Ideal Abstractions for Well-Structured Transition Systems

Damien Zufferey, Thomas Wies, Thomas A. Henzinger

VMCAI'12

Presented by

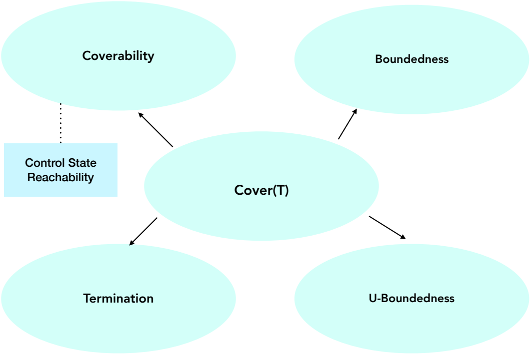
Jatin Arora   Shaan Vaidya

CS 735 FM-CAS '18

Outline

Motivation

- Consider a WSTS $T = (S, S_0, \rightarrow, \leq)$
- $Cover(T) = \downarrow Post^*(\downarrow S_0)$



- The covering set problem is not decidable in general

Motivation

- Backward coverability algorithm - not feasible in practice

Motivation

- Backward coverability algorithm - not feasible in practice
- Look for forward coverability algorithms e.g. Karp-Miller

Motivation

- Backward coverability algorithm - not feasible in practice
- Look for forward coverability algorithms e.g. Karp-Miller
- Forward algorithms usually compute the covering set
- More useful - characterises a good approximation of the reachability set

Motivation

- Backward coverability algorithm - not feasible in practice
- Look for forward coverability algorithms e.g. Karp-Miller
- Forward algorithms usually compute the covering set
- More useful - characterises a good approximation of the reachability set
- When is this decidable?

Preliminaries

- Upward Closure $\uparrow Y$ of a set $Y \subseteq X$ is $\uparrow Y = \{x \in X | \exists y \in Y . y \leq x\}$
- Downward Closure $\downarrow Y$ of a set $Y \subseteq X$ is $\downarrow Y = \{x \in X | \exists y \in Y . y \geq x\}$
- An upper bound $x \in X$ of a set $Y \subseteq X$ is such that $\forall y \in Y .\ y \leq x$
- The notion of lower bound is defined dually.
- A nonempty set $D \subseteq X$ is called directed if $\forall x, y \in D$, $\exists c$ st $c \in D$ and $x \leq c$ and $y \leq c$
- A set $I \subseteq X$ is an ideal of X if I is downward-closed and directed
- $Idl(X)$ denotes the set of all ideals of X also referred to as the *ideal completion of X*

Definitions

- A poset $L(\leq)$ is called a lattice if every two elements have a unique *lub* and *glb*

$$\mathcal{L} = (L, \leq, \top, \bot, \sqcup, \sqcap)$$

  where $\sqcup$, $\sqcap$ denote the *lub* and *glb* operators
  $\top$ and $\bot$ denote the greatest and least elements
- Complete lattice - all its subsets have a *lub* and a *glb*
- A monotone function $f : L \to L$ on a complete lattice L is called *continuous* if for every directed subset D of L, $\sqcup f(D) = f(\sqcup D)$

Kleene's fixed point theorem

Theorem : Given an increasing and continuous function over a complete lattice, $f : L \to L$, its least fixed point $lfp^{\leq}(f) \in L$ exists and is given by $\sqcup\{f^i(\bot) \mid i \in \mathbb{N}\}$

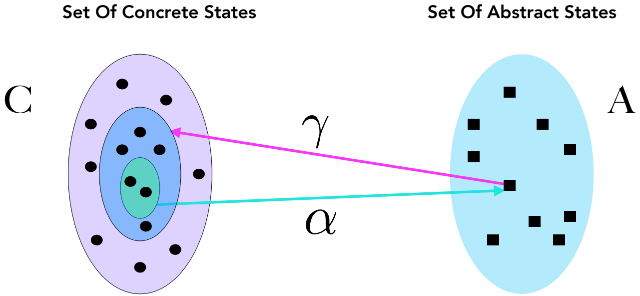
Proof :

