2. Abstract Interpretation

Goal: Compute an inductive invariant.

Problem: Reach(p) and BWReach(Bad) may not be computable.
Even if they are, it will take too long to work explicitly with single configurations.

Approach:
- Represent predicates in some symbolic domain, change the semantics of commands: They directly act on the symbolic representation.
- Essentially this amounts to defining a new semantics — we interpret the program in an abstract semantics.

Example:

$$
c = \quad x = 10;
$$

$$
c_\ell = \left[\begin{array}{l} \text{while } x > 0 \text{ do} \\ \quad \left.\begin{array}{l} x--; \\ x--; \end{array}\right] = c_i \\ \text{od} \end{array}\right.
$$

$$
c_a = [\text{assert } x \text{ even};
$$

Concrete:

$$
\begin{array}{c}
\downarrow \\
(c, x = 0) \; \dots \; (c, x = 100) \dots \\
\downarrow \\
(c_\ell; c_a, x = 10) \\
\downarrow \\
(c_i; c_\ell; c_a, x = 10) \\
\downarrow \\
(x--; c_\ell; c_a, x = 9) \\
\downarrow \\
(c_\ell; c_a, x = 8 \\
\downarrow \\
\vdots
\end{array}
$$

Abstract:

$$
\begin{array}{ll}
(c, x \text{ evenodd}) & \\
\downarrow & \\
(c_\ell; c_a, x \text{ even}) & \searrow \\
\downarrow & (c_a, x \text{ even}) \\
(c_i; c_\ell; c_a, x \text{ even}) & \downarrow \\
\downarrow & (\text{skip}, x \text{ even}) \\
(x--; c_\ell; c_a, x \text{ odd}) &
\end{array}
$$

- Abstract interpretation guarantees <u>soundness</u>.
- The theory behind this are Galois connections.

<u>Definition</u>:

- A <u>Galois</u> <u>connection</u> between lattices $(C, \subseteq)$ and $(A, \sqsubseteq)$ is a pair of monotonic functions $C \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} A$, α called the <u>abstraction</u> function and γ the <u>concretization</u>, so that

$$(G1) \qquad c \subseteq \gamma(\alpha(c)) \qquad \forall c \in C.$$

$$(G2) \qquad \alpha(\gamma(a)) \sqsubseteq a \qquad \forall a \in A.$$

- A function $f^\#: A \to A$ is a <u>sound approximation</u> of $f: C \to C$, if

$$\alpha \circ f \circ \gamma \sqsubseteq f^\#$$

- It is the <u>best approximation</u> of f, if

$$\alpha \circ f \circ \gamma = f^\#$$

- It is an <u>exact approximation</u> of f, if

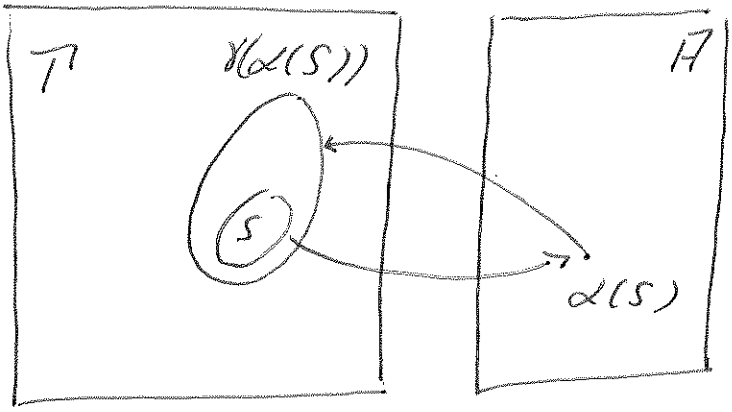
$$\alpha \circ f = f^\# \circ \alpha.$$

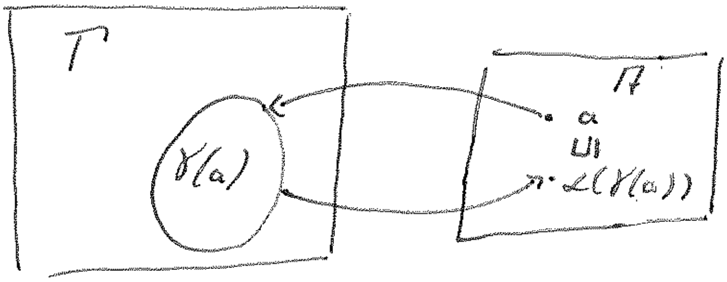
Often called sound/best/exact abstract transformer

<u>Illustration</u>:

In our setting, $(C, \subseteq)$ will be $(\mathbb{P}(T), \subseteq)$ or $(\mathbb{P}(\Sigma), \subseteq)$.

