Abstract Interpretation: fixpoint computation

Abstract Functions

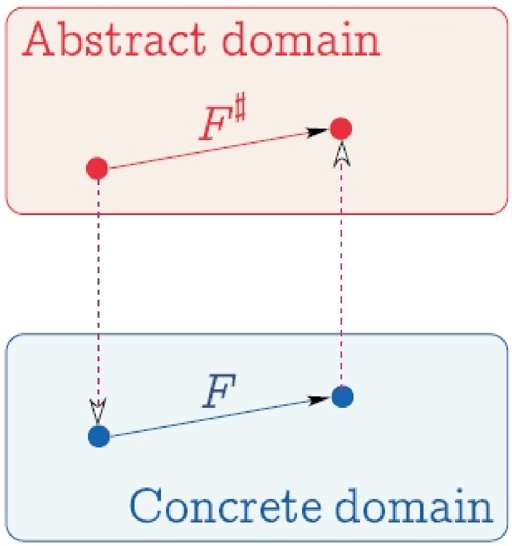


Figure by P.Cousot

There is always an optimal abstraction of the concrete function F, defined by $F^\sharp = \alpha \circ F \circ \gamma$.

However, for the correctness of the analysis it is sufficient that

$$\forall a \in \mathcal{D}^\sharp : \gamma(F^\sharp(a)) \supseteq F(\gamma(a)).$$

Fixpoint Theorems

- **Knaster-Tarski theorem**: If $F : L \to L$ is monotone and L is a complete lattice, the set of fixpoints of F is also a complete lattice.
- **Kleene theorem**: If $F : L \to L$ is monotone, L is a complete lattice and F preserves all least upper bounds then lfp(F) is the limit of the sequence:

$$\begin{cases} F_0 = \bot \\ F_{n+1} = F(F_n) \end{cases}$$

Approximate Semantics

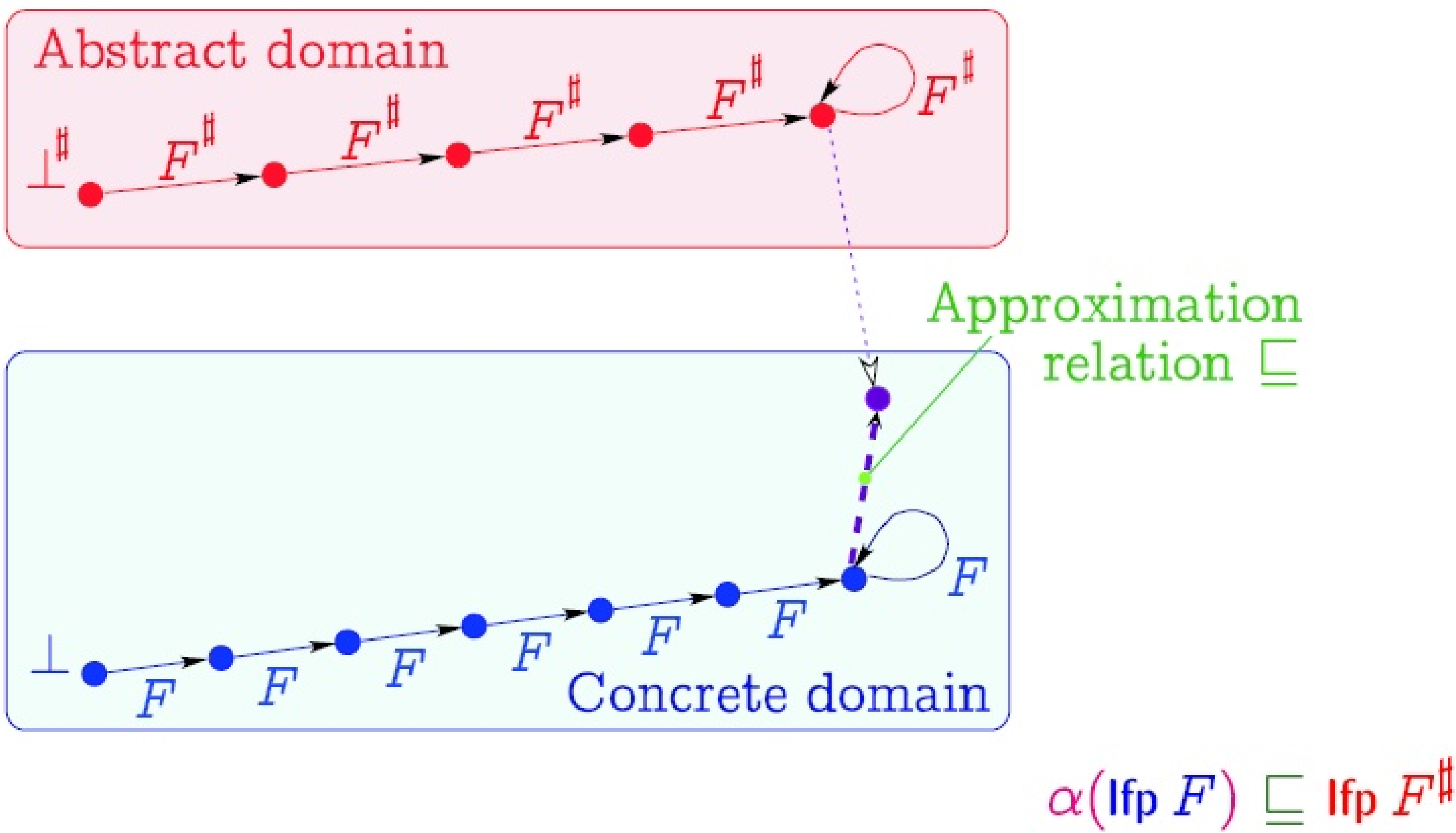


Figure by P.Cousot

Widening and Narrowing

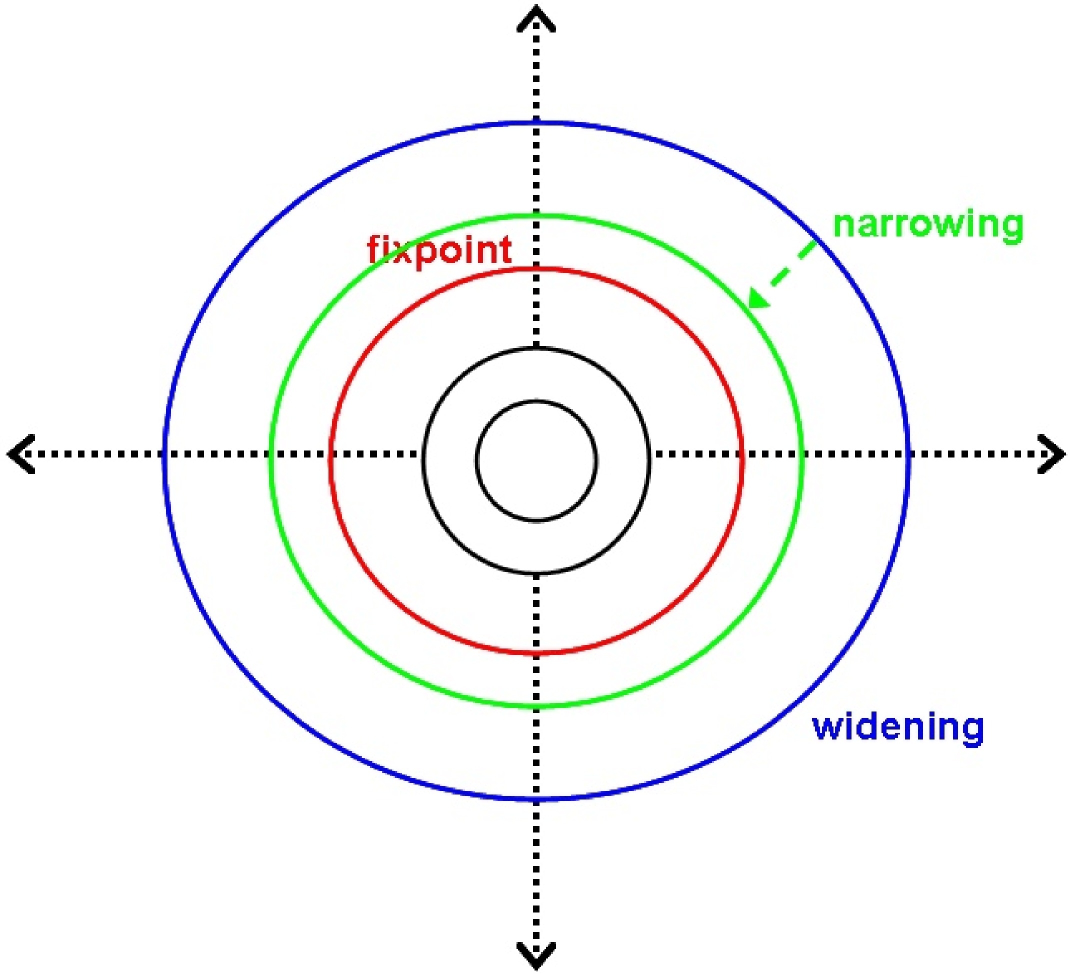


Figure by A.Venet

Convergence Acceleration by Widening

A widining operator on a partial order D is binary operator $\nabla : D \to D$ such that:

- It is an **upper bound operator**:

$$\forall x, y \in D : x \sqsubseteq x \nabla y, y \sqsubseteq x \nabla y$$

- It **enforces convergence**:

  for all increasing chains $x_0, x_1, \ldots$, the chain defined by $y_0 = x_0$, $y_{i+1} = y_i \nabla x_{i+1}$ is not strictly increasing (i.e. it converges after a finite number of steps).

Recovering Accuracy by Narrowing

A narrowing operator on a partial order D is binary operator $\Delta : D \to D$ such that:

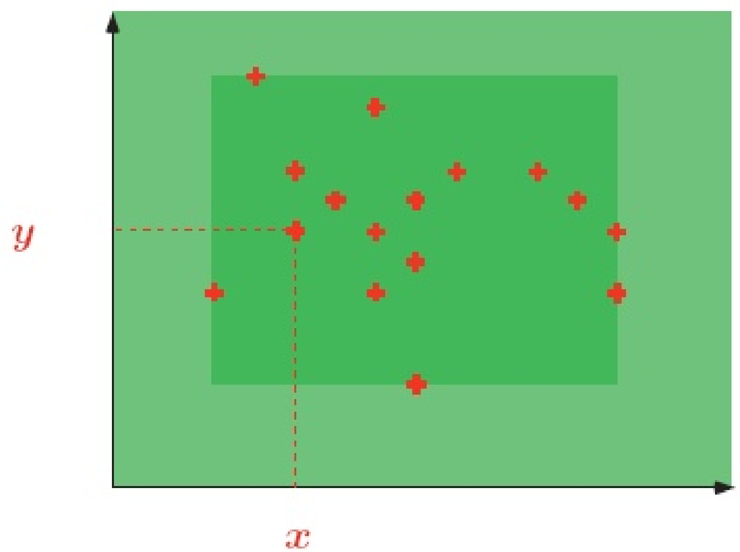
- It is an **abstract intersection operator**:

$$\forall x, y \in D : x \sqcap y \sqsubseteq x \Delta y$$

- It **enforces convergence**:

  for all decreasing chains $x_0, x_1, \ldots$, the chain defined by $y_0 = x_0$, $y_{i+1} = y_i \Delta x_{i+1}$ is not strictly decreasing, i.e. it converges after a finite number of steps.

