COVERABILITY IN WSTS

We want to find an algorithmic solution for COVERABILITY in WSTS

COVERABILITY

Given: WSTS $(S, \rightarrow, \leq)$, initial configuration $s_0 \in S$ and target $t \in S$

Question: $\exists t' \in S : s_0 \longrightarrow t' \geq t$

Def Let $(S, \leq)$ wqo and $B \subseteq S$. Then we call

$$B\uparrow := \{ s \in S \mid \exists b \in B : s \geq b \}$$

the upward closure of B and we call B upward closed (upcl.) set. The downward closure and the downward closed sets are defined analogously.

Def: We define the two following sets in WSTS $(S, \rightarrow, \leq)$

① $pre(X) = \{ s \in S \mid \exists x \in X : s \longrightarrow x \}$

② $post(X) = \{ s \in S \mid \exists x \in X : x \longrightarrow s \}$

With these two definitions we can reformulate / rephrase the question of the COVERABILITY-problem:

$$\exists t' \in S : s_0 \longrightarrow t' \geq t \Leftrightarrow t \in \mathcal{R}(s_0)\downarrow \Leftrightarrow s_0 \in pre^*(t\uparrow)\uparrow$$

where pre^* is the transitive-reflexive-closure of pre. Same for $post^*$.

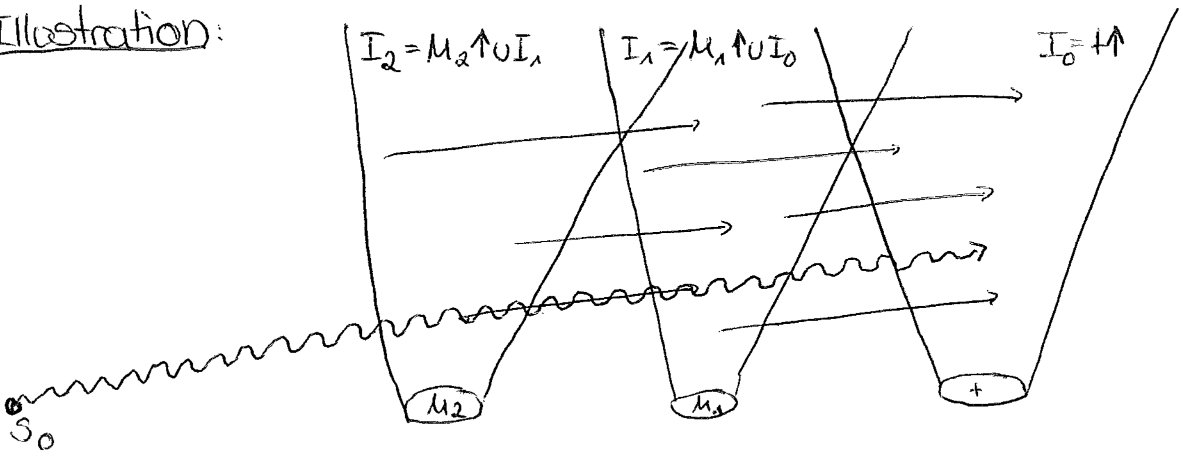
ABDULLA'S BACKWARDS SEARCH

Idea: ① Compute a fixpoint iteration $I_0 \subseteq I_1 \subseteq \dots \subseteq I_k \subseteq I_{k+1}$ and $t\uparrow = I_0$

② In each step compute pre of I_{i-1}

③ In the end check if $s_0 \in I_k$

Illustration:



So starting from an upcl. set I we want to decide whether $s_0 \in pred(I)\uparrow$.

Lemma Let $(S, \rightarrow, \leq)$ be a QOTS. Then $\leq$ is a simulation if and only if $pre^*(I)$ is upcl. for all upcl. sets $I \subseteq S$.

Proof Sheet 06 Ex 04.