- Observe that $f^0(\bot) = \bot \leq f^1(\bot)$ and since f is increasing, $\{f^i(\bot)\}$ is a non decreasing sequence
- Therefore $\mathbb{M} = \{\bot, f^0(\bot), f^1(\bot)), \ldots\}$ is a directed subset of L
- Let $m = \sqcup(\mathbb{M})$ and since f is continuous, we have

$$f(\sqcup(\mathbb{M})) = f(m) = \sqcup(f(\mathbb{M}))$$

- Also observe, $f(\mathbb{M}) = \mathbb{M} \backslash \{\bot\}$. But $\sqcup(\mathbb{M}) = \sqcup(\mathbb{M} \backslash \{\bot\})$, therefore, $f(m) = m$ i.e m is a fixed point.
- For any fixed point l, $f^0(\bot) = \bot \leq l$ which means $\forall i \; f^i(\bot) \leq l$ and therefore $m \leq l$

Abstract Framework



- Any operator *op* in the concrete domain can be lifted to the abstract domain as $op_A = \alpha \circ op \circ \gamma$

Abstract Framework

- Concrete Lattice $\mathcal{C} = (\mathcal{P}(S), \subseteq, \cup, \cap, S, \emptyset)$
- Abstract Lattice $\mathcal{A} = (A, \leq, \sqcup, \sqcap, \top, \bot)$
- Abstraction function $\alpha : \mathcal{P}(S) \rightarrow A$
- Concretization function $\gamma : A \rightarrow \mathcal{P}(S)$
- α and γ form a **Galois Connection** iff
  (i) $S_1 \subseteq \gamma(\alpha(S_1))$ for all $S_1 \subseteq S$
  (ii) $\alpha(\gamma(x)) \leq x$ for all $x \in A$
- Equivalently, $\forall S_1 \subseteq S, x \in A, \alpha(S_1) \leq x \Leftrightarrow S_1 \subseteq \gamma(x)$ (Prove!)
- If γ is also injective then (α, γ) is called Galois insertion

Abstraction Framework

- First, let's fix the WSTS under consideration as

$$T = (S, S_0, \to, \leq)$$

Abstraction Framework

- First, let's fix the WSTS under consideration as

$$T = (S, S_0, \rightarrow, \leq)$$

- The *concrete* domain $\mathcal{D}$ for our analysis would be the powerset over the states S

$$\mathcal{D} \stackrel{def}{=} \mathcal{P}(S)(\subseteq, \phi, S, \cup, \cap)$$

Abstraction Framework

- First, let's fix the WSTS under consideration as

$$T = (S, S_0, \to, \leq)$$

- The *concrete* domain $\mathcal{D}$ for our analysis would be the powerset over the states S

$$\mathcal{D} \stackrel{def}{=} \mathcal{P}(S)(\subseteq, \phi, S, \cup, \cap)$$

- An *abstract* domain could be $\mathcal{D}_{\uparrow} \stackrel{def}{=} \{\uparrow X : X \subseteq S\}(\sqsubseteq, \phi, S, \sqcup, \sqcap)$

Abstraction Framework

- First, let's fix the WSTS under consideration as

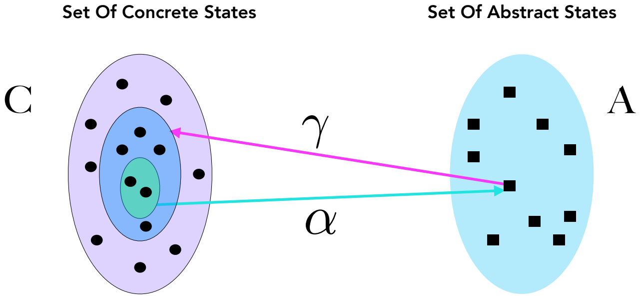
$$T = (S, S_0, \to, \leq)$$

- The *concrete* domain $\mathcal{D}$ for our analysis would be the powerset over the states S

$$\mathcal{D} \stackrel{def}{=} \mathcal{P}(S)(\subseteq, \phi, S, \cup, \cap)$$

- An *abstract* domain could be $\mathcal{D}_{\uparrow} \stackrel{def}{=} \{\uparrow X : X \subseteq S\}(\sqsubseteq, \phi, S, \sqcup, \sqcap)$
- We have already seen this in action!