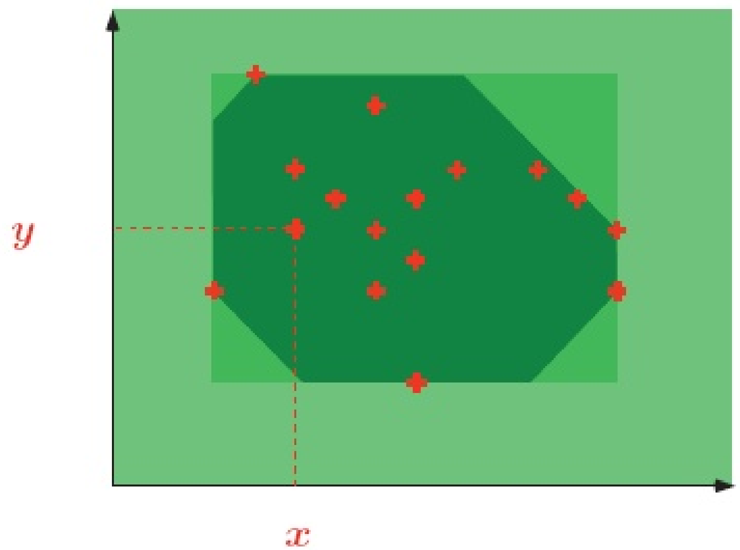
The Domain of Intervals



$$\begin{cases} x \in [19,\ 77] \\ y \in [20,\ 03] \end{cases}$$

Figure by P.Cousot

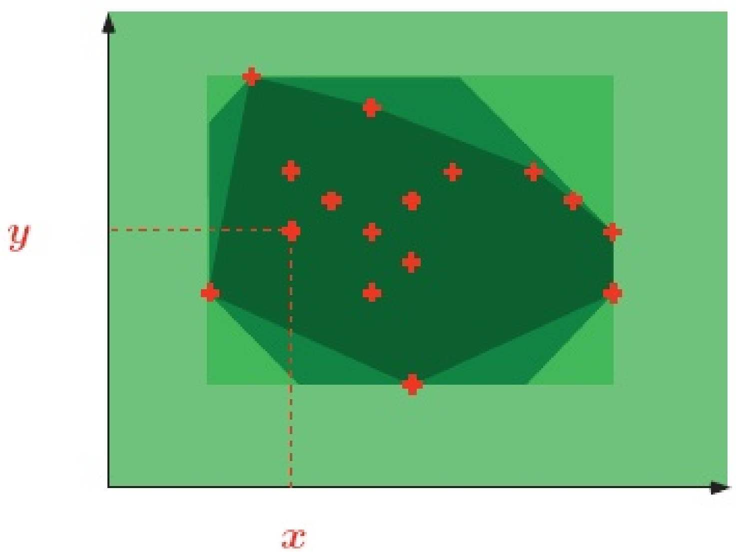
The Domain of Octagons



$$\begin{cases} 1 \leq x \leq 9 \\ x + y \leq 77 \\ 1 \leq y \leq 9 \\ x - y \leq 99 \end{cases}$$

Figure by P.Cousot

The Domain of Polyhedra



$$\begin{cases} 19x + 77y \leq 2004 \\ 20x + 03y \geq 0 \end{cases}$$

Figure by P.Cousot

Widening on the interval Domain

The lattice of intervals is
$L = \{\perp\} \cup \{[\ell, u] \mid \ell \in \mathbb{Z} \cup \{-\infty\},\ u \in \mathbb{Z} \cup \{+\infty\},\ \ell \leq u\}$.

$$
\begin{array}{rcl}
\perp \nabla x & = & x \\
x \nabla \perp & = & x \\
[\ell_0, u_0] \nabla [\ell_1, u_1] & = & [\text{if } \ell_1 < \ell_0 \text{ then } -\infty \text{ else } \ell_0, \\
 & & \ \text{if } u_0 < u_1 \text{ then } +\infty \text{ else } u_0]
\end{array}
$$

It is not monotone. For example $[0, 1] \sqsubseteq [0, 2]$ but
$[0, 1] \nabla [0, 2] = [0, +\infty] \not\sqsubseteq [0, 2] = [0, 2] \nabla [0, 2]$.

Widening on the interval Domain (threeshold)

Let k be a fixed positive integer constant.

$$\begin{array}{rcl}
\bot \nabla_k x & = & x \\
x \nabla_k \bot & = & x \\
[\ell_0, u_0] \nabla_k [\ell_1, u_1] & = & [\text{min}(\ell_0, \ell_1) \text{ if } \text{min}(\ell_0, \ell_1) > -k, \text{ else } -\infty \\
 & & \text{max}(u_0, u_1) \text{ if } \text{max}(u_0, u_1) < k, \text{ else } +\infty]
\end{array}$$

Observe that for all k, ∇_k is commutative, associative, and order-preserving. However, it is not reflexive. For instance, if $k = 7$ we get:

$$[-8, 4] \nabla [-8, 4] = [-\infty, 4]$$

Example: Convergence Acceleration by Widening

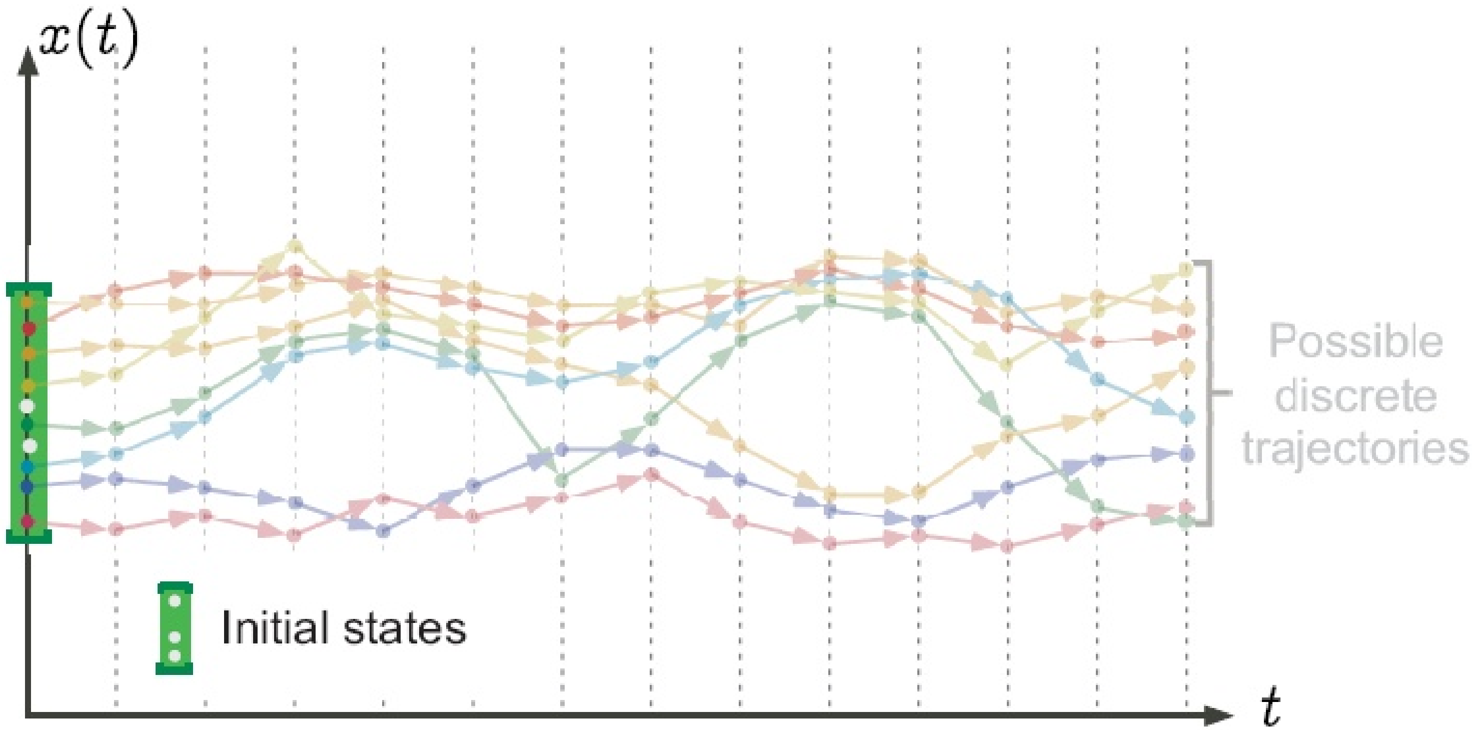


Figure by P.Cousot

Example: Convergence Acceleration by Widening !