So we have

$$pre^*(I) = pre^*(I)\uparrow = (I \cup pre(I) \cup pre^2(I) \cup \dots)\uparrow$$
$$= I\uparrow \cup (pre(I) \cup pre^2(I) \cup \dots)\uparrow$$
$$= I \cup pre(I \cup pre(I) \cup \dots)\uparrow$$

which means that $pre^*(I)$ is the least fixpoint of

$$F(X) = I \cup pre(X)\uparrow.$$

This least fixpoint exists by Kleene if you consider the following chain

$$I_0 := \emptyset \qquad I_{i+1} := I \cup pre(I_i)\uparrow$$

$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$

upcl

and $pre^*(I) = \bigcup_{i \in \mathbb{N}} I_i$.

But does this ascending chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ stabilize after finitely many steps? In other words can we compute the least fixpoint?

Theorem Consider a qo $(S, \leq)$. The following statements are equivalent:

① $(S, \leq)$ wqo.

② For every infinite $\subseteq$-increasing seq $I_0 \subseteq I_1 \subseteq I_2 \dots$ of upcl sets $I_j \subseteq S$, there is a $k \in \mathbb{N}$ with $I_k = I_{k+1}$.

③ For every infinite $\subseteq$-increasing seq $I_0 \subseteq I_1 \subseteq \dots$ of upcl. sets $I_j \subseteq S$, there is an $\ell \in \mathbb{N}$ with $I_\ell = I_{\ell+1} = I_{\ell+2} = \dots$

Proof

(① ⇒ ②) Towards a contradiction, assume $I_0 \subsetneq I_1 \subsetneq I_2 \dots$ Then there are $a_0 \in I_1 \setminus I_0$, $a_1 \in I_1 \setminus I_2 \dots$ Since I_j are upcl. $a_j \not\leq a_i$ with $i, j \in \mathbb{N}$, i
$a_0, a_1, a_2, \dots$ is a bad seqcence. ↯ to $(S, \leq)$ wqo

(② ⇒ ③) Towards a contradiction, assume there is an infinite seq. $I_0 \subseteq I_1 \subseteq \dots$ s.th $\forall k \in \mathbb{N}$ there is a $k_1 \in \mathbb{N}$ with $k < k_1$ and $I_k \subsetneq I_{k_1}$. For k_1 we can repeat the process and get a $k_2 > k_1$ with $I_{k_2} \subsetneq I_{k_1}$. Then $I_k \subseteq I_{k_1} \subseteq \dots$ is a seq violating ② ↯

(③ ⇒ ①) Consider $(a_i)_{i \in \mathbb{N}}$ in S. Define

$$I_0 := \{a_0\}\uparrow$$
$$I_1 := \{a_0, a_1\}\uparrow$$
$$\vdots$$

we obtain a seq $I_0 \subseteq I_1 \subseteq \dots$ By ③ we have $\ell \in \mathbb{N}$ with $I_\ell = {}_{\ell+1}$. This means $\exists j < \ell+1$ with $a_j \leq a_{\ell+1}$.

So yes, we can compute the LFP of F in finitely many steps.

Problem But to do so, we must be able to compute F. This is not possible in the general case. If $|I_j| = \infty$ we will have two problems

① We can not represent I_j.
② We cannot compute the pre of an infinite set.

Solution for ①: Consider only the minimal elements.

Def Let $(S, \leq)$ be wqo and $B \subseteq S$. A set of minimal elements of B is a set $min(B) \subseteq B$ containing for every $b \in B$ some $m \in min(B)$ with $m \leq b$ and $min(B)$ is an antichain.

Corollary $(S, \leq)$ wqo, $B \subseteq S$ upcl. Then $min(B)\uparrow = B\uparrow = B$ and $min(B)$ is finite.

Remark: $min(B)$ is not unique since have no antisymmetry $(a \leq b \wedge a \geq b \not\Rightarrow a = b)$
In practice, one of the two is used arbitrarily, but the choise is deterministic.
So we will represent I_j as $min(I_j)\uparrow$.

