#### POPL' 15 PC Workshop

# Abstract Interpolation by Dual Narrowing

Princeton University September 27 & 28, 2014

#### Abstract Interpreters

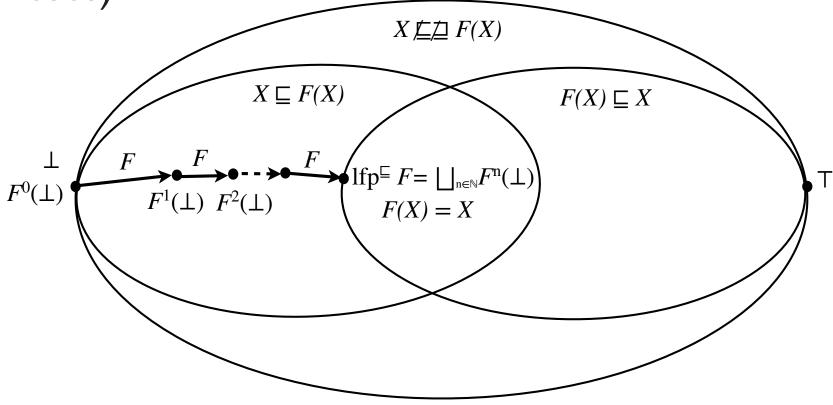
- Transitional abstract interpreters: proceed by induction on program steps
- Structural abstract interpreters: proceed by induction on the program syntax
- Main problem: over/under-approximate fixpoints in non-Noetherian abstract domains

# **Fixpoints**

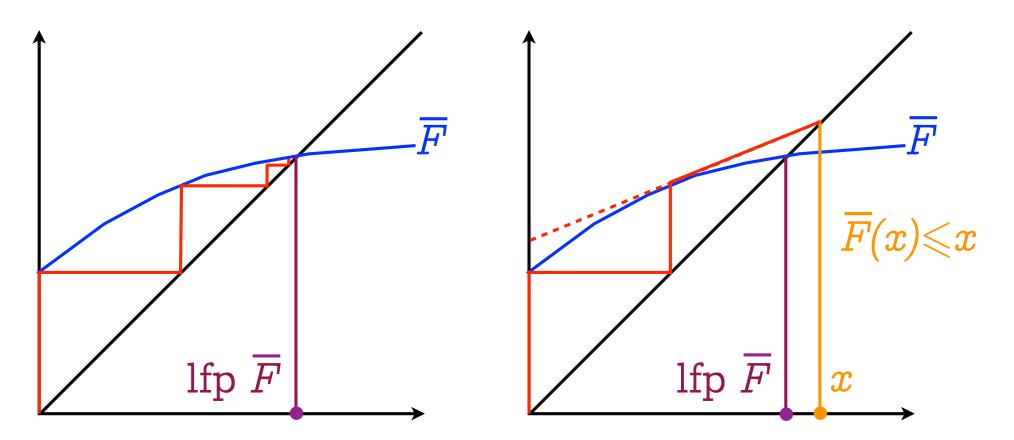
Poset < D, ⊑, ⊥, □>

Transformer: F ∈ D → D

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<sup>(\*)</sup>)

<sup>(\*)</sup> 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  $F(X^n) \not\subseteq X^n$ 

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

- Widening ∇:
  - $\bullet$   $Y \sqsubseteq X \nabla Y$

(extrapolation)

 Enforces convergence of increasing iterates with widening, limit X<sup>e</sup>

## Example of widenings

#### Primitive widening [1,2]

```
(x \ \overline{v} \ y) = \underline{\operatorname{cas}} \ x \in V_{a}, \ y \in V_{a} \ \underline{\operatorname{dans}}
- \square, ? \Longrightarrow y ;
- ?, \square \Longrightarrow x ;
- [n_{1}, m_{1}], [n_{2}, m_{2}] \Longrightarrow
- [\underline{\operatorname{si}} \ n_{2} < n_{1} \ \underline{\operatorname{alors}} \ -\infty \ \underline{\operatorname{sinon}} \ n_{1} \ \underline{\operatorname{fsi}} \ ;
\underline{\operatorname{sim}}_{2} > m_{1} \ \underline{\operatorname{alors}} + \infty \ \underline{\operatorname{sinon}} \ m_{1} \ \underline{\operatorname{fsi}} \ ;
\underline{\operatorname{fincas}} \ ;
```

$$[a_1, b_1] \overline{\nabla} [a_2, b_2] =$$

$$[\underline{if} \ a_2 < a_1 \underline{then} -\infty \underline{else} \ a_1 \underline{fi},$$

$$\underline{if} \ b_2 > b_1 \underline{then} +\infty \underline{else} \ b_1 \underline{fi}]$$

