Abstract interpretation

(Part 1: Fixpoints)

Class 4, Tuesday 10-05-2015, 5:10–7:00 PM, WWH–312

Patrick Cousot
pcousot@cs.nyu.edu  cs.nyu.edu/~pcousot
Objective of this class

• In this class, we justify the program analysis and verification methods that we have introduced informally so far:

  • Existence of least fixpoints of increasing functions (Tarski’s fixpoint theorem)

  • Application to deductive specifications

  • Galois connections

  • Fixpoint abstraction by a Galois connection

  • Iterative computation with convergence acceleration with widening/narrowing
Tarski fixpoint theorem
Fixpoint

• \( S \) set

• \( f \in S \rightarrow S \) function

• \( x \in S \) is a fixpoint of \( f \) iff \( f(x) = x \)

• A function may have no, one or many fixpoints

• If a function \( f \) has at least one fixpoint, it may or may not have a least fixpoint \( \text{lfp } f \) for a partial order \( \sqsubseteq \) such that
  
  • \( f(\text{lfp } f) = \text{lfp } f \)
  
  • If \( f(x) = x \) then \( \text{lfp } f \sqsubseteq x \)

• For different orders on \( S \), \( f \) may have different \( \text{lfp/gfp} \)
Example 1

- $F \in \mathbb{Z} \rightarrow \mathbb{Z}$
  - No fixpoint: $F(x) = x+1$
  - One fixpoint: $F(x) = 1$
  - Infinitely many fixpoints: $F(x) = x$

- $F \in \mathbb{N} \cup \{\infty\} \rightarrow \mathbb{N} \cup \{\infty\}$
  - $F(x) = x+1$ has one fixpoint (by defining $\infty + 1 = \infty$)
Example II: reachability equations in \( \mathbb{Z} \)

- \( P \triangleq 1x := 1; \text{while } ^2\text{true do } ^3x := (x + 1); \text{ od}^4. \)

\[
\begin{align*}
X_1 & = \mathbb{Z} \\
X_2 & = \{1\} \cup \{x + 1 \mid x \in X_3\} \\
X_3 & = X_2 \cap \{x \in \mathbb{Z} \mid \text{true}\} \\
X_4 & = X_2 \cap \{x \in \mathbb{Z} \mid \text{false}\}
\end{align*}
\]

- \( f(<X_1, X_2, X_3, X_4>) = <\mathbb{Z}, \{1\} \cup \{x+1 \mid x \in X_3\}, X_2, \emptyset> \)

- \( \text{lfp } f = <l_1, l_2, l_3, l_4> \) for componentwise \( \subseteq \) where

\[
\begin{align*}
l_1 & = \mathbb{Z} \\
l_2 & = \{z \in \mathbb{Z} \mid z > 0\} \\
l_3 & = \{z \in \mathbb{Z} \mid z > 0\} \\
l_4 & = \emptyset
\end{align*}
\]
Example: interval equations

- \( P \triangleq 1 x := 1 \); while \( 2 \) true \( do \) \( 3 x := (x + 1) \); od\(^4\).

\[
\begin{align*}
X_1 & = \{\min\_int, \max\_int\} \\
X_2 & = [1, 1] \sqcup \{X_3 = \emptyset ? \emptyset : \text{let } [a, b] = X_3 \text{ in} \\
& \quad \{\min(a + 1, \max\_int), \min(b + 1, \max\_int)\}\} \\
X_3 & = X_2 \cap \{\min\_int, \max\_int\} \\
X_4 & = X_2 \cap \emptyset
\end{align*}
\]

- \( f_1() = \text{INT}(\min\_int, \max\_int) \); \\
  \( f_2\ x_1\ x_3 = \text{join}(\text{INT}(1, 1)) (\text{add1}\ x_3) \); \\
  \( f_3\ x_2 = \text{meet}\ x_2 (\text{INT}(\min\_int, \max\_int)) \); \\
  \( f_4\ x_2 = \text{meet}\ x_2\ \text{EMPTY} \); \\
  \( f(x_1, x_2, x_3, x_4) = (f_1(), f_2\ x_1\ x_3, f_3\ x_2, f_4\ x_2) \);

- We would like to compute lfp\( f \) to get an interval invariant on \( x \) at each program point \( 1, 2, 3, \) and \( 4 \).
Poset

- A **poset** $<S, \sqsubseteq>$ is a set $S$ equipped with a partial order $\sqsubseteq$ (*reflexive* $\forall x \in S : x \sqsubseteq x$, *antisymmetric* $\forall x, y \in S : x \sqsubseteq y \land y \sqsubseteq x \implies x = y$, and *transitive* $\forall x, y, z \in S : x \sqsubseteq y \land y \sqsubseteq z \implies x \sqsubseteq z$)

- **Examples:**
  - $<\wp(S), \subseteq>$ (subsets of a set $S$ ordered by inclusion)
  - $<\mathbb{N}, \leq>$
  - $<\wp(\mathbb{Z}) \times \wp(\mathbb{Z}) \times \wp(\mathbb{Z}) \times \wp(\mathbb{Z}), \sqsubseteq>$ where, componentwise, $<x, y, z, t> \sqsubseteq <x', y', z', t'> \iff x \subseteq x' \land y \subseteq y' \land z \subseteq z' \land t \subseteq t'$
Complete lattice

• A complete lattice \(<S, \sqsubseteq>\) is a poset such that any subset \(X\) has a least upper bound (lub) \(\sqcup X \in S\) such that
  
  • \(\forall x \in X: x \sqsubseteq \sqcup X\)
  
  • \(\forall u \in S: (\forall x \in X: x \sqsubseteq u) \implies \sqcup X \sqsubseteq u\)
  
• It follows that \(<S, \sqsubseteq>\) has in infimum \(\bot \overset{\text{def}}{=} \sqcup \emptyset\), a supremum \(\top \overset{\text{def}}{=} \sqcup S\), and greatest lower bounds (glb)

\[\sqcap X \overset{\text{def}}{=} \sqcup \{ y \in S \mid \forall x \in X: y \sqsubseteq x \}\]

• Example: \(S\) is a set, its subsets \(<\wp(S), \subseteq, \emptyset, S, \cup, \cap>\) form a complete lattice. \(<\mathbb{N}, \leq>\) misses supremum!
Example: intervals $\mathcal{I}$

- $\mathcal{I} \overset{\text{def}}{=} \{\emptyset\} \cup \{[a, b] \mid a \in \mathbb{Z} \cup \{-\infty\} \land b \in \mathbb{Z} \cup \{+\infty\} \land a \leq b\}$

- **partial order** $\subseteq$: $\emptyset \subseteq \emptyset \subseteq [a, b]$

  $[a, b] \subseteq [c, d] \iff c \leq a \land b \leq d$

- **join** $\sqcup$: $\emptyset \sqcup x \overset{\text{def}}{=} x \sqcup \emptyset \overset{\text{def}}{=} x$

  $[a, b] \sqcup [c, d] \overset{\text{def}}{=} [\min(a, c), \max(b, d)]$

- **meet** $\sqcap$: $\emptyset \sqcap x \overset{\text{def}}{=} x \sqcap \emptyset \overset{\text{def}}{=} \emptyset$

  $[a, b] \sqcap [c, d] \overset{\text{def}}{=} \emptyset$

  \[\text{if } b < c \lor d < a\]

  \[\overset{\text{def}}{=} [\max(a, c), \min(b, d)]\]

  \[\text{otherwise}\]

- $<\mathcal{I}, \subseteq, \emptyset, [-\infty, +\infty], \sqcup, \sqcap> \text{ is a complete lattice}$
Cartesian product

- If <Li, ⊑i, ⊥i, Ti, ∪i, ∩i>, i ∈ Δ are complete lattices then 
  \(<\prod_{i \in Δ} Li, \sqsubseteq, \bot, T, \cup, \cap>\) is a complete lattice where

- \(\prod_{i \in Δ} x_i \sqsubseteq \prod_{i \in Δ} y_i \iff \forall i \in Δ: x_i \sqsubseteq y_i\)
- \(\bot \overset{\text{def}}{=} \prod_{i \in Δ} \bot_i\)
- \(T \overset{\text{def}}{=} \prod_{i \in Δ} T_i\)
- \(\prod_{i \in Δ} x_i \cup \prod_{i \in Δ} y_i \overset{\text{def}}{=} \prod_{i \in Δ} x_i \cup_i y_i\)
- \(\prod_{i \in Δ} x_i \cap \prod_{i \in Δ} y_i \overset{\text{def}}{=} \prod_{i \in Δ} x_i \cap_i y_i\)
- Example: environments mapping variables to intervals, invariants mapping program points to environments

All operations done componentwise
Increasing function

1. $f \in S \rightarrow S$ is increasing for $\subseteq$ iff

\[
\forall x, y \in S: x \subseteq y \implies f(x) \subseteq f(y)
\]
Componentwise increasing

• If $<L_i, \sqsubseteq_i>, i \in \Delta$ are posets

• $f_i \in \prod_{i \in \Delta} L_i \rightarrow L_i, i \in \Delta$ are $\sqsubseteq_i$-increasing

• $f \in \prod_{i \in \Delta} L_i \rightarrow \prod_{i \in \Delta} L_i$ is defined as

$$f(\prod_{i \in \Delta} x_i) \overset{\text{def}}{=} \prod_{i \in \Delta} f_i(\prod_{i \in \Delta} x_i)$$

$\implies f$ is $\sqsubseteq$-increasing (i.e. componentwise increasing)
Tarski’s fixpoint theorem

- Any increasing function \( f \in S \rightarrow S \) on a complete lattice \(<S, \subseteq, \bot, \top, \cup, \cap>\) has a least fixpoint \( \text{lfp} \ f \)
  
  - \( \text{lfp} \ f = \text{lfp} \ f \)
  
  - \( \forall x \in S: f(x) = x \implies \text{lfp} \ f \subseteq x \)

such that

- \( \text{lfp} \ f = \cap\{x \mid f(x) \subseteq x\} \)

if \( f(x) \subseteq x \) then \( x \) is called a post-fixpoint of \( f \)
Example

- \[
\begin{align*}
X_1 & = \mathbb{Z} \\
X_2 & = \{1\} \cup \{x+1 \mid x \in X_3\} \\
X_3 & = X_2 \cap \{x \in \mathbb{Z} \mid \text{true}\} \\
X_4 & = X_2 \cap \{x \in \mathbb{Z} \mid \text{false}\}
\end{align*}
\]

- \[f(<X_1,X_2,X_3,X_4>) = <\mathbb{Z}, \{1\} \cup \{x+1 \mid x \in X_2\}, X_2, X_2>\]

- \(f\) is componentwise increasing since \(X_1 \subseteq X'_1 \land X_2 \subseteq X'_2 \land X_3 \subseteq X'_3 \land X_4 \subseteq X'_4 \implies f(<X_1,X_2,X_3,X_4>) \subseteq f(<X'_1,X'_2,X'_3,X'_4>)\)

- \(\text{lfp} \ f\) exists and is

\[
\begin{align*}
l_1 & = \mathbb{Z} \\
l_2 & = \{z \in \mathbb{Z} \mid z > 0\} \\
l_3 & = \{z \in \mathbb{Z} \mid z > 0\} \\
l_4 & = \emptyset
\end{align*}
\]
Proof of Tarski’s fixpoint theorem