Abstraction Framework



Abstraction Framework

- For forward coverability, $\mathcal{D}_{\downarrow} \overset{def}{=} \{\downarrow X : X \subseteq S\}(\sqsubseteq, \phi, S, \sqcup, \sqcap)$

Abstraction Framework

- For forward coverability, $\mathcal{D}_{\downarrow} \stackrel{def}{=} \{\downarrow X : X \subseteq S\}(\sqsubseteq, \phi, S, \sqcup, \sqcap)$
- $\mathcal{D}_{\downarrow}$ is a complete lattice (Verify!)

Abstraction Framework

- For forward coverability, $\mathcal{D}_\downarrow \stackrel{def}{=} \{\downarrow X : X \subseteq S\}(\sqsubseteq, \phi, S, \sqcup, \sqcap)$
- $\mathcal{D}_\downarrow$ is a complete lattice (Verify!)
- $\alpha_\downarrow(X) \stackrel{def}{=} \downarrow X$, $\gamma_\downarrow(Y) \stackrel{def}{=} Y$

Abstraction Framework

- For forward coverability, $\mathcal{D}_{\downarrow} \stackrel{def}{=} \{\downarrow X : X \subseteq S\}(\sqsubseteq, \phi, S, \sqcup, \sqcap)$
- $\mathcal{D}_{\downarrow}$ is a complete lattice (Verify!)
- $\alpha_{\downarrow}(X) \stackrel{def}{=} \downarrow X$, $\gamma_{\downarrow}(Y) \stackrel{def}{=} Y$
- $(\alpha_{\downarrow}, \gamma_{\downarrow})$ forms a Galois insertion (Verify!)

Abstraction Framework

- For forward coverability, $\mathcal{D}_{\downarrow} \stackrel{def}{=} \{\downarrow X : X \subseteq S\}(\sqsubseteq, \phi, S, \sqcup, \sqcap)$
- $\mathcal{D}_{\downarrow}$ is a complete lattice (Verify!)
- $\alpha_{\downarrow}(X) \stackrel{def}{=} \downarrow X$, $\gamma_{\downarrow}(Y) \stackrel{def}{=} Y$
- $(\alpha_{\downarrow}, \gamma_{\downarrow})$ forms a Galois insertion (Verify!)
- $post_{\downarrow} \stackrel{def}{=} \alpha_{\downarrow} \circ post \circ \gamma_{\downarrow}$

Setting up the abstract domain

- $\mathcal{P}_{fin}(Idl(S))$ = the finite sets of ideals of $S(\leq)$

Setting up the abstract domain

- $\mathcal{P}_{fin}(Idl(S))$ = the finite sets of ideals of $S(\leq)$
- $L_1 \sqsubseteq L_2 \overset{def}{\iff} \forall I_1 \in L_1.\exists I_2 \in L_2.I_1 \subseteq I_2$

Setting up the abstract domain

- $\mathcal{P}_{fin}(Idl(S))$ = the finite sets of ideals of $S(\leq)$
- $L_1 \sqsubseteq L_2 \overset{def}{\iff} \forall I_1 \in L_1.\exists I_2 \in L_2.I_1 \subseteq I_2$
- Using $\mathcal{P}_{fin}(Idl(S))$, we intend to represent elements of $\mathcal{D}_{\downarrow}$ (Recall: Erdös Tarski Theorem)

Setting up the abstract domain

- $\mathcal{P}_{fin}(Idl(S))$ = the finite sets of ideals of $S(\leq)$
- $L_1 \sqsubseteq L_2 \overset{def}{\Longleftrightarrow} \forall I_1 \in L_1 . \exists I_2 \in L_2 . I_1 \subseteq I_2$
- Using $\mathcal{P}_{fin}(Idl(S))$, we intend to represent elements of $\mathcal{D}_{\downarrow}$ (Recall: Erdös Tarski Theorem)
- But $\sqsubseteq$ is a quasi order but not a partial order (Verify!)

