HARVARD
School of Engineering
and Applied Sciences

Abstract Interpretation:
Fixpoints, widening, and narrowing

CS252r Fall 2015

Slides from
Principles of Program Analysis
by Nielson, Nielson, and Hankin

http://www2.imm.dtu.dk/~riis/PPA/ppasup2004.html

The need for fix-points

- Let L be complete lattice
- Suppose $f{:}L \rightarrow L$ is program analysis for some program construct p
  - i.e. $p \vdash l_1 \triangleright l_2$ where $f(l_1)=l_2$
  - monotonic function
- If p is recursive or iterative program construct, want to find **least fixed point** (lfp) of f.
  - Most precise lattice element representing analysis of executing p unbounded number of times

Fixed points

Let $f : L \to L$ be a *monotone function* on a complete lattice $L = (L, \sqsubseteq, \sqcup, \sqcap, \bot, \top)$.

l is a *fixed point* iff $f(l) = l$ $\qquad$ $\mathit{Fix}(f) = \{l \mid f(l) = l\}$

Tarski's Theorem: *Fix(f)* is a complete lattice

Fixed points

Let $f : L \to L$ be a *monotone function* on a complete lattice $L = (L, \sqsubseteq, \sqcup, \sqcap, \bot, \top)$.

l is a *fixed point*	iff $f(l) = l$	$\mathit{Fix}(f) = \{l \mid f(l) = l\}$
f is *reductive* at l	iff $f(l) \sqsubseteq l$	$\mathit{Red}(f) = \{l \mid f(l) \sqsubseteq l\}$
f is *extensive* at l	iff $f(l) \sqsupseteq l$	$\mathit{Ext}(f) = \{l \mid f(l) \sqsupseteq l\}$

