VMCAI 2015

Abstracting Induction by Extrapolation and Interpolation

Mumbai, India
January 12th, 2015

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

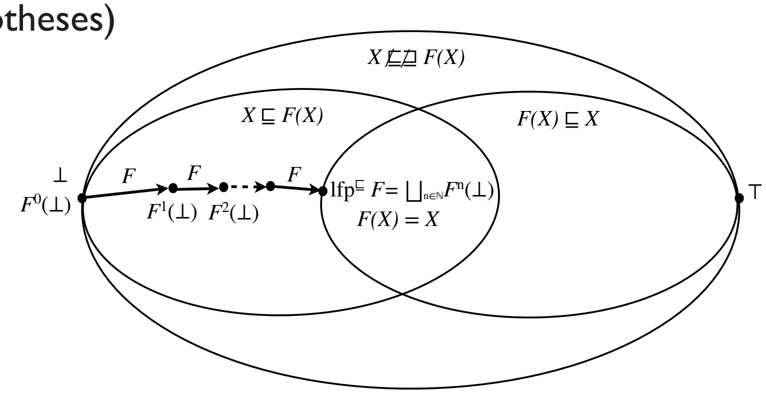
Abstract Interpreters

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

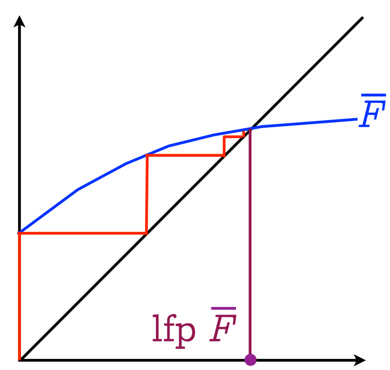
(*) Iterative fixpoint computations may not converge in finitely many steps
(**) Or convergence may be guaranteed but to slow.

Fixpoints

- Poset (or pre-order) $\langle D, \sqsubseteq, \bot, \sqcup \rangle$
- Transformer: $F \in D \longmapsto D$
- Least fixpoint: $\mathrm{lfp}^{\sqsubseteq} F = \bigsqcup_{n\in\mathbb{N}} F^n(\bot)$ (under appropriate hypotheses)

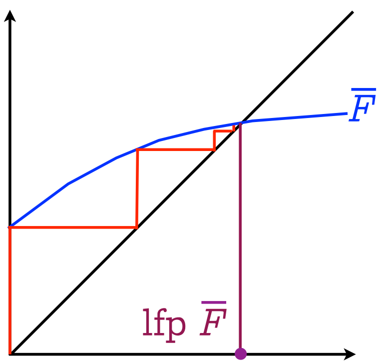


Convergence acceleration with widening

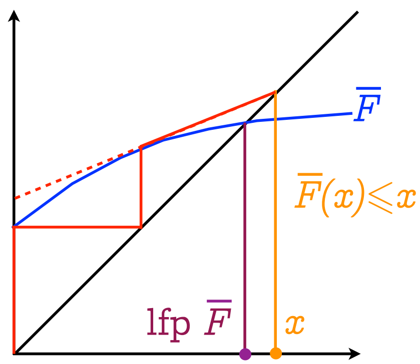


Infinite iteration

Convergence acceleration with widening



Infinite iteration



Accelerated iteration with widening
(e.g. with a widening based on the derivative as in Newton-Raphson method(*))

(*) Javier Esparza, Stefan Kiefer, Michael Luttenberger: Newtonian program analysis. J. ACM 57(6): 33 (2010)

Extrapolation by Widening

- $X^0 = \bot$ (increasing iterates with widening)

  $X^{n+1} = X^n \nabla F(X^n)$ when $F(X^n) \not\sqsubseteq X^n$

  $X^{n+1} = X^n$ when $F(X^n) \sqsubseteq X^n$
- Widening ∇:
  - $Y \sqsubseteq X \nabla Y$ (extrapolation)
  - Enforces convergence of increasing iterates with widening (to a limit X^ℓ)

The oldest widenings

- Primitive widening [1,2]

```
(x ∇̄ y) = cas x ∈ Va, y ∈ Va dans
   ⊢ □, ? => y ;
   ⊢ ?, □ => x ;
   ⊢ [n1,m1],[n2,m2] =>
        [si n2 < n1 alors -∞ sinon n1 fsi ;
            si m2 > m1 alors +∞ sinon m1 fsi] ;
   fincas ;
```

```
[a1, b1] ∇̄ [a2, b2] =
    [if a2 < a1 then -∞ else a1 fi,
          if b2 > b1 then +∞ else b1 fi]
```

- Widening with thresholds [3]

