Abstract Interpolation by Dual Narrowing

Patrick Cousot

Princeton University
September 27 & 28, 2014

Abstract Interpreters

- Transitional abstract interpreters: proceed by induction on program steps
- Structural abstract interpreters: proceed by induction on the program syntax
- Main problem: over/under-approximate fixpoints in non-Noetherian abstract domains

Fixpoints

- Poset $<D, \sqsubseteq, \bot, \top>$
- Transformer: $F \in D \mapsto D$
- Least fixpoint: $\text{lfp}\subseteq F = \bigcup_{n \in \mathbb{N}} F^n(\bot)$ (under appropriate hypotheses)

Convergence acceleration with widening

Infinite iteration

(e.g. with a widening based on the derivative as in Newton-Raphson method\(^{(7)}\))

Extrapolation by Widening

- $X^0 = \bot$ (increasing iterates with widening)
- $X_{n+1} = X_n \setminus F(X_n)$ when $F(X_n) \not\subseteq X_n$
- $X_{n+1} = X_n$ when $F(X_n) \subseteq X_n$

- Widening $\nabla$:
  - $Y \subseteq X \setminus Y$ (extrapolation)
  - Enforces convergence of increasing iterates with widening, limit $X^\ell$

Extrapolation with widening

$X \nabla F(X)$

Interpolation with narrowing

- $Y^0 = X^\ell$ (decreasing iterates with narrowing)
- $Y_{n+1} = Y_n \Delta F(Y_n)$ when $F(Y_n) \subseteq Y_n$
- $Y_{n+1} = Y_n$ when $F(Y_n) = Y_n$

- Narrowing $\Delta$:
  - $Y \not\subseteq X \implies Y \subseteq X \Delta Y \subseteq X$ (interpolation)
  - Enforces convergence of decreasing iterates with narrowing, $Y^\lambda$
Example of narrowing

- [2]  

\[ [a_1, b_1] \uparrow [a_2, b_2] = \]

\[ \left[ \begin{array}{l}
\text{if } a_1 = \infty \text{ then } a_2 \text{ else } \text{MIN}(a_1, a_2), \\
\text{if } b_1 = \infty \text{ then } b_2 \text{ else } \text{MAX}(b_1, b_2)
\end{array} \right] \]

Duality

- Convergence above the limit  
  Increasing iteration  
  Widening $\nabla$  
  Dual-narrowing $\tilde{\Delta}$

- Convergence below the limit  
  Decreasing iteration  
  Narrowing $\Delta$  
  Dual widening $\tilde{\nabla}$

Extrapolators ($\nabla$, $\tilde{\nabla}$) and interpolators ($\Delta$, $\tilde{\Delta}$)

- **Extrapolators:**

- **Interpolators:**

Interpolation with narrowing

Extrapolators, Interpolators, and Duals
Interpolation with dual narrowing

- $Z^0 = \bot$ (increasing iterates with dual-narrowing)
  
  $Z^{n+1} = F(Z^n) \triangleright Y$ when $F(Z^n) \not\subseteq Z^n$
  
  $Z^{n+1} = Z^n$ when $F(Z^n) \subseteq Z^n$

- Dual-narrowing $\Delta$:
  
  - $X \subseteq Y \implies X \subseteq \Delta Y \subseteq Y$ (interpolation)
  
  - Enforces convergence of increasing iterates with dual-narrowing

Example of dual-narrowing

- $[a, b] \Delta [c, d] \triangleq \{c = -\infty \ ? \ a \in [a + c)/2]\}, \{d = \infty \ ? \ b \in [(b + d)/2]\}$

- The first method we tried in the end 70’s with Radhia
  
  - Slow
  
  - Does not easily generalize (e.g. to polyhedra)

Relationship between narrowing and dual-narrowing

- $\tilde{\Delta} = \Delta^{-1}$
  
- $Y \subseteq X \implies Y \subseteq X \Delta Y \subseteq X$ (narrowing)
  
- $Y \subseteq X \implies Y \subseteq \tilde{Y} \subseteq X$ (dual-narrowing)

- Example: Craig interpolation

- Why not use a bounded widening (bounded by $B$)?
  
  - $F(X) \subseteq B \implies F(X) \subseteq F(X) \tilde{\Delta} B \subseteq B$ (dual-narrowing)
  
  - $X \subseteq F(X) \subseteq B \implies F(X) \subseteq X \bigvee_B F(X) \subseteq B$ (bounded widening)
Example of widenings (cont’d)

- Bounded widening (in \([\ell, h]\)):

\[ [a, b] \]

\[ [c, d] \]

\[ [a, b] \lor_{[\ell, h]} [c, d] \triangleq \frac{[c+\ell - 2\ell, b+d+2h]}{2} \]

Conclusion

- Abstract interpretation in infinite domains is traditionally by iteration with widening/narrowing.
- We shown how to use iteration with dual-narrowing.
- These ideas of the 70's generalize Craig interpolation from logic to arbitrary abstract domains.

The End, Thank You