Setting up the abstract domain

- $\mathcal{P}_{fin}(Idl(S))$ = the finite sets of ideals of $S(\leq)$
- $L_1 \sqsubseteq L_2 \overset{def}{\Longleftrightarrow} \forall I_1 \in L_1. \exists I_2 \in L_2. I_1 \subseteq I_2$
- Using $\mathcal{P}_{fin}(Idl(S))$, we intend to represent elements of $\mathcal{D}_{\downarrow}$ (Recall: Erdös Tarski Theorem)
- But $\sqsubseteq$ is a quasi order but not a partial order (Verify!)
- Consider the quotient $\mathcal{D}_{Idl}$ of $\mathcal{P}_{fin}(Idl(S))$ wrt the equivalence relation $\sqsubseteq \cap \sqsubseteq^{-1}$

Setting up the abstract domain

- Consider the quotient $\mathcal{D}_{Idl}$ of $\mathcal{P}_{fin}(Idl(S))$ wrt the equivalence relation $\sqsubseteq \cap \sqsubseteq^{-1}$

Setting up the abstract domain

- Consider the quotient $\mathcal{D}_{Idl}$ of $\mathcal{P}_{fin}(Idl(S))$ wrt the equivalence relation $\sqsubseteq \cap \sqsubseteq^{-1}$
- Identify each element in $\mathcal{D}_{Idl}$ with the set of maximal ideals - this set is unique

Setting up the abstract domain

- Consider the quotient $\mathcal{D}_{Idl}$ of $\mathcal{P}_{fin}(Idl(S))$ wrt the equivalence relation $\sqsubseteq \cap \sqsubseteq^{-1}$
- Identify each element in $\mathcal{D}_{Idl}$ with the set of maximal ideals - this set is unique
- Let *IdealDecomp* : $\mathcal{D}_{\downarrow} \longrightarrow \mathcal{D}_{Idl}$

Setting up the abstract domain

- Consider the quotient $\mathcal{D}_{Idl}$ of $\mathcal{P}_{fin}(Idl(S))$ wrt the equivalence relation $\sqsubseteq \cap \sqsubseteq^{-1}$
- Identify each element in $\mathcal{D}_{Idl}$ with the set of maximal ideals - this set is unique
- Let *IdealDecomp* : $\mathcal{D}_{\downarrow} \longrightarrow \mathcal{D}_{Idl}$
- $\mathcal{D}_{Idl}(\sqsubseteq, \phi, \top, \sqcup, \sqcap)$ is a complete lattice
- Let $\alpha = \mathit{IdealDecomp} \circ \alpha_{\downarrow}$ and $\gamma(L) = \bigcup_{I \in L} I$

Setting up the abstract domain

- Consider the quotient $\mathcal{D}_{Idl}$ of $\mathcal{P}_{fin}(Idl(S))$ wrt the equivalence relation $\sqsubseteq \cap \sqsubseteq^{-1}$
- Identify each element in $\mathcal{D}_{Idl}$ with the set of maximal ideals - this set is unique
- Let $IdealDecomp : \mathcal{D}_{\downarrow} \longrightarrow \mathcal{D}_{Idl}$
- $\mathcal{D}_{Idl}(\sqsubseteq, \phi, \top, \sqcup, \sqcap)$ is a complete lattice
- Let $\alpha = IdealDecomp \circ \alpha_{\downarrow}$ and $\gamma(L) = \bigcup_{I \in L} I$
- (α, γ) form a Galois Insertion between the concrete domain $\mathcal{P}(\mathcal{S})$ and the abstract domain $\mathcal{D}_{Idl}$
- $post_{Idl} = \alpha \circ post \circ \gamma$

Setting up the abstract domain

- $F_{Idl}(L) = \alpha(S_0) \sqcup post_{Idl}(L)$

Setting up the abstract domain

- $F_{Idl}(L) = \alpha(S_0) \sqcup post_{Idl}(L)$
- The lfp of the sequence $\{F^i_{Idl}(\perp)\}$ is exactly the ideal decomposition of the cover set

Setting up the abstract domain

- $F_{Idl}(L) = \alpha(S_0) \sqcup post_{Idl}(L)$
- The lfp of the sequence $\{F^i_{Idl}(\bot)\}$ is exactly the ideal decomposition of the cover set
- Effectivity Conditions for checking for lfp:
  - F_{Idl} must be computable
  - $I_1 \sqsubseteq I_2$ must be decidable ($F_{Idl}(I) \sqsubseteq I$)
- Height of D_{Idl}: Not necessarily finite $\Rightarrow$