• Let \( a \overset{\text{def}}{=} \bigcap \{ x \mid f(x) \subseteq x \} \)

• if \( f(x) \subseteq x \) then \( a \subseteq x \)

\[
\begin{align*}
\implies f(a) &\subseteq f(x) \subseteq x \quad \text{since } f \text{ is increasing} \\
\implies f(a) &\subseteq \bigcap \{ x \mid f(x) \subseteq x \} = a \quad \text{by def. glb} \\
\implies f(f(a)) &\subseteq f(a) \quad \text{since } f \text{ is increasing} \\
\implies f(a) &\in \{ x \mid f(x) \subseteq x \} \\
\implies a &\overset{\text{def}}{=} \bigcap \{ x \mid f(x) \subseteq x \} \subseteq f(a) \quad \text{by def. glb} \\
\implies a &\overset{\text{antisymmetric}}{=} f(a)
\end{align*}
\]
Proof of Tarski’s fixpoint theorem (cont’d)

• if \( x = f(x) \) then \( x \in \{ x' \mid f(x') \subseteq x' \} \)

\[ \implies a = \cap \{ x' \mid f(x') \subseteq x' \} \subseteq x \]

• if follows that \( a = \text{lfp } f \)
Properties of increasing functions

- Any increasing function \( f \in S \rightarrow S \) on a complete lattice \(<S, \subseteq, \bot, \top, \cup, \cap>\) satisfies

\[
\bigcup_{i \in \Delta} f(x_i) \subseteq f\left(\bigcup_{i \in \Delta} x_i\right)
\]

- Proof:

\[
\forall j \in \Delta: x_j \subseteq \bigcup_{i \in \Delta} x_i \quad \text{def. lub}
\]

\[
\implies \forall j \in \Delta: f(x_j) \subseteq f\left(\bigcup_{i \in \Delta} x_i\right) \quad f \text{ increasing}
\]

\[
\implies \bigcup_{j \in \Delta} f(x_j) \subseteq f\left(\bigcup_{i \in \Delta} x_i\right) \quad \text{def. lub} \quad \square
\]
Duality

- If a statement holds for \(<S, \sqsubseteq, \bot, T, \cup, \cap, \rangle\) then the order-reversing dual statement with substitutions \(\sqsubseteq/\sqsupseteq, T/\bot, \bot/T, \cap/\cup, \cup/\cap, \min/\max, \max/\min, \text{lub/glb}, \text{glb/lub}, \ldots\) also holds.

- Examples:
  - The dual of \(<S, \sqsubseteq, \bot, T, \cup, \cap, \rangle\) is \(<S, \sqsupseteq, T, \bot, \cap, \cup, \rangle\).
  - The dual of « increasing » is « increasing ».
  - The dual of « an increasing \(f \in S \rightarrow S\) on \(<S, \sqsubseteq, \bot, T, \cup, \cap, \rangle\) satisfies \(\sqcup_{i \in \Delta} f(x_i) \sqsubseteq f(\sqcup_{i \in \Delta} x_i)\) » is « an increasing \(f \in S \rightarrow S\) on \(<S, \sqsubseteq, \bot, T, \cup, \cap, \rangle\) satisfies \(\sqcap_{i \in \Delta} f(x_i) \sqsupseteq f(\sqcap_{i \in \Delta} x_i)\) ».
Duality in Tarski’s fixpoint theorem

• Any increasing function $f \in S \rightarrow S$ on a complete lattice $<S, \sqsubseteq, \bot, T, \sqcup, \sqcap>$ has a greatest fixpoint $\text{gfp } f$

  • $f(\text{gfp } f) = \text{gfp } f$
  
  • $\forall x \in S: f(x) = x \implies x \sqsubseteq \text{gfp } f$

such that

• $\text{gfp } f = \sqcup \{x \mid x \sqsubseteq f(x)\}$
Fixpoint iteration
Continuity

• Let $f \in S \longrightarrow S$ be a function on a complete lattice $<S, \sqsubseteq, \bot, T, u, p>$

• $f$ is continuous if and only if for all increasing chains $x_0 \sqsubseteq x_1 \sqsubseteq \ldots \sqsubseteq x_n \sqsubseteq x_{n+1} \sqsubseteq \ldots$ we have

$$f(\bigcup_{i\in\mathbb{N}} x_i) = \bigcup_{i\in\mathbb{N}} f(x_i)$$

• Example:  

Counter-example:
Continuous $\Rightarrow$ increasing

- if $x \sqsubseteq y$ and $f$ continuous

  then $x \sqsubseteq y \sqsubseteq y \sqsubseteq y \sqsubseteq y \sqsubseteq \ldots$

  so $f(y) = f(x \uplus y) = f(x) \uplus f(y)$

  hence $f(x) \sqsubseteq f(y)$ so $f$ is increasing
Example

\[
\begin{align*}
X_1 &= \mathbb{Z} \\
X_2 &= \{1\} \cup \{x + 1 \mid x \in X_3\} \\
X_3 &= X_2 \cap \{x \in \mathbb{Z} \mid \text{true}\} \\
X_4 &= X_2 \cap \{x \in \mathbb{Z} \mid \text{false}\}
\end{align*}
\]

\[f(<X_1,X_2,X_3,X_4>) = <\mathbb{Z}, \{1\} \cup \{x+1 \mid x \in X_2\}, X_2, \emptyset>\]

\[f \text{ preserves arbitrary joins since} \]

\[f(\bigcup_{i \in \mathbb{N}} <X_1^i,X_2^i,X_3^i,X_4^i>) = \bigcup_{i \in \mathbb{N}} f(<X_1^i,X_2^i,X_3^i,X_4^i>)\]

\[(\text{where} \bigcup_{i \in \mathbb{N}} <X_1^i,X_2^i,X_3^i,X_4^i> = <\bigcup_{i \in \mathbb{N}} X_1^i, \bigcup_{i \in \mathbb{N}} X_2^i, \bigcup_{i \in \mathbb{N}} X_3^i, \bigcup_{i \in \mathbb{N}} X_4^i> \text{ componentwise})\]

\[\text{So } f \text{ is continuous}\]
Iterative fixpoint calculation

- Let \( f \in S \rightarrow S \) be a continuous function on a complete lattice \(<S, \subseteq, \bot, T, \cup, \cap>\). Then

\[
\text{lfp } f = \bigcup_{n \in \mathbb{N}} f^n(\bot)
\]

where

- \( f^0(x) = x \) and
- \( f^{n+1}(x) = f(f^n(x)) \).
Example

- \( X^0 = \langle X_1^0, X_2^0, X_3^0, X_4^0 \rangle = \langle \emptyset, \emptyset, \emptyset, \emptyset \rangle \)
- ...
- \( X^{2n} = \langle X_1^{2n}, X_2^{2n}, X_3^{2n}, X_4^{2n} \rangle = \langle \mathbb{Z}, \{1, \ldots, n\}, \{1, \ldots, n\}, \emptyset \rangle \)
  \( X^{2n+1} = \langle \mathbb{Z}, \{1, \ldots, n+1\}, \{1, \ldots, n\}, \emptyset \rangle \)
- ...
- \( \bigcup_{n \in \mathbb{N}} X^n = \bigcup_{n \in \mathbb{N}} X^{2n} \cup X^{2n+1} \)
  \( = \langle \mathbb{Z}, \{ n \in \mathbb{Z} \mid n > 0 \}, \{ n \in \mathbb{Z} \mid n > 0 \}, \emptyset \rangle \)
Proof 

• $\bigcup_{n \in \mathbb{N}} f^n(\bot)$ is a fixpoint since $\bot \subseteq f(\bot) \subseteq f(f(\bot)) \subseteq \ldots \subseteq f^n(\bot) \subseteq f^{n+1}(\bot) \subseteq \ldots$ so, by continuity, 

$$f\left(\bigcup_{n \in \mathbb{N}} f^n(\bot)\right) = \bigcup_{n \in \mathbb{N}} f(f^n(\bot)) = \bot \cup \bigcup_{n \in \mathbb{N}} f^{n+1}(\bot) = \bigcup_{n \in \mathbb{N}} f^n(\bot)$$

• if $f(x) = x$ then $\bot \subseteq x$. If $f^n(\bot) \subseteq x$ then $f^{n+1}(\bot) = f(f^n(\bot)) \subseteq f(x) = x$ since $f$ is continuous hence increasing

so $\bigcup_{n \in \mathbb{N}} f^n(\bot) \subseteq x$

proving $\text{lfp } f = \bigcup_{n \in \mathbb{N}} f^n(\bot)$
Fixpoint proof methods
Fixpoint induction

• Let $f \in S \rightarrow S$ be an increasing function on a complete lattice $\langle S, \subseteq, \perp, T, \cup, \sqcap \rangle$ and $P \in S$

• $\text{lfp } f \subseteq P \iff \exists I \in S : f(I) \subseteq I \land I \subseteq P$

• Proof

  • Soundness ($\Leftarrow$): $I \in \{x \in S \mid f(x) \subseteq x\}$ so, by Tarski, $\text{lfp } f = \sqcap\{x \in S \mid f(x) \subseteq x\} \subseteq I \subseteq P$

  • Completeness ($\Rightarrow$): take $I = \text{lfp } f$
Example (Turing/Floyd invariance proof method)

- \( P \triangleq 1 \text{x := 1 ; while } \text{true do } 3 \text{x := (x + 1) ; od} \).

- \( f(<X_1,X_2,X_3,X_4>) = <\mathbb{Z}, \{1\} \cup \{x+1|x \in X_3\}, X_2, \emptyset> \)

- Prove that \( \mathrm{lfp} \ f \subseteq <\mathbb{Z}, \mathbb{N}, \mathbb{N}^+, \emptyset> \)

- We have \( f(<\mathbb{Z}, \mathbb{N}, \mathbb{N}^+, \emptyset>) = <\mathbb{Z}, \mathbb{N}^+, \mathbb{N}, \emptyset> \nsubseteq <\mathbb{Z}, \mathbb{N}, \mathbb{N}^+, \emptyset> \)

- With an inductive invariant \( <\mathbb{Z}, \mathbb{N}^+, \mathbb{N}^+, \emptyset> \) we have

  \[ f(<\mathbb{Z}, \mathbb{N}^+, \mathbb{N}^+, \emptyset>) = <\mathbb{Z}, \mathbb{N}^+, \mathbb{N}^+, \emptyset> \subseteq <\mathbb{Z}, \mathbb{N}^+, \mathbb{N}^+, \emptyset> \]

  and \( <\mathbb{Z}, \mathbb{N}^+, \mathbb{N}^+, \emptyset> \subseteq <\mathbb{Z}, \mathbb{N}, \mathbb{N}^+, \emptyset> \)

- Proving \( \mathrm{lfp} \ f \subseteq <\mathbb{Z}, \mathbb{N}, \mathbb{N}^+, \emptyset> \)
Application to deductive specifications
Even numbers

- $0 \in E$ \hspace{1cm} \text{axiom}

- \[
\frac{n \in E}{n+2 \in E} \hspace{1cm} \text{rule of inference}
\]

