Invariant Generation

CS156: Calculus of Computation

Zohar Manna Aaron R. Bradley

Outline

⇒ 0. Static Analysis

1. Interval Analysis
2. Karr's Analysis

Transition System

$$T: \ \langle V, L, \ell_0, \theta, \mathcal{T} \rangle$$

- V: variables, with domain $\mathsf{domain}(V)$
- L: locations
- ℓ_0: initial location
- θ: initial condition — assertion $\theta(V)$
- $\mathcal{T}$: transitions

$$\langle \ell, m, \rho \rangle \in \mathcal{T}$$

- ℓ: pre-location
- m: post-location
- ρ: transition relation — assertion $\rho(V, V')$

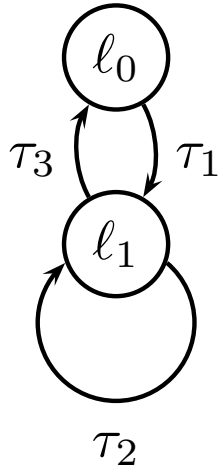
Example: Transition System

$$
\begin{array}{l}
\texttt{@}\ i = 0; \\
\texttt{while}\ (\ldots)\ \{ \\
\quad i := i + 1; \\
\}
\end{array}
$$

$$T_1 : \langle \underbrace{\{i : \mathbb{R}\}}_{V}, \underbrace{\{\ell_0\}}_{L}, \ell_0, \underbrace{i = 0}_{\theta}, \underbrace{\{\langle \ell_0, \ell_0, i' = i + 1 \rangle\}}_{\mathcal{T}} \rangle$$

Example: Transition System

$$
\begin{array}{l}
\texttt{@}\ n \geq 0; \\
\texttt{for}(i := 0;\ i < n;\ i := i + 1)\ \ \{ \\
\quad \texttt{for}(j := i - 1;\ j \geq 0;\ j := j - 1)\ \ \{ \\
\qquad \ldots \\
\quad \} \\
\}
\end{array}
$$



$$T_2 : \langle \underbrace{\{i, j, n : \mathbb{R}\}}_{V},\ \underbrace{\{\ell_0, \ell_1\}}_{L},\ \ell_0,\ \underbrace{i = 0\ \wedge\ n \geq 0}_{\theta},\ \underbrace{\{\tau_1, \tau_2, \tau_3\}}_{\mathcal{T}} \rangle$$

$$
\begin{array}{ll}
\tau_1 : & \langle \ell_0,\ \ell_1,\ i < n\ \wedge\ i' = i\ \wedge\ j' = i - 1\ \wedge\ n' = n \rangle \\
\tau_2 : & \langle \ell_1,\ \ell_1,\ j \geq 0\ \wedge\ i' = i\ \wedge\ j' = j - 1\ \wedge\ n' = n \rangle \\
\tau_3 : & \langle \ell_1,\ \ell_0,\ j < 0\ \wedge\ i' = i + 1\ \wedge\ j' = j\ \wedge\ n' = n \rangle
\end{array}
$$

$\mathsf{domain}(V) = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$

Computation

$$\sigma = \langle \ell^1, \overline{x}_1 \rangle, \langle \ell^2, \overline{x}_2 \rangle, \langle \ell^3, \overline{x}_3 \rangle, \ldots$$

- $\langle \ell^i, \overline{x}_i \rangle$
  - $\ell^i \in L$
  - $\overline{x}_i \in \mathsf{domain}(V)$
- initially:
  - $\ell^1 = \ell_0$
  - $\theta(\overline{x}_1)$
- consecution:

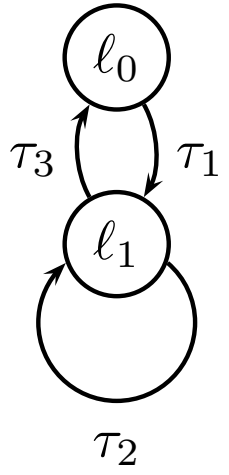
$$(\forall i \geq 1)(\exists \langle \ell, m, \rho \rangle \in \mathcal{T})(\ell^i = \ell \ \wedge \ \ell^{i+1} = m \ \wedge \ \rho(\overline{x}_i, \overline{x}_{i+1}))$$

Example: $\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1 \rangle\} \rangle$

$$\langle \ell_0, \langle i : 0 \rangle \rangle, \langle \ell_0, \langle i : 1 \rangle \rangle, \langle \ell_0, \langle i : 2 \rangle \rangle, \ldots$$

Example: Computation

```
@ n ≥ 0;
for(i := 0; i < n; i := i + 1) {
  for(j := i − 1; j ≥ 0; j := j − 1) {
    ...
  }
}
```



$$
\begin{array}{ll}
\cdots & \langle \ell_0,\ \langle i:3,\ j:-1,\ n:4\rangle\rangle \\
\xrightarrow{\tau_1} & \langle \ell_1,\ \langle i:3,\ j:2,\ n:4\rangle\rangle \\
\xrightarrow{\tau_2} & \langle \ell_1,\ \langle i:3,\ j:1,\ n:4\rangle\rangle \\
\xrightarrow{\tau_2} & \langle \ell_1,\ \langle i:3,\ j:0,\ n:4\rangle\rangle \\
\xrightarrow{\tau_2} & \langle \ell_1,\ \langle i:3,\ j:-1,\ n:4\rangle\rangle \\
\xrightarrow{\tau_3} & \langle \ell_0,\ \langle i:4,\ j:-1,\ n:4\rangle\rangle
\end{array}
$$

Collecting Semantics

$$\mathcal{C} : L \to 2^{\mathsf{domain}(V)}$$

- map from locations to subsets of $\mathsf{domain}(V)$
- $\mathcal{C}(\ell)$: the set of values (in $\mathsf{domain}(V)$) that occur at ℓ during some computation:

$$\overline{x} \in \mathcal{C}(\ell)$$

$$\Updownarrow$$

$$(\exists \sigma = \langle \ell^1, \overline{x}_1 \rangle, \langle \ell^2, \overline{x}_2 \rangle, \langle \ell^3, \overline{x}_3 \rangle, \ldots)(\exists i)(\ell_i = \ell \ \wedge \ \overline{x}_i = \overline{x})$$

Example: $\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1 \rangle\} \rangle$

$$\mathcal{C}(\ell_0) = \{\langle i : n \rangle \ : \ n \in \mathbb{Z}^+\}$$

Example: Collecting Semantics

$$T: \ \langle \{i, j, n : \mathbb{R}\},\ \{\ell_0, \ell_1\},\ \ell_0,\ i = 0 \ \wedge\ n \geq 0,\ \{\tau_1, \tau_2, \tau_3\} \rangle$$

$$\begin{aligned}
\tau_1: &\quad \langle \ell_0,\ \ell_1,\ i < n \ \wedge\ i' = i \ \wedge\ j' = i - 1 \ \wedge\ n' = n \rangle \\
\tau_2: &\quad \langle \ell_1,\ \ell_1,\ j \geq 0 \ \wedge\ i' = i \ \wedge\ j' = j - 1 \ \wedge\ n' = n \rangle \\
\tau_3: &\quad \langle \ell_1,\ \ell_0,\ j < 0 \ \wedge\ i' = i + 1 \ \wedge\ j' = j \ \wedge\ n' = n \rangle
\end{aligned}$$

$$\mathcal{C}(\ell_0) \ = \ \{\langle i : I,\ j : J,\ n : N \rangle \ :\ 0 \leq I \leq N \ \wedge\ I \in \mathbb{Z}\}$$

$$\mathcal{C}(\ell_1) \ = \ \left\{ \langle i : I,\ j : J,\ n : N \rangle \ : \begin{array}{l} 0 \leq I \leq N \ \wedge\ -1 \leq J < I \\ \wedge\ I, J \in \mathbb{Z} \end{array} \right\}$$

Assertion Map

$$\mu : L \to \mathcal{A}(V)$$

- map from locations to assertions over V

$$\mathcal{S} : \mathcal{A}(V) \to 2^{\mathsf{domain}(V)}$$

- map from assertions to subsets of $\mathsf{domain}(V)$
- $\mathcal{S}(\varphi) = \{\overline{x} \in \mathsf{domain}(V) \ : \ \varphi(\overline{x})\}$

Example: $\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1\rangle\}\rangle$

- $\mu(\ell_0) : \ i \geq 0$
- $\mathcal{S}(i \geq 0) = \{\langle i : n\rangle \ : \ n \in \mathbb{R}^+\}$