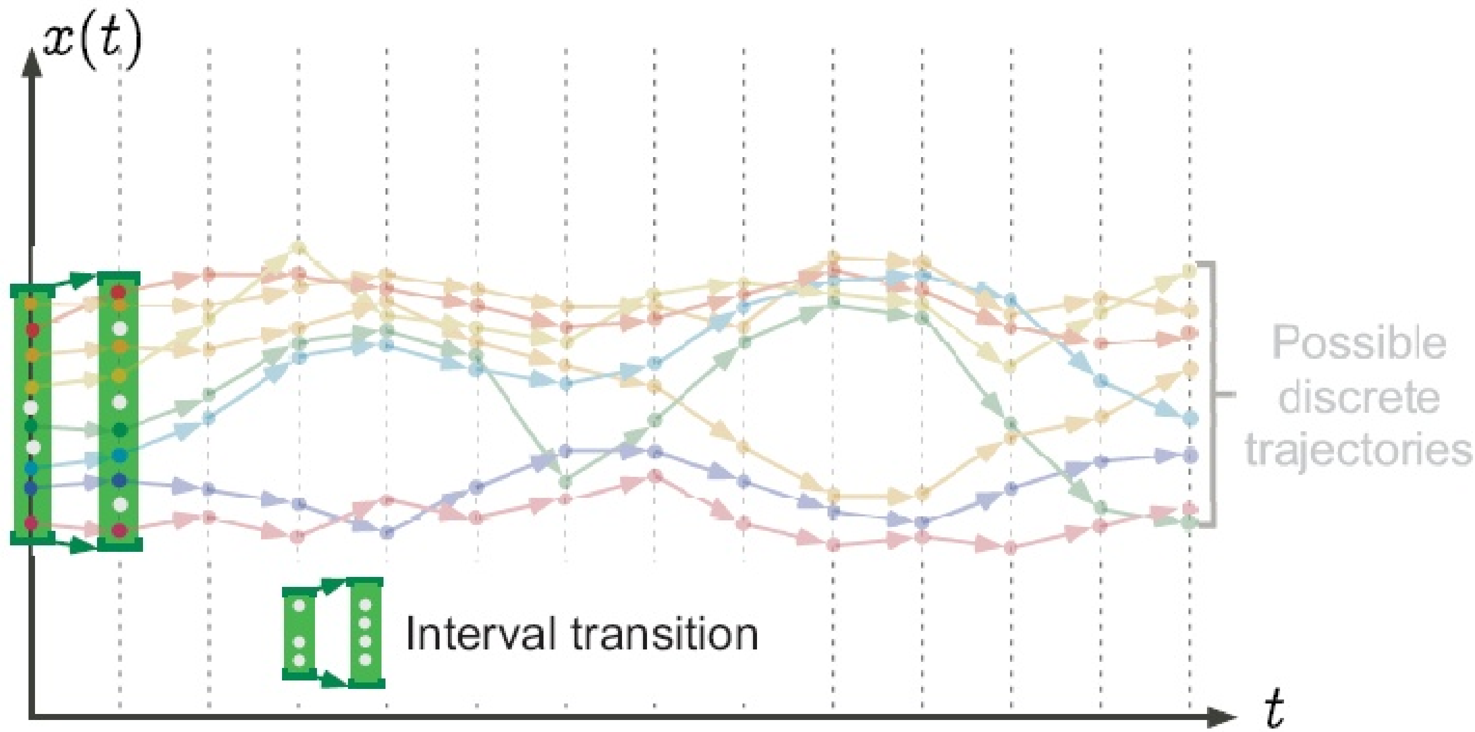


Figure by P.Cousot

Example: Convergence Acceleration by Widening !!

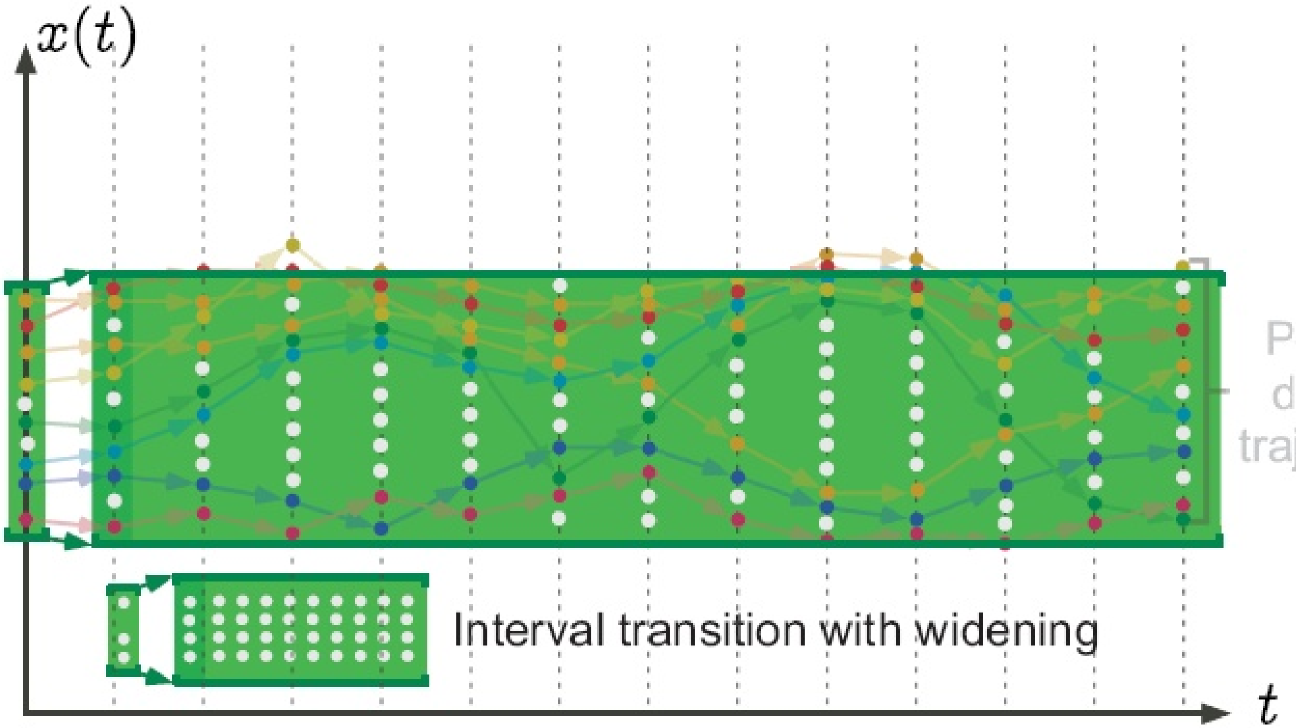


Figure by P.Cousot

Example: Convergence Acceleration by Widening !!!