- Can be understood as

\[
\emptyset \quad \{0\} \quad \{1\} \quad \{2\} \quad \{3\} \quad \ldots
\]

\[
0 \quad 2 \quad 3 \quad 4 \quad 5
\]

- $0 \ 2 \ 4$ is a proof that $4$ is even

- to prove $5$ is even, the only way is to prove $3$ is even, hence $1$ is even, which is impossible since not a conclusion of a rule
Deductive definition (specification)

- **U** universe
- **Set of rules** $R = \{ \frac{P_i}{c_i} \mid P_i \in \wp(U), c_i \in U, i \in \Delta \}$
- **Axioms:**
  - $\emptyset \Rightarrow c_i$
- **Inference rules:**
  - $\frac{P_i}{c_i}, P_i \neq \emptyset$
- **Proof of a:** $x_1 \ldots x_i \ x_{i+1} \ldots x_n = a$ such that
  - $\forall i \in [0,n]: \exists P \in R: P \subseteq \{x_1, \ldots, x_i\} \land x_{i+1} = c$
- **<U, R> defines** $S = \{a \mid \exists \text{ proof of } a\}$
Fixpoint definition

- From $X \subseteq U$ we can derive
  \[
  F(X) \overset{\text{def}}{=} \{ c \mid \exists P \subseteq X : \frac{P}{c} \in R \}
  \]
- if $X_i, i \in \Delta$ is an increasing chain then $F(\bigcup_{i \in \Delta} X_i) = \bigcup_{i \in \Delta} F(X_i)$ so $F$ continuous
- $F^n(\emptyset)$ is the set of elements which have a proof of length $n$ (proved by recurrence on $n$)
- So $\operatorname{lfp} F = \bigcup_{n \in \mathbb{N}} F^n(\emptyset) = \{ a \mid \exists \text{ proof of } a \} = S$
- Example: $E = \operatorname{lfp} \lambda X. \{ 0 \} \cup \{ n+2 \mid n \in X \}$ which iterates
  - $F^0(\emptyset) = \emptyset$, $F^1(\emptyset) = \{ 0 \}$, $F^2(\emptyset) = \{ 0, 2 \}$, $F^3(\emptyset) = \{ 0, 2, 4 \}$, etc
Fixpoint proof method

• Prove that even numbers are positive (with $U = \mathbb{Z}$)

• $F(\mathbb{N}) = \{0, 2, 3, 4, 5, \ldots\} \subseteq \mathbb{N}$

$\implies E = \text{lfp } F \subseteq \mathbb{N}$
THE END
Abstract Interpretation
(Part II: abstraction)

Class 05, Tuesday, 2015-10-13, 5:10–7:00, WWH–517

Patrick Cousot

pcousot@cs.nyu.edu  cs.nyu.edu/~pcousot
Galois connections
Galois connection

• Let \(<C, \sqsubseteq, \sqcup, \sqcap>\) and \(<A, \leq, \lor, \land>\) be posets (where the lub and glb may sometimes be undefined).

• A Galois connection is a pair \(<\alpha, \gamma>\) of functions

  • \(\alpha \in C \rightarrow A\), and

  • \(\gamma \in A \rightarrow C\), such that

  • \(\forall x \in C: \forall y \in A: \alpha(x) \leq y \iff x \sqsubseteq \gamma(y)\)

• Notation: \(<C, \sqsubseteq> \xrightleftharpoons[\alpha, \gamma]{} <A, \leq>\)
Example: Projection

• Let $S \overset{\text{def}}{=} L \times M$ (e.g. $L$ finite set of program points)

• $\alpha \in \wp(L \times M) \longrightarrow (L \longrightarrow \wp(M))$

• $\alpha(P) \overset{\text{def}}{=} \lambda \ell \cdot \{m \mid <\ell,m> \in P\}$

• $\gamma(Q) \overset{\text{def}}{=} \{<\ell,m> \mid m \in Q(\ell)\}$

• This is an isomorphism

\[
<\wp(L \times M), \subseteq> \xrightarrow{\gamma} <(L \longrightarrow \wp(M)), \subseteq> \xleftarrow{\alpha}
\]
Example: Cartesian abstraction

- Let $S \overset{\text{def}}{=} \prod_{i \in \Delta} M_i$

- $\alpha \in \mathcal{C}(\prod_{i \in \Delta} M_i) \longrightarrow \prod_{i \in \Delta} (\mathcal{C}(M_i))$

- $\alpha(X) \overset{\text{def}}{=} \prod_{i \in \Delta} \{ v \mid \exists x \in S : x[i \leftarrow v] \in X \}$
  
  where $x[i \leftarrow v]_i = v$ and $x[i \leftarrow v]_j = x_j$ when $i \neq j$

- $\gamma(Y) \overset{\text{def}}{=} \{ x \in \prod_{i \in \Delta} M_i \mid \forall i \in \Delta: x_i \in Y_i \}$
Example: interval abstraction

- \(<C, \subseteq> \overset{\text{def}}{=} <\wp(\mathbb{Z}), \subseteq>\)

- \(<A, \subseteq> \overset{\text{def}}{=} <\mathcal{I}, \subseteq>\)

- \(\mathcal{I} \overset{\text{def}}{=} \{\emptyset\} \cup \{[a, b] \mid a \in \mathbb{Z} \cup \{-\infty\} \land b \in \mathbb{Z} \cup \{+\infty\} \land a \leq b\}\)
  \(\emptyset \subseteq \emptyset \subseteq [a, b]\)
  \([a, b] \subseteq [c, d] \iff a \leq c \land b \leq d\)

- \(\alpha(\emptyset) \overset{\text{def}}{=} \emptyset \quad ([\min \emptyset, \max \emptyset] = [+\infty, -\infty] = \emptyset)\)
  \(\alpha(X) \overset{\text{def}}{=} \{\min X, \max X\}\)

- \(\gamma(\emptyset) \overset{\text{def}}{=} \emptyset\)
  \(\gamma([a, b]) \overset{\text{def}}{=} \{x \in \mathbb{Z} \mid a \leq x \leq b\}\)
Composition of Galois connections

- The composition of Galois connections

\[ \langle L, \subseteq \rangle \leftrightarrow \frac{\gamma_1}{\alpha_1} \quad \langle M, \subseteq \rangle \quad \text{and} \quad \langle M, \subseteq \rangle \leftrightarrow \frac{\gamma_2}{\alpha_2} \quad \langle N, \leq \rangle \]

is a Galois connection

\[ \langle L, \subseteq \rangle \leftrightarrow \frac{\gamma_1 \circ \gamma_2}{\alpha_2 \circ \alpha_1} \quad \langle N, \leq \rangle \]
Example: the abstraction for interval analysis

- \( \Lambda \overset{\text{def}}{=} \) finite set of program points
- \( \mathcal{X} \overset{\text{def}}{=} \) finite set of integer variables
- \( \mathcal{Z} \overset{\text{def}}{=} \) set of values of integer variables (e.g. \( \mathcal{Z} = \mathbb{Z} \) or \( \mathcal{Z} = [\text{min}_\text{int}, \text{max}_\text{int}] \))
- \( \mathcal{S} \overset{\text{def}}{=} \Lambda \times (\mathcal{X} \rightarrow \mathcal{Z}) \) states
  \(<\ell, \prod_{x \in \mathcal{X}} v_x> \in \mathcal{S} \) states that at program point \( \ell \), variable \( x \) has value \( v_x \in \mathcal{Z} \)
- \( \wp(\mathcal{S}) \) properties
  (set of possible values of variables at each program point)
Example: the abstraction for interval analysis

• Projection on program points

\[ \varphi(\Lambda x (x \rightarrow \mathbb{3})) \xrightarrow{\alpha_p} (\Lambda \rightarrow \varphi(x \rightarrow \mathbb{3})) \]

\[ \alpha_p(P) \overset{\text{def}}{=} \lambda \ell \cdot \{ \rho \mid <\ell, \rho > \in P \} \quad (\rho \text{ environment}) \]

• Cartesian abstraction on variables

\[ \varphi(x \rightarrow \mathbb{3}) \xrightarrow{\alpha_c} \prod_{x \in X} \varphi(\mathbb{3}) \]

\[ \alpha_c(X) \overset{\text{def}}{=} \prod_{x \in X} \{ v \in \mathbb{3} \mid \exists \rho \in X \rightarrow \mathbb{3} : \rho[x \leftarrow v] \in X \} \]

• Interval abstraction on integer values

\[ \varphi(\mathbb{3}) \xrightarrow{\alpha_i} \mathbb{I} \]

\[ \alpha_i(X) \overset{\text{def}}{=} [\min X, \max X] \quad (\emptyset \text{ when } X = \emptyset) \]
Example: the abstraction for interval analysis

- The interval abstraction of program properties is

\[ \wp(\Lambda \times (\mathcal{X} \rightarrow \mathcal{I})) \rightarrow (\Lambda \rightarrow \prod_{x \in \mathcal{X}} \mathcal{I}) \]

\[ \alpha(P) \overset{\text{def}}{=} \lambda \ell \cdot \prod_{x \in \mathcal{X}} \alpha_i(\alpha_c(\alpha_p(P)_\ell)_x) \]

\[ = \lambda \ell \cdot \prod_{x \in \mathcal{X}} \text{let } X =\{v \in \mathcal{I} \mid \exists \rho \in \mathcal{X} \rightarrow \mathcal{I} : \rho[x \leftarrow v] \in \{\rho \mid <\ell, \rho> \in P\}\} \text{ in } [\min X, \max X] \]

- This is a Galois connection

\[ <\wp(\Lambda \times (\mathcal{X} \rightarrow \mathcal{I})), \subseteq> \overset{\gamma}{\leftrightarrow} <(\Lambda \rightarrow \prod_{x \in \mathcal{X}} \mathcal{I}), \subseteq> \]

where \( \subseteq \) is interval inclusion for each variable and each program point
Properties of Galois connections
One adjoint determines the other

- $\alpha(x)$
  
  \[
  = \bigwedge \{ y \in A \mid \alpha(x) \leq y \}
  = \bigwedge \{ y \in A \mid x \subseteq \gamma(y) \}
  \]

  since $\alpha(x) \leq y \iff x \subseteq \gamma(y)$

- $\gamma(y)$
  
  \[
  = \bigvee \{ x \in C \mid x \subseteq \gamma(y) \}
  = \bigvee \{ x \in C \mid \alpha(x) \leq y \}
  \]

  since $\alpha(x) \leq y \iff x \subseteq \gamma(y)$

- So given $\gamma/\alpha$ there is a unique corresponding $\alpha/\gamma$
\( \alpha \text{ is increasing} \)

- \( \alpha(x) \preceq \alpha(x) \implies x \subseteq \gamma(\alpha(x)) \)
- \( \alpha(\gamma(y)) \preceq y \iff \gamma(y) \subseteq \gamma(y) \)
- \( x \subseteq y \)

\[ \implies x \subseteq y \subseteq \gamma(\alpha(y)) \]

\[ \implies \alpha(x) \preceq \alpha(y) \]