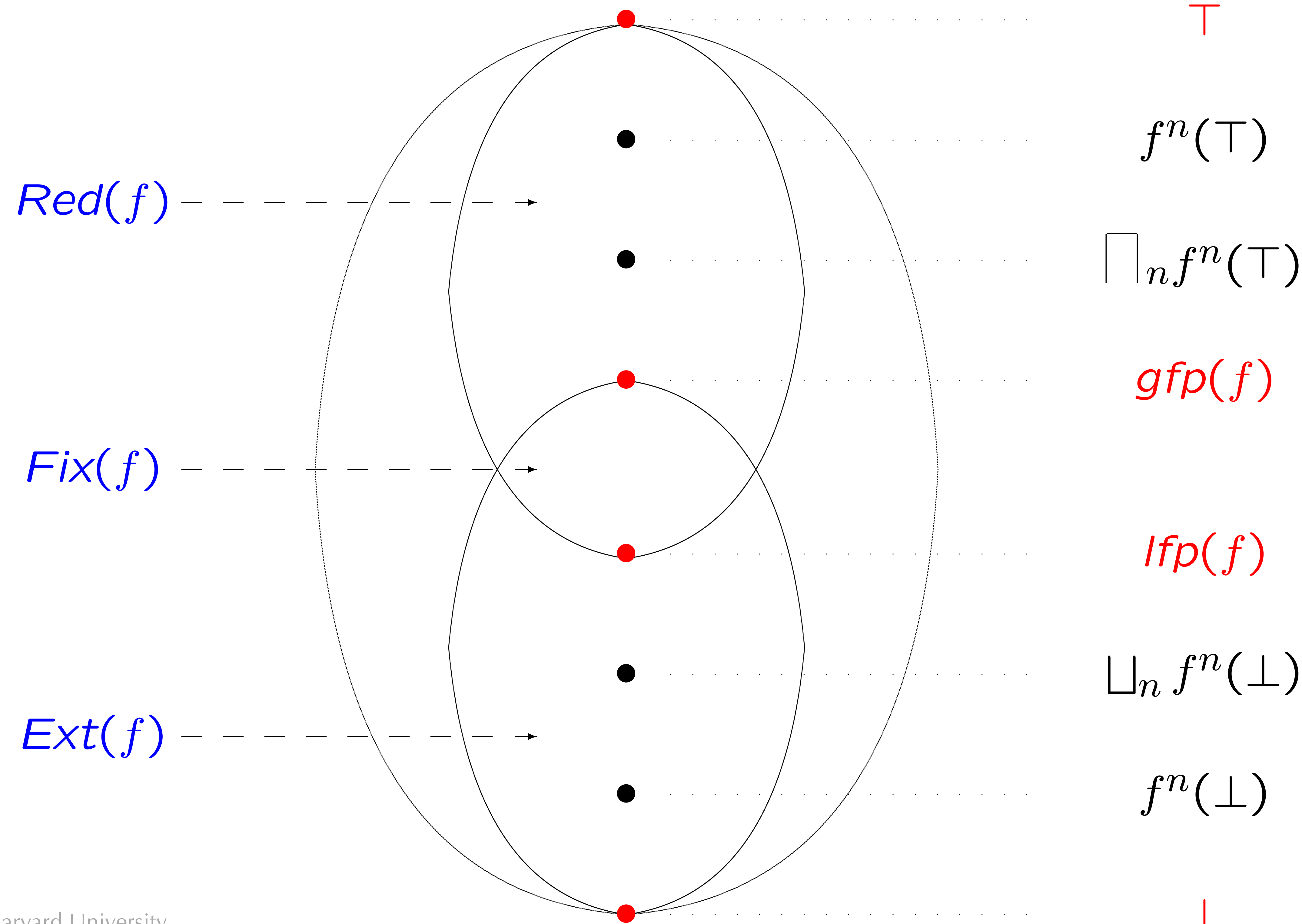
Tarski's Theorem ensures that

Tarski's Theorem: *Fix(f)* is a complete lattice

$$\mathit{lfp}(f) = \bigsqcap \mathit{Fix}(f) = \bigsqcap \mathit{Red}(f) \in \mathit{Fix}(f) \subseteq \mathit{Red}(f)$$

$$\mathit{gfp}(f) = \bigsqcup \mathit{Fix}(f) = \bigsqcup \mathit{Ext}(f) \in \mathit{Fix}(f) \subseteq \mathit{Ext}(f)$$

Fixed points of f



Need for approximation

- How do we find lfp(f)?
- Ideally use iterative sequence
  - $(f^n(\bot))_n = \bot, f(\bot), f(f(\bot)), \ldots$
- But:
  - may not stabilize
    - if L doesn't meet ascending chain condition
  - least upper bound of $(f^n(\bot))_n$ may not equal lfp(f)
    - Why?
    - No guarantee f is continuous, and so Kleene's fixed-point theorem doesn't apply
- Need to approximate...

Scott-continuous: $f{:}L \to L$ is Scott-continuous if for all $S \subseteq L$, we have $f(\bigsqcup S) = \bigsqcup f(S)$

Kleene's Fixed-Point Theorem: If $(L, \sqsubseteq)$ is a complete partial order and $f{:}L \to L$ is Scott-continuous, then f has a least fixed point, equal to LUB of $\bot, f(\bot), f(f(\bot)), \ldots$

One possibility

- Start with $\top$ and repeatedly apply f
  - i.e., $(f^n(\top))_n = \top, f(\top), f(f(\top)), \ldots$
- Even if it doesn't stabilize, will always be a sound approximation
  - for all i we have $\text{lfp}(f) \sqsubseteq f^n(\top)$
  - Means that can stop when we run out of patience, and have sound approximation
- But in practice, too imprecise.

Widening operators

- Key idea: replace $(f^n(\bot))_n$ with sequence $(f_\nabla{}^n)_n$ such that
  - $(f_\nabla{}^n)_n$ guaranteed to stabilize with safe (upper) approximation of lfp(f)
- ∇ is a **widening operator**
  - An upper bound operator satisfying a finiteness condition

Upper bound operators

Let $(l_n)_n$ be a sequence of elements of L. Define the sequence $(l_n^{\breve{\sqcup}})_n$ by:

$$l_n^{\breve{\sqcup}} = \begin{cases} l_n & \text{if } n = 0 \\ l_{n-1}^{\breve{\sqcup}} \mathbin{\breve{\sqcup}} l_n & \text{if } n > 0 \end{cases}$$

Upper bound operators

Let $(l_n)_n$ be a sequence of elements of L. Define the sequence $(l_n^{\breve{\sqcup}})_n$ by:

$$l_n^{\breve{\sqcup}} = \begin{cases} l_n & \text{if } n = 0 \\ l_{n-1}^{\breve{\sqcup}} \;\breve{\sqcup}\; l_n & \text{if } n > 0 \end{cases}$$

Fact: If $(l_n)_n$ is a sequence and $\breve{\sqcup}$ is an upper bound operator then $(l_n^{\breve{\sqcup}})_n$ is an ascending chain; furthermore $l_n^{\breve{\sqcup}} \sqsupseteq \bigsqcup\{l_0, l_1, \cdots, l_n\}$ for all n.