Invariant Assertion Map

Assertion map

$$\mu : L \to \mathcal{A}(V)$$

such that

$$(\forall \ell \in L)(\mathcal{C}(\ell) \subseteq \mathcal{S}(\mu(\ell)))$$

i.e., $\mu(\ell)$ is an **over approximation** to $\mathcal{C}(\ell)$.
Alternately,

$$(\forall \ell \in L)(\forall \overline{x} \in \mathsf{domain}(V))(\overline{x} \in \mathcal{C}(\ell) \to \mu(\ell)(\overline{x}))$$

Example: $\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1\rangle\}\rangle$

- $\mathcal{C}(\ell_0) = \{\langle i : n\rangle \ :\ n \in \mathbb{Z}^+\} \subseteq \{\langle i : n\rangle \ :\ n \in \mathbb{R}^+\} = \mathcal{S}(\mu(\ell_0))$
- so $\mu(\ell_0) :\ i \geq 0$ is an invariant map

Example: Invariant Assertion Map

$$\begin{aligned}\mu(\ell_0): &\quad 0 \le i \\ \mu(\ell_1): &\quad 0 \le i \ \wedge \ -1 \le j\end{aligned}$$

So

$$\begin{aligned}\mathcal{S}(\mu(\ell_0)) &= \{\langle i:I,\ j:J,\ n:N\rangle \ :\ 0 \le I\} \\ &\supseteq \{\langle i:I,\ j:J,\ n:N\rangle \ :\ 0 \le I \le N \ \wedge \ I \in \mathbb{Z}\} \\ \mathcal{S}(\mu(\ell_1)) &= \{\langle i:I,\ j:J,\ n:N\rangle \ :\ 0 \le I \ \wedge \ -1 \le J\} \\ &\supseteq \left\{\langle i:I,\ j:J,\ n:N\rangle \ :\ \begin{array}{l} 0 \le I \le N \ \wedge \ -1 \le J < I \\ \wedge\ I, J \in \mathbb{Z}\end{array}\right\}\end{aligned}$$

μ is an **invariant map**:

$$\mathcal{C}(\ell_0) \subseteq \mathcal{S}(\mu(\ell_0)) \quad \text{and} \quad \mathcal{C}(\ell_1) \subseteq \mathcal{S}(\mu(\ell_1))$$

Inductive Assertion Map

Assertion map

$$\mu : L \to \mathcal{A}(V)$$

such that

Initiation

$$\theta \models \mu(\ell_0)$$

i.e., $(\forall \overline{x} \in \mathsf{domain}(V))(\theta(\overline{x}) \to \mu(\ell_0)(\overline{x}))$

Consecution for all $\langle \ell, m, \rho \rangle \in \mathcal{T}$

$$\mu(\ell) \ \wedge \ \rho \ \models \ \mu(m)'$$

i.e., $(\forall \overline{x}, \overline{x}' \in \mathsf{domain}(V))(\mu(\ell)(\overline{x}) \ \wedge \ \rho(\overline{x}, \overline{x}') \ \to \ \mu(m)(\overline{x}'))$

Example: Inductive Assertion Map

$$\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1\rangle\}\rangle$$

$\mu(\ell_0) :\ i \geq 0$ is an inductive map:

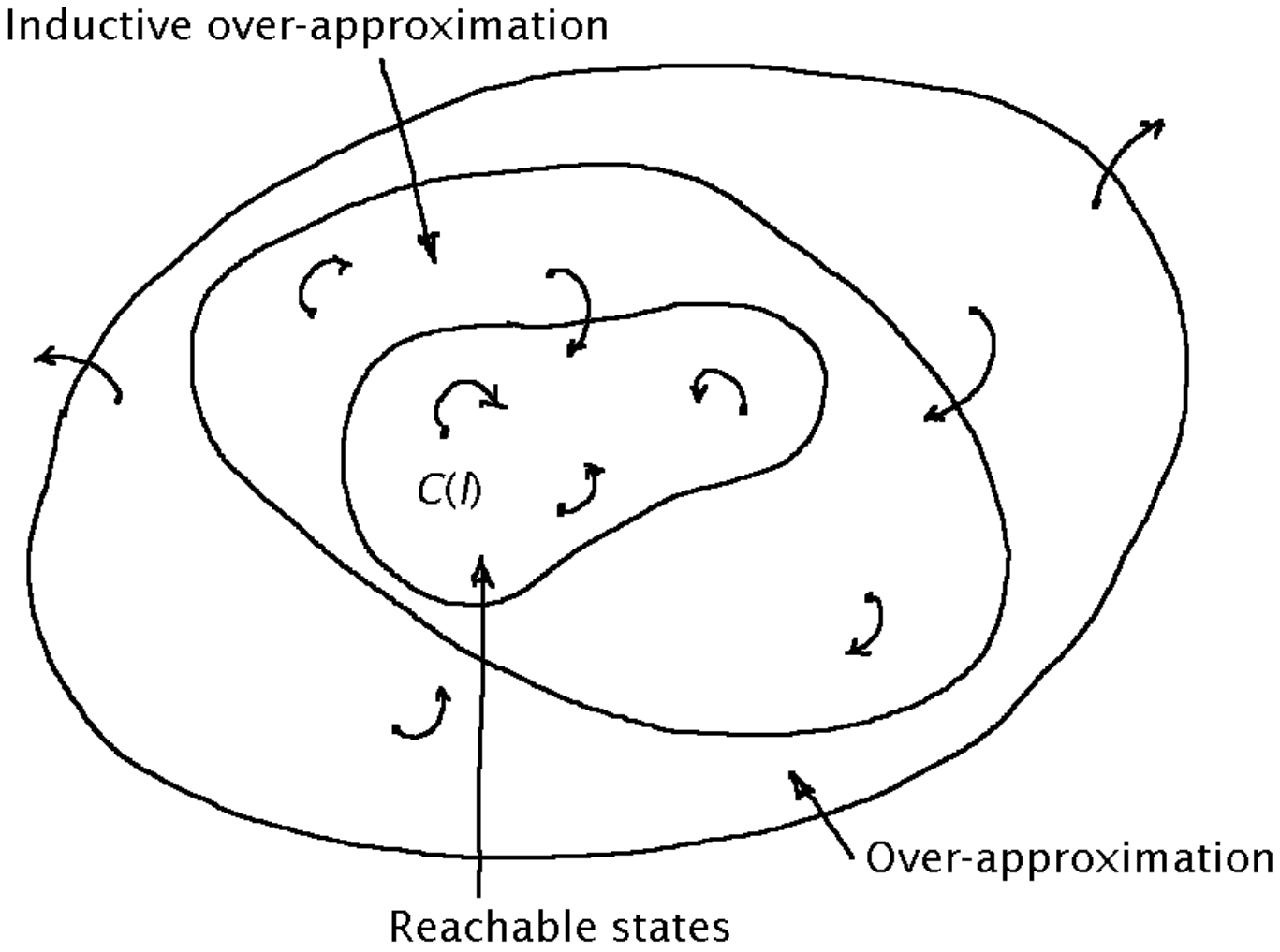
Initiation $\theta \models \mu(\ell_0)$

$$(\forall i)(i = 0 \rightarrow i \geq 0)$$

Consecution $\mu(\ell_0) \wedge i' = i + 1 \models \mu(\ell_0)'$

$$(\forall i, i')(i \geq 0 \wedge i' = i + 1 \rightarrow i' \geq 0)$$

Invariants: In Pictures



Example: Invariant *vs.* Inductive Invariant

$$T_3 : \ \langle \{n : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ n = 1,\ \{\langle \ell_0,\ \ell_0,\ n' = -n \rangle\} \rangle$$

