Discrete Fixpoint Approximation Methods in Program Static Analysis

P. Cousot

Département de Mathématiques et Informatique
École Normale Supérieure – Paris
<couso@dmi.ens.fr>
<http://www.dmi.ens.fr/~cousot>

Static Program analysis

- Automatic determination of runtime properties of infinite state programs
- Applications:
  - compilation (dataflow analysis, type inference),
  - program transformation (partial evaluation, parallelization/vectorization, . . .)
  - program verification (test generation, abstract debugging, . . .)
- Problems:
  - text inspection only (excluding executions or simulations)
  - undecidable
  - necessarily approximate

Example

```
0 1
```

```
{ n:Ω; i:Ω; j:Ω }
read_int(n);
{ n:1; i:Ω; j:Ω }
i := n;
{ n:[0,∞]; i:[0,∞]; j:(1,+∞)? }
while (i <> 0) do
  { n:[0,∞); i:[1,∞); j:[1,∞)? }
  j := 0;
  { n:[0,∞); i:[1,∞); j:[0,∞) }
  while (j <> i) do
    { n:[0,∞); i:[1,∞); j:[0,1073741822]!! }
    j := (j + 1)
    { n:[0,∞); i:[1,∞); j:[1,∞) }
  od;
  { n:[0,∞); i:[1,∞); j:[1,∞) }
i := (i - 1);
{ n:[0,∞); i:[0,1073741822]; j:[1,∞) }
od;
{ n:[0,∞); i:[0,0]; j:[1,∞)? }
```

1 Ω denotes uninitialization.
2 !! denotes inevitable error when the invariant is violated.
3 +∞ = 1073741823, −∞ = −1073741824.
4 This questionmark indicates possible uninitialization.

Abstract interpretation

Abstract interpretation [1, 2]:
- design method for static analysis algorithms;
- effective approximation of the semantics of programs;
- often, the semantics maps the program text to a model of computation obtained as the least fixpoint of an operator on a partially ordered semantic domain;
- effective approximation of fixpoints of posets;

References


Fixpoint semantics

Program semantics can be defined as least fixpoints \[3\]:

$$\text{lfp} \subseteq F$$

where

$$F(\text{lfp} \subseteq F) = \text{lfp} \subseteq F \quad F(x) = x \implies \text{lfp} \subseteq F \subseteq x$$

of a monotonic operator $$F \in \mathcal{L} \mapsto \mathcal{L}$$ on a complete partial order (CPO):

$$\langle \mathcal{L}, \subseteq, \bot, \top, \sqcup \rangle$$

where $$\langle \mathcal{L}, \subseteq \rangle$$ is a poset with infimum $$\bot$$ and the least upper bound (lub) $$\sqcup$$ of increasing chains exists.

Reference


Kleenean fixpoint theorem

- A map $$\varphi \in L \mapsto L$$ on a cpo $$\langle L, \subseteq, \bot, \top \rangle$$ is upper-continuous iff it preserves lubs of increasing chains $$x_i, i \in N$$:

$$\varphi(\bigsqcup_{i \in N} x_i) = \bigsqcup_{i \in N} \varphi(x_i)$$

- The least fixpoint of an upper-continuous map $$\varphi \in L \mapsto L$$ on a cpo $$\langle L, \subseteq, \bot, \top \rangle$$ is:

$$\text{lfp} \varphi = \bigsqcup_{n \geq 0} \varphi^n(\bot)$$

where the iterates $$\varphi^n(x)$$ of $$\varphi$$ from $$x$$ are:

- $$\varphi^0(x) \overset{\text{def}}{=} x$$;
- $$\varphi^{n+1}(x) \overset{\text{def}}{=} \varphi(\varphi^n(x))$$ for all $$x \in L$$.

