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** \((\text{lfp})\) of \( f \).
  • Most precise lattice element representing analysis of executing \( p \) unbounded number of times
Let \( f : L \rightarrow L \) be a monotone function on a complete lattice \( L = (L, \sqsubseteq, \sqcup, \sqcap, \bot, \top) \).

\( l \) is a fixed point iff \( f(l) = l \)

\[ \text{Fix}(f) = \{ l | f(l) = l \} \]

Tarski's Theorem: \( \text{Fix}(f) \) is a complete lattice
Fixed points

Let \( f : L \to L \) be a \textit{monotone function} on a complete lattice \( L = (L, \sqsubseteq, \cup, \cap, \bot, \top) \).

- \( l \) is a \textbf{fixed point} iff \( f(l) = l \)
- \( f \) is \textbf{reductive} at \( l \) iff \( f(l) \sqsubseteq l \)
- \( f \) is \textbf{extensive} at \( l \) iff \( f(l) \sqsupseteq l \)

\[ \text{Tarski's Theorem} \quad \text{ensures that} \]

\[ \text{Ifp}(f) = \bigsqcap \text{Fix}(f) = \bigsqcap \text{Red}(f) \subseteq \text{Fix}(f) \]

\[ \text{gfp}(f) = \bigsqcup \text{Fix}(f) = \bigsqcup \text{Ext}(f) \subseteq \text{Fix}(f) \]
Fixed points of $f$

- $\text{Red}(f)$
- $\text{Fix}(f)$
- $\text{Ext}(f)$

- $\top$
- $f^n(\top)$
- $\bigcap_n f^n(\top)$
- $\text{gfp}(f)$
- $\text{lfp}(f)$
- $\bigcup_n f^n(\bot)$
- $f^n(\bot)$
- $\bot$
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:** \(f:L \rightarrow L\) 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 \(f:L \rightarrow L\) 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 \(\text{lfp}(f)\)

- \(\nabla\) is a widening operator
  - An upper bound operator satisfying a finiteness condition
Let \((l_n)_n\) be a sequence of elements of \(L\). Define the sequence \((l_{\overset{\L}{\L}})_{n}\) by:

\[
l_{\overset{\L}{\L}} = \begin{cases} 
  l_n & \text{if } n = 0 \\
  l_{n-1} \L l_n & \text{if } n > 0
\end{cases}
\]
Upper bound operators

Let \((l_n)_n\) be a sequence of elements of \(L\). Define the sequence \((\hat{\square}_n)^n\) by:

\[
\hat{\square}_n = \begin{cases} 
    l_n & \text{if } n = 0 \\
    \hat{\square}_{n-1} \sqcup l_n & \text{if } n > 0
\end{cases}
\]

**Fact:** If \((l_n)_n\) is a sequence and \(\sqcup\) is an upper bound operator then \((\hat{\square}_n)^n\) is an ascending chain; furthermore \(\hat{\square}_n \sqcup \bigcup \{l_0, l_1, \ldots, l_n\}\) for all \(n\).
An upper bound operator:

\[ \text{int}_1 \supset \text{int} \supseteq \text{int}_2 = \begin{cases} \text{int}_1 \sqcup \text{int}_2 & \text{if } \text{int}_1 \subseteq \text{int} \lor \text{int}_2 \subseteq \text{int}_1 \\ \left[ -\infty, \infty \right] & \text{otherwise} \end{cases} \]

Example: \([1, 2] \supset [0, 2] [2, 3] = [1, 3]\) and \([2, 3] \supset [0, 2] [1, 2] = [\infty, \infty]\).
Example

An upper bound operator:

\[ \text{int}_1 \sqsupseteq^{\text{int}} \text{int}_2 = \begin{cases} \text{int}_1 \sqsubseteq \text{int}_2 & \text{if } \text{int}_1 \sqsubseteq \text{int} \lor \text{int}_2 \sqsubseteq \text{int}_1 \\ [\infty, \infty] & \text{otherwise} \end{cases} \]

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

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

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

- For monotonic function \( f: L \to L \) and widening operator \( \nabla \) 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 \( f \nabla^m \sqsupseteq \text{lfp}(f) \)
The widening operator applied to $f$.

\[ \text{Red}(f) \quad \Downarrow \quad f^0 \quad \Downarrow \quad f^1 \quad \Downarrow \quad \ldots \quad \Downarrow \quad f^m = f^{m+1} = \text{lfp}_{\Downarrow}(f) \]

Diagrammatically
We shall define a widening operator \( \nabla \) based on \( K \).
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 $K$. 
Let $z_i \in \mathbb{Z}' = \mathbb{Z} \cup \{-\infty, \infty\}$ and write:

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

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

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

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

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

Then \( (int_n^\triangledown)_n \) 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 $\text{lfp}_\triangledown(f)$

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

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

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

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

An operator $\triangle : L \times L \to L$ 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 $([f]_n^{\triangle})_n$

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

One can show that:

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

\[ [f]_\Delta^0 = \text{lfp}_{\nabla}(f) \]

\[ [f]_\Delta^1 \]

\[ \vdots \]

\[ [f]_\Delta^{m'-1} \]

\[ [f]_\Delta^m = [f]_\Delta^{m'+1} = \text{lfp}_{\nabla} \]
The complete lattice \((\text{Interval}, \subseteq)\) 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 \(z_1 < z_2 < z_3 < \ldots\)) 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 \(z_i < -N\)
Define $\Delta = \Delta_N$ by

$$\begin{align*}
\text{int}_1 \Delta \text{int}_2 &= \begin{cases}
\bot & \text{if } \text{int}_1 = \bot \lor \text{int}_2 = \bot \\
[z_1, z_2] & \text{otherwise}
\end{cases}
\end{align*}$$

where

$$\begin{align*}
z_1 &= \begin{cases}
\inf(\text{int}_1) & \text{if } N < \inf(\text{int}_2) \land \sup(\text{int}_2) = \infty \\
\inf(\text{int}_2) & \text{otherwise}
\end{cases}
\end{align*}$$

$$\begin{align*}
z_2 &= \begin{cases}
\sup(\text{int}_1) & \text{if } \inf(\text{int}_2) = -\infty \land \sup(\text{int}_2) < -N \\
\sup(\text{int}_2) & \text{otherwise}
\end{cases}
\end{align*}$$

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

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

and assume that $N = 3$.

Then the narrowing operator $\Delta_N$ will give the sequence $([n, \infty]^\Delta)_n$

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