Solution for ②: To solve this problem you have to consider the concrete WSTS and find an algorithm which decides $minpre(m) = min(pre(m\uparrow)\uparrow)$

Def: We call an effective WSTS pre-effective if minpre is decidable.

So $s_0 \in pre^*(I)$ iff $\exists i\ s_0 \in I_i$
iff $s_0 \in I_k$ for k s.th. $I_k = I_{k+1}$

ABDULLA'S BACKWARDS SEARCH

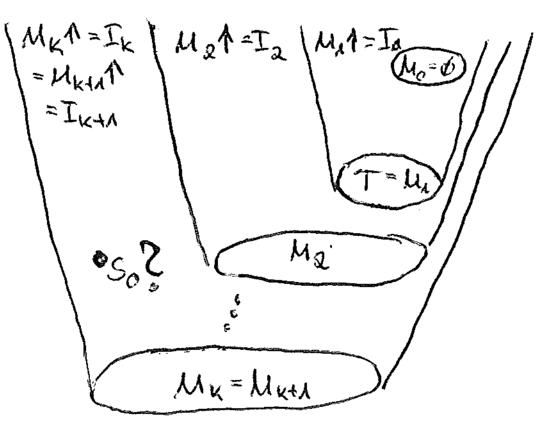
INPUT: $T \subseteq S$ finite set of targets and $T\uparrow = I$ and $s_0 \in S$
Compute the following sequence

$M_0 := \emptyset$

$M_{i+1} := min(B \cup \bigcup_{m \in M_i} minpre(m))$

If the LFP is found test for $s_0 \in M_k\uparrow$.

Illustration



Remark The function $minpre(m)$ has to have the effect of $min(pre(m\uparrow)\uparrow)$

Lemma $M_j\uparrow = I_j$ for all $j \in \mathbb{N}$

Proof by induction.

IB $n=0$ $\quad M_0 = \emptyset = I_0$

IS $j = j+1$ $\quad$
$$\begin{aligned} M_{j+1}\uparrow &= min(B \cup \bigcup_{m\in M_j} minpre(m))\uparrow \\ &= min(B \cup \bigcup_{m\in M_j} min(pre(m\uparrow)\uparrow)\uparrow \\ &= B\uparrow \cup (\bigcup_{m\in M_j} min(pre(m\uparrow)\uparrow)\uparrow \\ &= I \cup \bigcup_{m\in M_j} (min(pre(m\uparrow)\uparrow)\uparrow \\ &= I \cup \bigcup_{m\in M_j} pre(m\uparrow)\uparrow \\ &= I \cup pre(M_j\uparrow)\uparrow \\ &= I_{j+1} \end{aligned}$$

Theorem: COVERABILITY is decidable for a pre-effective WSTS (Abdulla 1996)

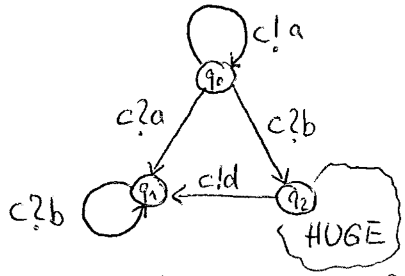
Proof: Let $I = T\uparrow$. Then there is ~~a~~ $s \in T\uparrow$ with $s_0 \rightarrow s$ iff $s_0 \in pre^*(I) = pre^*(I)\uparrow = \bigcup_{i\in\mathbb{N}} I_i$ with $I_0 := \emptyset$ and $I_{i+1} = I \cup pre(I_i)\uparrow$.
By lemma from above we have $\bigcup_{i\in\mathbb{N}} I_i = \bigcup_{i\in\mathbb{N}} M_i\uparrow$. By lemma $\exists k$ s. th. $M_{k+1}\uparrow = M_k\uparrow = \bigcup_{i\in\mathbb{N}} M_i\uparrow$
So the algorithm constructs

