pre}}_f(S) \in \mathcal{P}_\delta(D)$
- $\text{post}_f(S) \in \mathcal{P}_\delta(D)$
- $\text{pre}_f(S) \in \mathcal{P}_{\tilde{\delta}}(D)$
- $\widetilde{\text{post}}_f(S) \in \mathcal{P}_{\tilde{\delta}}(D)$.

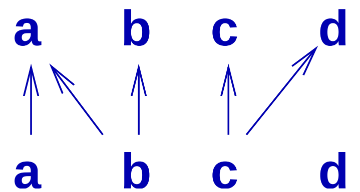
So, $\text{post}_{f^\flat} : A \rightarrow \mathcal{P}_\uparrow(A)$ *and* $\widetilde{\text{post}}_{f^\sharp} : A \rightarrow \mathcal{P}_\uparrow(A)$ *are* unsound.

Even worse, *there is no nontrivial overapproximating* $f^\sharp : A \rightarrow \mathcal{P}_\uparrow(A)$ to use with $\widetilde{\text{post}}$ because, for all $f^\sharp(a) \neq \emptyset$, upclosure implies that $\top_A \in f^\sharp(a)$, implying that $\overline{\gamma}(f^\sharp(a)) = C$. A similar problem arises for a nontrivial underapproximating $f^\flat : A \rightarrow \mathcal{P}_\downarrow(A)$.

What can we do ?

Solution: ***Invert*** $f : C \to \mathcal{P}(C)$ ***to*** $f^{-1} : C \to \mathcal{P}(C)$

If $f : C \to \mathcal{P}(C)$ is 

then $f^{-1} : C \to \mathcal{P}(C)$ is 

That is, $f^{-1}(c) = \{d \mid c \in f(d)\}$.

Proposition: [Loiseaux95] : $(f^{-1})^{-1} = f$, $\quad \mathrm{post}_f = \mathrm{pre}_{f^{-1}}$, and $\widetilde{\mathrm{post}}_f = \widetilde{\mathrm{pre}}_{f^{-1}}$.

Proposition: For $f : A \to \mathcal{P}_\delta(A)$, $\delta \in \{\downarrow, \uparrow\}$, $f^{-1} : A \to \mathcal{P}_{\tilde{\delta}}(A)$ is well defined and monotonic.

Underapproximating post_f *and* $\widetilde{\mathrm{post}}_f$

$$[\![\phi\overline{\langle f\rangle}]\!] \;=\; \mathrm{post}_f[\![\phi]\!] \;=\; \mathrm{pre}_{f^{-1}}[\![\phi]\!],$$

where $f : C \to \mathcal{P}(C)$

The inductively defined underapproximation is

$$[\![\phi\overline{\langle f\rangle}]\!]^A_{ind} = (\overline{\alpha_u} \circ \mathrm{pre}_{f^{-1}} \circ \overline{\gamma})[\![\phi]\!]^A.$$

This is soundly underapproximated by

$$[\![\phi\overline{\langle f\rangle}]\!]^A = \mathrm{pre}_{(f^{-1})^\flat_{best}}[\![\phi]\!]^A,$$

where $(f^{-1})^\flat_{best} : A \to \mathcal{P}_\uparrow(A)$

is $(f^{-1})^\flat_{best} = \overline{\alpha_\uparrow} \circ (\{\!|\cdot|\!\} \circ f^{-1})^* \circ \gamma.$

The same development applied to $\widetilde{\mathrm{post}}_f$ yields

$$[\![\phi\overline{[f]}]\!] = \widetilde{\mathrm{post}}_f[\![\phi]\!] = \widetilde{\mathrm{pre}}_{f^{-1}}[\![\phi]\!].$$

The most precise underapproximation is

$$[\![\phi\overline{\langle f\rangle}]\!]^{A}_{ind} = (\overline{\alpha_u} \circ \widetilde{\mathrm{pre}}_{f^{-1}} \circ \overline{\gamma})[\![\phi]\!]^{A}_{ind} = \widetilde{\mathrm{pre}}_{(f^{-1})^{\sharp}_{best}}[\![\phi]\!]^{A}_{ind},$$

where $(f^{-1})^{\sharp}_{best} : A \to \mathcal{P}_{\downarrow}(A)$

is $(f^{-1})^{\sharp}_{best} = \overline{\alpha_o} \circ (f^{-1})^{*} \circ \gamma.$

Computing abstract postconditions as preconditions of inverted state-transition relations is implemented in Steffen's fixpoint analysis machine [Steffen95] .

Summary

- We reviewed how to use *exact assertions* with an overapproximating Galois connection and how to apply *domain completions* to make assertions exact.
- When it is impractical to make assertions exact, we employed the *underapproximation Galois connection* on assertion sets.
- We proved that the forall-precondition transformer, $\widetilde{\mathrm{pre}}_f$, is best underapproximated by $\widetilde{\mathrm{pre}}_{f^\sharp_{best}}$.
- We used a *powerdomain of up-closed sets* to define $f^\flat_{best}$ and underapproximated pre_f by $\mathrm{pre}_{f^\flat_{best}}$.
- We formalized a *focussed* version of $\mathrm{pre}_{f^\flat_{best}}$ and proved it is the best approximation of pre_f when γ preserves joins.
- We inverted f to f^{-1} and applied the above machinery to underapproximate post_f and $\widetilde{\mathrm{post}}_f$.

References **This talk:** `www.cis.ksu.edu/~schmidt/papers`

1. R. Cleaveland, P. Iyer, and D. Yankelevich. Optimality in abstractions of model checking. SAS'95.

2. P. Cousot. PhD thesis, Genoble, 1978.

3. P. Cousot and R.Cousot. Systematic design of program analysis frameworks. POPL'79.

4. P. Cousot and R.Cousot. Temporal abstract interpretation. POPL'00.

5. D. Dams, et al. Abstract interpretation of reactive systems. *ACM TOPLAS* 19(1997).

6. R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM* 47(2000).

7. C. Loiseaux, et al. Property preserving abstractions for the verification of concurrent systems. *Formal Methods in System Design* 6(1995).

8. D.A. Schmidt, A calculus of logical relations for over- and underapproximating static analyses. SAS'04 and *Science of Comp. Prog.*, in press.

9. B. Steffen, et al. The fixpoint analysis machine. CONCUR'95.