Example

An upper bound operator:

$$int_1 \,\breve{\sqcup}^{int}\, int_2 = \begin{cases} int_1 \sqcup int_2 & \text{if } int_1 \sqsubseteq int \;\vee\; int_2 \sqsubseteq int_1 \\ [-\infty, \infty] & \text{otherwise} \end{cases}$$

Example: $[1,2]\breve{\sqcup}^{[0,2]}[2,3] = [1,3]$ and $[2,3]\breve{\sqcup}^{[0,2]}[1,2] = [-\infty,\infty]$.

Example

An upper bound operator:

$$int_1 \check{\sqcup}^{int} int_2 = \begin{cases} int_1 \sqcup int_2 & \text{if } int_1 \sqsubseteq int \lor int_2 \sqsubseteq int_1 \\ [-\infty, \infty] & \text{otherwise} \end{cases}$$

Example: $[1,2] \check{\sqcup}^{[0,2]} [2,3] = [1,3]$ and $[2,3] \check{\sqcup}^{[0,2]} [1,2] = [-\infty, \infty]$.

Transformation of:	$[0,0], [1,1], [2,2], [3,3], [4,4], [5,5], \cdots$
If $int = [0, \infty]$:	$[0,0], [0,1], [0,2], [0,3], [0,4], [0,5], \cdots$
If $int = [0, 2]$:	$[0,0], [0,1], [0,2], [0,3], [-\infty,\infty], [-\infty,\infty], \cdots$

