Approximations

MPRI 2–6: Abstract Interpretation,
application to verification and static analysis

Antoine Miné

year 2013–2014

course 02-A
27 September 2013

Abstractions in the concretization framework

Given a concrete $(C, \leq)$ and an abstract $(A, \sqsubseteq)$ posets and a monotonic concretization $\gamma : A \to C$

($\gamma(a)$ is the "meaning" of a in C; we use intervals in our examples)

- $a \in A$ is a sound abstraction of $c \in C$ if $c \leq \gamma(a)$.

  (e.g.: $[0, 10]$ is a sound abstraction of $\{0, 1, 2, 5\}$ in the integer interval domain)

- $g : A \to A$ is a sound abstraction of $f : C \to C$ if $\forall a \in A$: $(f \circ \gamma)(a) \leq (\gamma \circ g)(a)$.

  (e.g.: $\lambda([a, b].[-\infty, +\infty]$ is a sound abstraction of $\lambda X.\{\, x + 1 \mid x \in X \,\}$ in the interval domain)

- $g : A \to A$ is an exact abstraction of $f : C \to C$ if $f \circ \gamma = \gamma \circ g$.

  (e.g.: $\lambda([a, b].[a + 1, b + 1]$ is an exact abstraction of $\lambda X.\{\, x + 1 \mid x \in X \,\}$ in the interval domain)

Abstractions in the Galois connection framework

Assume now that $(C, \leq) \xleftarrow[\alpha]{\gamma} (A, \sqsubseteq)$.

- sound abstractions
  - $c \leq \gamma(a)$ is equivalent to $\alpha(c) \sqsubseteq a$.
  - $(f \circ \gamma)(a) \leq (\gamma \circ g)(a)$ is equivalent to $(\alpha \circ f \circ \gamma)(a) \sqsubseteq g(a)$.

- Given $c \in C$, its best abstraction is $\alpha(c)$.

  (proof: recall that $\alpha(c) = \sqcap \{ a \,|\, c \leq \gamma(a) \}$, so, $\alpha(c)$ is the smallest sound abstraction of c)

  (e.g.: $\alpha(\{0, 1, 2, 5\}) = [0, 5]$ in the interval domain)

- Given $f : C \rightarrow C$, its best abstraction is $\alpha \circ f \circ \gamma$

  (proof: g sound $\iff \forall a, (\alpha \circ f \circ \gamma)(a) \sqsubseteq g(a)$, so $\alpha \circ f \circ \gamma$ is the smallest sound abstraction of f)

  (e.g.: $g([a, b]) = [2a, 2b]$ is the best abstraction in the interval domain of $f(X) = \{ 2x \,|\, x \in X \}$; it is not an exact abstraction as $\gamma(g([0, 1])) = \{0, 1, 2\} \supsetneq \{0, 2\} = f(\gamma([0, 1]))$)

Composition of sound, best, and exact abstractions

If g and g' soundly abstract respectively f and f' then:

- if f is monotonic,
  then $g \circ g'$ is a sound abstraction of $f \circ f'$,
  (proof: $\forall a,\ (f \circ f' \circ \gamma)(a) \leq (f \circ \gamma \circ g')(a) \leq (\gamma \circ g \circ g')(a)$)
- if g, g' are exact abstractions of f and f',
  then $g \circ g'$ is an exact abstraction,
  (proof: $f \circ f' \circ \gamma = f \circ \gamma \circ g' = \gamma \circ g \circ g'$)
- if g and g' are the best abstractions of f and f',
  then $g \circ g'$ is not always the best abstraction!
  (e.g.: $g([a,b]) = [a, \min(b,1)]$ and $g'([a,b]) = [2a, 2b]$ are the best abstractions of $f(X) = \{\, x \in X \mid x \leq 1 \,\}$ and $f'(X) = \{\, 2x \mid x \in X \,\}$ in the interval domain, but $g \circ g'$ is not the best abstraction of $f \circ f'$ as $(g \circ g')([0,1]) = [0,1]$ while $(\alpha \circ f \circ f' \circ \gamma)([0,1]) = [0,0]$)

Fixpoint transfer

If we have:

- a Galois connection $(C, \leq) \xleftarrow[\alpha]{\gamma} (A, \sqsubseteq)$ between CPOs
- monotonic concrete and abstract functions
  $f : C \to C$, $f^\sharp : A \to A$
- a commutation condition $\alpha \circ f = f^\sharp \circ \alpha$
- an element a and its abstraction $a^\sharp = \alpha(a)$

then $\alpha(\mathrm{lfp}_a\, f) = \mathrm{lfp}_{a^\sharp}\, f^\sharp$.

(proof on next slide)

Fixpoint transfer (proof)

Proof:

By the constructive Tarksi theorem, $\text{lfp}_a\, f$ is the limit of transfinite iterations: $a_0 \stackrel{\text{def}}{=} a$, $a_{n+1} \stackrel{\text{def}}{=} f(a_n)$, and $a_n \stackrel{\text{def}}{=} \bigvee \{\, a_m \mid m < n \,\}$ for limit ordinals n.
Likewise, $\text{lfp}_{a^\sharp}\, f^\sharp$ is the limit of a transfinite iteration $a^\sharp_n$.
We prove by transfinite induction that $a^\sharp_n = \alpha(a_n)$ for all ordinals n:

- $a^\sharp_0 = \alpha(a_0)$, by definition;
- $a^\sharp_{n+1} = f^\sharp(a^\sharp_n) = f^\sharp(\alpha(a_n)) = \alpha(f(a_n)) = \alpha(a_{n+1})$ for successor ordinals, by commutation;
- $a^\sharp_n = \bigsqcup \{\, a^\sharp_m \mid m < n \,\} = \bigsqcup \{\, \alpha(a_m) \mid m < n \,\} = \alpha(\bigvee \{\, a_m \mid m < n \,\}) = \alpha(a_n)$ for limit ordinals, by commutation and the fact that α is always continuous in Galois connections.

Hence, $\text{lfp}_{a^\sharp}\, f^\sharp = \alpha(\text{lfp}_a\, f)$.

Fixpoint approximation

If we have:

- a complete lattice $(C, \leq, \vee, \wedge, \bot, \top)$
- a monotonic concrete function f
- a sound abstraction $f^\sharp : A \to A$ of f
  $(\forall x^\sharp: (f \circ \gamma)(x^\sharp) \leq (\gamma \circ f^\sharp)(x^\sharp))$
- a post-fixpoint $a^\sharp$ of $f^\sharp$ $\quad (f^\sharp(a^\sharp) \sqsubseteq a^\sharp)$

then $a^\sharp$ is a sound abstraction of lfp f: lfp $f \leq \gamma(a^\sharp)$.

Proof:

By definition, $f^\sharp(a^\sharp) \sqsubseteq a^\sharp$.
By monotony, $\gamma(f^\sharp(a^\sharp)) \leq \gamma(a^\sharp)$.
By soundness, $f(\gamma(a^\sharp)) \leq \gamma(a^\sharp)$.
By Tarski's theorem lfp $f = \wedge \{\, x \mid f(x) \leq x \,\}$.
Hence, lfp $f \leq \gamma(a^\sharp)$.