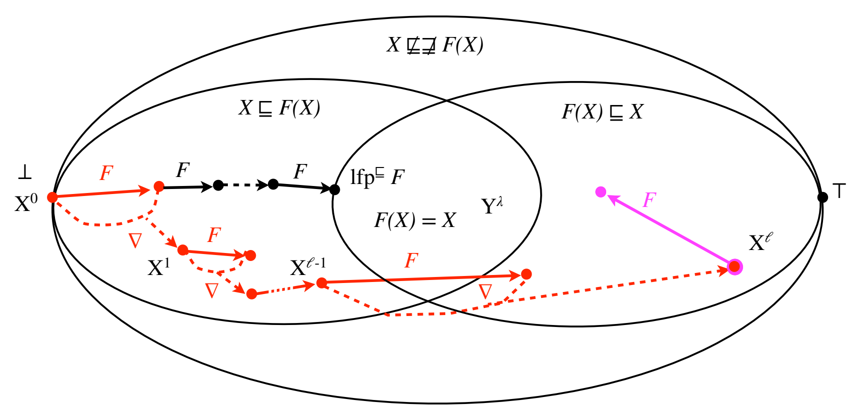
$\forall x \in \bar{L}_2, \bot \nabla_2(j)\, x = x \nabla_2(j) \bot = x$

$[l_1, u_1] \nabla_2(j) [l_2, u_2]$

$= [\textit{if } 0 \leq l_2 < l_1 \textit{ then } 0 \textit{ elsif } l_2 < l_1 \textit{ then } -b-1 \textit{ else } l_1 \textit{ fi},$
$\textit{if } u_1 < u_2 \leq 0 \textit{ then } 0 \textit{ elsif } u_1 < u_2 \textit{ then } b \textit{ else } u_1 \textit{ fi}]$

[1] Patrick Cousot, Radhia Cousot: Vérification statique de la cohérence dynamique des programmes, Rapport du contrat IRIA-SESORI No 75-032, 23 septembre 1975.
[2] 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
[3] Patrick Cousot, Semantic foundations of program analysis, Ch. 10 of Program flow analysis: theory and practice, N. Jones & S. Muchnick (eds), Prentice Hall, 1981.

Extrapolation with widening



Interpolation with narrowing

- $Y^0 = X^\ell$ (decreasing iterates with narrowing)

  $Y^{n+1} = Y^n \mathbin{\Delta} F(Y^n)$ when $F(Y^n) \sqsubset Y^n$

  $Y^{n+1} = Y^n$ when $F(Y^n) = Y^n$

- Narrowing Δ:
  - $Y \sqsubseteq X \implies Y \sqsubseteq X \mathbin{\Delta} Y \sqsubseteq X$ (interpolation)
  - Enforces convergence of decreasing iterates with narrowing (to a limit Y^λ)

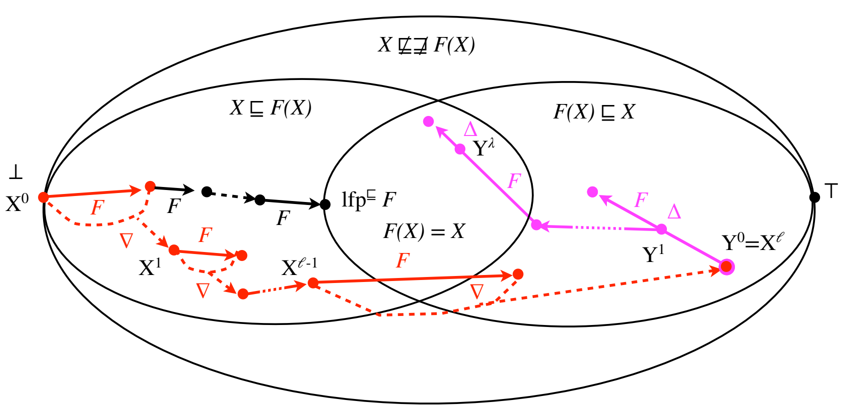
The oldest narrowing

- [2]

```
[a1,b1] Δ̄ [a2,b2] =
   [if a1 = -∞ then a2 else MIN (a1,a2),
        if b1 = +∞ then b2 else MAX (b1,b2)]
```

[2] 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

Interpolation with narrowing



Could stop when $F(X) \not\sqsubseteq X \wedge F(F(X)) \sqsubseteq F(X)$ but not the current practice.