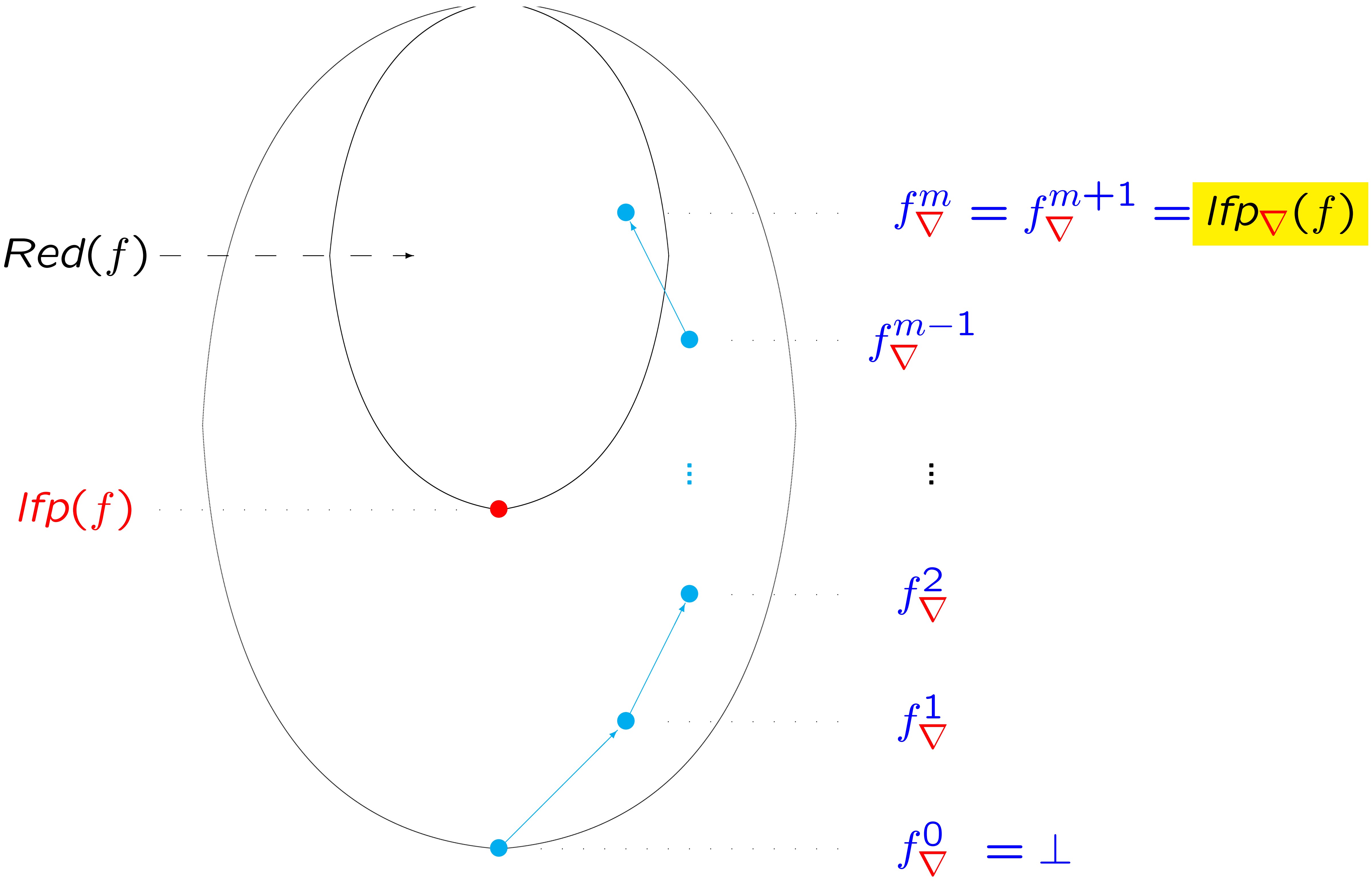
Widening operators

- Operator $\nabla : L \times L \to L$ is a **widening operator** iff
  - ∇ is an upper bound operator
  - for all ascending chains $(l_n)_n$ the ascending chain $(l^{\nabla}_n)_n$ eventually stabilizes
    - $l^{\nabla}_n = l_n$ if $n = 0$
    - $l^{\nabla}_n = l^{\nabla}_{n-1} \nabla l_n$ otherwise

Widening operators

- For monotonic function f: $L \rightarrow L$ and widening operator ∇ define $(f_\nabla^{n})_n$ by
  - $f_\nabla^{n} = \bot$ if $n = 0$
  - $f_\nabla^{n} = f_\nabla^{n-1}$ if $n > 0$ and $f(f_\nabla^{n-1}) \sqsubseteq f_\nabla^{n-1}$
  - $f_\nabla^{n} = f_\nabla^{n-1} \nabla f(f_\nabla^{n-1})$ otherwise
- This is an ascending chain that eventually stabilizes
  - when $f(f_\nabla^{m}) \sqsubseteq f_\nabla^{m}$ for some m
- Tarski's Thm then gives $f_\nabla^{m} \sqsupseteq \text{lfp}(f)$

Diagrammatically



Example

We shall define a widening operator ∇ based on K.

Example

We shall define a widening operator ∇ based on K.

Idea: $[z_1, z_2] \nabla [z_3, z_4]$ is

$$[\ \mathrm{LB}(z_1, z_3)\ ,\ \mathrm{UB}(z_2, z_4)\ ]$$

where

- $\mathrm{LB}(z_1, z_3) \in \{z_1\} \cup K \cup \{-\infty\}$ is the best possible lower bound, and
- $\mathrm{UB}(z_2, z_4) \in \{z_2\} \cup K \cup \{\infty\}$ is the best possible upper bound.

The effect: a change in any of the bounds of the interval $[z_1, z_2]$ can only take place finitely many times – corresponding to the cardinality of K.

Example

Let $z_i \in \mathbf{Z}' = \mathbf{Z} \cup \{-\infty, \infty\}$ and write:

$$\mathrm{LB}_K(z_1, z_3) = \begin{cases} z_1 & \text{if } z_1 \leq z_3 \\ k & \text{if } z_3 < z_1 \ \wedge \ k = \max\{k \in K \mid k \leq z_3\} \\ -\infty & \text{if } z_3 < z_1 \ \wedge \ \forall k \in K : z_3 < k \end{cases}$$

$$\mathrm{UB}_K(z_2, z_4) = \begin{cases} z_2 & \text{if } z_4 \leq z_2 \\ k & \text{if } z_2 < z_4 \ \wedge \ k = \min\{k \in K \mid z_4 \leq k\} \\ \infty & \text{if } z_2 < z_4 \ \wedge \ \forall k \in K : k < z_4 \end{cases}$$

$$\mathit{int}_1 \mathbin{\nabla} \mathit{int}_2 = \begin{cases} \bot & \text{if } \mathit{int}_1 = \mathit{int}_2 = \bot \\ [\ \mathrm{LB}_K(\inf(\mathit{int}_1), \inf(\mathit{int}_2))\ ,\ \mathrm{UB}_K(\sup(\mathit{int}_1), \sup(\mathit{int}_2))\ ] & \text{otherwise} \end{cases}$$

Example

Consider the ascending chain $(int_n)_n$

$$[0,1],[0,2],[0,3],[0,4],[0,5],[0,6],[0,7],\cdots$$

and assume that $K = \{3, 5\}$.