\( \gamma \circ \alpha \) extensive

\( \alpha \circ \gamma \) reductive

\( \alpha \) increasing
α preserves existing joins

- Assume that $X \subseteq C$ and $\sqcup X$ does exists in $C$
- We show that $\alpha^\triangleright(X) = \{\alpha(x) \mid x \in X\}$ has a lub in $A$ which is $\alpha(\sqcup X)$
  - $\alpha(\sqcup X)$ is an upper bound of $\alpha^\triangleright(X)$

  \[
  \forall x \in X: \quad x \subseteq \sqcup X
  \]

  \[
  \implies \forall x \in X: \quad \alpha(x) \leq \alpha(\sqcup X) \quad \alpha \text{ increasing}
  \]

  \[
  \implies \alpha(\sqcup X) \text{ is an upper bound of } \alpha^\triangleright(X)
  \]

\[
\alpha^\triangleright(X) \triangleq \{\alpha(x) \mid x \in X\}
\]
\( \alpha \) preserves existing joins (cont’d)

- \( \alpha(\sqcup X) \) is the least upper bound

\[
\text{assume } \forall x \in X: \alpha(x) \preceq u \implies x \subseteq \gamma(u) \\
\implies \sqcup X \subseteq \gamma(u) \\
\implies \alpha(\sqcup X) \preceq u
\]

so \( \alpha(\sqcup X) = \bigvee \alpha\downarrow(X) \) (lub in A)
Duality

• The dual of \( \langle C, \sqsubseteq \rangle \xleftrightarrow{\gamma} \langle A, \sqsubseteq \rangle \) that is

\[
\forall x \in C: \forall y \in A: \alpha(x) \leq y \iff x \sqsubseteq \gamma(y)
\]

is

\[
\forall x \in C: \forall y \in A: \alpha(x) \geq y \iff x \sqsupseteq \gamma(y)
\]

that is \( \langle C, \sqsupseteq \rangle \xleftrightarrow{\gamma} \langle A, \sqsupseteq \rangle \)

or

\[
\forall y \in A: \forall x \in C: \gamma(y) \sqsubseteq x \iff y \leq \alpha(x)
\]

that is \( \langle A, \sqsubseteq \rangle \xleftrightarrow{\alpha} \langle C, \sqsubseteq \rangle \)

• Examples: \( \alpha \) is increasing \( \implies \) \( \gamma \) is increasing

\( \alpha \) preserves existing joins \( \implies \) \( \gamma \) preserves existing meets
Equivalent definition

- \(<C, \sqsubseteq> \iff <A, \preceq>

1. \(\forall x \in C: \alpha(x) \preceq \alpha(x) \implies x \sqsubseteq \gamma(\alpha(x))\)

2. \(\forall y \in A: \alpha(\gamma(y)) \preceq y\) by duality

3. \(x \sqsubseteq x' \implies x \sqsubseteq \gamma(\alpha(x')) \implies \alpha(x) \sqsubseteq \alpha(x')\)

4. \(\gamma\) increasing by duality

- Reciprocally
  
  - \(\alpha(x) \preceq y \implies \gamma(\alpha(x)) \sqsubseteq \gamma(y) \implies x \sqsubseteq \gamma(y)\)
  
  - \(x \sqsubseteq \gamma(y) \implies \alpha(x) \preceq \alpha(\gamma(y)) \implies \alpha(x) \preceq y\) i.e. by duality
\[ \alpha \circ \gamma \circ \alpha = \alpha \]

- \( \forall x \in C: x \subseteq \gamma(\alpha(x)) \implies \alpha(x) \leq \alpha(\gamma(\alpha(x))) \) \( \alpha \) increasing
- \( \forall y \in A: \alpha(\gamma(y)) \leq y \implies \alpha(\gamma(\alpha(x))) \leq \alpha(x) \) for \( y = \alpha(x) \)
- \( \forall x \in C: \alpha(x) = \alpha(\gamma(\alpha(x))) \) by antisymmetry

\[ \gamma \circ \alpha \circ \gamma = \gamma \] by duality
Galois retraction

- \(<C, \sqsubseteq> \xrightarrow{\gamma} <A, \sqsubseteq>\) and \(\alpha\) surjective (onto)

written \(<C, \sqsubseteq> \xrightarrow{\gamma} <A, \sqsubseteq>\)

- iff \(\forall y \in A: \alpha \circ \gamma(y) = y\)

Proof

- \((\Rightarrow)\) If \(y \in A: \exists x \in C: \alpha(x) = y\), so \(\alpha \circ \gamma(y) = \alpha \circ \gamma(\alpha(x)) = \alpha(x) = y\)

- \((\Leftarrow)\) Reciprocally, \(\forall y \in A: \exists x \in C: \alpha(x) = y\), choosing \(x = \gamma(y)\) \(\Box\)
Function abstraction
Analysis and verification problems

- Let $f \in S \rightarrow S$ be an increasing function on a complete lattice $<S, \subseteq, \perp, T, \cup, \cap>$

- **Analysis problem:** compute $P \in S$ such that $\text{lfp } f \subseteq P$
  - Ideally, $P = \text{lfp } f$ but $\text{lfp } f$ may not be computable (undecidability)

- **Verification problem:** given $f$ and $P$, check that $f(P) \subseteq P$
  (which by Tarski implies that $\text{lfp } f \subseteq P$)
  - $P$ might not be inductive that is $\text{lfp } f \subseteq P$ but $f(P) \subseteq P$
  so we/are back to the analysis problem, calculate $I \in S$: $f(I) \subseteq I \land I \subseteq P$
General idea

- Abstract/simplify \( f \in S \longrightarrow S \) into \( f^\# \in S^\# \longrightarrow S^\# \) such that:
  - \( f^\# \) is computable
  - a \( P^\# \) is computable such that \( \text{lfp } f^\# \preceq P^\# \)
  - \( P \) can be derived from \( P^\# \) such that \( \text{lfp } f \subseteq P \)
- We are back to the same problem by in a hopefully simpler world \( S^\# \) instead of \( S \)
- We can use a galois connection:
  \[
  \langle S, \subseteq \rangle \overset{\gamma}{\iff} \langle S^\#, \preceq \rangle \overset{\alpha}{\iff} \]

Intuition for function abstraction

\[ f \]
Higher-order Galois connection

- $f \in S \rightarrow S$, increasing
- $f^\# \in S^\# \rightarrow S^\#$, increasing
- A Galois connection on arguments and results
  \[ \langle S, \subseteq \rangle \leftrightarrow \begin{array}{c} \gamma \\alpha \end{array} \langle S^\#, \preceq \rangle \]
  can be lifted to increasing functions
  \[ \langle S \rightarrow S, \subseteq \rangle \leftrightarrow \begin{array}{c} \dot{\gamma} \\dot{\alpha} \end{array} \langle S^\# \rightarrow S^\#, \preceq \rangle \]
  for the pointwise ordering $f \preceq g \iff \forall x: f(x) \leq g(x)$

with $\dot{\alpha} = \lambda f \cdot \alpha \circ f \cdot \gamma$ and $\dot{\gamma} = \lambda f^\# \cdot \gamma \circ f^\# \circ \alpha$
Proof

• $\alpha(f) \preceq f^#$

$\iff \lambda f \cdot \alpha \circ f \circ \gamma(f) \preceq f^#$  \hspace{1cm} \text{def. } \alpha \cdot$

$\iff \alpha \circ f \circ \gamma \preceq f^#$  \hspace{1cm} \text{def. } \lambda$-application

$\iff \forall y: \alpha(f(\gamma(y))) \preceq f^#(y)  \hspace{1cm} \text{pointwise def. } \preceq \text{ and } \circ$

$\iff \forall y: f(\gamma(y)) \sqsubseteq \gamma(f^#(y))  \hspace{1cm} \text{Galois connection}$

$\implies \forall x: f(\gamma(\alpha(x))) \sqsubseteq \gamma(f^#(\alpha(x)))  \hspace{1cm} \text{for } y = \alpha(x)$

$\implies \forall x: f(x) \sqsubseteq \gamma(f^#(\alpha(x)))  \hspace{1cm} \text{since } x \sqsubseteq \gamma(\alpha(x)), f \text{ increasing}$

$\iff f \sqsubseteq \lambda f^# \cdot \gamma \circ f^# \circ \alpha(f^#) = \gamma(f^#)  \hspace{1cm} \text{def. } \sqsubseteq, \circ, \text{ and } \lambda$-app.
Reciprocally

- \( f \sqsubseteq \hat{\gamma}(f^\#) \)

\[
\iff \forall x: f(x) \sqsubseteq \gamma(f^\#(\alpha(x))) \quad \text{as proved above}
\]

\[
\implies \forall y: f(\gamma(y)) \sqsubseteq \gamma(f^\#(\alpha(\gamma(y))))
\]

\[
\iff \forall y: \alpha(f(\gamma(y))) \preceq f^\#(\alpha(\gamma(y)))
\]

\[
\implies \forall y: \alpha(f(\gamma(y))) \preceq f^\#(y) \quad \text{by } \alpha(\gamma(y)) \preceq y, f^\# \text{ increasing}
\]

\[
\iff \alpha \circ f \circ \gamma \preceq f^#
\quad \text{def. } \preceq, \circ, \text{ and } \lambda\text{-app.} \quad \square
\]
Fixpoint Abstraction
Exact fixpoint abstraction

- Let \( f \in S \to S \) be an continuous function on a complete lattice \(<S, \subseteq, \bot, \top, \cup, \cap>\) and a Galois retraction \(<S, \subseteq> \xrightarrow{\gamma} <S^\#, \preceq>\).

Assume that \( f^\# \in S^\# \to S^\# \) satisfies \( \alpha \circ f = f^\# \circ \alpha \).

Then

- \( f^\# = \alpha \circ f \circ \gamma \)
- \( \alpha(\text{lfp } f) = \text{lfp } f^\# = \bigvee_{n \in \mathbb{N}} f^{\#n}(\alpha(\bot)) \)
- Note: \( f^\# \) is not assumed to be continuous.
Idea of the proof

- The abstract iterates are the abstraction of the concrete iterates

\[
\bigcup_{n \in \mathbb{N}} f^n(\bot) \xrightarrow{\alpha} \bigvee_{n \in \mathbb{N}} f^#(\alpha(\bot))
\]

Limit: \(\alpha\) preserves lubs

Induction step: commutation
\(\alpha \circ f = f^# \circ \alpha\)

Basis

New York University, CIMS, Graduate Division, Computer Science, Course CSCI-GA.3033-005-2015, Principles of Software Security
Proof

• $\alpha \circ f = f^\# \circ \alpha \implies \alpha \circ f \circ \gamma = f^\# \circ \alpha \circ \gamma = f^\#$ (retraction)

• $f^\#$ is increasing (composition of increasing functions)

• $\alpha(\text{lfp } f) = \alpha(f(\text{lfp } f)) = f^\#(\alpha(\text{lfp } f))$ by $\alpha \circ f = f^\# \circ \alpha$

  so $\alpha(\text{lfp } f)$ is a fixpoint of $f^\#$

• We have $\text{lfp } f = \bigsqcup_{n \in \mathbb{N}} f^n(\bot)$ since $f$ is continuous

• $f^\#^0(\alpha(\bot)) = \alpha(\bot) = \alpha(f^0(\bot))$ is the infimum of $<S^\#, \preceq>$

• Assume by induction hypothesis that $f^\#^n(\alpha(\bot)) = \alpha(f^n(\bot))$
Proof

• $f^{#n+1}(\alpha(\bot)) = f^#(f^{#n}(\alpha(\bot))) = f^#(\alpha(f^{n}(\bot))) = \alpha(f(f^{n}(\bot))) = \alpha(f^{n+1}(\bot))$ by $\alpha \circ f = f^# \circ \alpha$

• $\alpha(lfp \ f) = \alpha(\bigcup_{n \in \mathbb{N}} f^n(\bot)) = \bigvee_{n \in \mathbb{N}} \alpha(f^n(\bot)) = \bigvee_{n \in \mathbb{N}} f^{#n}(\alpha(\bot))$

• if $f^#(y) = y$ is a fixpoint of $f^#$
  
  • $\alpha(\bot) \leq y$ since $\alpha(\bot)$ is the infimum of $<S^#, \leq>$
  
  • $f^{#n}(\alpha(\bot)) \leq y$ induction hypothesis

  \[ \iff f^{#n+1}(\alpha(\bot)) = f^#(f^{#n}(\alpha(\bot))) \leq f^#(y) = y \quad \text{f# increas.} \]

  • $\alpha(lfp \ f) = \bigvee_{n \in \mathbb{N}} f^{#n}(\alpha(\bot)) \leq y$ def. lub

• $\alpha(lfp \ f) = lfp \ f^#$ \hfill $\square$
Applicable to interval analysis?