Then

(G1) 

(G2) 

Sound approximation:

$$\begin{tikzcd} c \arrow[r, "f"] & c' \arrow[d, "\alpha"] \\ & a'' \\ a \arrow[uu, "\gamma"] \arrow[r, "f^\#"] & a' \end{tikzcd} \qquad a'' \sqsubseteq a'$$

<u>Lemma (Equivalent formulation of Galois connections)</u>:

$C \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} A$ is a Galois connection iff

$[\forall c \in C.\ \forall a \in A.\ \alpha(c) \sqsubseteq a$ iff $c \subseteq \gamma(a)]$.

<u>Proof</u>:

"⇒" Consider $c \in C$, $a \in A$.

Let $\alpha(c) \sqsubseteq a$. (Monotonicity of γ).

Then $c \overset{(G1)}{\subseteq} \gamma(\alpha(c)) \subseteq \gamma(a)$.

The other implication is similar.

"⇐" We show (G1):

We have $\alpha(c) \sqsubseteq \alpha(c)$.

Hence, $c \subseteq \gamma(\alpha(c))$.

The proof for (G2) is similar.

For monotonicity, let $c_1 \subseteq c_2$.

Then $c_1 \subseteq c_2 \subseteq \gamma(\alpha(c_2))$. Hence, $\alpha(c_1) \sqsubseteq \alpha(c_2)$.

For γ: similar.

□

There are several important results about Galois connections.

Theorem (Properties of Galois connections):

Let $C \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} A$ be a Galois connection.

1.) The concretization is uniquely determined by the abstraction as

$$\gamma(a) := \bigsqcup \{c \in C \mid \alpha(c) \sqsubseteq a\}, \quad \text{f.a. } a \in A.$$

2.) The abstraction is uniquely determined by the concretization as

$$\alpha(c) := \sqcap \{a \in A \mid c \sqsubseteq \gamma(a)\}.$$

3.) α is completely additive in Rat

$$\alpha(\bigsqcup C') = \underbrace{\bigsqcup \alpha(C')}_{= \{\alpha(c) \mid c \in C'\}}, \quad \text{f.a. } C' \subseteq C$$

4.) γ is completely multiplicative,

$$\gamma(\sqcap A') = \sqcap \gamma(A'), \quad \text{f.a. } A' \subseteq A.$$

Proof:

1.) „$\sqsupseteq$" If $\alpha(c) \sqsubseteq a$, then $c \sqsubseteq \gamma(a)$ by the equivalent formulation.
Hence, $\gamma(a)$ is an upper bound for all c in $\{c \in C \mid \alpha(c) \sqsubseteq a\}$.
Then the least upper bound is smaller.

„$\sqsubseteq$" $\alpha(\gamma(a)) \sqsubseteq a$ by (G2),
$\gamma(a)$ is in the set $\{c \in C \mid \alpha(c) \sqsubseteq a\}$.

 2.) Similar.

3.) „$\subseteq$" To prove $\alpha(\bigcup C') \sqsubseteq \bigsqcup \alpha(C')$,

we show

$$\bigcup C' \subseteq \gamma(\bigsqcup \alpha(C'))$$

Then the equivalent formulation gives the result.

Let $c \in C'$.

Then $\alpha(c) \sqsubseteq \bigsqcup \alpha(C')$.

By monotonicity of γ:

$$\gamma(\alpha(c)) \subseteq \gamma(\bigsqcup \alpha(C')).$$

Since $c \subseteq \gamma(\alpha(c))$ by (61),

$\gamma(\bigsqcup \alpha(C'))$ is an upper bound f.a. $c \in C'$.

„$\supseteq$" Let $c \in C'$.

Then $\alpha(c) \sqsubseteq \alpha(\bigcup C')$.

Hence, $\alpha(\bigcup C')$ is an upper bound

for $\alpha(C') = \{\alpha(c) \mid c \in C'\}$

So it is larger than the least upper bound.

$\square$

4.) Similar.

Our goal is to approximate

$Reach(p) = Init \rightarrow^*$

This is the least fixed point of the function

$$pt : \mathbb{P}(T) \rightarrow \mathbb{P}(T)$$
$$pt(S) := Init \cup S \cup S\rightarrow.$$

We give a general result
on how to approximate fixed points.