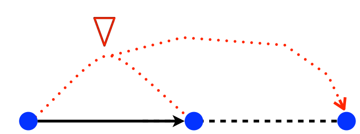
Duality

-

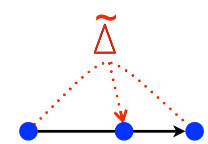
	Convergence above the limit	Convergence below the limit
Increasing iteration	Widening ∇	Dual-narrowing $\tilde{\Delta}$
Decreasing iteration	Narrowing Δ	Dual widening $\tilde{\nabla}$

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

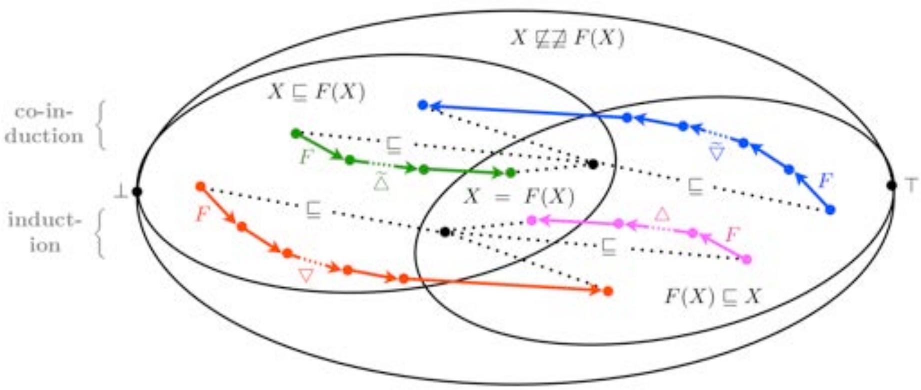
- Extrapolators:



- Interpolators:



Extrapolators, Interpolators, and Duals



Interpolation with dual narrowing

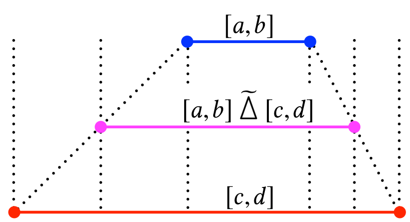
- $Z^0 = \bot$ (increasing iterates with dual-narrowing)

  $Z^{n+1} = F(Z^n) \,\widetilde{\Delta}\, Y^\lambda$ when $F(Z^n) \not\sqsubseteq Z^n$

  $Z^{n+1} = Z^n$ when $F(Z^n) \sqsubseteq Z^n$

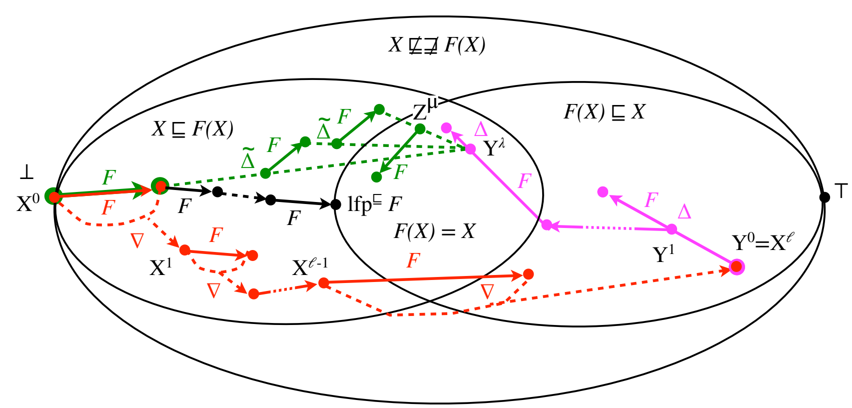
- Dual-narrowing $\widetilde{\Delta}$:
  - $X \sqsubseteq Y \implies X \sqsubseteq X \,\widetilde{\Delta}\, Y \sqsubseteq Y$ (interpolation)
  - Enforces convergence of increasing iterates with dual-narrowing

Example of dual-narrowing

- 

- $[a,b] \,\widetilde{\Delta}\, [c,d] \triangleq [\![c = -\infty \;?\; a : \lfloor (a+c)/2 \rfloor]\!], [\![d = \infty \;?\; b : \lceil (b+d)/2 \rceil]\!]]$
- The first method we tried in the late 70's with Radhia
  - Slow
  - Does not easily generalize (e.g. to polyhedra)