Tarski’s Fixpoint Theorem

A monotonic map $$\varphi \in L \mapsto L$$ on a complete lattice:

$$\langle L, \subseteq, \bot, \top, \sqcup, \sqcap \rangle$$

has a least fixpoint:

$$\text{lfp} \varphi = \cap \{x \in L \mid \varphi(x) \subseteq x\}$$

and, dually, a greatest fixpoint:

$$\text{gfp} \varphi = \cup \{x \in L \mid x \subseteq \varphi(x)\}$$

Chaotic/asynchronous iterations

- Convergent iterates $$L = \bigsqcup_{n \geq 0} F^n(P)$$ of a monotonic system of equations on a poset:

$$X = F(X) \begin{cases} X_1 = F_1(X_1, \ldots, X_n) \\ \vdots \\ X_n = F_n(X_1, \ldots, X_n) \end{cases}$$

starting from a prefixpoint $$(P \subseteq F(P))$$ always converge to the same limit $$L$$ whichever chaotic or asynchronous iteration strategy is used.
Example: reachability analysis

- Program:
  \[
  \begin{align*}
  &\{ X_1 \} \\
  &x := 1; \\
  &\{ X_2 \} \\
  &\text{while } (x < 1000) \text{ do} \\
  &\quad \{ X_3 \} \\
  &\quad x := x + 1; \\
  &\quad \{ X_4 \} \\
  &\od;
  \end{align*}
  \]
- System of equations:
  \[
  \begin{align*}
  X_1 &= \{ \Omega \} \\
  X_2 &= \{ 1 \} \cup X_4 \\
  X_3 &= \{ x \in X_2 \mid x < 1000 \} \\
  X_4 &= \{ x + 1 \mid x \in X_3 \} \\
  X_5 &= \{ x \in X_2 \mid x \geq 1000 \}
  \end{align*}
  \]
- Reachable states:
  \[
  \begin{align*}
  X_1 &= \{ \Omega \} \\
  X_2 &= \{ x \mid 1 \leq x \leq 1000 \} \\
  X_3 &= \{ x \mid 1 \leq x < 1000 \} \\
  X_4 &= \{ x + 1 \mid x \in X_3 \} \\
  X_5 &= \{ 1000 \}
  \end{align*}
  \]

Effective fixpoint approximation

- Simplify the fixpoint system of semantic equations: Galois connections;
- Accelerate convergence of the iterates: widening/narrowing;

Definition of Galois connections

Given posets \( (P, \sqsubseteq) \) and \( (Q, \preceq) \), a Galois connection is a pair of maps such that:

\[
\begin{align*}
\alpha \in P &\rightarrow Q \\
\gamma \in Q &\rightarrow P
\end{align*}
\]

\( \forall x \in P : \forall y \in Q : \alpha(x) \preceq y \iff x \sqsubseteq \gamma(y) \)

in which case we write:

\[
(P, \sqsubseteq) \xrightarrow{\alpha} (Q, \preceq)
\]

Equivalent definition of Galois connections

\[
\begin{align*}
\langle P, \sqsubseteq \rangle &\xrightarrow{\alpha} \langle Q, \preceq \rangle \quad \text{Galois connection} \\
\alpha &\in \langle D^\ast, \sqsubseteq \rangle \xrightarrow{m} \langle Q, \preceq \rangle \\
\gamma &\in \langle Q, \preceq \rangle \xrightarrow{m} \langle P, \sqsubseteq \rangle \\
\forall x \in P : x &\sqsubseteq \gamma \circ \alpha(x) \quad \alpha \text{ monotone} \\
\forall y \in Q : \alpha \circ \gamma(y) &\preceq y \quad \gamma \circ \alpha \text{ extensive} \\
\end{align*}
\]
Duality principle

• We write \(\leq^{-1}\) or \(\geq\) for the inverse of the partial order \(\leq\).

• Observe that:
  \[
  \langle P, \sqsubseteq \rangle \overset{\gamma}{\leftarrow} \langle Q, \preceq \rangle \]
  if and only if
  \[
  Q(\geq) \overset{\alpha}{\leftarrow} P(\sqsubseteq) \]

• duality principle: if a theorem is true for all posets, then so is its dual obtained by substituting \(\geq\), \(\succ\), \(\bot\), \(\top\), \(\vee\), \(\wedge\), \(\alpha\), \(\gamma\) etc. respectively for \(\leq\), \(<\), \(\sqsubseteq\), \(\sqsupseteq\), \(\land\), \(\lor\), \(\gamma\), \(\alpha\), etc.

