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 $L = (L, \sqsubseteq, \sqcup, \sqcap, \bot, \top)$. 

Tarski's Theorem ensures that $\text{lfp } f = \text{Fix } f = \text{Red } f \in \text{Fix } f \subseteq \text{Red } f$.
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 $f(l) = l$,
  \[ \text{Fix}(f) = \{ l \mid f(l) = l \} \]
- $f$ is **reductive** at $l$ iff $f(l) \sqsubseteq l$,
  \[ \text{Red}(f) = \{ l \mid f(l) \sqsubseteq l \} \]
- $f$ is **extensive** at $l$ iff $f(l) \sqsupseteq l$,
  \[ \text{Ext}(f) = \{ l \mid f(l) \sqsupseteq l \} \]

**Tarski’s Theorem** ensures that

\[
\text{lfp}(f) = \bigcap \text{Fix}(f) = \bigcap \text{Red}(f) \subseteq \text{Fix}(f) \subseteq \text{Red}(f)
\]
\[
\text{gfp}(f) = \bigcup \text{Fix}(f) = \bigcup \text{Ext}(f) \subseteq \text{Fix}(f) \subseteq \text{Ext}(f)
\]}
Fixed points of $f$
Need for approximation

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

• \(\nabla\) is a widening operator
  • An upper bound operator satisfying a finiteness condition
Upper bound operators

\( \triangleright : L \times L \rightarrow L \) is an upper bound operator iff

\[ l_1 \sqsubseteq l_1 \triangleright l_2 \sqsubseteq l_2 \]

for all \( l_1, l_2 \in L \).
Upper bound operators

\( \sqcup : L \times L \rightarrow L \) is an upper bound operator iff

\[ l_1 \sqsubseteq l_1 \sqcup l_2 \sqsupseteq l_2 \]

for all \( l_1, l_2 \in L \).

Let \((l_n)_n\) be a sequence of elements of \( L \). Define the sequence \((\sqcup l_n)_n\) by:

\[ l_n = \begin{cases} 
    l_n & \text{if } n = 0 \\
    l_{n-1} \sqcup l_n & \text{if } n > 0 
\end{cases} \]

**Fact:** If \((l_n)_n\) is a sequence and \( \sqcup \) is an upper bound operator then \((\sqcup l_n)_n\) is an ascending chain; furthermore \( l_n \sqsupseteq \sqcup \{l_0, l_1, \ldots, l_n\} \) for all \( n \).
Let $\textit{int}$ be an arbitrary but fixed element of $\text{Interval}$.

An upper bound operator:

$$
\text{int}_1 \uparrow^{\text{int}} \text{int}_2 = \begin{cases} 
\text{int}_1 \sqcup \text{int}_2 & \text{if } \text{int}_1 \sqsubseteq \text{int} \lor \text{int}_2 \sqsubseteq \text{int}_1 \\
[-\infty, \infty] & \text{otherwise}
\end{cases}
$$
Let \( int \) be an arbitrary but fixed element of \textit{Interval}.

An upper bound operator:

\[
\text{int}_1 \uparrow^{\text{int}} \text{int}_2 = \begin{cases} \text{int}_1 \sqcup \text{int}_2 & \text{if int}_1 \subseteq \text{int} \lor \text{int}_2 \subseteq \text{int}_1 \\ [-\infty, \infty] & \text{otherwise} \end{cases}
\]

Example: \([1, 2] \uparrow^{[0,2]} [2, 3] = [1, 3]\) and \([2, 3] \uparrow^{[0,2]} [1, 2] = [-\infty, \infty]\).

Transformation of: \([0, 0], [1, 1], [2, 2], [3, 3], [4, 4], [5, 5], \ldots\)

If \( \text{int} = [0, \infty] \):
\([0, 0], [0, 1], [0, 2], [0, 3], [0, 4], [0, 5], \ldots\)

If \( \text{int} = [0, 2] \):
\([0, 0], [0, 1], [0, 2], [0, 3], [-\infty, \infty], [-\infty, \infty], \ldots\)

© 2011 Stephen Chong, Harvard University
Widening operators

• Operator $\triangledown : L \times L \rightarrow L$ is a \textit{widening operator} iff
  
  • $\triangledown$ is an upper bound operator
  
  • for all ascending chains $(l_n)_n$ the ascending chain $(\triangledown_n)_n$ eventually stabilizes
    
    • $\triangledown_n = l_n$ if $n = 0$
    
    • $\triangledown_n = \triangledown_{n-1} \triangledown l_n$ otherwise
Widening operators

• For monotonic function \( f: L \rightarrow L \) and widening operator \( \nabla \) define \((f^{\nabla n})_n\) by
  
  • \( f^{\nabla n} = \perp \) 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

\[ \text{Red}(f) \rightarrow \text{lfp}(f) \]

\[ f^m \downarrow = f^{m+1} = \text{lfp}_{\downarrow}(f) \]

© 2011 Stephen Chong, Harvard University
Example

Let $K$ be a finite set of integers, e.g. the set of integers explicitly mentioned in a given program.
Let $K$ be a finite set of integers, e.g. the set of integers explicitly mentioned in a given program.