- Collecting semantics: $\mathcal{C}(\ell_0) = \{\langle n : -1 \rangle, \langle n : 1 \rangle\}$
- Invariant map: $\mu_1(\ell_0) : \ n \leq 1$
  - $\mathcal{C}(\ell_0) \subseteq \mathcal{S}(\mu_1(\ell_0))$
  - But not **inductive**:

    $$(\forall n, n')(n \leq 1 \ \wedge \ n' = -n \ \rightarrow \ n' \leq 1)$$

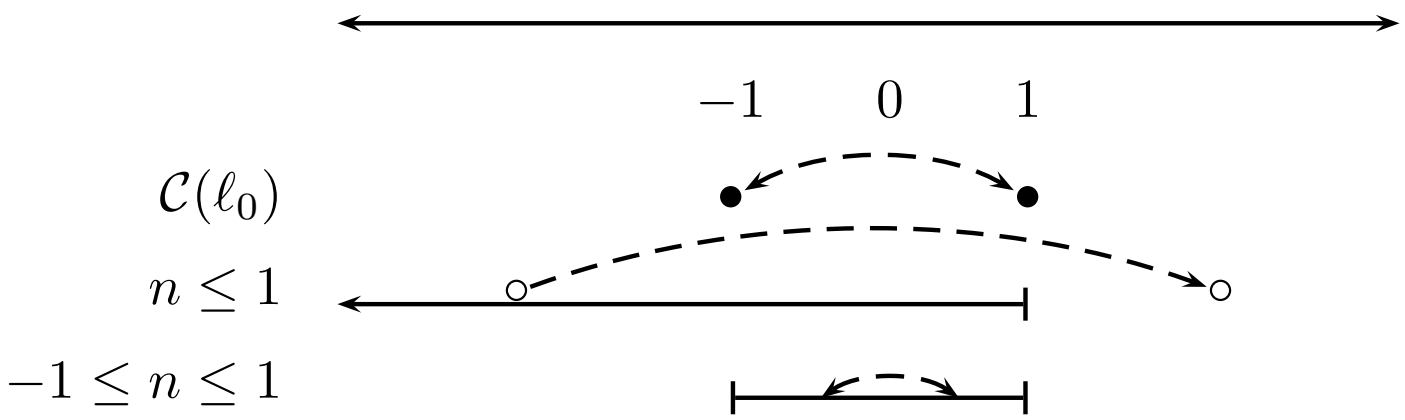
    is invalid — consider $n = -3,\ n' = 3$.
- Inductive map: $\mu_2(\ell_0) : \ -1 \leq n \leq 1$
  - $\mathcal{C}(\ell_0) \subseteq \mathcal{S}(\mu_2(\ell_0))$
  - Initiation: $(\forall n)(n = 1 \ \rightarrow \ -1 \leq n \leq 1)$
  - Consecution:

    $$(\forall n, n')(-1 \leq n \leq 1 \ \wedge \ n' = -n \ \rightarrow \ -1 \leq n' \leq 1)$$

Example: Invariant *vs.* Inductive Invariant

$$\langle \{n : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ n = 1,\ \{\langle \ell_0,\ \ell_0,\ n' = -n \rangle\} \rangle$$

In pictures:



All are invariants, but only $\mathcal{C}(\ell_0)$ and $-1 \leq n \leq 1$ are inductive.

Post

$$\mathsf{post} : \mathcal{A}(V) \times \mathcal{T} \to \mathcal{A}(V)$$

- map from assertions and transitions to assertions
- general definition:

$$\mathsf{post}(\varphi, \langle \ell, m, \rho \rangle) = (\exists \overline{x}^0)(\varphi(\overline{x}^0) \ \wedge \ \rho(\overline{x}^0, \overline{x}))$$

- $\mathsf{post}(\varphi, \tau)$ holds on the **τ-successors** of **φ-states**

Example: $\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1 \rangle\} \rangle$

$$\begin{aligned} \mathsf{post}(\mu(\ell_0),\ \tau) &= \mathsf{post}(i \geq 0,\ \tau) \\ &= (\exists i_0)(i_0 \geq 0 \ \wedge \ i = i_0 + 1) \\ &\Leftrightarrow \ i \geq 1 \end{aligned}$$

Inductive Map Using Post

Initiation

$$\theta \models \mu(\ell_0)$$

Consecution for all $\langle \ell, m, \rho \rangle \in \mathcal{T}$

$$\mathsf{post}(\mu(\ell), \langle \ell, m, \rho \rangle) \ \models \ \mu(m)$$

Example: $\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1 \rangle\} \rangle$

Initiation $\theta \ \models \ \mu(\ell_0)$

$$(\forall i)(i = 0 \ \rightarrow \ i \geq 0)$$

Consecution $\mathsf{post}(\mu(\ell_0),\ \tau) \ \models \ \mu(\ell_0)$

$$(\forall i)((\exists i_0)(i_0 \geq 0 \ \wedge \ i = i_0 + 1) \ \rightarrow \ i \geq 0)$$

$$\Updownarrow$$

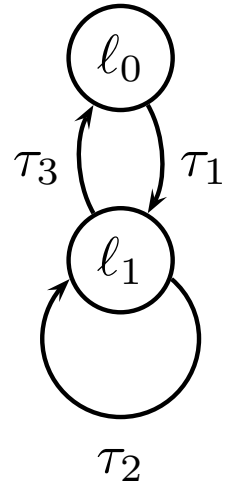
$$(\forall i)(i \geq 1 \ \rightarrow \ i \geq 0)$$

Example: Inductive Map Using Post

$$\begin{aligned}
&\mathsf{post}(\mu(\ell_0), \tau_1) \\
&\quad = \mathsf{post}(0 \le i,\ \langle \ell_0,\ \ell_1,\ i \le n\ \wedge\ i' = i\ \wedge\ j' = i - 1\ \wedge\ n' = n \rangle) \\
&\quad = (\exists i_0, n_0)(0 \le i_0\ \wedge\ i_0 \le n_0\ \wedge\ i = i_0\ \wedge\ j = i_0 - 1\ \wedge\ n = n_0) \\
&\quad = 0 \le i\ \wedge\ i \le n\ \wedge\ j = i - 1 \\
&\quad \models \mu(\ell_1) :\ 0 \le i\ \wedge\ -1 \le j
\end{aligned}$$

$$\begin{aligned}
&\mathsf{post}(\mu(\ell_1), \tau_2)\ =\ 0 \le i\ \wedge\ -1 \le j \\
&\quad \models \mu(\ell_1) :\ 0 \le i\ \wedge\ -1 \le j
\end{aligned}$$

$$\begin{aligned}
&\mathsf{post}(\mu(\ell_1), \tau_3)\ =\ 1 \le i\ \wedge\ -1 \le j \\
&\quad \models \mu(\ell_0) :\ 0 \le i
\end{aligned}$$



$\Rightarrow \mu$ is an **inductive map**.

Forward Propagation (FP)

FP(T : $\langle V, L, \ell_0, \theta, \mathcal{T} \rangle$)

$\mu(\ell_0) := \theta$

$\mu(\ell) :=$ false for $\ell \in L \setminus \{\ell_0\}$

$Q := \{\ell_0\}$

while $(|Q| > 0)$ do

$\underline{\ell} := \text{choose}(Q)$

for each $\tau \doteq \langle \underline{\ell}, m, \rho \rangle \in \mathcal{T}$ do