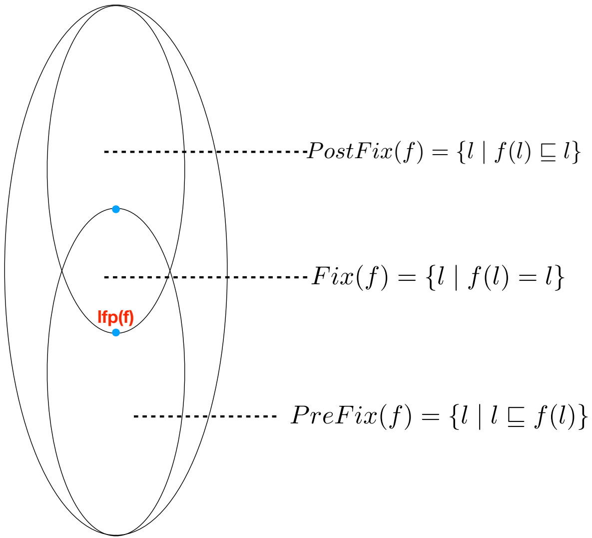
Setting up the abstract domain

- $F_{Idl}(L) = \alpha(S_0) \sqcup post_{Idl}(L)$
- The lfp of the sequence $\{F^i_{Idl}(\perp)\}$ is exactly the ideal decomposition of the cover set
- Effectivity Conditions for checking for lfp:
  - F_{Idl} must be computable
  - $I_1 \sqsubseteq I_2$ must be decidable $(F_{Idl}(I) \sqsubseteq I)$
- Height of D_{Idl}: Not necessarily finite $\Rightarrow$
- Stabilization of $\{F^i_{Idl}(\perp)\}$ is still not guaranteed

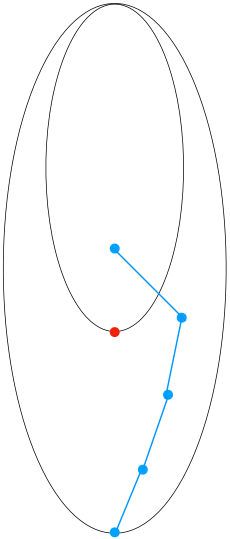
Solution: Widening

- Let $\nabla : \mathcal{P}(X) \rightharpoonup X$ be a partial function with the following conditions:
  - *Covering* : For all $Y \subseteq X$, if $\nabla(Y)$ is defined then for all $y \in Y, y \subseteq \nabla(Y)$
  - *Termination* : For every ascending chain $\{x_i\}_{i \in \mathbb{N}}$ in $X(\subseteq)$, the sequence $y_0 = x_0, y_i = \nabla(\{x_0, \ldots, x_i\})$, is well-defined and an ascending stabilizing chain

Widening


$PostFix(f) = \{l \mid f(l) \sqsubseteq l\}$
$Fix(f) = \{l \mid f(l) = l\}$
lfp(f)
$PreFix(f) = \{l \mid l \sqsubseteq f(l)\}$

Widening



Widening

- We will construct the widening operator ∇ for abstract domain $\mathcal{D}_{Idl}$ using the widening operator ∇_S for $Idl(S)$

Widening

- We will construct the widening operator ∇ for abstract domain $\mathcal{D}_{Idl}$ using the widening operator ∇_S for $Idl(S)$
- ∇_S is domain-specific for each class of WSTS

Widening

- We will construct the widening operator ∇ for abstract domain $\mathcal{D}_{Idl}$ using the widening operator ∇_S for $Idl(S)$
- ∇_S is domain-specific for each class of WSTS
- Lifting the widening operator from a base domain to its powerset domain is not easy to do in general

Widening

- We will construct the widening operator ∇ for abstract domain $\mathcal{D}_{Idl}$ using the widening operator ∇_S for $Idl(S)$
- ∇_S is domain-specific for each class of WSTS
- Lifting the widening operator from a base domain to its powerset domain is not easy to do in general
- Assume $S(\leq)$ is a bqo (not just a wqo)

Widening

- We will construct the widening operator ∇ for abstract domain $\mathcal{D}_{Idl}$ using the widening operator ∇_S for $Idl(S)$
- ∇_S is domain-specific for each class of WSTS
- Lifting the widening operator from a base domain to its powerset domain is not easy to do in general
- Assume $S(\leq)$ is a bqo (not just a wqo)
- Advantage: Now, $Idl(S)$ and $\mathcal{P}(S)$ are bqos

Widening

- Given ∇_S is a monotonic widening operator over $Idl(S)$ and $S(\leq)$ is a bqo