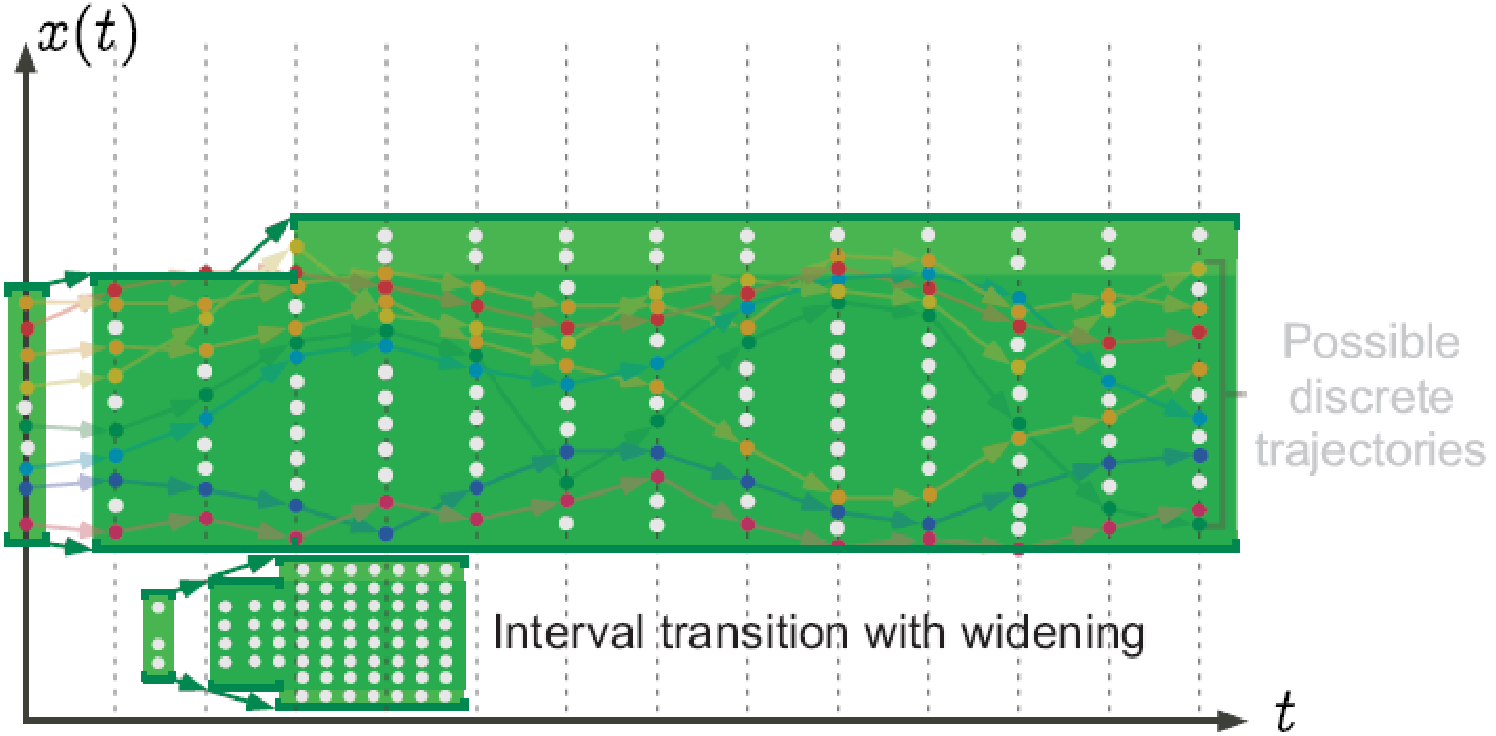


Figure by P.Cousot

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\begin{cases} x_1 = [1,1] \\ x_2 = (x_1 \cup x_3) \cap [-\infty, 9999] \\ x_3 = x_2 \oplus [1,1] \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{cases} \qquad \begin{cases} x_1 = \varnothing \\ x_2 = \varnothing \\ x_3 = \varnothing \\ x_4 = \varnothing \end{cases}$$

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\begin{cases} \underline{x_1 = [1,1]} \\ x_2 = (x_1 \cup x_3) \cap [-\infty, 9999] \\ x_3 = x_2 \oplus [1,1] \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} \underline{x_1 = [1,1]} \\ x_2 = \varnothing \\ x_3 = \varnothing \\ x_4 = \varnothing \end{cases}$$

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\begin{cases} x_1 = [1,1] \\ \underline{x_2 = (x_1 \cup x_3) \cap [-\infty, 9999]} \\ x_3 = x_2 \oplus [1,1] \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{cases} \qquad \begin{cases} x_1 = [1,1] \\ \underline{x_2 = [1,1]} \\ x_3 = \varnothing \\ x_4 = \varnothing \end{cases}$$

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\left\{\begin{array}{l} x_1 = [1,1] \\ x_2 = (x_1 \cup x_3) \cap [-\infty, 9999] \\ \underline{x_3 = x_2 \oplus [1,1]} \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{array}\right. \qquad \left\{\begin{array}{l} x_1 = [1,1] \\ x_2 = [1,1] \\ \underline{x_3 = [2,2]} \\ x_4 = \varnothing \end{array}\right.$$

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$
\begin{cases}
x_1 = [1, 1] \\
x_2 = (x_1 \cup x_3) \cap [-\infty, 9999] \\
x_3 = x_2 \oplus [1, 1] \\
x_4 = (x_1 \cup x_3) \cap [10000, +\infty]
\end{cases}
\qquad
\begin{cases}
x_1 = [1, 1] \\
x_2 = [1, 2] \\
x_3 = [2, 2] \\
x_4 = \varnothing
\end{cases}
$$

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\begin{cases} x_1 = [1, 1] \\ x_2 = (x_1 \cup x_3) \cap [-\infty, 9999] \\ \underline{x_3 = x_2 \oplus [1, 1]} \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{cases} \qquad \begin{cases} x_1 = [1, 1] \\ x_2 = [1, 2] \\ \underline{x_3 = [2, 3]} \\ x_4 = \varnothing \end{cases}$$

There is a convergence issue!