if post$(\mu(\underline{\ell}), \tau) \not\models \mu(m)$

then $\mu(m) := \mu(m) \vee \text{post}(\mu(\underline{\ell}), \tau)$

$Q := Q \cup \{m\}$

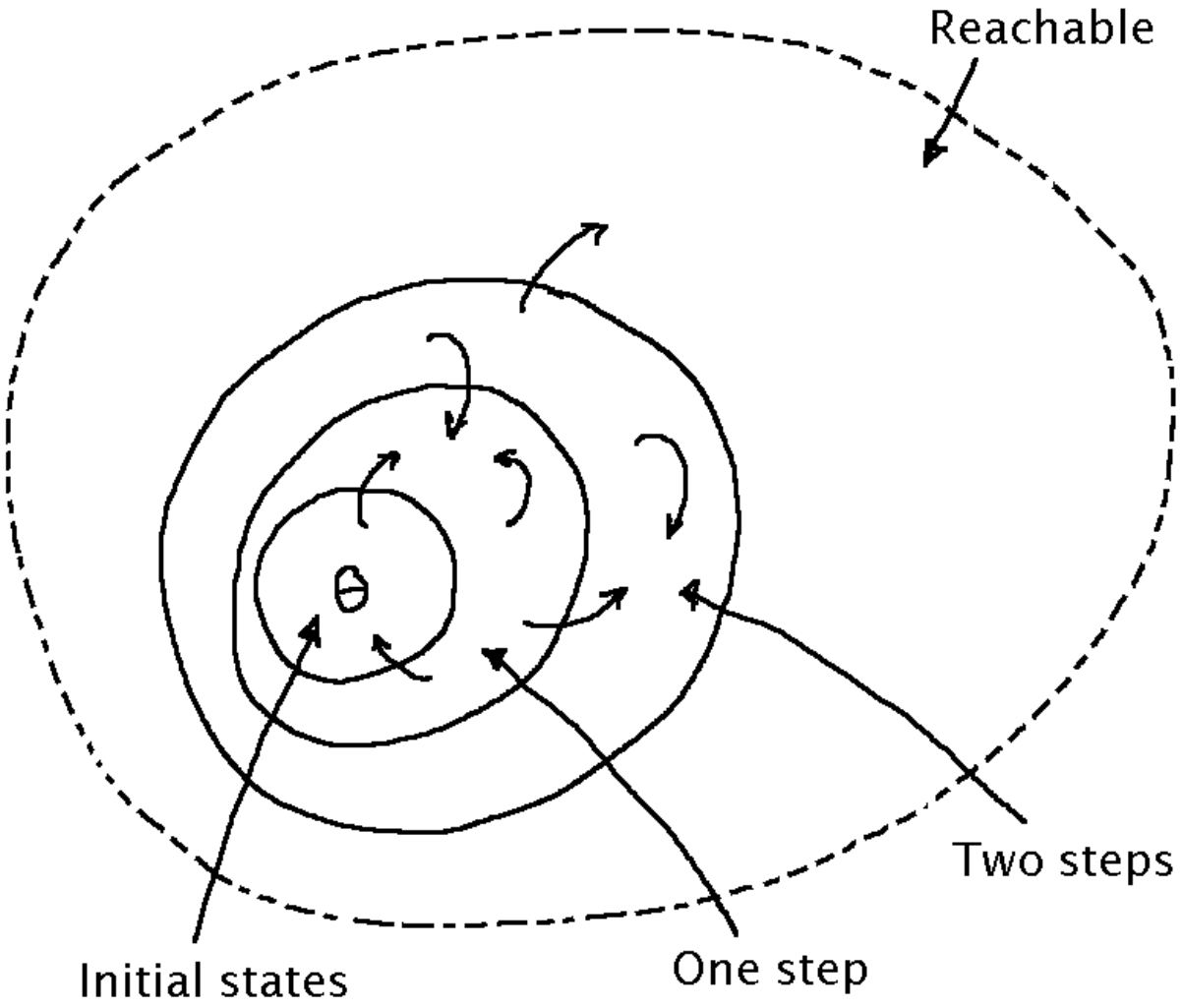
done

done

If FP terminates, then the computed μ is an inductive map.

In fact, $\mathcal{S}(\mu(\ell)) = \mathcal{C}(\ell)$.

FP: In Pictures



FP: Remarks

- Computing

$$\mathsf{post}(\mu(\ell), \tau) \;\models\; \mu(m)$$

  requires checking FOL validity in general — undecidable!

- No guarantee of convergence.
  Example: $\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1 \rangle\} \rangle$
  - Initially: $\mu(\ell_0) := \theta \;\Rightarrow\; \mu(\ell_0) := i = 0$
  - After N iterations:

$$\underbrace{\mathsf{post}\left(\bigvee_{n=0}^{N} i = n,\ \tau\right)}_{\bigvee_{n=1}^{N+1} i=n} \not\models \bigvee_{n=0}^{N} i = n$$

$$\Rightarrow\; \mu(\ell_0) := \bigvee_{n=0}^{N+1} i = n$$

FP: Finite State Systems

Claim:
FP is an algorithm for computing the collecting semantics of Boolean circuits.

1. $\mathsf{post}(\mu(\ell), \tau) \models \mu(m)$ is decidable (PL validity).
2. $\mu(\ell)$ can change only a finite number of times:
   - If $\mathsf{post}(\mu(\ell), \tau) \not\models \mu(m)$, then $\mathcal{S}(\mu(m))$ becomes larger ($\mu(m) := \mu(m) \vee \mathsf{post}(\mu(\ell), \tau)$).
   - $|2^{\mathsf{domain}(V)}| = 2^{2^{|V|}}$ is finite.
   - $\mathcal{S}(\mu(\ell))$ can only increase a finite number of times.

Applications:

- Explicit-state model checking: compute sets of bit-vectors.
- Symbolic model checking: represent sets with Boolean formulae (BDD representation).

FP: Infinite State Systems (General Programs)

1. Computing

$$\mathsf{post}(\mu(\ell), \tau) \models \mu(m)$$

   is undecidable in general.

   $\Rightarrow$ Choose decidable assertion domain (*e.g.*, $T_{\mathbb{R}}$, $T_{\mathbb{Z}}$, *etc.*).

2. FP does not converge in general.

   $\Rightarrow$ Guess approximating assertion (**widen**).

Assertion Domains

Goal: Make $\mathsf{post}(\mu(\ell), \tau) \models \mu(m)$ decidable.

Domains:

- Intervals: conjunctions of simple inequalities

$$\bigwedge_i \ell_i \leq x_i \leq u_i \quad \text{for} \quad \ell_i, u_i \in \mathbb{R} \cup \{-\infty, \infty\}$$

- $T_{\mathbb{R}}^{=}$: conjunctions of affine equations (Karr's analysis)

$$\sum_j a_j x_j = b$$

- $T_{\mathbb{R}}$: conjunctions of affine inequalities (polyhedra)

$$\sum_j a_j x_j \geq b$$

Assertion Domains

- $T_{\mathbb{Z}}$: conjunctions of affine inequalities

$$\sum_j a_j x_j \geq b$$

- Boolean combinations of fixed set of predicates (predicate abstraction)

$$\{x > 0, x < -3, \mathsf{null}(a), \ldots\} \qquad \mathsf{null}(a) \ \vee \ x > 0$$

- ...

Outline

0. Static Analysis
⇒ 1. Interval Analysis
2. Karr's Analysis

Interval Domain

$$T: \langle V = \overline{x} = \{x_1, \ldots, x_n\}, L, \ell_0, \theta, \mathcal{T} \rangle$$

Representation:

- $\widehat{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$
- $[\mathbf{l}, \mathbf{u}] = [\ell_1, u_1] \times \cdots \times [\ell_n, u_n]$
  where $[\mathbf{l}, \mathbf{u}]$ for $\mathbf{l}, \mathbf{u} \in \widehat{\mathbb{R}}^n$
- $[\infty, -\infty]$ is the canonical representation of the empty interval
  - $[\ell, u]$ where $\ell > u \Rightarrow [\infty, -\infty]$
  - convention: $[\infty, -\infty] + [-\infty, \infty] = [\infty, -\infty]$

Domain element: $[\mathbf{l}, \mathbf{u}]$

$$\overline{x} \in [\mathbf{l}, \mathbf{u}] \;\Leftrightarrow\; \bigwedge_i x_i \in [\ell_i, u_i] \;\Leftrightarrow\; \bigwedge_i \ell_i \leq x_i \leq u_i$$

Interval Arithmetic

Standard manipulations, *e.g.*:

- $\min[\ell, u] = \ell$
- $\max[\ell, u] = u$
- $[\ell_1, u_1] + [\ell_2, u_2] = [\ell_1 + \ell_2, u_1 + u_2]$
- for a constant c,

$$c[\ell_1, u_1] = \begin{cases} [c\ell_1, cu_1] & c \geq 0 \\ [cu_1, c\ell_1] & c < 0 \end{cases}$$

Interval Logic

- Disjunction:

$$x \in [\ell_1, u_1] \ \vee \ x \in [\ell_2, u_2] \ \Leftrightarrow \ x \in [\ell_1, u_1] \cup [\ell_2, u_2]$$
$$\Rightarrow \ x \in [\min(\ell_1, \ell_2), \max(u_1, u_2)]$$

  Called the **interval hull**. Over approximation!
  Ex: $[1, 3] \cup [5, \infty] = [1, \infty]$

- Conjunction:

$$x \in [\ell_1, u_1] \ \wedge \ x \in [\ell_2, u_2] \ \Leftrightarrow \ x \in [\ell_1, u_1] \cap [\ell_2, u_2]$$
$$\Leftrightarrow \ x \in \underbrace{[\max(\ell_1, \ell_2), \min(u_1, u_2)]}_{[\infty,-\infty] \text{ if necessary}}$$

  Ex: $[1, 3] \cap [2, \infty] = [2, 3]$

Post: Assignment

Use basic operations to define post efficiently:

$$\mathsf{post}([\mathbf{l},\mathbf{u}],\ x'_k = \sum_j a_j x_j\ \wedge\ \bigwedge_{i\neq k} x'_i = x_i)$$

$$= (\exists \overline{x}^0)\left(\overline{x}^0 \in [\mathbf{l},\mathbf{u}]\ \wedge\ x_k = \sum_j a_j x_j^0\ \wedge\ \bigwedge_{i\neq k} x_i = x_i^0\right)$$

$$= x_k \in \sum_j a_j[\ell_j,u_j]\ \wedge\ \bigwedge_{i\neq k} x_i \in [\ell_i,u_i]$$

$$= [\ell_1,u_1]\times\cdots\underbrace{[\min\sum_j a_j[\ell_j,u_j],\max\sum_j a_j[\ell_j,u_j]]}_{x_k}\cdots\times[\ell_n,u_n]$$