<u>Theorem (Fixed-Point Transfer):</u>

Let $(C, \subseteq) \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} (A, \sqsubseteq)$ be a Galois connection.

Let $f^\#$ be a sound approximation of f,

both monotonic.

Then
$$lfp.\, f \subseteq \gamma(lfp.\, f^\#)$$

If $f^\#$ is an exact approximation of f,

even
$$\alpha(lfp.\, f) = lfp.\, f^\# \text{ holds}$$

For the proof, we use

<u>Theorem (Knaster-Tarski):</u>

Let $(C, \subseteq)$ be a complete lattice

and $f: C \to C$ monotonic.

Then
$$lfp.\, f = \bigcap \underbrace{\underset{\{c \in C \mid f(c) \subseteq c\}.}{\underset{\shortparallel}{Prefix(f)}}}_{\text{meet over all prefix points.}}$$

<u>Proof (of the fixed-point transfer result):</u>

- We show that every prefix point of $f^\#$
also yields a prefix point of f (via γ).

Then we are done:

$$\mathrm{lfp}.f^\# \in \mathrm{Prefix}(f^\#)$$

and so

$$\gamma(\mathrm{lfp}.f^\#) \in \mathrm{Prefix}(f)$$

and so

$$\mathrm{lfp}.f = \sqcap \mathrm{Prefix}(f) \subseteq \gamma(\mathrm{lfp}.f^\#).$$

<u>Note</u>: In our setting, this translates into saying that $\gamma(\mathrm{lfp}.f^\#)$ is an inductive invariant.

Let $a \in \mathrm{Prefix}(f^\#)$, meaning

$$f^\#(a) \sqsubseteq a.$$

We have

$$f(\gamma(a))$$

$$\{G1\} \subseteq \gamma(\underline{\alpha}(f(\underline{\gamma}(a))))$$

$$\{f^\#\text{ sound}\} \subseteq \gamma(f^\#(a))$$

$$\{\gamma\text{ monotonic}\} \subseteq \gamma(a).$$

- Assume $f^\#$ is exact. We already have $\mathrm{lfp}.f \subseteq \gamma(\mathrm{lfp}.f^\#)$. Hence, by the equivalent formulation of Galois connections, we have $\alpha(\mathrm{lfp}.f) \sqsubseteq \mathrm{lfp}.f^\#$.

For $\mathrm{lfp}.f^\# \sqsubseteq \alpha(\mathrm{lfp}.f)$

it suffices to note that $\alpha(\mathrm{lfp}.f)$

is a fixed point of $f^\#$:

$$f^\#(\alpha(\mathrm{lfp}.f))$$

$$\{\text{exact}\} = \alpha(f(\mathrm{lfp}.f))$$

$$\{\mathrm{lfp}.f\} = \alpha(\mathrm{lfp}.f).$$

$\square$

<u>Constructing A and $\to^\#$:</u>

We start from an abstraction of the states and add the control flow.

Let

$$(\mathcal{P}(\Sigma), \subseteq) \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} (A\Sigma, \leq)$$

be a Galois connection.

An <u>abstract configuration</u> is a pair

$$(c, as) \in W(COM) \times A\Sigma =: \Gamma^\#.$$

Let $[\![com]\!]^\#$ be a sound approximation of $[\![com]\!]$, f.a. $com \in COM$.

We define the transition relation

$$\to^\# \subseteq \Gamma^\# \times \Gamma^\#$$

by

$$(COM^\#) \quad \frac{}{(com, as) \to^\# (skip, [\![com]\!]^\# as)}.$$

The remaining rules are as before.

There are alternatives of how to define the abstract predicates (A, E):

$$A := \mathbb{P}(T^{\#}) \qquad // \text{ more precise}$$

$$A := W(COM) \to AE \qquad // \text{ more effizient.}$$

In the former case,

$$\{(c, as_1)\} \sqcup \{(c, as_2)\} = \{(c, as_1), (c, as_2)\}.$$

In the latter case,

$$\{(c, as_1)\} \sqcup \{(c, as_2)\} = \{(c, as_1 \vee as_2)\}.$$

The lifting of $\to^{\#}$ to abstract predicates will reflect this choice.

<u>Lemma:</u>

$\to^{\#}$ is a sound approximation of $\to$, for both choices.