- \( f(X) = X \cap \{0\} \)

- Assume \( \exists f^\#: \alpha \circ f = f^\# \circ \alpha \) then \( f^\# = \alpha \circ f \circ \gamma \) so
  
  \[
  f^\#([a,b]) = \alpha \circ f \circ \gamma ([a,b]) = \alpha \circ f (\{x \mid a \leq x \leq b\}) = \alpha ((0 \in [a,b]? \{0\}:\emptyset)) = (0 \in [a,b]?[0,0]:\emptyset)
  \]

- But then for \( X = \{-1,1\} \) we have \( \alpha \circ f \neq f^\# \circ \alpha \) since
  
  - \( \alpha \circ f(X) = \alpha (\emptyset) = \emptyset \)
  
  - \( f^\# \circ \alpha (X) = f^\#([-1,1]) = [0,0] \)

  a contradiction!
The End
Abstract Interpretation
(Part III: fixpoint approximation)

Class 07, Friday 2015-10-16, 5:10–7:00, WWH–517

Patrick Cousot
pcousot@cs.nyu.edu  cs.nyu.edu/~pcousot
Fixpoint approximation
Fixpoint approximation

- Let $f \in S \rightarrow S$ be an increasing function on a complete lattice $\langle S, \subseteq, \bot, T, \cup, \cap \rangle$ and a Galois connection

  $\langle S, \subseteq \rangle \xleftrightarrow[\gamma, \alpha] \langle S^\#, \preceq \rangle$.

Assume that $f^\# \in S^\# \rightarrow S^\#$ is increasing and satisfies

$$\forall x \in S: \alpha \circ f(x) \preceq f^\# \circ \alpha(x).$$

Then

- $\forall y \in S^\#: f \circ \gamma(y) \subseteq \gamma \circ f^\#(y)$ and reciprocally
- $\alpha(\text{lfp } f) \preceq \text{lfp } f^\#$
Idea of the proof

- The abstract iterates over-approximate the abstraction of the concrete iterates.

Limit: \( \alpha \) preserves lubs

Induction step: commutation
\( \alpha \circ f \subseteq f \# \circ \alpha \) & \( f \# \) increasing

Basis
Proof

• \( \alpha \circ f(x) \leq f^\# \circ \alpha(x) \)

\[\implies \alpha \circ f \circ \gamma(y) \leq f^\# \circ \alpha \circ \gamma(y) \leq f^\#(y) \quad \text{Gc & } f^\# \text{ increasing} \]

\[\implies f \circ \gamma(y) \subseteq \gamma \circ f^\#(y) \quad \text{Gc} \]

• Reciprocally

\[f \circ \gamma(y) \subseteq \gamma \circ f^\#(y) \]

\[\implies f \circ \gamma \circ \alpha(x) \subseteq \gamma \circ f^\# \circ \alpha(x) \quad \text{for } y = \alpha(x) \]

\[\implies f(x) \subseteq \gamma \circ f^\# \circ \alpha(x) \quad \text{Gc & } f \text{ increasing} \]

\[\implies \alpha \circ f(x) \leq f^\# \circ \alpha(x) \quad \text{Gc} \]
Proof (cont’d)

• \( \forall y \in S^\#: f \circ \gamma(y) \subseteq \gamma \circ f^\#(y) \)

\[ \implies f \circ \gamma(lfp f^\#) \subseteq \gamma \circ f^\#(lfp f^\#) = \gamma(lfp f^\#) \]

\[ \implies \gamma(lfp f^\#) \in \{x \mid f(x) \subseteq x\} \]

\[ \implies lfp f = \bigcap\{x \mid f(x) \subseteq x\} \subseteq \gamma(lfp f^\#) \quad \text{Tarski, def. glb} \]

\[ \implies \alpha(lfp f) \preceq lfp f^\# \quad \text{Gc} \quad \square \]
Example: incrementation for intervals

• \( f \in \wp([\text{min\_int}, \text{max\_int}]) \rightarrow \wp([\text{min\_int}, \text{max\_int}]) \)

\[
f(X) \overset{\text{def}}{=} \{x+1 \in [\text{min\_int}, \text{max\_int}] \mid x \in X\}
\]

(if \( X \) is the set of possible values of variable \( x \) before assignment \( x := x+1 \), then \( f(X) \) is the set of possible values of variable \( x \) after this assignment, usually written \( \text{post}[[x := x+1]] X \))

• \( \alpha(X) \overset{\text{def}}{=} [\text{min } X, \text{max } X] \)  
  \( (\emptyset \text{ when } X = \emptyset) \)
Example: incrementation for intervals

- \( \min f(X) \) where \( X \in P([\min_{\text{int}}, \max_{\text{int}}]) \setminus \{\emptyset\} \)
  
  \[
  = \min \{x+1 \in [\min_{\text{int}}, \max_{\text{int}}] | x \in X \}
  
  = \min \left( \min \{x+1 \in [\min_{\text{int}}, \max_{\text{int}}] | x \in X \setminus \{\max_{\text{int}}\}, \min \{x+1 \in [\min_{\text{int}}, \max_{\text{int}}] | x \in X \cap \{\max_{\text{int}}\} \right) 
  
  \text{since } X = (X \setminus \{\max_{\text{int}}\}) \cup (X \cap \{\max_{\text{int}}\})
  
  = \min \left( \min \{x+1 | x \in X \setminus \{\max_{\text{int}}\}, (\max_{\text{int}} \in X ? \min \emptyset : \min \emptyset) \right) \text{ where } \min \emptyset = +\infty
  
  = \min \left( \min \{x+1 | x \in X \setminus \{\max_{\text{int}}\}, +\infty \right)
  
  = \min \{x+1 | x \in X \setminus \{\max_{\text{int}}\}\}
  
  = \min(X \setminus \{\max_{\text{int}}\}) + 1\]
Example: incrementation for intervals

- \( \max f(X) \) where \( X \in \wp([\text{min\_int}, \text{max\_int}]) \setminus \{\emptyset\} \)

\[
= \max \{ x+1 \in [\text{min\_int}, \text{max\_int}] \mid x \in X \}
= \max ( \max \{ x+1 \in [\text{min\_int}, \text{max\_int}] \mid x \in X \setminus \{\text{max\_int}\} \}, \max \{ x+1 \in [\text{min\_int}, \text{max\_int}] \mid x \in X \cap \{\text{max\_int}\} \}) \quad \text{since } X = (X \setminus \{\text{max\_int}\}) \cup (X \cap \{\text{max\_int}\})
= \max ( \max \{ x+1 \mid x \in X \setminus \{\text{max\_int}\} \}, -\infty ) \quad \text{max } \emptyset = -\infty
= \max \{ x+1 \mid x \in X \setminus \{\text{max\_int}\} \}
= \max (X \setminus \{\text{max\_int}\}) + 1
\leq (\max (X) = \text{max\_int} \quad ? \quad \text{max\_int} : \max (X) + 1) \)
Example: incrementation for intervals

- \( \alpha \circ f(X) \)

Where \( X \in \varnothing([\min\_\text{int}, \max\_\text{int}]) \)

\[
\begin{align*}
\alpha \circ f(X) &= (f(X) = \varnothing \ ? \ \varnothing : [\min f(X), \max f(X)]) \\
&= (X = \varnothing \lor X = \{\max\_\text{int}\} \ ? \ \varnothing : [\min f(X), \max f(X)]) \\
&= (X = \varnothing \lor X = \{\max\_\text{int}\} \ ? \ \varnothing : [\min(X \setminus \{\max\_\text{int}\}) + 1, \max f(X)]) \\
&= (X = \varnothing \lor X = \{\max\_\text{int}\} \ ? \ \varnothing : [\min(X) + 1, \max f(X)]) \\
\end{align*}
\]

Since \( X \neq \{\max\_\text{int}\} \) implies \( \min(X) = \min(X \setminus \{\max\_\text{int}\}) \)

\[
\begin{align*}
\subseteq & (X = \varnothing \lor X = \{\max\_\text{int}\} \ ? \ \varnothing : [\min(X) + 1, (\max (X) = \max\_\text{int} \ ? \ \max\_\text{int} : \max (X) + 1)]) \\
\end{align*}
\]

.../...
Example: incrementation for intervals

\[(X = \emptyset \lor X = \{\text{max\_int}\} \quad \emptyset : [\min(X)+1, (\max(X) = \text{max\_int} \quad \text{max\_int} : \max(X) +1)])\]

\[= (\alpha(X) = \emptyset \lor \alpha(X) = \{\text{max\_int}\} \quad \emptyset : \text{let } \alpha(X) = [a,b'] \text{ in } a +1, (b' = \text{max\_int} \quad \text{max\_int} : b' +1))\]

\[= (\alpha(X) = \emptyset \lor \alpha(X) = [\text{max\_int}, \text{max\_int}] \quad \emptyset : \text{let } [a,b'] = \alpha(X) \text{ in let } b = \min(b', \text{max\_int}-1) \text{ in } [a+1, b+1])\]

\[= f^# \circ \alpha(X)\]

so

\[f^#(Y) \overset{\text{def}}{=} (Y = \emptyset \lor Y = [\text{max\_int}, \text{max\_int}] \quad \emptyset : \text{let } [a,b'] = Y \text{ in let } b = \min(b', \text{max\_int}-1) \text{ in } [a+1, b+1])\]
Example: incrementation for intervals

- The abstraction cannot be precise

- Counter-example:
  \[ X = \{0, \text{max}_\text{int}\} \text{ so } f(X) = \{1\} \text{ and } \alpha \circ f(X) = [1,1] \]
  but
  \[ f'(\alpha(X)) = f'([0, \text{max}_\text{int}]) = [1, \text{max}_\text{int}] \]
  since intervals cannot make the distinction between \(\{0, \text{max}_\text{int}\}\) and \(\{0,1,2,...,\text{max}_\text{int}-1,\text{max}_\text{int}\}\)
Example: incrementation for intervals

- \( f^\#(Y) \overset{\text{def}}{=} (Y = \emptyset \lor Y = [\text{max}\_\text{int}, \text{max}\_\text{int}]?) \emptyset : \text{let } [a, b'] = Y \text{ in let } b = \min (b', \text{max}\_\text{int} - 1) \text{ in } [a + 1, b + 1] \)

is more precise than

- \( g^\#(X_3) = (X_3 = \emptyset ? \emptyset : \text{let } [a, b] = X_3 \text{ in } [\min(a + 1, \text{max}\_\text{int}), \min(b + 1, \text{max}\_\text{int})]) \)

which is also correct since

- \( \alpha \circ f(X) \subseteq f^\# \circ \alpha(X) \subseteq g^\# \circ \alpha(X) \)

where \( \subseteq \) is the partial order on intervals.
Also imprecise for tests!