Example:

$$\mathsf{post}([-1,3]\times[5,\infty],\ x'_1 = x_1\ \wedge\ x'_2 = x_2 + 3x_1)$$

$$= [-1,3]\times([5,\infty]+3[-1,3]) = [-1,3]\times[2,\infty]$$

Post: Assignment

If the assignment cannot be handled within interval domain:

$$\mathsf{post}([\mathbf{l}, \mathbf{u}],\ x'_k = ?\ \wedge \bigwedge_{i \neq k} x'_i = x_i)$$
$$= [\ell_1, u_1] \times \cdots \underbrace{[-\infty, \infty]}_{x_k} \cdots \times [\ell_n, u_n]$$

Example:

$$\mathsf{post}([-1, 3] \times [5, \infty],\ x'_1 = x_1\ \wedge\ x'_2 = x_2 + \mathtt{f}(3x_1))$$
$$= [-1, 3] \times [-\infty, \infty]$$

Post: Guard

$$\mathsf{post}([\mathbf{l},\mathbf{u}],\ ax_k \geq b\ \wedge\ \overline{x}' = \overline{x}) \quad \text{for } a > 0$$

$$= (\exists \overline{x}^0)\left(\overline{x}^0 \in [\mathbf{l},\mathbf{u}]\ \wedge\ x_k^0 \in \left[\frac{b}{a},\infty\right]\ \wedge\ \overline{x} = \overline{x}^0\right)$$

$$= [\ell_1,u_1] \times \cdots \underbrace{\left[\max\left(\ell_k,\frac{b}{a}\right),\min(u_k,\infty)\right]}_{x_k} \cdots \times [\ell_n,u_n]$$

Similar for $ax_k \leq b$ and $ax_k = b$, for $a > 0$.

Ex: $\mathsf{post}([1,3]\times[-2,9],\ x_2 \geq 0\ \wedge\ \overline{x}' = \overline{x})\ =\ [1,3]\times[0,9]$

If the guard cannot be handled within interval domain:

$$\mathsf{post}([\mathbf{l},\mathbf{u}],\ ?\ \wedge\ \overline{x}' = \overline{x})\ =\ [\mathbf{l},\mathbf{u}]$$

Ex: $\mathsf{post}([1,3]\times[-2,9],\ x_2\%2 = 0\ \wedge\ \overline{x}' = \overline{x})\ =\ [1,3]\times[-2,9]$

Post: Guard

General affine guard:

$$\mathsf{post}([\mathbf{l},\mathbf{u}],\ \sum_j a_j x_j \geq b\ \wedge\ \overline{x}' = \overline{x})$$

$$= (\exists \overline{x}^0)\left(\overline{x}^0 \in [\mathbf{l},\mathbf{u}]\ \wedge\ \sum_j a_j x_j \geq b\ \wedge\ \overline{x} = \overline{x}^0\right)$$

$$= \max \sum_j a_j[\ell_j, u_j] \geq b\ \wedge\ \overline{x} \in [\mathbf{l},\mathbf{u}]$$

$$= \begin{cases} [\mathbf{l},\mathbf{u}] & \text{if } \max \sum_j a_j[\ell_j,u_j] \geq b \\ [\infty,-\infty]^n & \text{otherwise} \end{cases}$$

Example:

$$\mathsf{post}([-\infty,0]\times[1,\infty],\ x_1 \geq x_2\ \wedge\ \overline{x}' = \overline{x}) = [\infty,-\infty]\times[\infty,-\infty]$$

$$\mathsf{post}([-\infty,100]\times[1,\infty],\ x_2 \geq x_1\ \wedge\ \overline{x}' = \overline{x}) = [-\infty,100]\times[1,\infty]$$

Post

In interval domain,

- post maps hypercubes to hypercubes
- post can be computed efficiently — no QE
- $\mathsf{post}(\mu(\ell), \tau) \models \mu(m)$ can be checked efficiently:

$$(\forall \overline{x})(\overline{x} \in [\mathbf{l}^1, \mathbf{u}^1] \rightarrow \overline{x} \in [\mathbf{l}^2, \mathbf{u}^2])$$

$$\Updownarrow$$

$$\bigwedge_i (\ell_i^1 \geq \ell_i^2 \wedge u_i^1 \leq u_i^2)$$

i.e., check containment $[\mathbf{l}^1, \mathbf{u}^1] \subseteq [\mathbf{l}^2, \mathbf{u}^2]$

Example

$$T_3 : \ \langle \{n : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ n = 1,\ \{\langle \ell_0,\ \ell_0,\ n' = -n \rangle\} \rangle$$

- $\mu(\ell_0) := [1, 1]$
- $\mathsf{post}([1, 1],\ \langle \ell_0, \ell_0, n' = -n \rangle) = [-1, -1]$
  - $\mathsf{post}(\mu(\ell), \tau) \ \models \ \mu(m)$?
    No: $[-1, -1] \not\subseteq [1, 1]$
  - $\mu(\ell_0) := [1, 1] \cup [-1, -1] = [-1, 1]$
- $\mathsf{post}([-1, 1],\ \langle \ell_0, \ell_0, n' = n \rangle) = [-1, 1]$
  - $\mathsf{post}(\mu(\ell), \tau) \ \models \ \mu(m)$?
    Yes: $[-1, 1] \subseteq [-1, 1]$

$\mu(\ell_0) = [-1, 1]$, *i.e.*, $\mu(\ell_0) : \ -1 \leq n \leq 1$ is an inductive map.

Convergence

$$\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1\rangle\}\rangle$$

- $\mu(\ell_0) := [0, 0]$
- $\mathsf{post}([0, 0],\ \langle \ell_0, \ell_0, i' = i + 1\rangle) = [1, 1]$
  - $\mathsf{post}(\mu(\ell), \tau) \models \mu(m)$?
    No: $[1, 1] \not\subseteq [0, 0]$
  - $\mu(\ell_0) := [0, 0] \cup [1, 1] = [0, 1]$
- $\mathsf{post}([0, 1],\ \langle \ell_0, \ell_0, i' = i + 1\rangle) = [1, 2]$
  - $\mathsf{post}(\mu(\ell), \tau) \models \mu(m)$?
    No: $[1, 2] \not\subseteq [0, 1]$
  - $\mu(\ell_0) := [0, 1] \cup [1, 2] = [0, 2]$
- After n iterations: $\mu(\ell_0) := [0, n] \cup [1, n + 1] = [0, n + 1]$

FP does not converge on interval domain!

Widen

Goal: Guess over approximation to force convergence.

Interval widening:

- $[\ell_1, u_1] \bigtriangledown [\ell_2, u_2] = [\underbrace{\ell_2 < \ell_1 \ ? \ -\infty \ : \ \ell_1}_{ite(\ell_2<\ell_1,\ -\infty,\ \ell_1)}, \underbrace{u_2 > u_1 \ ? \ \infty \ : \ u_1}_{ite(u_2>u_1,\ \infty,\ u_1)}]$
- Special case: widening with empty interval:

$$[\infty, -\infty] \bigtriangledown [\ell, u] = [\ell, u] \bigtriangledown [\infty, -\infty] = [\infty, -\infty]$$

Extend component-wise to $[\mathbf{l}^1, \mathbf{u}^1] \bigtriangledown [\mathbf{l}^2, \mathbf{u}^2]$.

Examples:

- $[1, 4] \bigtriangledown [1, 5] = [1, \infty]$
- $[1, 4] \bigtriangledown [0, 5] = [-\infty, \infty]$
- $[\infty, -\infty] \bigtriangledown [0, 5] = [\infty, -\infty]$

Widen Step

Suppose

$$\mathsf{post}(\mu(\ell), \tau) \not\models \mu(m)$$

after many (how many?) iterations of FP.