#### Widening with thresholds [3]

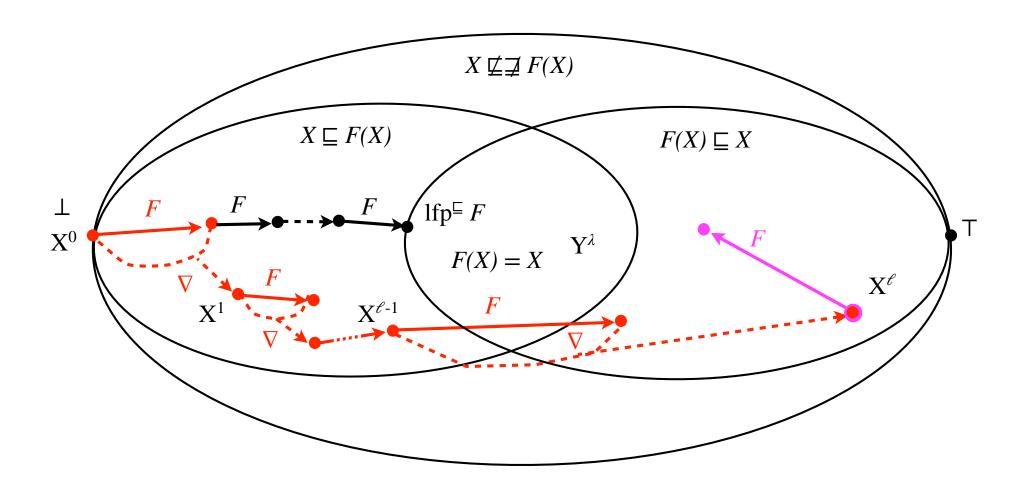
```
\forall x \in \bar{L}_2, \perp \nabla_2(j) x = x \nabla_2(j) \perp = x
[l_1, u_1] \nabla_2(j) [l_2, u_2]
= [if \ 0 \le l_2 < l_1 \ then \ 0 \ elsif \ l_2 < l_1 \ then \ -b - 1 \ else \ l_1 \ fi,
if \ u_1 < u_2 \le 0 \ then \ 0 \ elsif \ u_1 < u_2 \ then \ b \ else \ u_1 \ fi]
```

<sup>[1]</sup> Patrick Cousot, Radhia Cousot: Vérification statique de la cohérence dynamique des programmes, Rapport du contrat IRIA-SESORI No 75-032, 23 septembre 1975.

<sup>[2]</sup> 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

<sup>[3]</sup> 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

$$\bullet$$
 Y<sup>0</sup> = X <sup>$\ell$</sup> 

(decreasing iterates with narrowing)

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

- Narrowing  $\Delta$ :
  - $\bullet \ \ Y \sqsubseteq X \implies \ \ Y \sqsubseteq X \ \Delta \ \ Y \sqsubseteq X$

(interpolation)

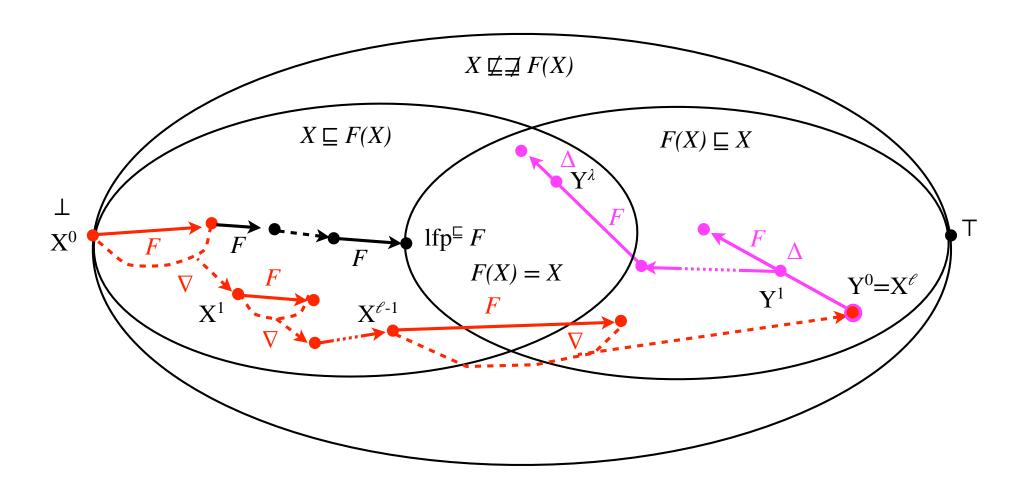
• Enforces convergence of decreasing iterates with narrowing,  $Y^{\lambda}$ 