Widening

- Given ∇_S is a monotonic widening operator over $Idl(S)$ and $S(\leq)$ is a bqo
- For a finite ascending chain $C = \{L_i\} \subseteq \mathcal{D}_{Idl}$ define
  $\nabla : \mathcal{P}(\mathcal{D}_{Idl}) \rightharpoonup \mathcal{D}_{Idl}$:
  $\nabla(\{L_0\}) = L_0$
  $\nabla(\{L_0, \ldots, L_k\}) =$
  $\nabla(\{L_0, \ldots, L_{k-1}\}) \sqcup \{\nabla_S(\mathcal{I}) \mid \mathcal{I}$ is a maximal ascending chain in $\nabla(\{L_0, \ldots, L_{k-1}\}) \sqcup L_k\}$

Widening: Proof

1. ∇ is a widening operator for the domain $\mathcal{D}_{Idl}$

Widening: Proof

1. ∇ is a widening operator for the domain $\mathcal{D}_{Idl}$
2. Covering Property: Easy to Verify
3. Termination Condition
   - Assume there is an ascending chain L_i for which $W_0 = \{L_0\}, W_{i+1} = \nabla(L_0, \ldots L_{i+1})$ is not stabilising
   - Consider $I_i \in W_i$, st $I_i \not\subset I$ for all $I \in W_{i-1}$
   - $\{I_i\}$ has an ascending subsequence in $Idl(S)(\subseteq)$ (bqo!)
   - Consider the sequence $J_0 = I_{i_0}$ and $J_{k+1} = \nabla_S(\{I_{i_0}, \ldots I_{i_k}\})$.
   - $\{J_i\}$ stabilises, say $J_j = J_{j+1}$ where j is the index where it does
   - $I_{i_{j+1}} \subseteq J_{j+1} = J_j \subseteq I$ st $I \in W_{i_j}$

Using the widening operator

- The stabilisation of the sequence $\{y_i\}_{i \in \mathbb{N}}$ defined earlier is not easy to verify in practice

Using the widening operator

- The stabilisation of the sequence $\{y_i\}_{i \in \mathbb{N}}$ defined earlier is not easy to verify in practice
- This is because it is possible that in the sequence, $y_i = y_{i+1}$ but the sequence has not stabilised yet

Using the widening operator

- The stabilisation of the sequence $\{y_i\}_{i \in \mathbb{N}}$ defined earlier is not easy to verify in practice
- This is because it is possible that in the sequence, $y_i = y_{i+1}$ but the sequence has not stabilised yet
- We therefore define our analysis in terms of the widening sequence $\{W_i\}_{i \in \mathbb{N}}$ as follows:

$$W_0 = \phi$$

$$W_{i+1} = \nabla(\{W_0, \ldots, W_i, F_{Idl}(W_i) \sqcup W_i\})$$

Using the widening operator

- The stabilisation of the sequence $\{y_i\}_{i\in\mathbb{N}}$ defined earlier is not easy to verify in practice
- This is because it is possible that in the sequence, $y_i = y_{i+1}$ but the sequence has not stabilised yet
- We therefore define our analysis in terms of the widening sequence $\{W_i\}_{i\in\mathbb{N}}$ as follows:

$$W_0 = \phi$$

$$W_{i+1} = \nabla(\{W_0, \ldots, W_i, F_{Idl}(W_i) \sqcup W_i\})$$

- Here, $W_i = W_{i+1}$ would also imply that $W_{i+2} = \nabla(\{W_0, \ldots, W_i, F_{Idl}(W_i) \sqcup W_i\}) = W_i$ and similarly for further iterates

$Cover(T)$

$$Cover(T) \subseteq \bigcup_{i \in \mathbb{N}} \{W_i\}$$

- The covering property of the widening operator means that $W_i \sqsupseteq F^i_{Idl}(\perp)$ at each step of the sequence

Completion of a WSTS

- Let $\mathcal{S} = (X, \xrightarrow{\Sigma}, \leq)$ be a labeled WSTS. The completion of $\mathcal{S}$ is the labeled transition system $\widehat{S} = (Idl(X), \overset{\Sigma}{\rightsquigarrow}, \subseteq)$ such that $I \overset{a}{\rightsquigarrow} J$ if, and only if,

$$J \in IdealDecomp(\downarrow Post_{\mathcal{S}}(I, a))$$

Levels

An infinite sequence of ideals $I_0, I_1 \dots \in Idl(X)$ is an acceleration candidate if $I_0 \subset I_1 \subset \dots$ is strictly increasing.