- \( f(X) = X \cap \{0\} \) where \( X \in \wp(\mathbb{Z}) \)

- \( \alpha \circ f(X) \)

\[
\begin{align*}
= & \text{ if } f(X)=\emptyset \text{ then } \emptyset \text{ else } [\min X \cap \{0\}, \max X \cap \{0\}] \\
= & (X=\emptyset \lor 0 \not\in X \mid \emptyset : [\min \{0\}, \max \{0\}]) \\
= & (X = \emptyset ? \emptyset : (0 \not\in X ? \emptyset : [0,0])) \\
\leq & (\alpha(X)=\emptyset ? \emptyset : \text{let } [a,b]=\alpha(X) \text{ in } (0\not\in[a,b] ? \emptyset : [0,0])) \\
= & (\alpha(X)=\emptyset ? \emptyset : \text{let } [a,b]=\alpha(X) \text{ in } (a>0 \lor b<0 ? \emptyset : [0,0])) \\
= & f\# \circ \alpha(X)
\end{align*}
\]
Also imprecise for tests!

- $f(X) = X \cap (\mathbb{Z} / \{0\})$ where $X \in \wp(\mathbb{Z})$

- $f^\#(Y) \overset{\text{def}}{=} (Y=\emptyset \ ? \ \emptyset : \text{let } [a,b]=Y \text{ in } (a=b=0 \ ? \ \emptyset : a=0 \ ? [1,b] : b=0 \ ? [a,-1] : [a,b] ) )$

- For the test if $x = 0$ then ... else ... we get imprecision on both branches
The End
Abstract Interpretation
(Part IV: convergence acceleration)

Class 8, Monday 10-19-2015, 5:10–7:00, WWH–312

Patrick Cousot
pcousot@cs.nyu.edu  cs.nyu.edu/~pcousot
Convergence acceleration
Intervals do not satisfy the ascending chain condition

- $\implies$ fixpoint iteration may not converge
General idea

- Iterate $f$ up from $\bot$ with widening $\triangledown$ to over-approximate lfp $f$ to a s.t. $f(a) \subseteq a$ and improve by iterating down from $a$ with narrowing $\Delta$

- Dual holds for gfp using dual widening and dual narrowing (flip figure upside down)
Intuition for widening

\[ x^2 = x^1 \nabla f(x^1) \]

\[ x^1 = x^0 \nabla f(x^0) \]

Extrapolation

\[ f(x^2) \]

\[ f(x^1) \]

\[ f(x^0) \]
Intuition for narrowing

\[ x^1 = x^0 \Delta f(x^0) \]
\[ x^2 = x^1 \nabla f(x^1) \]

Interpolation
# Duality

<table>
<thead>
<tr>
<th>Iteration</th>
<th>Iteration starts from</th>
<th>Iteration stabilizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widening</td>
<td>( \nabla ) below</td>
<td>above</td>
</tr>
<tr>
<td>Narrowing</td>
<td>( \Delta ) above</td>
<td>above</td>
</tr>
<tr>
<td>Dual widening</td>
<td>( \tilde{\nabla} ) above</td>
<td>below</td>
</tr>
<tr>
<td>Dual narrowing</td>
<td>( \tilde{\Delta} ) below</td>
<td>below</td>
</tr>
</tbody>
</table>

Observe that the static analysis time does not depend at all upon the number of iterations in the concrete execution of the while-loop.
Convergence acceleration: widening
Iteration with widening (I)

• **Iteration for** \( f \in S \rightarrow S \) (continuous on \( <S, \sqsubseteq> \)):
  \[ \bot, f(\bot), f^2(\bot), \ldots, f^n(\bot), f^{n+1}(\bot), \ldots, \bigcup_{n \in \mathbb{N}} f^n(\bot) = \text{lfp } f \]

• **Iteration for** \( f \) (increasing) **with widening** \( \triangledown \):
  \[
  f^0 \overset{\text{def}}{=} \bot,
  f^1 \overset{\text{def}}{=} \bot \triangledown f(\bot) = f(\bot),
  f^2 \overset{\text{def}}{=} f^1 \triangledown f(f^1),
  \\
  \ldots,
  f^{n+1} \overset{\text{def}}{=} f^n \triangledown f(f^n), \text{ when } f(f^\ell) \nsubseteq f^\ell
  \\
  \ldots,
  f^{\ell+1} \overset{\text{def}}{=} f^\ell \text{ when } f(f^\ell) \subseteq f^\ell
  \]
Iteration with widening (II)

- This is equivalent to

\[ f^0 \overset{\text{def}}{=} \bot, \]

\[ \ldots, \]

\[ f^{n+1} \overset{\text{def}}{=} f^n \triangleright' f(f^n) \]

\[ \ldots, \]

\[ f^{\ell+1} = f^{\ell} \]

where

\[ x \triangleright' y \overset{\text{def}}{=} \left( f(y) \sqsubseteq y \quad ? \quad y : x \triangleright y \right) \]
Widening

- $\nabla \in S \times S \rightarrow S$ such that

1. $\forall x, y \in S: x \subseteq x \nabla y$

2. $\forall x, y \in S: y \subseteq x \nabla y$

3. For any increasing chain $y_0 \subseteq y_1 \subseteq \ldots \subseteq y_n \subseteq y_{n+1} \subseteq \ldots$, the sequence $x_0 \overset{\text{def}}{=} y_0, \ldots, x_{n+1} \overset{\text{def}}{=} x_n \nabla y_n, \ldots$ is ultimately stationary (that is $\exists \ell: \forall n \geq \ell: x_n = x^{\ell}$)
Example: refined widening for intervals

- $\emptyset \triangledown x = x \triangledown \emptyset = x$

- $[a,b] \triangledown [c,d] =$

$$
\left( \begin{array}{c}
\begin{array}{c}
1 \leq c < a \quad ? \quad 1 : 0 \leq c < a \quad ? \quad 0 : -1 \leq c < a \quad ? \quad -l : c < a \quad ? \quad -\infty : a,
\end{array} \\
\begin{array}{c}
b < d \leq -l \quad ? \quad -l : b < d \leq 0 \quad ? \quad 0 : b < d \leq l \quad ? \quad l : b < d \quad ? \quad +\infty : b
\end{array}
\end{array} \right)
$$

- More generally, can use more thresholds than $-\infty, -l, 0, l, +\infty$
Example: widening for polyhedra

\[ P = \{ (x, y) \mid 0 \leq x \land x \leq y \land y \leq x \}; \]
\[ Q = \{ (x, y) \mid 0 \leq x \leq y \leq x + 1 \}; \]
\[ P \sqcup Q = \{ (x, y) \mid 0 \leq x \leq y \}; \]
Convergence acceleration with widening

- An iteration \(<f^n, n \in \mathbb{N}>\) for an increasing \(f \in S \rightarrow S\) on a complete lattice \(<S, \sqsubseteq, \bot, \top, \sqcup, \sqcap, \land, \lor, \triangledown, \sqcup, \sqcap>\) with widening \(\triangledown\) is ultimately stationary. Its limit \(f^\ell\) is such that \(\text{lfp } f \sqsubseteq f^\ell\).

- Proof: \(<f^n, n \in \mathbb{N}>\) is an increasing chain for \(\sqsubseteq\) since

\[
f^0 \overset{\text{def}}{=} \bot \sqsubseteq f^1
\]

\[
f^n \sqsubseteq f^n \triangledown f(f^n) \overset{\text{def}}{=} f^{n+1}
\]

by hypothesis 1. on \(\triangledown\). It follows that \(<f(f^n), n \in \mathbb{N}>\) is an increasing chain for \(\sqsubseteq\) since \(f\) is increasing.

Hypothesis 3. on \(\triangledown\) implies that \(<f^n, n \in \mathbb{N}>\) is ultimately stationary.
Proof (cont’d)

• For the limit $f^\lambda$ we have $f^\lambda = f^{\lambda+1} = f^\lambda \triangledown f(f^\lambda)$

By hypothesis 2. on $\triangledown$, $f(f^\lambda) \subseteq f^\lambda \triangledown f(f^\lambda) = f^\lambda$, proving that $\exists n \in \mathbb{N}: f(f^n) \subseteq f^n$

• Let $\ell$ be the smallest $n$ such that $f(f^n) \subseteq f^n$

• We have $f^\ell \in \{x \mid f(x) \subseteq x\}$ so, by Tarski, $\text{lfp } f = \cap \{x \mid f(x) \subseteq x\} \subseteq f^\ell$
An increasing widening can’t be terminating

• Let $\nabla$ be a widening increasing in its first parameter and $x, y \in S$

• If $y \sqsubseteq x$ then $x \nabla y = y$ (since the iterates have converged when $y = f(x) \sqsubseteq x$, see form II)

• So $y \sqsubseteq y \implies y \nabla y = y$

• If $\nabla$ is increasing then $x \sqsubseteq y \implies x \nabla y \sqsubseteq y \nabla y = y$

• It follows that $x \sqsubseteq y \implies x \nabla y \sqsubseteq y$, which prevents any extrapolation in the second parameter!
Example of non-increasing widening

- $[1,1] \subseteq [1,2]

- $[1,1] \triangledown [1,2] = [1, +\infty] \notin [1,2] \triangledown [1,2] = [1,2]$
Convergence acceleration: narrowing
Iteration with narrowing

• Iteration for \( f \) (increasing) with narrowing \( \Delta \):

\[
\begin{align*}
  f^0 & \overset{\text{def}}{=} a, & \text{where } f(a) \sqsubseteq a \\
  \ldots, \\
  f_{n+1} & \overset{\text{def}}{=} f_n \Delta f(f_n), & \text{when } f(f_{\ell}) \neq f_{\ell} \\
  \ldots, \\
  f_{\ell+1} & \overset{\text{def}}{=} f_{\ell} & \text{when } f(f_{\ell}) = f_{\ell}
\end{align*}
\]
Narrowing

• $\Delta \in S \times S \longrightarrow S$ such that

1. $\forall x, y \in S: \ y \sqsubseteq x \implies x \Delta y \sqsubseteq x$

2. $\forall x, y \in S: \ y \sqsubseteq x \implies y \sqsubseteq x \Delta y$

3. For any decreasing chain $y^0 \sqsupseteq y^1 \sqsupseteq \ldots \sqsupseteq y^n \sqsupseteq y^{n+1} \sqsupseteq \ldots$, the sequence $x^0 \overset{\text{def}}{=} y^0, \ldots, x^{n+1} \overset{\text{def}}{=} x^n \Delta y^n, \ldots$ is ultimately stationary (that is $\exists \ell: \forall n \geq \ell: x^n = x^\ell$)
Convergence acceleration with narrowing

- An iteration \(<f^n, n \in \mathbb{N}>\) for an increasing \(f \in S \rightarrow S\) on a complete lattice \(<S, \sqsubseteq, \perp, \top, \sqcup, \sqcap>\) starting from \(a \in S\) such that \(f(a) \sqsubseteq a\) with narrowing \(\Delta\) is ultimately stationary and such that \(\forall n \in \mathbb{N}: \text{lfp } f \sqsubseteq f^n\).