# Example of narrowing

• [2]

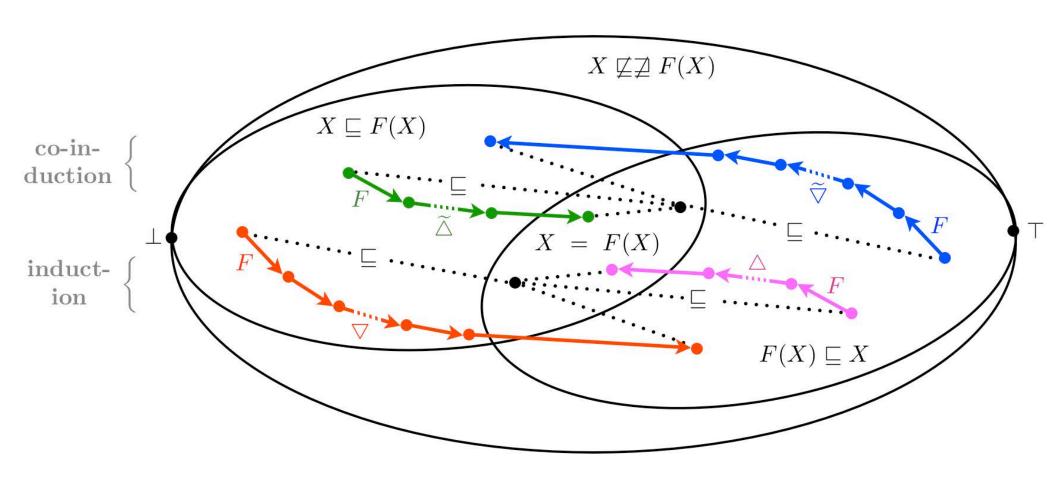
```
\begin{bmatrix} a_1,b_1 \end{bmatrix} \bar{\Delta} \begin{bmatrix} a_2,b_2 \end{bmatrix} =
\begin{bmatrix} \underline{if} \ a_1 = -\infty \ \underline{then} \ a_2 \ \underline{else} \ MIN \ (a_1,a_2), \\ \underline{if} \ b_1 = +\infty \ \underline{then} \ b_2 \ \underline{else} \ MAX \ (b_1,b_2) \end{bmatrix}
```

## Interpolation with narrowing



fincas erate conver-[Semi-]dual abstract in the convertion methods The strictly increasing infinite chain tes the least has an upper bound which is  $[1, +\infty]$ . applying the function as in Def. 2, its derivative is used to accelerate converthe widening fincas gence and ultimately reach a Fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter approblem is a fire flypofor who cabeter approblem in a fire flypofor who cabeter appropriate approp ition ||properthe pro fixpoint [36]. A similar wideninghis limilicity sused tily [18 creasing infinite chains, in **c**onvergence të massing or X THE exting abstonate evaluation will plusting to introduce the entire interest of a second entire transfer of the entire entire transfer of the entire ent es are useful [6], the narrowing [7] and their duals [11]. In [5], the approximation propere objective is ties of extrapolation operators are considered separately from their convergence decreasing properties. Their approvimation properties are isoful to approximate missing or perations. Independently, their convergence properties are useful inition de v s cost ination of iterations for fixpoint approximation The objective elow the limit to over-approximate or under-approximate the limit of increasing or decreasing  $(x, \bar{y}, y)$ fixpoint iterations, so that the various possibilities are to sufficiently as (v, v,) owi<u>ng</u> Ã on of the least  $\overline{\widetilde{f \nabla}}$ Convergence above the limit Convergence below the limit wing" of abstract values den Widening ∇ Increasing iteration [Semi-]dual abstract induction methods  $X \not\sqsubseteq \not\supseteq F(X)$  $X \sqsubseteq F(X)$ 