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\begin{cases} x_1 = [1,1] \\ \underline{x_2 = (x_1 \cup x_3) \cap [-\infty, 9999]} \\ x_3 = x_2 \oplus [1,1] \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{cases} \qquad \begin{cases} x_1 = [1,1] \\ \underline{x_2 = [1,3]} \\ x_3 = [2,3] \\ x_4 = \varnothing \end{cases}$$

There is a convergence issue!!

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$
\begin{cases}
x_1 = [1,1] \\
x_2 = (x_1 \cup x_3) \cap [-\infty, 9999] \\
\underline{x_3 = x_2 \oplus [1,1]} \\
x_4 = (x_1 \cup x_3) \cap [10000, +\infty]
\end{cases}
\qquad\qquad
\begin{cases}
x_1 = [1,1] \\
x_2 = [1,3] \\
\underline{x_3 = [2,4]} \\
x_4 = \varnothing
\end{cases}
$$

There is a convergence issue!

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\begin{cases} x_1 = [1,1] \\ \underline{x_2 = (x_1 \cup x_3) \cap [-\infty, 9999]} \\ x_3 = x_2 \oplus [1,1] \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{cases} \qquad \begin{cases} x_1 = [1,1] \\ \underline{x_2 = [1,4]} \\ x_3 = [2,4] \\ x_4 = \varnothing \end{cases}$$

There is a convergence issue!!

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$
\begin{cases}
x_1 = [1, 1] \\
x_2 = (x_1 \cup x_3) \cap [-\infty, 9999] \\
\underline{x_3 = x_2 \oplus [1, 1]} \\
x_4 = (x_1 \cup x_3) \cap [10000, +\infty]
\end{cases}
\qquad
\begin{cases}
x_1 = [1, 1] \\
x_2 = [1, 4] \\
\underline{x_3 = [2, 5]} \\
x_4 = \varnothing
\end{cases}
$$

There is a convergence issue!

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$
\begin{cases}
x_1 = [1,1] \\
\underline{x_2 = (x_1 \cup x_3) \cap [-\infty, 9999]} \\
x_3 = x_2 \oplus [1,1] \\
x_4 = (x_1 \cup x_3) \cap [10000, +\infty]
\end{cases}
\qquad
\begin{cases}
x_1 = [1,1] \\
\underline{x_2 = [1, +\infty]} \\
x_3 = [2,5] \\
x_4 = \varnothing
\end{cases}
$$

We applied a threeshold widening operator on intervals (with k=5)

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\begin{cases} x_1 = [1,1] \\ x_2 = (x_1 \cup x_3) \cap [-\infty, 9999] \\ \underline{x_3 = x_2 \oplus [1,1]} \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} x_1 = [1,1] \\ x_2 = [1, +\infty] \\ \underline{x_3 = [2, +\infty]} \\ x_4 = \varnothing \end{cases}$$

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\begin{cases} x_1 = [1,1] \\ \underline{x_2 = (x_1 \cup x_3) \cap [-\infty, 9999]} \\ x_3 = x_2 \oplus [1,1] \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{cases} \qquad \begin{cases} x_1 = [1,1] \\ \underline{x_2 = [1, 9999]} \\ x_3 = [2, \infty] \\ x_4 = \emptyset \end{cases}$$

Narrowing the solution (decreasing chaotic iterative fixpoint computation)

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\left\{\begin{aligned} x_1 &= [1,1] \\ x_2 &= (x_1 \cup x_3) \cap [-\infty, 9999] \\ \underline{x_3} &\underline{= x_2 \oplus [1,1]} \\ x_4 &= (x_1 \cup x_3) \cap [10000, +\infty] \end{aligned}\right.$$

$$\left\{\begin{aligned} x_1 &= [1,1] \\ x_2 &= [1, 9999] \\ \underline{x_3} &\underline{= [2, 10000]} \\ x_4 &= \varnothing \end{aligned}\right.$$

Example: interval analysis

```
x =  1;
while (x < 10000)
  x = x + 1;
print (x);
```

$$\begin{cases} x_1 = [1,1] \\ x_2 = (x_1 \cup x_3) \cap [-\infty, 9999] \\ \underline{x_3 = x_2 \oplus [1,1]} \\ x_4 = (x_1 \cup x_3) \cap [10000, +\infty] \end{cases}$$

$$\begin{cases} x_1 = [1,1] \\ x_2 = [1, 9999] \\ x_3 = [2, 10000] \\ x_4 = [10000, 10000] \end{cases}$$

Example: interval analysis

`x = 1;`	**x** $\in$ **[1,1]**	
`while (x < 10000)`	**x** $\in$ **[1, 9.999]**	
`  x = x + 1;`	**x** $\in$ **[2, 10.000]**	**No overflow!**
`print (x)`	**x** $\in$ **[10.000, 10.000];**	