- Proof:
  - \(f^0 = a\) so \(f(a) \sqsubseteq a \implies f(f^0) \sqsubseteq f^0 \implies \text{lfp } f \sqsubseteq f(f^0) \sqsubseteq f^0\)
  - Assume, by induction hypothesis that \(\text{lfp } f \sqsubseteq f(f^n) \sqsubseteq f^n\)

\[f^{n+1} = f^n \Delta f(f^n)\]

\(\implies \text{lfp } f \sqsubseteq f(f^n) \sqsubseteq f^{n+1} \sqsubseteq f^n\) \hspace{1cm} \text{def. } \Delta \hspace{1cm} \ldots/\ldots\)
Convergence acceleration with narrowing

\[ \implies \text{lfp } f \subseteq f(f^n) \subseteq f^{n+1} \subseteq f^n \]

\[ \implies f(\text{lfp } f) \subseteq f(f(f^n)) \subseteq f(f^n) \subseteq f^n \]

\[ \implies \text{lfp } f \subseteq f(f^{n+1}) \subseteq f^{n+1} \]

- The chain \( f^0 = a \supseteq \ldots \supseteq f^n \supseteq f^{n+1} \supseteq \ldots \) is decreasing so \( f^0 \supseteq f(f^0) \supseteq \ldots \supseteq f(f^n) \supseteq f(f^{n+1}) \supseteq \ldots \) is also decreasing since \( f \) is increasing, so by hypothesis on \( \Delta \), the sequence \( f^0 \overset{\text{def}}{=} f^0, \ldots, f^{n+1} \overset{\text{def}}{=} f^n \Delta f(f^n), \ldots \) is ultimately stationary (that is \( \exists \ell : \forall n \geq \ell : f^n = f^\ell \)). \qed
Erroneous interpretation of the power of widenings/narrowings
Erroneous opinions on widening

• “the widening approach to program static analysis is useless since it is always possible to perform an iterative static analysis using a finite abstract domain”

  5

• “widenings can always be designed by further abstraction in an abstract domain satisfying the ascending chain condition”

  6.

---


Origin of the error

• There is a confusion between
  • **Analyzing a given program** (it is then possible to design a finite abstract domain specifically for that given program to produce the same result as the analysis with widening)
  • **Analyzing any program of a programming language** (since then the abstract domain that works for all programs of the language to produce the same result as the analysis with widening **must be infinite**)

Proof

• Consider the infinite family of programs

\[ P = \{ x := 1; \text{while } x \leq n \text{ do } x := x+1 \text{ od } \mid n \in \mathbb{N}^+ \} \]

(we have handled the case \( n = 100 \)).

• A static analysis of any program in the family \( P \) by iteration with widening/narrowing will find the loop invariant \( x \in [1,n+1] \).

• An analysis in a finite domain or a domain satisfying the ascending chain condition will fails on infinitely many programs where the widening/narrowing succeeds since \([1,2] \sqsubseteq [1,3] \sqsubseteq \ldots \sqsubseteq [1,n] \sqsubseteq \ldots\)
Design methodology for a static analyzer
Design of abstract interpretation-based static analyzers

• Express the concrete analysis problem in fixpoint form \( \text{lfp } f \) where \( f \in S \rightarrow S \) is increasing/continuous on a complete lattice \( <S, \subseteq, \perp, T, \cup, \sqcap> \)

• Design an abstraction \( <S, \subseteq> \xmapsto{\gamma_{\alpha}} <S^#, \leq> \)

• Design an abstract transformer \( f^# \) such that \( \forall x \in S: \alpha \circ f(x) \leq f^# \circ \alpha(x) \)

• If \( S^# \) satisfies the ascending chain condition (ACC) then compute \( \text{lfp } f^# \) iteratively (such that \( \alpha(\text{lfp } f) \leq \text{lfp } f^# \))

(ACC): every ascending/increasing chain is ultimately stationary.
Design of abstract interpretation-based static analyzers

- Otherwise, design a widening $\nabla$ and a narrowing $\Delta$
- Compute the iteration for $f^\#$ with widening $\nabla$ which convergence to $a \in S$ such that $\alpha(lfp f) \subseteq f^\#(a) \subseteq a$
- To improve precision, compute the iteration for $f$ with narrowing $\Delta$ starting from $a$. It converges and all iterates $b$ satisfy $\alpha(lfp f) \subseteq f^\#(b) \subseteq b$
- If experience shows that the analysis is too imprecise, refine $\nabla$ and $\Delta$
- If experience still shows that the analysis is too imprecise, refine the abstraction $\alpha$. 
Static analyzer for a programming language

• Proceed by induction on the syntax of the programming language,

• or use the internal compiler representation of programs
Bad news

• For undecidable problems, there are infinitely many programs for which the analysis will be too imprecise, whichever refined it is!

• This is inherent to undecidable problems

• No way out with full automation (can always rely on the user)
Good news

- **In practice**, it is possible to make the analysis refined enough to achieve the **required precision** and coarse enough to achieve **reasonable computation costs**

- The cannot be proved but results from experience


Conclusion
Conclusion

- Program analysis/verification is **undecidable** so any automatic method will fail on infinitely many program (hopefully not the ``natural” ones)

- **Manual/computer assisted methods** (theorem proving) cannot be fully automatic and so require specific expertise and have a high labor cost

- **Exhaustive methods** (e.g. model checking) do not scale up on large software

- **Abstract interpretation** does scale up thanks to abstraction and convergence acceleration; and can be made precise enough for practical purposes
Bibliography
References

• **Historical references:**
  
  • Patrick Cousot, Radhia Cousot: Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints. POPL 1977: 238-252
  
  • Patrick Cousot, Radhia Cousot: Systematic Design of Program Analysis Frameworks. POPL 1979: 269-282

• **Introductions/surveys:**
  
  • Patrick Cousot, Radhia Cousot: A gentle introduction to formal verification of computer systems by abstract interpretation. Logics and Languages for Reliability and Security 2010: 1-29

• **Static analysers:**
  
  • Francesco Logozzo, Michael Barnett, Manuel Fähndrich, Patrick Cousot, Radhia Cousot: A semantic integrated development environment. SPLASH 2012: 15-16
  
APPENDIX
Non-increasing convergence acceleration

• In the iterates with widening for \( f^\#, f^\# \) is usually not increasing (e.g. when itself computed with widenings as in the case of imbricated loops)

• The proofs of the convergence acceleration theorem have to be revisited.
Convergence acceleration theorem for $\nabla$

1. $f \in S \rightarrow S$ is increasing on the complete lattice $<S, \sqsubseteq, \bot, T, \sqcup, \sqcap>$

2. $\nabla \in S^\# \times S^\# \rightarrow S^\#$ is a terminating widening i.e.

   1. $\forall x, y \in S^\#: \gamma(y) \sqsubseteq \gamma(x \nabla y)$

   2. for any sequence $<y^n, n \in \mathbb{N}>$ of elements of $S$, the sequence $x^0 \overset{\text{def}}{=} y^0, \ldots, x^{n+1} \overset{\text{def}}{=} x^n \nabla y^n, \ldots$ is \textit{ultimately stationary} (that is $\exists \ell: \forall n \geq \ell: x^n = x^\ell$)

3. $f^\# \in S^\# \rightarrow S^\#$ is s.t. $\forall y \in S^\#: f \circ \gamma(y) \sqsubseteq \gamma \circ f^\#(y)$

$\implies$ the limit $f^{\#\ell}$ of the iterates $<f^{\#n}, n \in \mathbb{N}>$ for $f^\#$ from $a \in S^\#$ with widening $\nabla$ satisfies $f(\gamma(f^{\#\ell})) \sqsubseteq \gamma(f^{\#\ell})$ and $\text{lfp } f \sqsubseteq \gamma(f^{\#\ell})$
Proof

- The iterates $<f^n, n \in \mathbb{N}>$ have the form $f^n = a, \ldots, f^{n+1} = f^n \triangledown f(f^n)$ and so by 2.2 are ultimately stationary at rank $\ell$: $\forall n \geq \ell: f^n = f^\ell$

- $\gamma(f^\ell(f^\ell)) \subseteq \gamma(f^\ell \triangledown f(f^\ell))$ by 2.1

  $\implies \gamma(f^\ell(f^\ell))) \subseteq \gamma(f^\ell)$

  by convergence $f^\ell+1 = f^\ell \triangledown f(f^\ell) = f^\ell$

  $f \circ \gamma(f^\ell) \subseteq \gamma \circ f(f^\ell)$ by 3.

  $\implies f \circ \gamma(f^\ell) \subseteq \gamma(f^\ell)$ transitivity

  $\implies \text{lfp } f \subseteq \gamma(f^\ell)$ 1. and Tarski fixpoint th. $\square$
Convergence acceleration theorem for $\Delta$

1. $f \in S \rightarrow S$ is increasing on the complete lattice $<S, \subseteq, \bot, T, \sqcup, \sqcap>$

2. $\Delta \in S^\# \times S^\# \rightarrow S^\#$ is a terminating narrowing i.e.
   