Example 1 of Galois connection

If

• \(\varnothing \in P \longrightarrow Q\)

• \(\alpha \in \wp(P) \longrightarrow \wp(Q)\)
  \[
  \alpha(X) \overset{\text{def}}{=} \{ f(x) \mid x \in X \} \]

• \(\gamma \in \wp(Q) \longrightarrow \wp(P)\)
  \[
  \gamma(Y) \overset{\text{def}}{=} \{ x \mid \varnothing(x) \in Y \} \]

then

\[
\langle \wp(P), \subseteq \rangle \overset{\gamma}{\leftarrow} \langle \wp(Q), \subseteq \rangle
\]

Example 2 of Galois connection

If

• \(\rho \subseteq P \times Q\)

• \(\alpha \in \wp(P) \longrightarrow \wp(Q)\)
  \[
  \alpha(X) = \text{post}[\rho]X \quad \text{post-image}
  \]
  \[
  \overset{\text{def}}{=} \{ y \mid \exists x \in X : (x, y) \in \rho \}
  \]

• \(\gamma \in \wp(Q) \longrightarrow \wp(P)\)
  \[
  \gamma(Y) = \text{pre}[\rho]Y \quad \text{dual pre-image}
  \]
  \[
  \overset{\text{def}}{=} \{ x \mid \forall y : (x, y) \in \rho \Rightarrow y \in Y \}
  \]

then

\[
\langle \wp(P), \subseteq \rangle \overset{\gamma}{\leftarrow} \langle \wp(Q), \subseteq \rangle
\]

Example 3 of Galois connections

If \(S\) and \(T\) are sets then

\[
\langle \wp(S \longrightarrow T), \subseteq \rangle \overset{\gamma}{\leftarrow} \langle S \longrightarrow \wp(T), \subseteq \rangle
\]

where:

\[
\alpha(F) \overset{\text{def}}{=} \lambda x \{ f(x) \mid f \in F \}
\]

\[
\gamma(\varnothing) \overset{\text{def}}{=} \{ f \in S \longrightarrow T \mid \forall x \in S : f(x) \in \varnothing(x) \}
\]
Moore families

- A Moore family is a subset of a complete lattice \( \langle L, \sqsubseteq, \bot, \top, \sqcap, \sqcup \rangle \) containing \( \top \) and closed under arbitrary glbs \( \sqcap \);
- If \( \langle P, \sqsubseteq \rangle \xrightarrow{\gamma_1/\alpha_1} \langle Q, \preceq \rangle \) and \( \langle P, \sqsubseteq, \bot, \top, \sqcap, \sqcup \rangle \) is a complete lattice then \( \gamma(Q) \) is a Moore family.
- A consequence is that one can reason upon the abstract semantics using only \( P \) and the image of \( P \) by the upper closure operator \( \gamma \circ \alpha \) (instead of \( Q \)).
- Intuition:
  - The upper-approximation of \( x \in P \) is any \( y \in \gamma(Q) \) such that \( x \sqsubseteq y \);
  - The best approximation of \( x \) is \( \gamma \circ \alpha(x) \).

Preservation of lubs/glbs

- If \( \langle P, \sqsubseteq \rangle \xrightarrow{\gamma/\alpha} \langle Q, \preceq \rangle \), then \( \alpha \) preserves existing lubs: if \( \sqcup X \) exists, then \( \alpha(\sqcup X) \) is the lub of \( \{ \alpha(x) \mid x \in X \} \).
  By the duality principle:
- If \( \langle P, \sqsubseteq \rangle \xrightarrow{\gamma/\alpha} \langle Q, \preceq \rangle \) then \( \gamma \) preserves existing glbs: if \( Y \subseteq Q \) and \( \sqcap Y \) exists, then \( \gamma(\sqcap Y) \) is the glb of \( \{ \gamma(y) \mid y \in Y \} \).