Instead of

$$\mu(m) := \mu(m) \vee \mathsf{post}(\mu(\ell), \tau)$$

do

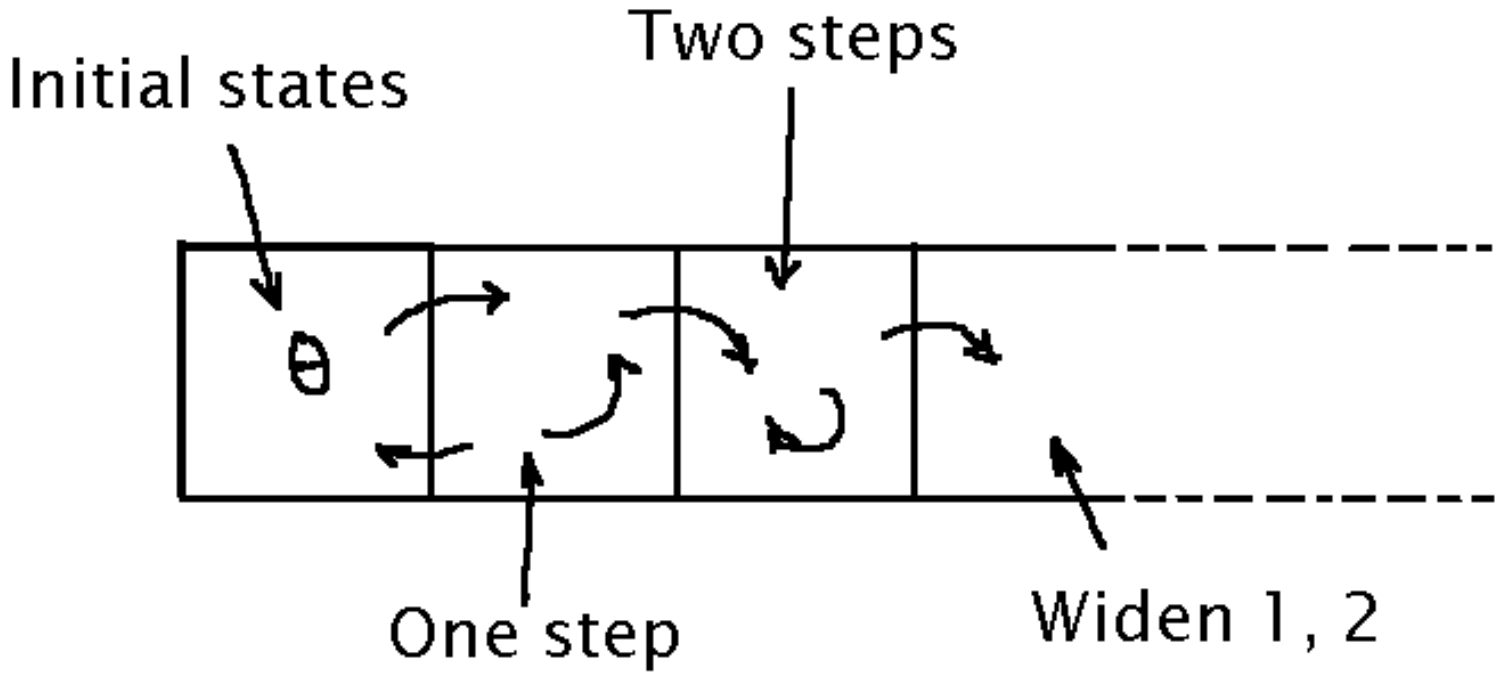
$$\mu(m) := \mu(m) \bigtriangledown (\mu(m) \vee \mathsf{post}(\mu(\ell), \tau))$$

Remark:

μ is still an inductive map on termination of FP, but

$\mathcal{C}(\ell) \subseteq \mathcal{S}(\mu(\ell))$ in general (instead of $\mathcal{C}(\ell) = \mathcal{S}(\mu(\ell))$).

Widen: In Pictures



Example: Widen

$$\langle \{i : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i = 0,\ \{\tau : \langle \ell_0,\ \ell_0,\ i' = i + 1\rangle\}\rangle$$

- $\mu(\ell_0) := [0, 0]$
- $\mathsf{post}([0, 0],\ \tau) = [1, 1]$
  - $\mathsf{post}(\mu(\ell), \tau) \models \mu(m)?$ No: $[1, 1] \not\subseteq [0, 0]$
  - $\mu(\ell_0) := [0, 0] \cup [1, 1] = [0, 1]$
- $\mathsf{post}([0, 1],\ \tau) = [1, 2]$
  - $\mathsf{post}(\mu(\ell), \tau) \models \mu(m)?$ No: $[1, 2] \not\subseteq [0, 1]$
  - $\mu(\ell_0) := [0, 1] \bigtriangledown ([0, 1] \cup [1, 2]) = [0, \infty]$
- $\mathsf{post}([0, \infty],\ \tau) = [1, \infty]$
  - $\mathsf{post}(\mu(\ell), \tau) \models \mu(m)?$ Yes: $[1, \infty] \subseteq [0, \infty]$

$\mu(\ell_0) = [0, \infty]$, *i.e.*, $\mu(\ell_0) :\ i \geq 0$ is an inductive map.

Standard Procedure

1. **(Domain)** Fix representation of class of assertions.
   Ex: $[\mathbf{l}, \mathbf{u}]$
2. **(Post)** Define post efficiently with respect to domain.
   Efficient definition must be over approximation of true post.
   Ex: $\mathsf{post}([\mathbf{l}, \mathbf{u}], \tau)$
3. **(Entailment)** Define efficient check of $\mathsf{post}(\mu(\ell), \tau) \models \mu(m)$.
   Ex: $[\mathbf{l}^1, \mathbf{u}^1] \subseteq [\mathbf{l}^2, \mathbf{u}^2]$
4. **(Disjunction)** Define over approximation of disjunction.
   Used in step $\mu(m) := \mu(m) \vee \mathsf{post}(\mu(\ell), \tau)$.
   Ex: $[\mathbf{l}^1, \mathbf{u}^1] \cup [\mathbf{l}^2, \mathbf{u}^2]$ (interval hull)
5. **(Widen)** Define widen operation if FP does not converge.
   Ex: $[\mathbf{l}^1, \mathbf{u}^1] \bigtriangledown [\mathbf{l}^2, \mathbf{u}^2]$

Outline

0. Static Analysis
1. Interval Analysis

⇒ 2. Karr's Analysis

Motivation

```
@ i1 = i2 = k = 0;
while (...) {
  if (...) {
    i1 := i1 + 1;
    k := k + 1;
  }
  else {
    i2 := i2 + 1;
    k := k + 1;
  }
}
```

$$\langle \{i_1, i_2, k : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i_1 = i_2 = k = 0,\ \{\tau_1, \tau_2, \tau_3\} \rangle$$

$$\tau_1 : \quad i_1' = i_1 + 1 \ \wedge\ i_2' = i_2 \ \wedge\ k' = k + 1$$

$$\tau_2 : \quad i_1' = i_1 \ \wedge\ i_2' = i_2 + 1 \ \wedge\ k' = k + 1$$

Goal: Deduce $i_1 + i_2 = k$.

1. Domain

$$T : \langle V = \{x_1, \ldots, x_n\}, L, \ell_0, \theta, \mathcal{T} \rangle$$

Conjunctions of affine equations:

$$\bigwedge_{i=1}^{m} \left(\sum_j a_{i,j} x_j = b_i \right)$$

Dual representation:

1. **(Constraint)**

   $$Ax = b$$

   for $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$.

2. **(Vertex)** Basis X of $Ax = b$.

2. Post

- $\mathsf{post}(S,\ x'_k = \sum_j a_j x_j + b\ \wedge\ \bigwedge_{i \neq k} x'_i = x_i)$
  - Application of affine transformation to affine space S.
  - Use vertex representation.
- $\mathsf{post}(S,\ x'_k = ?\ \wedge\ \bigwedge_{i \neq k} x'_i = x_i)$
  - Non-affine assignment.
  - $\mathsf{post}(S,\ x'_k = ? \ldots) = \mathsf{post}(S,\ x'_k = 0 \ldots) \cup \mathsf{post}(S,\ x'_k = 1 \ldots)$
  - $\cup$ defined below.
- $\mathsf{post}(S,\ \sum_j a_j x_j = b\ \wedge\ \overline{x}' = \overline{x})$
  - Conjunction of two affine spaces (S and $\sum_j a_j x_j = b$).
  - Use constraint representation.
- $\mathsf{post}(S,\ ?\ \wedge\ \overline{x}' = \overline{x}) = S$ (non-affine guard)

3, 4, 5

3. Entailment

$\mathsf{post}(\mu(\ell), \tau) \models \mu(m)$

Check $S_1 \subseteq S_2$.