$$M_0, M_1, M_2, \dots, M_k$$

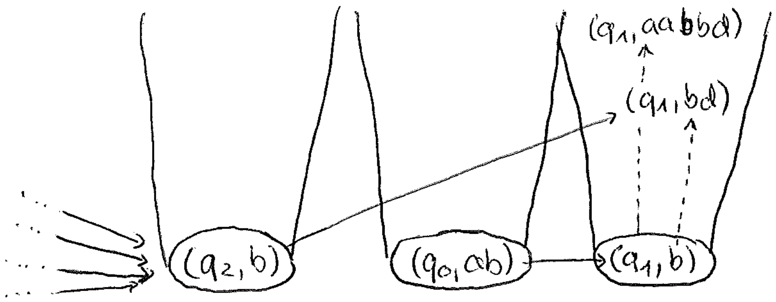
and stops when $M_k\uparrow = M_{k+1}\uparrow$. Then it checks if $s_0 \in M_k\uparrow$. Both is possible to do since $\leq$ is decidable.

FORWARDS SEARCH

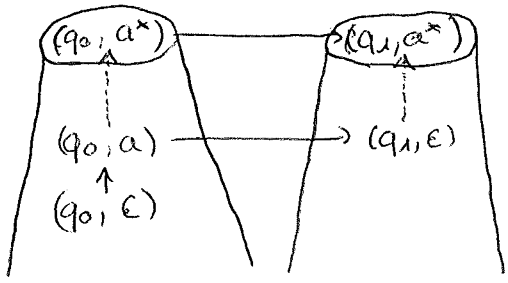
Problem: Consider the following LCS



If we would start Abdulla's Backwards Search with the target (q_1, b) the algorithm would have to explore this HUGE-part of the LCS instead of answering this obvious problem. We will never be able to reach q_2 via $q_0 \xrightarrow{c?b} q_2$ since this transition is not enabled.
So we want a sound method to narrow the search space of Abdulla's Backwards Search



Backwards Search



Forwards Search

Idea: Guess forward inductive invariants containing γ_0 and not $t=(q_1,b)$. These invariants are going to be dwcl. sets, which can contain infinitely many elements.

Question How do we finitely (algorithmically) represent downward closed sets?

Def Let $(S,\leq)$ be a qo. Then a pair $(L, [\![\,]\!])$ is called an Adequate Domain of Limits (ADL) if L is the set of Limits elements with $L \cap S = \emptyset$ and $[\![\,]\!] : L \cup S \to \mathcal{P}(S)$.

(L1) For $\ell \in L$. $[\![\ell]\!]$ dwcl. Moreover, $[\![s]\!] = \{s\}\downarrow$ for $s \in S$.

(L2) There is a top element $\top \in L$ with $[\![\top]\!] = S$.

(L3) For any dwcl. set $D \subseteq S$, there is a finite set $D' \subseteq S \cup L$ with $[\![D']\!] = D$.

It turns out that every wqo has an (canonical) ADL.

Def Let $(S,\leq)$ be a qo.

① We call $D \subseteq S$ directed if $\forall x,y \in D \; \exists z \in D$ s.th. $z \geq x$ and $z \geq y$

② A set $I \subseteq S$ is an ideal if it is dwcl. and directed

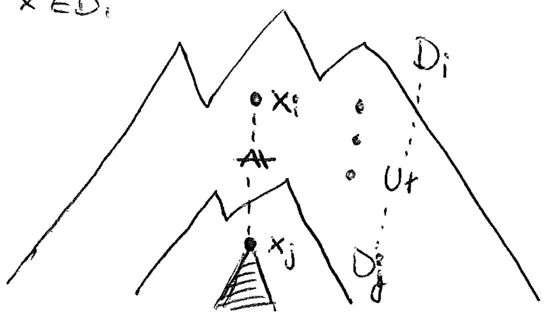
We write Ideals(S) for the set of all ideals of S.

Lemma: Let $(S,\leq)$ be a wqo. Then any seq $D_1 \supsetneq D_2 \supsetneq \ldots$ of dwcl. sets is finite.