Refining the Abstract Semantics

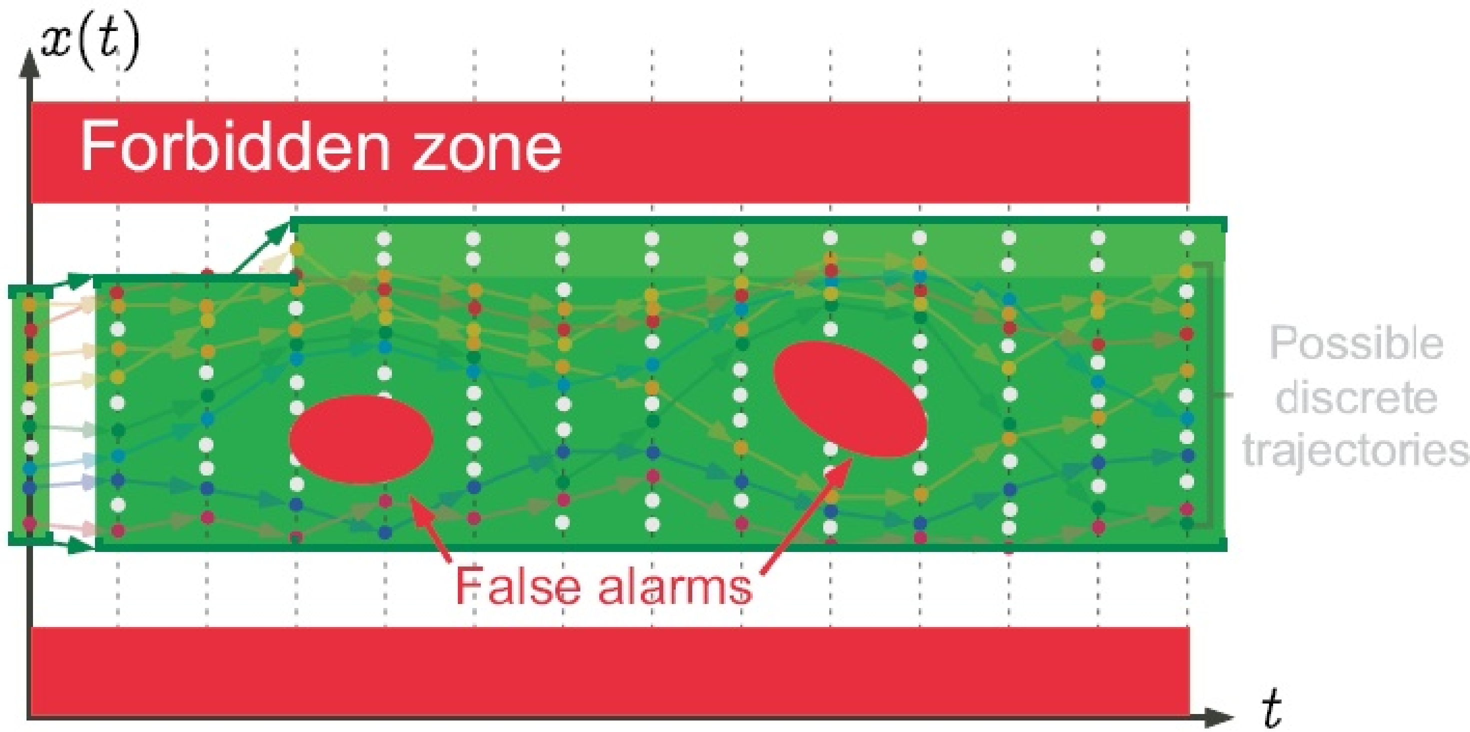


Figure by P.Cousot

Refining the Abstract Semantics: Partitioning

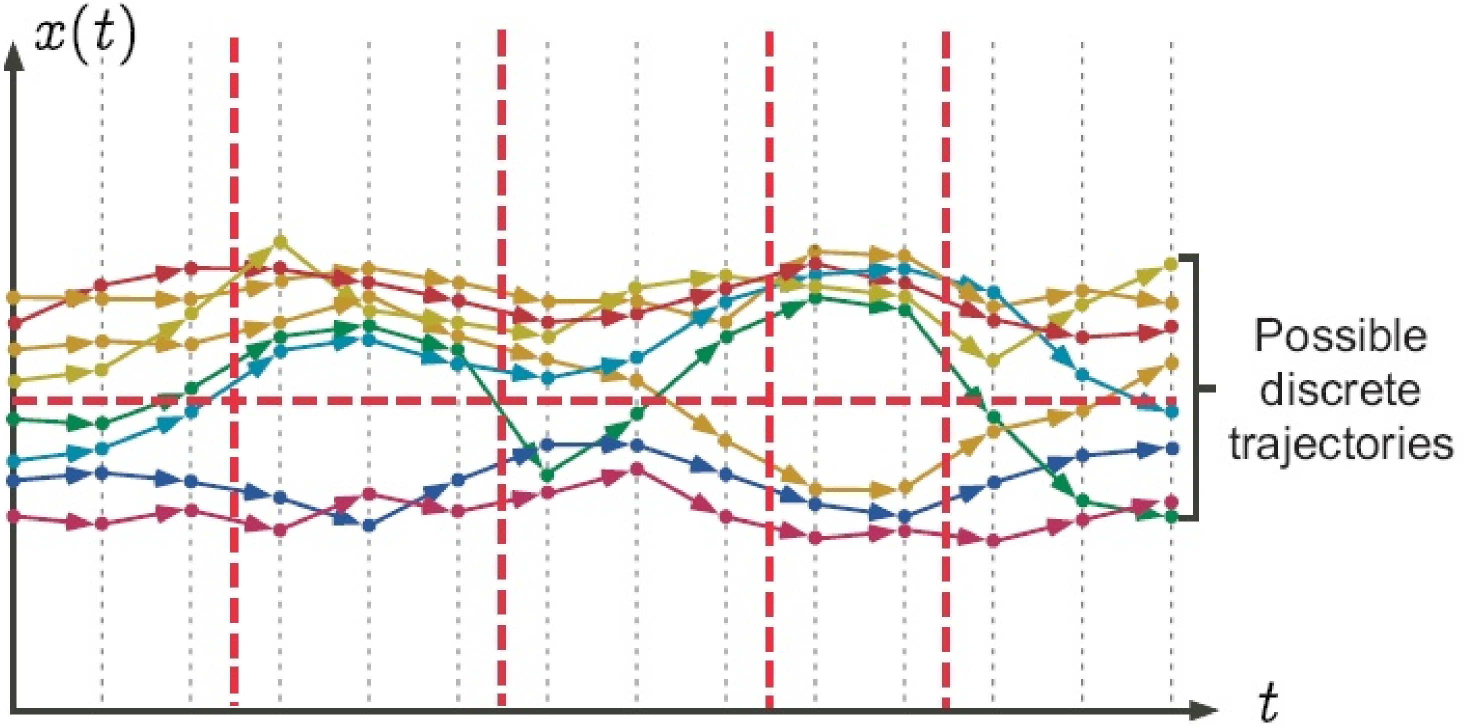


Figure by P.Cousot