Use both representations.

4. Disjunction

Affine hull of the union of S_1 and S_2.

Use vertex representation: $X_1 \cup X_2$

5. Widen

If $S_1 \subset S_2$, then $\mathsf{dim}(S_1) < \mathsf{dim}(S_2)$.

$\mathsf{dim}(S) \leq n$.

$\Rightarrow$ FP converges on domain of affine equations.

$\Rightarrow$ Widening is not needed.

Background: Linear Equation $Ax = 0$

$$Ax = 0$$

- A is an $m \times n$ matrix, *i.e.*, $A \in \mathbb{R}^{m \times n}$
- x is an n vector, *i.e.*, $x \in \mathbb{R}^n$
- 0 is an m vector, $[0 \ \cdots \ 0]^\mathsf{T}$

For us, $A \in \mathbb{Q}^{m \times n}$.

Example:

$$\underbrace{\begin{bmatrix} 3 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}}_{x} = \underbrace{\begin{bmatrix} 0 \\ 0 \end{bmatrix}}_{0}$$

Background: Linear Space

Set of vectors:

Represent set of $\mathbb{R}^n$ vectors

$$\{x^1, x^2, \ldots, x^k\}$$

by $n \times k$ matrix

$$X = [x^1 \; x^2 \; \cdots \; x^k] \; .$$

Notation: $|X| = k$

Linear space:

$$\mathsf{lin}(X) \; = \; \left\{ \sum_{j=1}^{m} \lambda_j x_j \; : \; m \geq 0, \; x^j \in X, \; \lambda_j \in \mathbb{R} \right\}$$

X is a **basis** if for all $x \in X$, $x \notin \mathsf{lin}(X - \{x\})$.

If X is a basis, then $|X| \leq n$.

Background: Affine Equation $Ax = b$

$$Ax = b$$

- A is an $m \times n$ matrix, *i.e.*, $A \in \mathbb{R}^{m \times n}$
- x is an n vector, *i.e.*, $x \in \mathbb{R}^n$
- b is an m vector, *i.e.*, $b \in \mathbb{R}^n$

For us, $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$.

Example:

$$\underbrace{\begin{bmatrix} 3 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}}_{x} = \underbrace{\begin{bmatrix} -1 \\ 0 \end{bmatrix}}_{b}$$

Background: Affine Space

Affine space:

$$\mathsf{aff}(X) \;=\; \left\{ \sum_{j=1}^{m} \lambda_j x_j \;:\; m \geq 0,\; x^j \in X,\; \lambda_j \in \mathbb{R},\; \sum_{j=1}^{m} \lambda_j = 1 \right\}$$

X is a **basis** if for all $x \in X$, $x \notin \mathsf{aff}(X - \{x\})$.
If X is a basis, then $|X| \leq n + 1$.

What is the difference between linear and affine spaces?
All linear spaces contain the origin (0).
An affine space need not contain the origin.

Background: Elementary Operations

1. Interchange two rows.
2. Multiply row by nonzero scalar.
3. Add one row to another.

Applying elementary operations to A in

$$Ax = 0$$

does not change the set of solutions.

Applying elementary operations to $[A\ b]$ in

$$Ax = b$$

does not change the set of solutions.

Background: Row-Reduced Echelon Form (RREF)

- Each nonzero row has 1 as first nonzero entry.
- For column in which 1 is leading for a row, other entries are 0.
- Zero rows (if any) are at bottom of matrix.
- "Stairstep" pattern.

Example:

$$\begin{bmatrix} 1 & 0 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 1 & -\frac{2}{3} & \frac{1}{3} \end{bmatrix}$$

Background: Solving $Ax = 0$

Solution to $Ax = 0$ is **null space** of A,

$$y \in \mathsf{lin}(\mathsf{null}(A)) \;\Leftrightarrow\; Ay = 0$$

Computing $\mathsf{null}(A)$:

- Put A in RREF.
- Free dimensions: $\{f_1, \ldots, f_\ell\}$ s.t. no leading 1 in column f_i.
- Construct basis B:
  - $B_{f_i,i} = 1$
  - for $j = n$ to 1 do
    1. if row j is all zeros, $B_{j,i} = 0$ for $i \notin \{f_1, \ldots, f_\ell\}$
    2. else some column i is leading 1: solve for $x_i = \sum a_k f_k$
    3. $B_{j,k} = a_k$
    4. substitute $\sum a_k f_k$ for x_i in rows 1 to $j - 1$

Example 1: $Ax = 0$

$$Ax = 0$$

$$\begin{bmatrix} 3 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$\mathsf{null}(A)$:

- RREF:

$$\begin{bmatrix} 3 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & \frac{2}{3} \\ 1 & 1 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & \frac{2}{3} \\ 0 & 1 & -\frac{2}{3} \end{bmatrix}$$

- Free dimensions: $\{3\}$

Example 1: $Ax = 0$

$$\begin{bmatrix} 1 & 0 & \frac{2}{3} \\ 0 & 1 & -\frac{2}{3} \end{bmatrix}$$

- Construct basis B:
  - $B_0 \;=\; [\; ?\; ?\; 1\;]^\mathsf{T}$
  - $j = 3$

    $B_1 \;=\; [\; ?\; ?\; 1\;]^\mathsf{T}$

    $j = 2$

    $x_2 - \frac{2}{3}x_3 = 0 \;\Rightarrow\; x_2 = \frac{2}{3}x_3$

    $B_2 \;=\; [\; ?\; \frac{2}{3}\; 1\;]^\mathsf{T}$

    substitute into row 1: no change

    $j = 1$

    $x_1 + \frac{2}{3}x_3 = 0 \;\Rightarrow\; x_1 = -\frac{2}{3}x_3$

    $B_3 \;=\; [\; -\frac{2}{3}\; \frac{2}{3}\; 1\;]^\mathsf{T}$

$\Rightarrow\; \mathsf{null}(A) = [-2\; 2\; 3]^\mathsf{T}$

Example 2: $Ax = 0$

$$Ax = 0$$

$$\begin{bmatrix} 3 & 0 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$\mathsf{null}(A)$:

- RREF:

$$\begin{bmatrix} 3 & 0 & 2 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & \frac{2}{3} \end{bmatrix}$$

- Free dimensions: $\{2, 3\}$

Example 2: $Ax = 0$

$$\begin{bmatrix} 1 & 0 & \frac{2}{3} \end{bmatrix}$$

- Construct basis B:
  - $B_0 = \begin{bmatrix} ? & ? \\ 1 & ? \\ ? & 1 \end{bmatrix}$
  - $j = 3, 2$

    $B_1 = \begin{bmatrix} ? & ? \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$ $\Rightarrow$ $\mathsf{null}(A) = \begin{bmatrix} 0 & -2 \\ 1 & 0 \\ 0 & 3 \end{bmatrix}$

    $j = 1$

    $x_1 + \frac{2}{3}x_3 = 0 \Rightarrow x_1 = -\frac{2}{3}x_3$

    $B_2 = \begin{bmatrix} 0 & -\frac{2}{3} \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$

Background: Solving $Ax = b$

- Put $[A\ b]$ in RREF.
- Solve from RREF for one solution z.
- Compute $\mathsf{null}(A)$ (extract from RREF).
- Construct basis B:

$$\{z\} \cup \{z + x \ : \ x \in \mathsf{null}(A)\}$$

Call B the **solution basis**, $\mathsf{soln}(A, b)$.

$$y \in \mathsf{aff}(\mathsf{soln}(A, b)) \Leftrightarrow Ay = b$$

Example 3: $Ax = b$

$$\begin{bmatrix} 3 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \end{bmatrix}$$

- RREF:

$$\left[\begin{array}{ccc|c} 3 & 0 & 2 & -1 \\ 1 & 1 & 0 & 0 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & 0 & \frac{2}{3} & -\frac{1}{3} \\ 1 & 1 & 0 & 0 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & 0 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 1 & -\frac{2}{3} & \frac{1}{3} \end{array}\right]$$

- Solve for z:
  - Free variables: $\{x_3\}$. Let $x_3 = 1$.
  - $x_2 - \frac{2}{3}(1) = \frac{1}{3} \;\Rightarrow\; x_2 = 1$
  - $x_1 + \frac{2}{3}(1) = -\frac{1}{3} \;\Rightarrow\; x_1 = -1$