Unique adjoint

In a Galois connection, one function uniquely determines the other:
- If \( \langle P, \sqsubseteq \rangle \xrightarrow{\gamma_1/\alpha_1} \langle Q, \preceq \rangle \) and \( \langle P, \sqsubseteq \rangle \xrightarrow{\gamma_2/\alpha_2} \langle Q, \preceq \rangle \), then \( \alpha_1 = \alpha_2 \) if and only if \( \gamma_1 = \gamma_2 \).

\[ \forall x \in P : \alpha(x) = \cap \{ y \mid x \sqsubseteq \gamma(y) \} \]
\[ \forall y \in Q : \gamma(y) = \cup \{ x \mid \alpha(x) \preceq y \} \]

Complete join preserving abstraction function and complete meet preserving concretization function

- Let \( \langle P, \sqsubseteq \rangle \) and \( \langle Q, \preceq \rangle \) be posets.
- If
  1. \( \alpha \in P(\sqcup) \xrightarrow{\alpha} Q(\sqcup) \)
  2. \( \sqcup \{ x \mid \alpha(x) \preceq y \} \) exists for all \( y \in Q \),
  then
\[ \langle P, \sqsubseteq \rangle \xrightarrow{\gamma/\alpha} \langle Q, \preceq \rangle \]
where \( \forall y \in Q : \gamma(y) = \sqcup \{ x \mid \alpha(x) \preceq y \} \).
- By duality, if
  1. \( \gamma \in Q(\sqcap) \xrightarrow{\gamma} P(\sqcap) \)
  2. \( \sqcap \{ y \mid x \sqsubseteq \gamma(y) \} \) exists for all \( x \in P \),
  then
\[ \langle P, \sqsubseteq \rangle \xleftarrow{\gamma/\alpha} \langle Q, \preceq \rangle \]
where \( \forall x \in P : \alpha(x) = \sqcap \{ y \mid x \sqsubseteq \gamma(y) \} \).
**Galois surjection & injection**

If $\langle P, \sqsubseteq \rangle \xrightarrow{\gamma} \langle Q, \preceq \rangle$, then:
- $\alpha$ is onto
- iff $\gamma$ is one-to-one
- iff $\alpha \circ \gamma$ is the identity

By the duality principle, if $\langle P, \sqsubseteq \rangle \xleftarrow{\gamma} \langle Q, \preceq \rangle$, then:
- $\alpha$ is one-to-one
- iff $\gamma$ is onto
- iff $\gamma \circ \alpha$ is the identity

Notation:

| $\langle P, \sqsubseteq \rangle \xrightarrow{\gamma} \langle Q, \preceq \rangle$ | Galois connection |
| $\langle P, \sqsubseteq \rangle \xleftarrow{\gamma} \langle Q, \preceq \rangle$ | Galois surjection |
| $\langle P, \sqsubseteq \rangle \xrightarrow{\gamma} \langle Q, \preceq \rangle$ | Galois injection |
| $\langle P, \sqsubseteq \rangle \xleftarrow{\gamma} \langle Q, \preceq \rangle$ | Galois bijection |

with $\leftarrow$ denoting ‘into’ and $\rightarrow$ denoting ‘onto’.

---

**The image of a complete lattice by a Galois surjection is a complete lattice**

- If $\langle P, \sqsubseteq \rangle \xrightarrow{\gamma} \langle Q, \preceq \rangle$ and $\langle P, \sqsubseteq, \bot, \top, \sqcap, \sqcup, \sqsubseteq \rangle$ is a complete lattice, then so is $\langle Q, \preceq \rangle$ with:
  - $0 = \alpha(\bot)$ infimum
  - $1 = \alpha(\top)$ supremum
  - $\vee Y = \alpha(\sqcup_{y \in Y} \gamma(y))$ lub
  - $\wedge Y = \alpha(\sqcap_{y \in Y} \gamma(y))$ glb

---

**The image of a Cpo by a Galois surjection is a Cpo**

- If $\langle P, \sqsubseteq, \bot, \top, \sqcap, \sqcup, \sqsubseteq \rangle$ is a cpo and $\langle Q, \preceq \rangle$ is a poset and $\langle P, \sqsubseteq \rangle \xrightarrow{\gamma} \langle Q, \preceq \rangle$, then $\langle Q, \preceq, 0, \vee \rangle$ is a cpo with:
  - $0 \overset{\text{def}}{=} \alpha(\bot)$
  - $\vee X \overset{\text{def}}{=} \alpha(\sqcup_{x \in X} \gamma(x))$