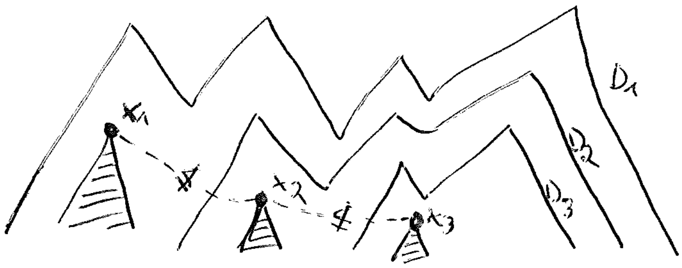
Proof Towards a contradiction, assume there is a sequence $D_1 \supsetneq D_2 \supsetneq \ldots$ of dwcl. sets which is infinite. Since all D_i are dwcl. we have for $x' \in S$, $x \in D_j \Rightarrow x' \in D_j$. Hence, the sequence $x_1, x_2, \ldots$ where for all $i<j$ $x_i \in D_i$ but $x_i \notin D_j$ is a bad seqence. This contradicts $(S,\leq)$ wqo. These x_i exists since $D_i \supsetneq D_{i+1}$.

Illustration

a) $x_i' \leq x \Rightarrow x' \in D_i$



b) $x_1, x_2, \dots$ s.th $\forall j: i<j$, $x_i \in D_i$, $x_i \notin D_j$



Lemma: Let $I \subseteq S$ be a dwcl. set and $(S, \leq)$ wqo. Then the following claims are equivalent:

① I is directed.

② $\forall D_1, D_2 \subseteq S$ dwcl. $I \subseteq D_1 \cup D_2 \Leftrightarrow I \subseteq D_1$ or $I \subseteq D_2$.

③ $\forall D_1, D_2 \subseteq S$ dwcl. $I = D_1 \cup D_2 \Rightarrow I = D_1$ or $I = D_2$.

Proof

①$\Rightarrow$② Assume I is dwcl and directed. Towards a contradiction let D_1, D_2 dwcl. sets s.th. $I \subseteq D_1 \cup D_2$ but $I \nsubseteq D_1$ and $I \nsubseteq D_2$. So there exist an $x_1 \in I$ with $x_1 \notin D_1$ and an $x_2 \in I$ with $x_2 \notin D_2$. But since I is directed there is a $y \in I$ so that $x_1 \leq y$ and $x_2 \leq y$. Since $I \subseteq D_1 \cup D_2$, we have $y \in D_1$ or $y \in D_2$. Because of D_1, D_2 dwcl sets either $x_1 \in D_1$ or $x_2 \in D_2$ ↯. Conversely, $I \subseteq D_1 \cup D_2$ holds if we have $I \subseteq D_1$ or $I \subseteq D_2$.

②$\Rightarrow$③ follows directly from ②

③$\Rightarrow$① Assume I is dwcl. and $\forall D_1, D_2 \subseteq S$ dwcl. we have $I = D_1 \cup D_2$ implies $I = D_1$ or $I = D_2$. Towards a contradiction, assume that I is not directed. So there exist $v_1, v_2 \in I$ s.th. there is no $u \in I$ with $u \geq v_1$ and $u \geq v_2$. We define

$$B_1 := \{x \in S \mid \exists u \in I: u \geq x \wedge u \geq v_1\}$$
$$B_2 := \{x \in S \mid \exists u \in I: u \geq x \wedge u \geq v_2\}$$

So we have $v_1 \in B_1$ but $v_2 \notin B_1$ and $v_2 \in B_2$ but $v_1 \notin B_2$. Hence, $I = B_1 \cup B_2$ but $I \neq B_1$ and $I \neq B_2$ ↯

Lemma Let $(S, \leq)$ be wqo. Then every dwcl. set D is a finite union of ideals.

