POPL'15 PC Workshop

Abstract Interpolation by Dual Narrowing

Princeton University
September 27 & 28, 2014

Patrick Cousot

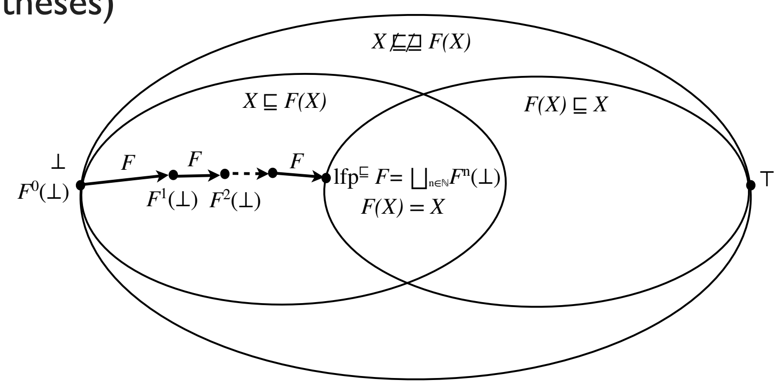
pcousot@cs.nyu.edu cs.nyu.edu/~pcousot

Abstract Interpreters

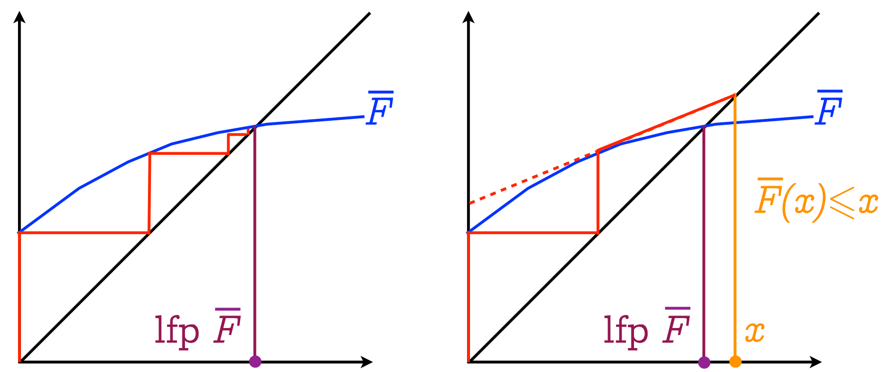
- Transitional abstract interpreters: proceed by induction on program steps
- Structural abstract interpreters: proceed by induction on the program syntax
- Main problem: over/under-approximate fixpoints in non-Noetherian abstract domains

Fixpoints

- Poset <D, ⊑, ⊥, ⊔>
- 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

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)

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

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

- Widening ∇:
  - $Y \sqsubseteq X \mathbin{\nabla} Y$ (extrapolation)
  - Enforces convergence of increasing iterates with widening, limit X^ℓ

Example of 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]

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

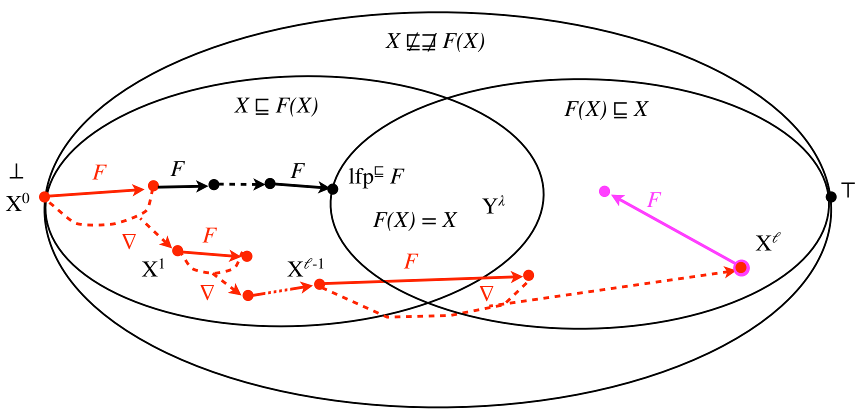
$[l_1, u_1] \mathbin{\nabla_2(j)} [l_2, u_2]$

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

$\textit{if } u_1 < u_2 \leq 0 \textit{ then } 0 \textit{ elsif } u_1 < u_2 \textit{ then } b \textit{ else } u_1 \textit{ fi}]$

[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. Muchnich (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, Y^λ