#### Extrapolators, Interpolators, and Duals



#### Interpolation with dual narrowing

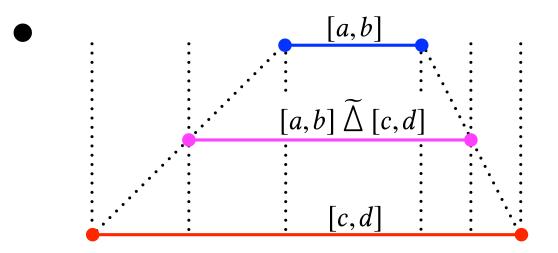
•  $Z^0 = \bot$  (increasing iterates with dual-narrowing)

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

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

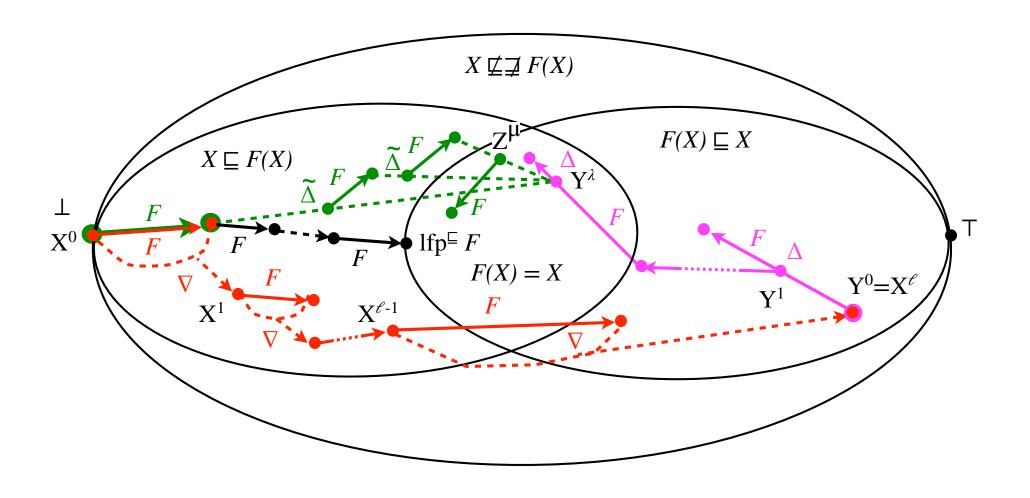
- Dual-narrowing  $\tilde{\Delta}$ :
  - $\bullet \ \ X \sqsubseteq Y \ \implies \ \ X \sqsubseteq X \widetilde{\Delta} \ Y \sqsubseteq Y \qquad \text{(interpolation)}$
  - Enforces convergence of increasing iterates with dual-narrowing

## Example of dual-narrowing



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



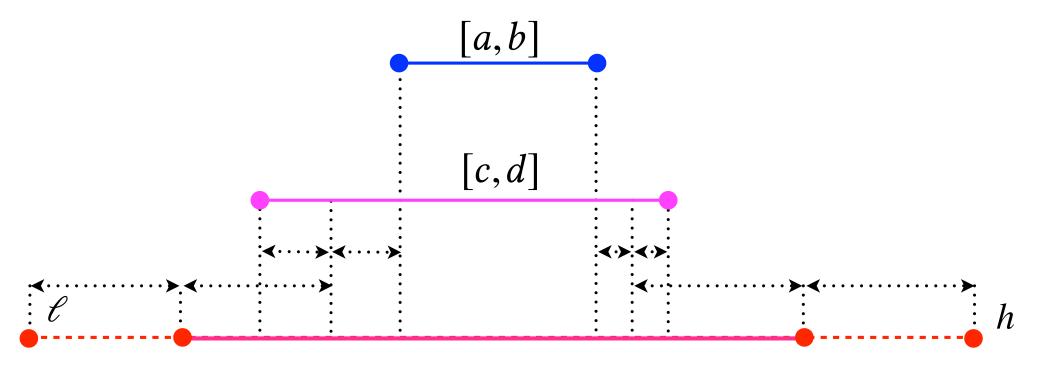
#### Relationship between narrowing and dual-narrowing

$$\bullet \quad \widetilde{\Delta} = \Delta^{-1}$$

- $\bullet \ \ Y \sqsubseteq X \implies Y \sqsubseteq X \triangle Y \sqsubseteq X$  (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)?
  - $F(X) \sqsubseteq B \Longrightarrow F(X) \sqsubseteq F(X) \widetilde{\Delta} B \sqsubseteq B$  (dual-narrowing)
  - $X \sqsubseteq F(X) \sqsubseteq B \Longrightarrow F(X) \sqsubseteq X \nabla_B F(X) \sqsubseteq B$  (bounded widening)

## Example of widenings (cont'd)

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



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

#### 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