We shall define a widening operator $\triangledown$ based on $K$.

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

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

where

- $\text{LB}(z_1, z_3) \in \{z_1\} \cup K \cup \{-\infty\}$ is the best possible lower bound, and
- $\text{UB}(z_2, z_4) \in \{z_2\} \cup K \cup \{\infty\}$ 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 $z_i \in \mathbb{Z}' = \mathbb{Z} \cup \{-\infty, \infty\}$ and write:

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

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

$$\text{int}_1 \downarrow \text{int}_2 = \begin{cases} \bot & \text{if } \text{int}_1 = \text{int}_2 = \bot \\ [\text{LB}_K(\inf(\text{int}_1), \inf(\text{int}_2)), \text{UB}_K(\sup(\text{int}_1), \sup(\text{int}_2))] & \text{otherwise} \end{cases}$$
Consider the ascending chain \((\text{int}_n)_n\)

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

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

Then \((\text{int}_n^\nabla)_n\) is the chain

\[ [0, 1], [0, 3], [0, 3], [0, 5], [0, 5], [0, \infty], [0, \infty], \ldots \]

which eventually stabilises.
Defining widening operators

• Suppose we have two complete lattices, $L$ and $M$, and a Galois connection $(L, \alpha, \gamma, M)$ 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 $\nabla_M$ for $M$
  • Define $l_1 \nabla_L l_2 = \gamma(\alpha(l_1) \nabla_M \alpha(l_2))$
  • $\nabla_L$ is widening operator if either
    (i) $M$ has no infinite ascending chains or
    (ii) $(L, \alpha, \gamma, M)$ is Galois insertion and $\nabla_M$ is widening operator.
Improving on lfp$_\triangledown$(f)

• Widening gives upper approximation lfp$_\triangledown$(f) of lfp(f)

• But $f(lfp$_\triangledown$(f)) \subseteq lfp$_\triangledown$(f)$ so we can improve approximation by considering sequence $(f^n(lfp$_\triangledown$(f)))_n$

• For all $i$ we have $lfp(f) \subseteq f^i(lfp$_\triangledown$(f)) \subseteq lfp$_\triangledown$(f)$
  • So can stop anytime with an upper approximation

• Defining a **narrowing operator** gives a way to describe when to stop
Narrowing operator

An operator $\Delta : L \times L \rightarrow L$ is a narrowing operator iff

- $l_2 \sqsubseteq l_1 \Rightarrow l_2 \sqsubseteq (l_1 \Delta l_2) \sqsubseteq l_1$ for all $l_1, l_2 \in L$, and

- for all descending chains $(l_n)_n$ the sequence $(l_n^\Delta)_n$ eventually stabilises.

We construct the sequence $([f]^n_\Delta)_n$

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

One can show that:

- $( [f]^n_\Delta)_n$ is a descending chain where all elements satisfy $\text{lfp}(f) \sqsubseteq [f]^n_\Delta$

- the chain eventually stabilises so $[f]^{m'}_{\Delta} = [f]^{m'+1}_{\Delta}$ for some value $m'$
The narrowing operator \( \Delta \) applied to \( f \).

\[
\text{Red}(f) \Rightarrow \ldots \Rightarrow [f]_{\Delta}^0 = \text{lfp}_\nabla(f) \Rightarrow [f]_{\Delta}^1 \Rightarrow \ldots \Rightarrow [f]_{\Delta}^{m'-1} \Rightarrow [f]_{\Delta}^m = [f]_{\Delta}^{m'+1} = \text{lfp}_\nabla
\]
Example

The complete lattice \((\text{Interval}, \sqsubseteq)\) has two kinds of infinite descending chains:

- those with elements of the form \([-\infty, z], z \in \mathbb{Z}\)
- those with elements of the form \([z, \infty], z \in \mathbb{Z}\)

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

\([z_1, \infty], [z_2, \infty], [z_3, \infty], \ldots\)

(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 $\Delta = \Delta_N$ by

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

where

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

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

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 $\Delta_N$ will give the sequence $([n, \infty]^{\Delta})_n$

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