   1. $\forall x, y \in S^\# : \gamma(y) \subseteq \gamma(x \triangle y)$
   
   2. for any sequence $<y^n, n \in \mathbb{N}>$ of elements of $S$, the sequence $x^0 \overset{\text{def}}{=} y^0, \ldots, x^{n+1} \overset{\text{def}}{=} x^n \Delta y^n, \ldots$ is ultimately stationary (that is $\exists \ell : \forall n \geq \ell : x^n = x^\ell$)

3. $f^\# \in S^\# \rightarrow S^\#$ is s.t. $\forall y \in S^\# : f \circ \gamma(y) \subseteq \gamma \circ f^\#(y)$

$\implies$ the iterates $<f^{\#n}, n \in \mathbb{N}>$ of $f^\#$ from $a \in S^\#$ such that lfp $f \subseteq \gamma(a)$ with narrowing $\Delta$ converge and satisfy $\forall n \in \mathbb{N} : \text{lfp } f \subseteq \gamma(f^{\#n})$
Proof

- Let \(<f^n, n \in \mathbb{N}>\) be the iterates of \(f^#\) from \(a \in S^#\) with \(\Delta\) so \(f^0 = a\) and \(f^{n+1} = f^n \Delta f^#(f^n)\). By 2.2, it is ultimately stationary

- \(\text{lfp } f \subseteq \gamma(f^0)\) since \(f^0 = a\) and \(\text{lfp } f \subseteq \gamma(a)\)

- Assume \(\text{lfp } f \subseteq \gamma(f^n)\) by ind. hyp.

\[
\Rightarrow \quad \text{lfp } f = f(\text{lfp } f) \subseteq f(\gamma(f^n)) \subseteq \gamma(f^#(f^n))
\]

fixpoint property, \(f\) increasing and 3.

\[
\gamma(f^#(f^n)) \subseteq \gamma(f^n \Delta f^#(f^n)) = \gamma(f^{n+1}) \quad \text{2.1 & def. } f^{n+1}
\]

\[
\Rightarrow \quad \text{lfp } f \subseteq \gamma(f^{n+1}) \quad \text{by transitivity} \quad \square
\]
Exercices
Exercice 1

• Show that the interval widening is overapproximating in both its arguments, not increasing in its first argument, increasing in its second argument, and terminating.
Exercice 2

Let \( <S, \sqsubseteq, \top> \) be a poset with supremum \( \top \). Let \( T = \{T_1, \ldots, T_n\} \) be finitely many elements of \( S \) such that \( T_1 \sqsubseteq T_2 \sqsubseteq \ldots \sqsubseteq T_n = \top \). Define the widening with thresholds \( T \) as

\[
X \triangledown_T Y = \{Y \sqsubseteq X \land X \sqsubseteq \min\{t \in T \mid X \sqsubseteq t \land Y \sqsubseteq t\}\}
\]

Prove \( \triangledown_T \) that is a terminating widening.
Exercice 3

• Prove formally that a static analysis of any program of the form

\[ x := 1; \text{ while } x \leq n \text{ do } x := x+1 \text{ od } \]  \hspace{1cm} (**)

where \( n \in \mathbb{N}^+ \) on integer intervals and widening/narrowing will converge and automatically discover the loop invariant \( x \in [1,n+1] \)

• Hint: generalize the case \( n=100 \) that we handled (not forgetting that \( n \) is a given, although unknown, natural and not a program variable, in which case more refined domains such as octagons or polyhedra are required).
Answers
Exercice 1

\textbf{Proof} — Obviously $\emptyset \subseteq \emptyset \triangleleft y$ and $y \subseteq y = \emptyset \triangleleft y$. Similarly, $\emptyset \subseteq x \triangleleft \emptyset$ and $x \subseteq x = x \triangleleft \emptyset$. We must prove $[a, b] \subseteq [a, b] \triangleleft [c, d]$ that is $(\{ c < a \mid -\infty : a \} \leq a$ and $b \leq (\{ d > b \mid +\infty : b \})$ and $[c, d] \subseteq [a, b] \triangleleft [c, d]$ that is $(\{ c < a \mid -\infty : a \} \leq c$ and $d \leq (\{ d > b \mid +\infty : b \})$ which obviously hold.

The interval widening is not increasing in its first argument since $[0, 1] \subseteq [0, 2]$ but $[0, 1] \triangleleft [0, 2] = [0, +\infty] \not\subseteq [0, 2] = [0, 2] \triangleleft [0, 2]$. 

The interval widening is increasing in its second argument (i.e. if $y \subseteq y'$ then $\forall x : x \triangledown y \subseteq x \triangledown y'$).

- If $x = \emptyset$ then $x \triangledown y = \emptyset \triangledown y = y \subseteq y' = \emptyset \triangledown y' = x \triangledown y'$.

- Else $x = [a, b] \neq \emptyset$. Then:
  - If $y = \emptyset$ then $x \triangledown y = x \triangledown \emptyset = x \subseteq x \triangledown y'$ since $\triangledown$ is overapproximating.
  - Else $y = [a', b'] \neq \emptyset$ so $y \subseteq y'$ implies $y' = [a'', b''] \neq \emptyset$ with $a'' \leq a'$ and $b' \leq b''$.
    * For the lower bound, we have:
      - If $a' < a$ so $a'' \leq a' < a$ hence we have $x \triangledown y = [a, \_\_] \triangledown [a', \_] = [-\infty, \_] \subseteq x \triangledown y' = [a, \_\_] \triangledown [a'', \_] = [-\infty, \_\_]
      - Else, $a'' \geq a$, hence $x \triangledown y = [a, \_\_] \triangledown [a', \_] = [a, \_] \subseteq x \triangledown y' = [a, \_\_] \triangledown [a'', \_] = (\_\_ a'' \geq a \_\_] \triangledown [a, \_\_] : [-\infty, \_\_])$.
    * idem, for the upper bound.
To show that the interval widening is terminating, assume, by reductio ad absurdum, that \( \langle y^n, n \in \mathbb{N} \rangle \) is not ultimately stationary. Without loss of generality, \( \langle y^n, n \in \mathbb{N} \rangle \) can be assumed to be strictly increasing so none of \( \langle y^n, n \geq 1 \rangle \) is \( \emptyset \). Consider the lower bound \( a_3 < a_2 < a_1 \) of \( y^i = [a_i, b_i] \). By definition of the widening \( y^{n+1} = y^n \triangledown x^n \), we have \( a_2 = +\infty \) so the contradiction \( a_3 < a_2 \).
Exercice 2

**Proof** — \( \nabla_T \) is a upper bound. If \( Y \subseteq X \) then \( X \nabla_T Y = X = X \cup Y \). Otherwise, \( Y \subseteq X = T_i \) with \( T_i \supseteq X \) and \( T_i \supseteq Y \).

\( \nabla_T \) enforces convergence. Given \( \langle X_i, i \in \mathbb{N} \rangle \) define \( Y_0 = X_0, \ldots, Y_{i+1} = Y_i \nabla X_i \). Assume that \( \langle Y_i, i \in \mathbb{N} \rangle \) is a strictly ascending chain. We have \( Y_1 = X_0 \nabla_T X_1 = T_{i_1} \) (since otherwise \( X_1 \subseteq X_0 \) and \( Y_1 = X_0 \) so \( \langle Y_i, i \in \mathbb{N} \rangle \) would not be a strictly increasing chain). Assume by induction hypothesis that \( Y_k = T_{i_k} \) with \( T_{i_1} \subseteq \ldots \subseteq T_{i_k} \). Then \( Y_{k+1} = T_{i_k} \nabla_T X_{k+1} \) since we cannot have \( X_{k+1} \subseteq Y_{k+1} \) which would imply that \( Y_{k+1} = T_{i_k} \) in contradiction with the hypothesis that \( \langle Y_i, i \in \mathbb{N} \rangle \) is a strictly ascending chain. So \( Y_{k+1} = T_{i_{k+1}} \) with \( T_{i_{k+1}} \supseteq T_{i_k} \). But \( T_{i_{k+1}} \neq T_{i_k} \) since otherwise \( \langle Y_i, i \in \mathbb{N} \rangle \) would not be a strictly increasing chain. It follows, by recurrence that \( \forall k \in \mathbb{N} : Y_k = T_{i_k} \) so \( \langle T_{i_k}, k \in \mathbb{N} \rangle \) is strictly increasing, a contradiction.
Exercice 3

• The equation to be solved is

\[
X = \{ \text{let } X' = (X \cap [-\infty, n]) \text{ in } [1, 1] \cup (| X' = \emptyset \Rightarrow \emptyset : \text{let } [a, b] = X' \text{ in } [\min(a + 1, +\infty), \min(b + 1, +\infty)] ) \}
\]

For all \( n \in [1, +\infty] \), the increasing iterates from \( \emptyset \) with widening will be as follows.

\[
\hat{X}^0 = \emptyset
\]
\[
X^\uparrow = X^0 \triangleleft \begin{cases} \\
[1, 1] \cup X' = \emptyset ? \emptyset : \text{let } [a, b] = X' \text{ in } \\
[\min(a + 1, +\infty), \min(b + 1, +\infty)] \end{cases}
\]

\[
= \emptyset \triangleleft ([1, 1] \cup \emptyset)
\]

\[
= \emptyset \triangleleft [1, 1]
\]

\[
= [1, 1]
\]

\[
X^2 = X^\uparrow \triangleleft \begin{cases} \\
[1, 1] \cup X' = \emptyset ? \emptyset : \text{let } [a, b] = X' \text{ in } \\
[\min(a + 1, +\infty), \min(b + 1, +\infty)] \end{cases}
\]

\[
= [1, 1] \triangleleft ([1, 1] \cup [2, 2])
\]

\[
= [1, 1] \triangleleft [1, 2]
\]

\[
= [1, +\infty]
\]

\[
X^3 = X^2 \triangleleft \begin{cases} \\
[1, 1] \cup X' = \emptyset ? \emptyset : \text{let } [a, b] = X' \text{ in } \\
[\min(a + 1, +\infty), \min(b + 1, +\infty)] \end{cases}
\]

\[
= [1, +\infty] \triangleleft ([1, 1] \cup [2, n + 1])
\]

\[
= [1, +\infty] \triangleleft [1, n + 1]
\]

\[
= [1, +\infty]
\]
For all \( n \in [1, +\infty] \), the decreasing iterates from \([1, +\infty]\) with narrowing will have the following form.

\[
X^0 = X^3 = [1, +\infty]
\]

\[
X^1 = X^0 \Delta \left( \begin{array}{l}
\text{let } X' = (X^0 \cap [-\infty, n]) \text{ in} \\
[1, 1] \cup \{ \text{X' = \emptyset ? \emptyset : let } [a, b] = X' \text{ in} \\
\min(a + 1, +\infty), \min(b + 1, +\infty) \} \end{array} \right)
\]

\[
= [1, +\infty] \Delta ([1, 1] \cup [2, n + 1])
\]

\[
= [1, +\infty] \Delta [1, n + 1]
\]

\[
= [1, n + 1]
\]

\[
X^2 = X^1 \Delta \left( \begin{array}{l}
\text{let } X' = (X^1 \cap [-\infty, n]) \text{ in} \\
[1, 1] \cup \{ \text{X' = \emptyset ? \emptyset : let } [a, b] = X' \text{ in} \\
\min(a + 1, +\infty), \min(b + 1, +\infty) \} \end{array} \right)
\]

\[
= [1, n + 1] \Delta ([1, 1] \cup [2, n + 1])
\]

\[
= [1, n + 1] \Delta [1, n + 1]
\]

\[
= [1, n + 1]
\]
Notice that this is a mathematical reasoning which could only be mechanized using a proof checker or theorem prover. However, given a value for \( n \), the corresponding computation can effectively be implemented by a computer program. This means that for all given \( n \in [1, +\infty) \), a static analyzer will be able to automatically determine the loop invariant \( x \in [1, n + 1] \) at program point \(^2\) without any human intervention.

It follows that

**Theorem** \( \text{There exist abstractions in infinite domains with widening/-narrowing that it is impossible to perform automatically, soundly, and with the same precision with any abstract domain satisfying the ascending chain condition.} \)

□
Proof Consider interval analysis. Assume there exists an abstract domain which can be used to analyze all programs in the family \( P(n), n \geq 1 \) considered in example (***) with the same precision. This means that to express the final result this abstract domain must contain the infinite strictly ascending chain \([1, n + 1], n \geq 1\) since otherwise there is some \( n \) for which the result of analyzing \( P(n) \) would be unsound (in case an incorrect interval is returned) or less precise (in case \([1, n + 1]\) would not be exactly expressible in this abstract domain satisfying ACC). Notice that one could try larger and larger abstract domain to successively incorporate more and more intervals. However, this process would not terminate on the program of example (***) on integers.

\[\square\]
The End