Then $(int_n^{\nabla})_n$ is the chain

$$[0,1],[0,3],[0,3],[0,5],[0,5],[0,\infty],[0,\infty],\cdots$$

which eventually stabilises.

Defining widening operators

- Suppose we have two complete lattices, L and M, and a Galois connection (L, α, γ, M) between them
- One possibility: replace analysis $f{:}L \rightarrow L$ with analysis $g{:}M \rightarrow M$
  - Can **induce** g from f
  - But may reduce precision of analysis
- Another possibility
  - Use M just to ensure convergence of fixedpoints
  - Assume upper bound operator ∇_M for M
  - Define $l_1 \nabla_L l_2 = \gamma(\ \alpha(l_1)\ \nabla_M\ \alpha(l_2)\ )$
  - ∇_L is widening operator if either
    (i) M has no infinite ascending chains or
    (ii) (L, α, γ, M) is Galois insertion and ∇_M is widening operator

Improving on $\mathrm{lfp}_\nabla(f)$

- Widening gives upper approximation $\mathrm{lfp}_\nabla(f)$ of $\mathrm{lfp}(f)$

- But $f(\mathrm{lfp}_\nabla(f)) \sqsubseteq \mathrm{lfp}_\nabla(f)$ so we can improve approximation by considering sequence $(f^n(\mathrm{lfp}_\nabla(f)))_n$
- For all i we have $\mathrm{lfp}(f) \sqsubseteq f^i(\mathrm{lfp}_\nabla(f)) \sqsubseteq \mathrm{lfp}_\nabla(f)$
    - So can stop anytime with an upper approximation

- Defining a **narrowing operator** gives a way to describe when to stop

Narrowing operator

An operator $\triangle : L \times L \to L$ is a *narrowing operator* iff

- $l_2 \sqsubseteq l_1 \;\Rightarrow\; l_2 \sqsubseteq (l_1 \triangle l_2) \sqsubseteq l_1$ for all $l_1, l_2 \in L$, and
- for all descending chains $(l_n)_n$ the sequence $(l_n^{\triangle})_n$ eventually stabilises.

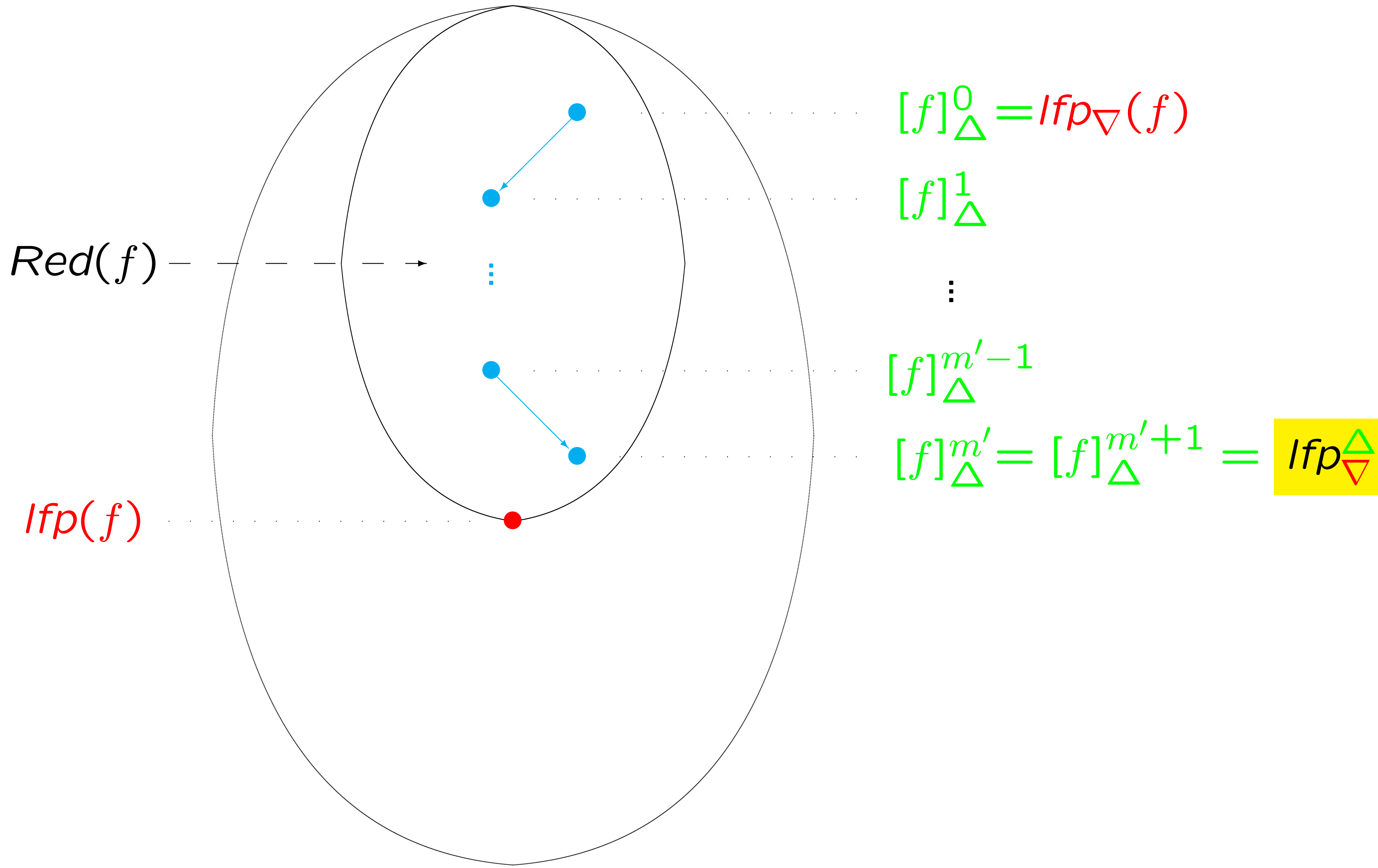
We construct the sequence $([f]^n_{\triangle})_n$