  $\Rightarrow\; z = [-1\ 1\ 1]^{\mathsf{T}}$

Example 3: $Ax = b$

- $\mathsf{null}(A) = [-2\ 2\ 3]^{\mathsf{T}}$
- Construct basis B:

$$\left\{ \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} -2 \\ 2 \\ 3 \end{bmatrix} \right\} = \begin{bmatrix} -1 & -3 \\ 1 & 3 \\ 1 & 4 \end{bmatrix}$$

$\mathsf{soln}(A, b) = B$

Example 4: $Ax = b$

$$\begin{bmatrix} 3 & 0 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -1 \end{bmatrix}$$

- RREF:

$$\left[\begin{array}{ccc|c} 3 & 0 & 2 & -1 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & 0 & \frac{2}{3} & -\frac{1}{3} \end{array}\right]$$

- Solve for z:
  - Free variables: $\{x_2, x_3\}$. Let $x_2 = 1$, $x_3 = 1$.
  - $x_1 + \frac{2}{3}(1) = -\frac{1}{3} \Rightarrow x_1 = -1$

  $\Rightarrow z = [-1\ 1\ 1]^{\mathsf{T}}$

Example 4: $Ax = 0$

- $\mathsf{null}(A) = \begin{bmatrix} 0 & -2 \\ 1 & 0 \\ 0 & 3 \end{bmatrix}$
- Construct basis B:

$$\left\{ \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} -2 \\ 0 \\ 3 \end{bmatrix} \right\} = \begin{bmatrix} -1 & -1 & -3 \\ 1 & 2 & 1 \\ 1 & 1 & 4 \end{bmatrix}$$

$\mathsf{soln}(A, b) = B$

Duality

Two representations of a linear space.

$$Ax = 0 \;\Leftrightarrow\; x \in \mathsf{lin}(X)$$

- $Ax = 0$ is the **constraint representation**.
- X is the **vertex representation**.

Two representations of an affine space.

$$Ax = b \;\Leftrightarrow\; x \in \mathsf{aff}(X)$$

- $Ax = b$ is the **constraint representation**.
- X is the **vertex representation**.

Duality: Changing Representation (Linear)

$$Ax = 0 \;\Rightarrow\; x \in \mathsf{lin}(X)$$

$X = \mathsf{null}(A)$

$$Ax = 0 \;\Leftarrow\; x \in \mathsf{lin}(X)$$

Set up equation:

$$X^{\mathsf{T}} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = 0$$

Then

$$A^{\mathsf{T}} = \mathsf{null}(X^{\mathsf{T}})$$

Duality: Changing Representation (Affine)

$$Ax = b \;\Rightarrow\; x \in \mathsf{aff}(X)$$

Given constraint representation $Ax = b$ of affine space S.

Define

$$\mathsf{c2v}(A, b) \stackrel{\text{def}}{=} \mathsf{soln}(A, b)$$

Then $X = \mathsf{c2v}(A, b)$ is a vertex representation of S.

Duality: Changing Representation (Affine)

$$Ax = b \;\Leftarrow\; x \in \mathsf{aff}(X)$$

Given vertex representation X of S.

Set up equation:

$$\underbrace{\begin{bmatrix} & -1 \\ X^{\mathsf{T}} & \vdots \\ & -1 \end{bmatrix}}_{C} \begin{bmatrix} a_1 \\ \vdots \\ a_n \\ b \end{bmatrix} = 0$$

Then

$$\begin{bmatrix} A^{\mathsf{T}} \\ b^{\mathsf{T}} \end{bmatrix} = \mathsf{null}(C)$$

Define $\mathsf{v2c}(X)$ to return A, b.

Then for $A, b = \mathsf{v2c}(X)$, $Ax = b$ is a constraint representation of S.

Basic Operations

Given: Two affine spaces S_1, S_2.

Intersection

$$\begin{array}{lll} S_1: & A_1 x & = b_1 \\ S_2: & A_2 x & = b_2 \end{array} \quad \Rightarrow \quad S_1 \cap S_2: \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} x = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

$$x \in S_1 \cap S_2 \;\Leftrightarrow\; (x \in S_1 \;\wedge\; x \in S_2)$$

Union (Affine Hull)

$$\begin{array}{ll} S_1: & X_1 \\ S_2: & X_2 \end{array} \quad \Rightarrow \quad S_1 \cup S_2: \; X_1 \cup X_2 \quad (i.e., \, [X_1 \; X_2])$$

$$(x \in S_1 \;\vee\; x \in S_2) \;\Rightarrow\; x \in S_1 \cup S_2$$

Basic Operations

Containment

$$\begin{array}{ll} S_1: & X \\ S_2: & Ax = b \end{array} \quad \Rightarrow \quad S_1 \subseteq S_2: \ (\forall x \in X)[Ax = b]$$

$S_1 \subseteq S_2$ iff $x \in S_1 \ \Rightarrow \ x \in S_2$.

Use to implement convergence check $\mathsf{post}(\mu(\ell), \tau) \ \models \ \mu(m)$.

Transformation For transform $x_k = a^\mathsf{T} x + b$ and $S_1: \ X$,

$$[\![x_k = a^\mathsf{T} x + b]\!] S_1 = \{[x_1 \cdots x_{k-1} \quad a^\mathsf{T} x + b \quad x_{k+1} \cdots x_n]^\mathsf{T} \ : \ x \in X\}$$

Minimization Minimize representation.

$S: \ Ax = b$

$$\mathsf{minc}(A, b) \stackrel{\text{def}}{=} \mathsf{v2c}(\mathsf{c2v}(A, b))$$

$S: \ X$

$$\mathsf{minv}(X) \stackrel{\text{def}}{=} \mathsf{c2v}(\mathsf{v2c}(X))$$

Post: Assignment

Affine assignment:

$$\mathsf{post}(S,\ x'_k = a^{\mathsf{T}}x + b\ \wedge\ \bigwedge_{i \neq k} x'_i = x_i)\ =\ [\![x_k = a^{\mathsf{T}}x + b]\!]S$$

Non-affine assignment:

$$\mathsf{post}(S,\ x'_k = ?\ \wedge\ \bigwedge_{i \neq k} x'_i = x_i)\ =\ [\![x_k = 0]\!]S \cup [\![x_k = 1]\!]S$$

Post: Guard

Affine guard:

$$\mathsf{post}(S,\ a^{\mathsf{T}}x = b\ \wedge\ \overline{x}' = \overline{x})\ =\ S \cap (a^{\mathsf{T}}x = b)$$

Non-affine guard:

$$\mathsf{post}(S,\ ?\ \wedge\ \overline{x}' = \overline{x})\ =\ S$$

Example

$$\langle \{i_1, i_2, k : \mathbb{R}\},\ \{\ell_0\},\ \ell_0,\ i_1 = i_2 = k = 0,\ \{\tau_1, \tau_2, \tau_3\} \rangle$$

$$\tau_1 : \quad i_1' = i_1 + 1 \ \wedge\ i_2' = i_2 \ \wedge\ k' = k + 1$$

$$\tau_2 : \quad i_1' = i_1 \ \wedge\ i_2' = i_2 + 1 \ \wedge\ k' = k + 1$$

Q	$\mu(\ell_0)$	$\mathsf{post}(\mu(\ell_0), \tau_1)$	$\mathsf{post}(\mu(\ell_1), \tau_2)$	
$\{\ell_0\}$	$i_1 = i_2 = k = 0$ $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$	(1)
$\{\ell_0\}$	$i_1 + i_2 = k$ $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 1 \\ 1 & 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 1 & 2 & 2 \end{bmatrix}$	(2)
$\{\}$	$i_1 + i_2 = k$			(3)

Example: Comments

1. $\mathsf{post}(\mu(\ell_0), \tau_1) \not\models \mu(\ell_0)$ $\quad (1 = 0 = 1 = 0?\ \text{No.})$
   $\mathsf{post}(\mu(\ell_0), \tau_2) \not\models \mu(\ell_0)$ $\quad (0 = 1 = 1 = 0?\ \text{No.})$
   $\Rightarrow \mu(\ell_0) := \mu(\ell_0) \vee \mathsf{post}(\mu(\ell_0), \tau_1) \vee \mathsf{post}(\mu(\ell_0), \tau_2)$

2. $\mathsf{post}(\mu(\ell_0), \tau_1) \models \mu(\ell_0)$ $\quad (\text{plug columns into } i_1 + i_2 = k)$
   $\mathsf{post}(\mu(\ell_0), \tau_2) \models \mu(\ell_0)$ $\quad (\text{plug columns into } i_1 + i_2 = k)$

3. Convergence.