Definition

The n^{th} level of Ideals(X) is inductively defined as

$$Acc_0(X) = Ideals(X)$$

$$Acc_n(X) = \{\bigcup_{i \in \mathbb{N}} I_i : I_0, I_1, \dots \in Acc_{n-1}(X)\}$$

where $I_0, I_1, \dots$ is an acceleration candidate in $Acc_{n-1}(X)$
Note that $Acc_n(X) \subseteq Acc_{n-1}(X)$. We say that Idl(X) has finitely many levels if there exists n such that $Acc_n(X) = \emptyset$.

Ideals($\mathbb{N}^d$) $= (\mathbb{N} \cup \{\omega\})^d$
$Acc_n(\mathbb{N}^d) = \{I \in \mathbb{N}^d_\omega : I$ has at least n occurrences of $\omega\}$

Acceleration in WSTS

Let $\mathcal{S} = (X, \xrightarrow{\Sigma}, \leq)$ be a WSTS st $\widehat{\mathcal{S}}$ is deterministic.
Let $w \in \Sigma^+$ and $I \in \text{Ideals}(X)$ The *acceleration of I under w* is defined as

$$w^\infty(I) \stackrel{def}{=} \begin{cases} \bigcup_{k \in N} w^k(I) & \text{if } I \subset w(I) \\ I & \textit{otherwise} \end{cases}$$

Note that $w^\infty(I)$ is also an ideal

Let $\mathcal{S} = (X, \xrightarrow{\Sigma}, \leq)$ be a WSTS such that $\mathcal{S}$ has strong monotonicity, and $\widehat{\mathcal{S}}$ is deterministic and has strict strong monotonicity. For every $I \in \text{Ideal}(X)$ and $w \in \Sigma^+$,

1. if $Post_{\widehat{\mathcal{S}}}(I, w) \neq \phi$ and $I \in Acc_n(X)$ for some $n \in \mathbb{N}$, then $w(I) \in Acc_n(X)$
2. if $I \subset w(I)$ and $I \in Acc_n(X)$ for some $n \in \mathbb{N}$, then $w^\infty(I) \in Acc_{n+1}(X)$

The Ideal Karp Miller Algorithm

Algorithm 4.1: Ideal Karp-Miller algorithm.

initialize a tree $\mathcal{T}$ with root $r\colon \langle I_0, 0\rangle$

while $\mathcal{T}$ contains an unmarked node $c\colon \langle I, n\rangle$ **do**

    if c has an ancestor $c'\colon \langle I', n'\rangle$ s.t. $I' = I$ **then** **mark** c

    else

        if c has an ancestor $c'\colon \langle I', n'\rangle$ s.t. $I' \subset I$

            and $n' = n$ `/* no acceleration occurred between` c' `and` c `*/` **then**

            $w \leftarrow$ sequence of labels from c' to c

            replace $c\colon \langle I, n\rangle$ by $c\colon \langle w^\infty(I), n+1\rangle$

        for $a \in \Sigma$ **do**

            if $a(I)$ is defined **then**

                add arc labeled by a from c to a new child $d\colon \langle a(I), n\rangle$

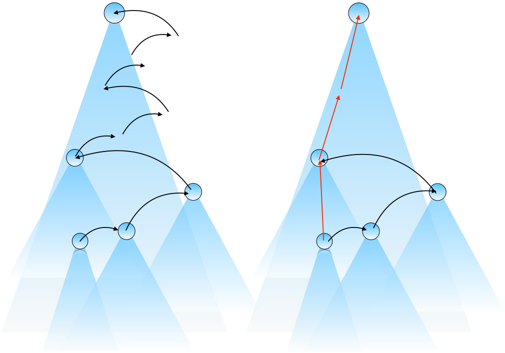
        mark c

return $\mathcal{T}$

Conditions for termination

- $\mathcal{S}$ has strong monotonicity
- $\widehat{\mathcal{S}}$ is deterministic and has strict strong monotonicity
- Ideals(X) has finitely many levels

Acceleration vs Widening



Summary

- We know that computing the cover set is undecidable in general because it decides boundedness
- We looked at a class of WSTS where we can compute the cover set using the notion of acceleration and levels
- We also looked at another work around that gives good approximations to cover set in practice with mild constraints on WSTS