---

**Pointwise extension of Galois connections**

- If $\langle S \rightarrowtail P, \sqsubseteq \rangle \xrightarrow{\gamma} \langle S \rightarrowtail Q, \preceq \rangle$ then:

  $\langle S \mapsto P, \sqsubseteq \rangle \xrightarrow{\gamma} \langle S \mapsto Q, \preceq \rangle$

  where:
  - $\hat{\alpha}(f) \overset{\text{def}}{=} \alpha \circ f$
  - $\hat{\gamma}(g) \overset{\text{def}}{=} \gamma \circ g$
**Lifting Galois connections at higher-order**

If
\[ \langle P_1, \sqsubseteq_1 \rangle \xleftarrow{\gamma_1} \alpha_1 \xrightarrow{\alpha_1} \langle Q_1, \preceq_1 \rangle \]
\[ \langle P_2, \sqsubseteq_2 \rangle \xleftarrow{\gamma_2} \alpha_2 \xrightarrow{\alpha_2} \langle Q_2, \preceq_2 \rangle \]
then
\[ \langle P_1 \xrightarrow{m} P_2, \sqsubseteq_2 \rangle \xleftarrow{\gamma} \alpha \xrightarrow{\alpha} \langle Q_1 \xrightarrow{m} Q_2, \preceq_2 \rangle \]
where
\[ \varphi \sqsubseteq \psi \iff \forall x : \varphi(x) \sqsubseteq \psi(x) \]
\[ \alpha(\varphi) \equiv \alpha_2 \circ \varphi \circ \gamma_1 \]
\[ \gamma(\psi) \equiv \gamma_2 \circ \psi \circ \alpha_1 \]

**Example: interval analysis**

- **Concrete/exact:**
  \[ D \overset{\text{def}}{=} \{ x \in \mathbb{N} \mid \min_{\text{int}} \leq x \leq \max_{\text{int}} \} \]
  \[ D_\Omega \overset{\text{def}}{=} D \cup \{ \Omega \} \]
  variables & uninitialization
  \[ n \geq 1 \]
  program points
  \[ V \]
  \[ S \overset{\text{def}}{=} [1, n] \rightarrow (V \rightarrow D_\Omega) \]
  states
- **Abstract/approximate:**
  \[ I \overset{\text{def}}{=} \{ [a, b] \mid x \in \mathbb{N} \mid a \leq x \leq b \} \]
  intervals
  \[ \gamma(\Omega) \overset{\text{def}}{=} \{ \Omega \} \]
  concretization
  \[ \gamma([a, b]) \overset{\text{def}}{=} \{ x \in \mathbb{N} \mid a \leq x \leq b \} \]
  \[ \gamma(\Omega, [a, b]) \overset{\text{def}}{=} \gamma(\Omega) \cup \gamma([a, b]) \]
  abstract
  \[ L \overset{\text{def}}{=} [1, n] \rightarrow (V \rightarrow A) \]
  domain
  \[ \gamma \in A \mapsto \psi(D_\Omega) \]
  concretization
  \[ \gamma(P) \overset{\text{def}}{=} \{ \rho \mid x \in \mathbb{N} \mid \forall v \in V : \rho(i)(v) \in \gamma(P(i)(v)) \} \]
  \[ P \sqsubseteq Q \overset{\text{def}}{=} \gamma(P) \subseteq \gamma(Q) \]
  ordering

- **Galois connexion:**
  \[ \langle \varphi(S), \sqsubseteq \rangle \xleftarrow{\gamma} \alpha \xrightarrow{\alpha} \langle L, \sqsubseteq \rangle \]

**Composition of Galois connections**

The composition of Galois connections is a Galois connection:

\[ \left( \langle P, \sqsubseteq \rangle \xleftarrow{\gamma} \langle P, \sqsubseteq \rangle \land \langle Q, \sqsubseteq \rangle \right) \]
\[ \Rightarrow \langle P, \sqsubseteq \rangle \xleftarrow{\gamma \circ \alpha} \langle Q, \sqsubseteq \rangle \]