Refining the Abstract Semantics: Partitioning

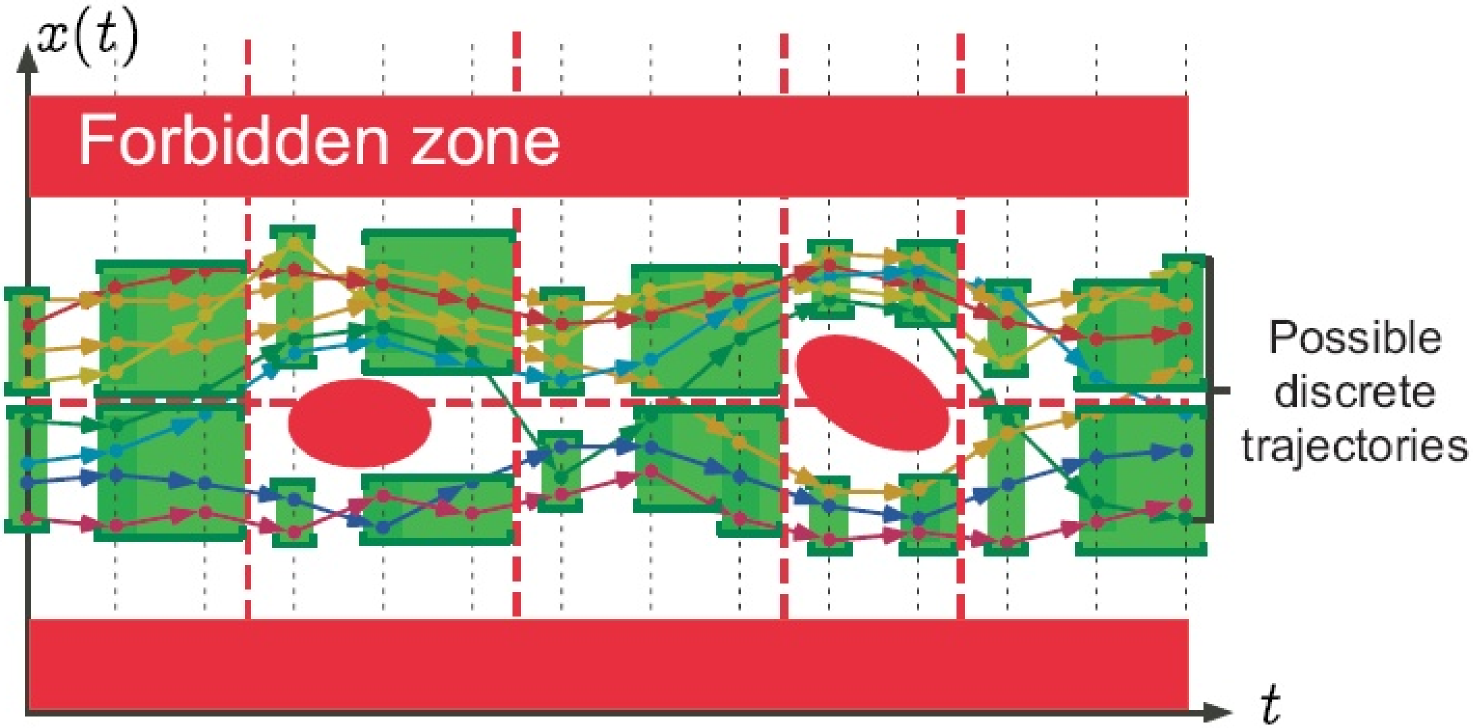


Figure by P.Cousot

Overall Architecture

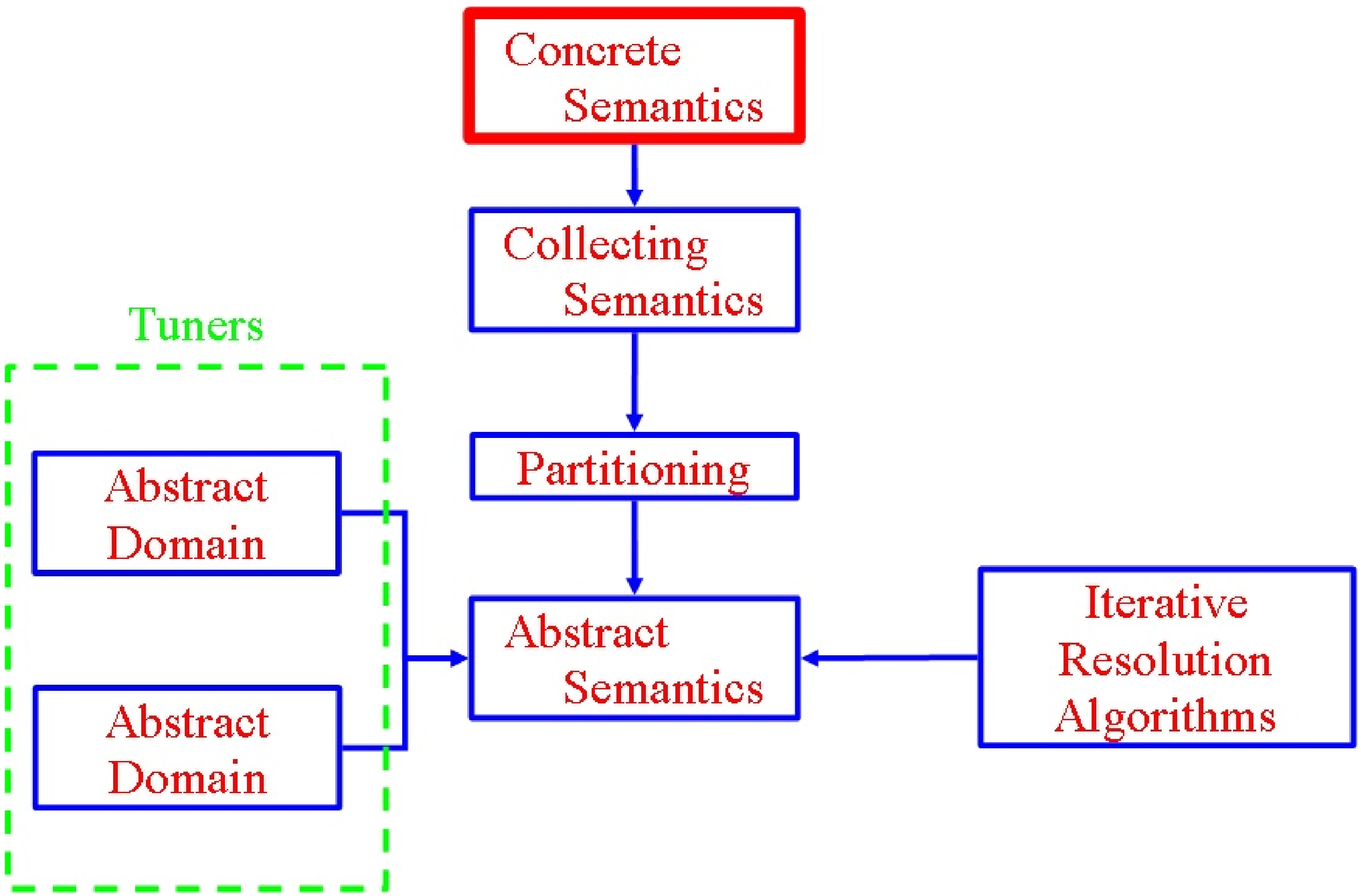


Figure by A.Venet