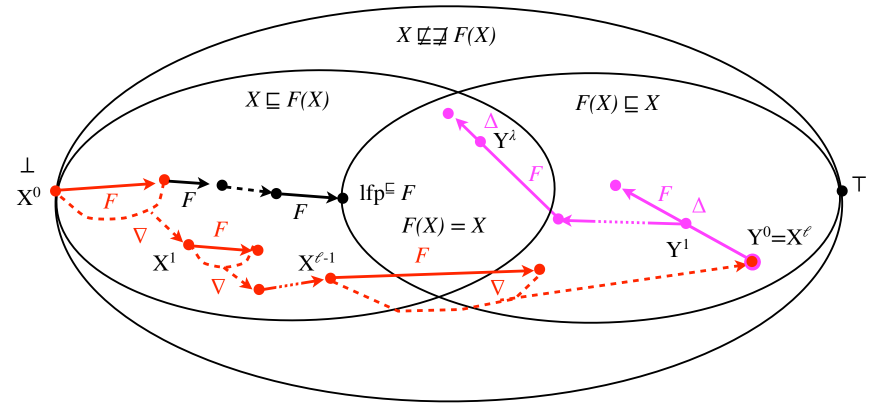
Example of narrowing

- [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



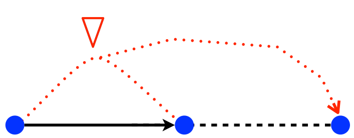
Duality

-

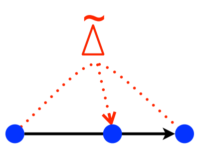
	Convergence above the limit	Convergence below the limit
Increasing iteration	Widening ∇	Dual-narrowing $\widetilde{\Delta}$
Decreasing iteration	Narrowing Δ	Dual widening $\widetilde{\nabla}$

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

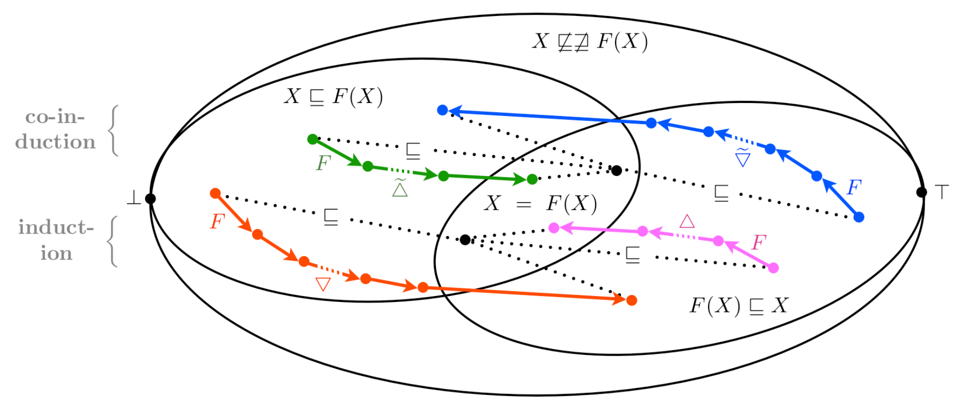
- Extrapolators:



- Interpolators:



Extrapolators, Interpolators, and Duals



Interpolation with dual narrowing

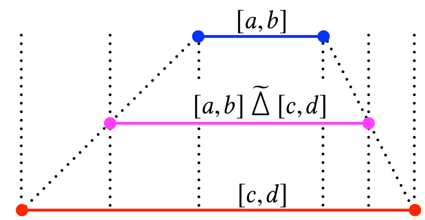
- $Z^0 = \bot$ (increasing iterates with dual-narrowing)

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

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

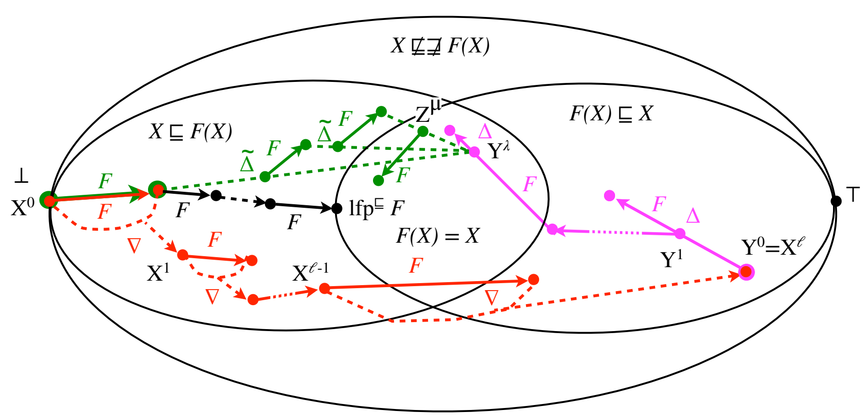
- Dual-narrowing $\widetilde{\Delta}$:
  - $X \sqsubseteq Y \implies X \sqsubseteq X\ \widetilde{\Delta}\ Y \sqsubseteq Y$ (interpolation)
  - Enforces convergence of increasing iterates with dual-narrowing

Example of dual-narrowing

- 

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

Interpolation with dual-narrowing

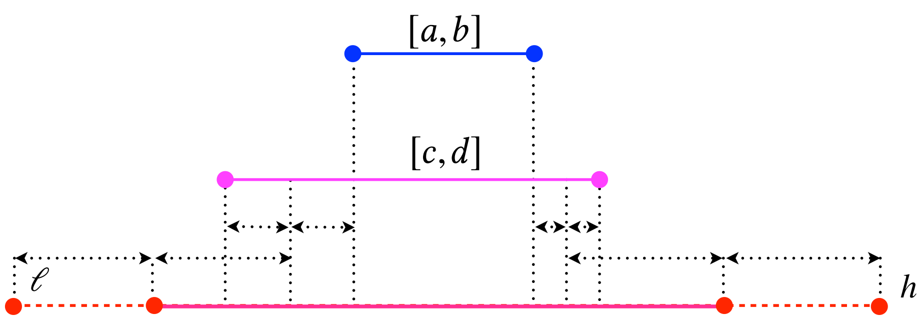


Relationship between narrowing and dual-narrowing

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



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

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