**Kleenean fixpoint abstraction**

If \( \langle D, \sqsubseteq, \bot, \sqcup \rangle \) is a cpo, \( \langle Q, \preceq \rangle \) is a poset,
\[ F \in \mathcal{P} \xrightarrow{m} D, F^\sharp \in Q \xrightarrow{m} Q, \]
and
\[ F^\sharp \circ \alpha = \alpha \circ F \]
then
\[ \alpha(\text{lfp} \sqsubseteq F) = \text{lfp} \preceq F^\sharp \]
Kleenian fixpoint approximation

If \( \langle D, \sqsubseteq, \bot, \sqcup \rangle \) is a cpo, \( \langle Q, \preceq \rangle \) is a poset,
\( F \in \mathcal{P}_{m} \mapsto \downarrow D \), \( F^\sharp \in \mathcal{A}_{m} \mapsto \downarrow \mathcal{A} \), and
\[
F^\sharp \circ \alpha \preceq \alpha \circ F
\]
\[
\langle D, \sqsubseteq \rangle \xrightarrow{\alpha} \langle D^\sharp, \preceq \rangle
\]
then
\[
\alpha(\text{lfp} \subseteq F) \preceq \text{lfp} \preceq F^\sharp
\]

Infinite strictly increasing chains

- Because of infinite (or very long) strictly increasing chains, the fixpoint iterates may not converge (or very slowly);
- Because of infinite (or very long) strictly decreasing chains, the local decreasing iterates may not converge (or not rapidly enough);
- The design strategy of using a more abstract domain satisfying the ACC often yields too imprecise results;
- It is often both more precise and faster to speed up convergence using widenings along increasing chains and narrowings along decreasing ones.

Interval lattice

Slow fixpoint iterations

--- program:
\[
0: x := 1;
1: \text{while true do}
2: x := (x + 1)
3: \text{od (false)}
\]
4:
--- forward abstract equations:
\[
X0 = (\text{INIT} 0)
X1 = \text{assign}[|x, 1|](X0) U X3
X2 = \text{assert}[|\text{true}|](X1)
X3 = \text{assign}[|x, (x + 1)|](X2)
X4 = \text{assert}[|\text{false}|](X1)
--- iterations from:
X0 = \{ x:_O_ \} X1 = \_\_ X2 = \_\_ X3 = \_\_ X4 = \_\_
---
X0 = \{ x:_O_ \} X1 = \{ x:[1,1] \} X2 = \{ x:[1,1] \} X3 = \{ x:[2,2] \} X4 = \{ x:[2,2] \}
---
X0 = \{ x:_O_ \} X1 = \{ x:[1,1] \} X2 = \{ x:[1,1] \} X3 = \{ x:[2,2] \} X4 = \{ x:[2,2] \}
---
X0 = \{ x:_O_ \} X1 = \{ x:[1,2] \} X2 = \{ x:[1,2] \} X3 = \{ x:[2,3] \} X4 = \{ x:[2,3] \}
---
X0 = \{ x:_O_ \} X1 = \{ x:[1,3] \} X2 = \{ x:[1,3] \} X3 = \{ x:[2,4] \} X4 = \{ x:[2,4] \}
---
X0 = \{ x:_O_ \} X1 = \{ x:[1,4] \} X2 = \{ x:[1,4] \} X3 = \{ x:[2,5] \} X4 = \{ x:[2,5] \}
---
**Widening**

Definition: A widening $\nabla \in P \times P \rightarrow P$ on a poset $(P, \sqsubseteq)$ satisfies:
- $\forall x, y \in P : x \sqsubseteq (x \nabla y) \land y \sqsubseteq (x \nabla y)$
- For all increasing chains $x^0 \sqsubseteq x^1 \sqsubseteq \ldots$
  - the increasing chain $y^0 \overset{\text{def}}{=} x^0, \ldots, y^{n+1} \overset{\text{def}}{=} y^n \nabla x^{n+1}, \ldots$ is not strictly increasing.

Use:
- Approximate missing lubs.
- Convergence acceleration.