Interpolation with dual-narrowing

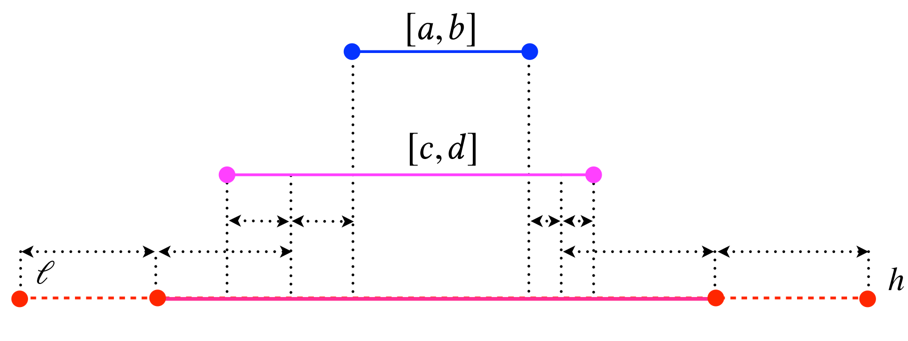


Relationship between narrowing and dual-narrowing

- $\widetilde{\Delta} = \Delta^{-1}$
- $Y \sqsubseteq X \implies Y \sqsubseteq X \mathbin{\Delta} Y \sqsubseteq X$ (narrowing)
- $Y \sqsubseteq X \implies Y \sqsubseteq Y \mathbin{\widetilde{\Delta}} X \sqsubseteq X$ (dual-narrowing)
- Example: Craig interpolation
- Why not use a bounded widening (bounded by B)?
  - $F(X) \sqsubseteq B \implies F(X) \sqsubseteq F(X) \mathbin{\widetilde{\Delta}} B \sqsubseteq B$ (dual-narrowing)
  - $X \sqsubseteq F(X) \sqsubseteq B \implies F(X) \sqsubseteq X \nabla_B F(X) \sqsubseteq B$ (bounded widening)

Example of widenings (cont'd)

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



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

More in the paper...

Widenings

Widenings are not increasing

- A well-known fact

  $[1,1] \subseteq [1,2]$ but $[1,1] \nabla [1,2] = [1, \not\infty] \subseteq [1,2] \nabla [1,2] = [1,2]$

- A widening cannot both:
  - Be increasing in its first parameter
  - Enforce termination of the iterates
  - Avoid useless over-approximations as soon as a solution is found(*)

(*) A counter-example is $x \nabla y = \top$

Soundness

Soundness

- In the paper, the fixpoint approximation soundness theorems are expressed with minimalist hypotheses:
  - No need for complete lattices, complete partial orders (CPO's):
    - The concrete domain is a poset
    - The abstract domain is a pre-order
    - The concretization is defined for the abstract iterates only.

Soundness (cont'd)

- No need for increasingness/monotony hypotheses for fixpoint theorems (Tarski, Kleene, etc)
  - The concrete transformer is increasing and the limit of the iterations does exist in the concrete domain
  - No hypotheses on the abstract transformer (no need for fixpoints in the abstract)
  - Soundness hypotheses on the extrapolators/interpolators with respect to the concrete
- In addition, termination hypotheses on the extrapolators/interpolators ensure convergence in finitely many steps

Soundness (cont'd)

- No need for increasingness/monotony hypotheses for fixpoint theorems (Tarski, Kleene, etc)
  - The concrete transformer is increasing and the limit of the iterations does exist in the concrete domain
  - No hypotheses on the abstract transformer (no need for fixpoints in the abstract)
  - Soundness hypotheses on the extrapolators/ interpolators with respect to the concrete

Examples of interpolators

Craig interpolation

- Craig interpolation:

  Given $\mathrm{P} \Longrightarrow \mathrm{Q}$ find I such that $\mathrm{P} \Longrightarrow \mathrm{I} \Longrightarrow \mathrm{Q}$ with $\mathrm{var(I)} \subseteq \mathrm{var(P)} \cap \mathrm{var(Q)}$

  is a dual narrowing (already observed by Vijay D'Silva and Leopold Haller as an inversed narrowing)

Craig interpolation

- Craig interpolation:

  Given $\mathrm{P} \Longrightarrow \mathrm{Q}$ find I such that $\mathrm{P} \Longrightarrow \mathrm{I} \Longrightarrow \mathrm{Q}$ with $\mathrm{var(I)} \subseteq \mathrm{var(P)} \cap \mathrm{var(Q)}$

  is a dual narrowing (already observed by Vijay D'Silva and Leopold Haller as an inversed narrowing)
- This evidence looked very controversial to some reviewers

Craig interpolation

- Craig interpolation:

  Given $P \Longrightarrow Q$ find I such that $P \Longrightarrow I \Longrightarrow Q$ with $\text{var}(I) \subseteq \text{var}(P) \cap \text{var}(Q)$

  is a dual narrowing (already observed by Vijay D'Silva and Leopold Haller as an inversed narrowing)

- This evidence looked very controversial to some reviewers
- The generalization of an idea does not diminish in any way the merits and originality of this idea

Conclusion

Conclusion

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

The End, Thank You