$$[f]^n_{\triangle} = \begin{cases} \mathit{lfp}_{\nabla}(f) & \text{if } n = 0 \\ [f]^{n-1}_{\triangle} \triangle f([f]^{n-1}_{\triangle}) & \text{if } n > 0 \end{cases}$$

One can show that:

- $([f]^n_{\triangle})_n$ is a descending chain where all elements satisfy $\mathit{lfp}(f) \sqsubseteq [f]^n_{\triangle}$
- the chain eventually stabilises so $[f]^{m'}_{\triangle} = [f]^{m'+1}_{\triangle}$ for some value m'

Diagrammatically



Example

The complete lattice (**Interval**, $\sqsubseteq$) has two kinds of infinite descending chains:

- those with elements of the form $[-\infty, z]$, $z \in \mathbf{Z}$
- those with elements of the form $[z, \infty]$, $z \in \mathbf{Z}$

Idea: Given some fixed non-negative number N
the narrowing operator $\triangle_N$ will force an infinite descending chain

$$[z_1, \infty], [z_2, \infty], [z_3, \infty], \cdots$$

(where $z_1 < z_2 < z_3 < \cdots$) to stabilise when $z_i > N$

Similarly, for a descending chain with elements of the form $[-\infty, z_i]$ the narrowing operator will force it to stabilise when $z_i < -N$

Example

Define $\triangle = \triangle_N$ by

$$int_1 \;\triangle\; int_2 \;=\; \begin{cases} \bot & \text{if } int_1 = \bot \;\vee\; int_2 = \bot \\ [z_1, z_2] & \text{otherwise} \end{cases}$$

where

$$z_1 \;=\; \begin{cases} \inf(int_1) & \text{if } N < \inf(int_2) \wedge \sup(int_2) = \infty \\ \inf(int_2) & \text{otherwise} \end{cases}$$

$$z_2 \;=\; \begin{cases} \sup(int_1) & \text{if } \inf(int_2) = -\infty \wedge \sup(int_2) < -N \\ \sup(int_2) & \text{otherwise} \end{cases}$$

Consider the infinite descending chain $([n, \infty])_n$

$$[0,\infty],[1,\infty],[2,\infty],[3,\infty],[4,\infty],[5,\infty],\cdots$$

and assume that $N = 3$.

Then the narrowing operator $\triangle_N$ will give the sequence $([n, \infty]^{\triangle})_n$

$$[0,\infty],[1,\infty],[2,\infty],[3,\infty],[3,\infty],[3,\infty],\cdots$$

Summary

- Given monotonic $f{:}L \rightarrow L$ where L is a lattice
- Approximating least fixed point of f accurately and quickly a key challenge of program analysis
- Widening operators
- Widening following by narrowing