**Fixpoint upper approximation by widening**

- Any iteration sequence with widening is increasing and stationary after finitely many iteration steps;
- Its limit $L \nabla$ is a post-fixpoint of $F$, whence an upper-approximation of the least fixpoint $\lfp F \sqsubseteq F^\ast$: $\lfp F \sqsubseteq L \nabla$

---

**Iteration sequence with widening**

- Let $F$ be a monotonic operator on a poset $(P, \sqsubseteq)$;
- Let $\nabla \in P \times P \rightarrow P$ be a widening;
- The iteration sequence with widening $\nabla$ for $F$ from $\bot$ is $X^n, n \in \mathbb{N}$:
  - $X^0 = \bot$
  - $X^{n+1} = X^n$ if $F(X^n) \sqsubseteq (X^n)$
  - $X^{n+1} = X^n \nabla F(X^n)$ if $F(X^n) \not\sqsubseteq X^n$

**Example of widening for intervals**

$[a, b] \nabla [a', b'] \overset{\text{def}}{=} \Omega$
- $[a, b] \nabla [a', b'] = \langle \Omega, [a, b] \rangle$
- $\Omega \nabla \langle \Omega, [a, b] \rangle = \langle \Omega, [a, b] \rangle$
- $[a, b] \nabla \Omega = \Omega$
- $\Omega \nabla \Omega = \Omega$
- $\langle \Omega, [a, b] \rangle \nabla [a', b'] \overset{\text{def}}{=} \langle \Omega, [a, b] \nabla [a', b'] \rangle$
- $\langle \Omega, [a, b] \rangle \nabla \langle \Omega, [a', b'] \rangle = \langle \Omega, [a, b] \nabla [a', b'] \rangle$
**Widening for systems of equations**

A very rough idea:

- compute the dependence graph of the system of equations;
- widen at cut-points;
- iterate according to the weak topological ordering

---

**Interval program analysis example with widening**

labelled program:

```plaintext
--
0: x := 1;
1: y := 1000;
2: while (x < y) do
3:  x := (x + 1)
4: od
5:
--
```

iterations with widening from:

```plaintext
X0 = { x:_O_; y:_O_ }  X1 = _L_  X2 = _L_
X3 = _L_  X4 = _L_  X5 = _L_
```

---

```
X0 = { x:_O_; y:_O_ }
X1 = { x:[1,1]; y:_O_ }
widening at 2 by { x:[1,1]; y:[1000,1000] }
X2 = { x:[1,1]; y:[1000,1000] }
X3 = { x:[1,1]; y:[1000,1000] }
X4 = { x:[2,2]; y:[1000,1000] }
widening at 2 by { x:[1,2]; y:[1000,1000] }
X2 = { x:[1,1000]; y:[1000,1000] }
X3 = { x:[1,999]; y:[1000,1000] }
X4 = { x:[2,1000]; y:[1000,1000] }
X2 = { x:[1,1000]; y:[1000,1000] }
X3 = { x:[1,999]; y:[1000,1000] }
X4 = { x:[2,1000]; y:[1000,1000] }
X5 = { x:[1000,1000]; y:[1000,1000] }
```

---

**Example**

labelled program:

```plaintext
--
0: x := 1;
1: y := 1000;
2: while (x < y) do
3:  x := (x + 1)
4: od
5:
--
```

forward abstract equations:

```plaintext
X0 = (INIT 0)
X1 = assign[x, 1](X0)
X2 = assign[y, 1000](X1) U X4
X3 = assert[(x < y)](X2)
X4 = assign[x, (x + 1)](X3)
X5 = assert[(y < x) ∨ (x = y)](X2)
```

forward graph with 6 vertices:

```plaintext
0 : (1)
1 : (2)
2 : (3, 5)
3 : (4)
4 : (2)
5 : ()
```

forward weak topological order: 0 1 ( 2 3 4 ) 5

forward cut & check points: {2}

---

**Narrowing**

- Since we have got a post-fixpoint $L^\triangledown$ of $F \in P \longrightarrow P$, its iterates $F^n(L^\triangledown)$ are all upper approximations of $\text{lfp } F$.
- To accelerate convergence of this decreasing chain, we use a narrowing $\triangledown \in P \times P \longrightarrow P$ on the poset $(P, \sqsubseteq)$ satisfying:

  - $\forall x, y \in P : y \subseteq x$ $\implies$ y $\sqsubseteq x \triangledown y$ $\sqsubseteq x$
  - For all decreasing chains $x^0 \sqsubseteq x^1 \sqsubseteq \ldots$, the decreasing chain $y^0 \triangledown x^0, \ldots, y^n \triangledown A \triangledown y^n \triangledown x^{n+1}, \ldots$ is not strictly decreasing.
Decreasing iteration sequence with narrowing

- Let $F$ be a monotonic operator on a poset $\langle P, \sqsubseteq \rangle$;
- Let $\triangle \in P \times P \rightarrow P$ be a narrowing;
- The iteration sequence with narrowing $\triangle$ for $F$ from the postfixpoint $P^*$ is $Y^n$, $n \in \mathbb{N}$:
  - $Y^0 = P$
  - $Y^{n+1} = Y^n$ if $F(Y^n) = Y^n$
  - $Y^{n+1} = Y^n \triangle F(Y^n)$ if $F(Y^n) \neq Y^n$

Fixpoint upper approximation by narrowing

- Any iteration sequence with narrowing starting from a postfixpoint $P$ of $F^*$ is decreasing and stationary after finitely many iteration steps;
- if $\text{lfp}^\subseteq F$ does exist and $\text{lfp}^\subseteq F \sqsubseteq P$ then its limit $L^\triangle$ is a fixpoint of $F$, whence an upper-approximation of the least fixpoint $\text{lfp}^\subseteq F$:
  $$\text{lfp}^\subseteq F \sqsubseteq L^\triangle \sqsubseteq P$$

Example of narrowing for intervals

if $x \leq x' \leq y' \leq y$ then $[x,y] \triangle [x',y'] = \text{narrow } x \ y \ x' \ y'$

let narrow $x \ y \ x' \ y'$ =
  (if (x = $\text{min_int}$) then $x'$ else x),
  (if (y = $\text{max_int}$) then $y'$ else y) ;

Trivially extended to initialization & interval analysis.

Program analysis example with narrowing

labelled program:
--
0: x := 1;
1: y := 1000;
2: while (x < y) do
3: x := (x + 1)
4: od {((y < x) | (x = y))}
5: --

iterations with narrowing from:
--
X0 = { x: _O_; y: _O_ }
X1 = { x: [1,1]; y: _O_ }
X2 = { x: [1,1000]; y: [1000,1000] }
X3 = { x: [1,999]; y: [1000,1000] }
X4 = { x: [2,1000]; y: [1000,1000] }
X5 = { x: [1000,1000]; y: [1000,1000] }
--
X0 = { x: _O_; y: _O_ }
X1 = { x: [1,1]; y: _O_ }
X2 = { x: [1,1000]; y: [1000,1000] }
X3 = { x: [1,999]; y: [1000,1000] }
X4 = { x: [2,1000]; y: [1000,1000] }
X5 = { x: [1000,1000]; y: [1000,1000] }
--
stable
**Widenings and Narrowings are not Dual**

- The iteration with \textit{widen}ing starts from below the least fixpoints and stabilizes above;
- The iteration with \textit{narrowing} starts from above the least fixpoints and stabilizes above;
- In general, widenings and narrowing are \textit{not} monotonic.

---

**Improving the Precision of Widenings/Narrowings**

- **Threshold:**
- Widening/narrowing (and stabilization checks) at cut points;
- **Computation history-based** extrapolation:
  A simple example:
  - Do not widen/narrow if a component of the system of fixpoint equations was computed for the first time since the last widening/narrowing;
  - Otherwise, do not widen/narrow the abstract values of variables which were not “assigned to” \footnote{more precisely which did not appear in abstract equations corresponding to an assignment to these variables} since the last widening/narrowing.

---

**Conclusion**

- A very elementary introduction to abstract interpretation;
- For more details, see e.g. \url{http://www.dmi.ens.fr/~cousot}