Proof: Towards a contradiction, assume there are dwcl sets that are not a finite union of ideals. Among all dwcl. sets of S that are not a finite union of ideals will be a minimal one M. We have $M \neq \emptyset$ otherwise it is a finite union of ideals. So $\exists A, B$ dwcl s.th $M = A \cup B$ but $A \neq M$ and $B \neq M$ because M is not an ideal. By the minimality of M, B and A are finite unions of ideals and so is M as a consequence.

Def Let $(S, \rightarrow, \leq)$ be WSTS. Then the completion of $(S, \rightarrow, \leq)$ is a QOTS $(\hat{S}, \hat{\rightarrow}, \subseteq)$ where

① $\hat{S} = \text{Ideals}(S)$

② $I \hat{\rightarrow} J$ when $\text{post}(I)\downarrow = J_1 \cup \dots \cup J_k$ is canonical decomposition of $\text{post}(I)$ and $J = J_i$ for some $1 \leq i \leq k$.

Moreover, we call the completion $(\hat{S}, \hat{\rightarrow}, \subseteq)$ post-effective if

① $\hat{S}$ is recursive enumerable

② $\subseteq$ is decidable

③ $\hat{\text{post}}$ is decidable

The $\hat{\text{post}}$ is the version of post lifted to $(\hat{S}, \hat{\rightarrow}, \subseteq)$:

$\hat{\text{post}}(I) = \{I' \in S \mid I \hat{\rightarrow} I'\}$

With this we can introduce the algorithm for the fwd search

FORWARD SEARCH

INPUT: $(S, \rightarrow, \leq)$ effective WSTS with post-effective completion $s_0 \in S$, $t \in S$

Run the following two semi-algorithm in parallel

Ⓐ Explore $\mathcal{R}(s_0)$, stop with "yes" if we found $t' \in \mathcal{R}(s_0)$, $t' \geq t$

Ⓑ Enumerate finite unions of ideals $J_1 \cup \dots \cup J_k$ in $\hat{S}$, stop with "no" when

a) $J_1 \cup \dots \cup J_k \supseteq \hat{\text{post}}(J_1 \cup \dots \cup J_k)$

b) $s_0 \in J_1 \cup \dots \cup J_k$

c) $t \notin J_1 \cup \dots \cup J_k$

Theorem COVERABILITY is decidable for WTST with a post-effective completion.

Proof: Give $s_0 \in S$ we need to decide whether some given $t \in S$ is in $post^*(\{s_0\})\downarrow$.

Ⓐ Assume t is coverable. Then the semi-algorithm Ⓐ will terminate with "yes"

Conversely, if t is not coverable the algorithm will fail to find a suitable path and either not terminate or terminate with no answer (in the case the state space is finite)

Ⓑ Assume t is not coverable. Then the semi-algorithm Ⓑ will eventually consider the downward-closed set $post^*(\{s_0\})\downarrow$ which clearly satisfies the conditions and the algorithm would correctly answer "no".

Conversely, when t is coverable, no downward-closed set can satisfy the conditions of being a fwd. ind. inv. containing s_0 but not t, so the enumeration would not terminate.

Therefore, in all cases one of the two algorithms will terminate with the correct answer.

It remains to clarify why a) - c) are decidable:

a) $\underbrace{\hat{post}(I_1)\downarrow \cup \dots \cup \hat{post}(I_k)}_{\text{finite}} \subseteq \underbrace{I_1 \cup \dots \cup I_k}_{\text{finite}}$ is decidable since $\hat{post}$ is decidable (post-effective completion) and $\subseteq$ is decidable (post-effective completion and previous lemma)

b) $s_0 \in I_1 \cup \dots \cup I_k \Leftrightarrow \{s_0\}\downarrow \subseteq I_1 \cup \dots \cup I_k$ is again decidable because of the previous lemma and the post-effectiveness of $(\hat{S}, \xrightarrow{}, \subseteq)$

c) $t \notin I_1 \cup \dots \cup I_k \Leftrightarrow \{t\}\downarrow \not\subseteq I_1 \cup \dots \cup I_k$ analogously.