Well-Structured Transition Systems

Goal: Algorithmic verification of programs

→ Programs ≙ Infinite state systems
(Pushdown automata, Petri Nets, ...)

→ Decide reachability/coverability on such systems.

→ Not always possible ∴ often undecidable.

→ Define general class of transition systems where reachability/coverability is decidable → WSTS.

→ WSTSs cover many inf. state systems (Petri Nets, Lossy Channel Systems, ...)

Problem: How to decide coverability over inf. many states?
⇒ Need termination argument.
⇝ well-quasi ordering.

Ramsey's Theorem:

Helpful tool for infinite combinatorics.

Theorem: Let (V, E) be an infinite undirected complete graph and C a finite set of colors. Let $f: E \to C$ be a coloring of the edges.

Then, there is an infinite complete subgraph (V', E') and a color $c \in C$ s.th. for all edges $e \in E'$ we have $f(e) = c$.

Proof:

Since V is infinite, we can assume $\mathbb{N} \subseteq V$.
We show it for the case $\mathbb{N} = V$. The more general case then follows.

Let $<$ be the ordering on $\mathbb{N}$ and let $C = \{1, \dots, b\}$. We construct an infinite sequence

$(v_0, V_0, c_0), (v_1, V_1, c_1), \dots$ with

- $v_0 < v_1 < v_2 < \dots$
- $V_0 \supseteq V_1 \supseteq V_2 \supseteq \dots$ and all V_i infinite
- $f(\{v_i, x\}) = c_i \quad \forall x \in V_i$
- $v_{i+1} \in V_i \quad \forall i$.

We construct the sequence by induction.

IB: • Choose v_0 arbitrary

• c_0 is a color that colors inf. many edges connected to v_0.
Note that there are inf. many edges $\{v_0, x\}$ and only fin. many colors $\Rightarrow c_0$ had to exist.

• $V_0 = \{x \in V \mid f(\{v_0, x\}) = c_0\}$.

IS: Assume we already constructed $(v_0, V_0, c_0), \dots, (v_n, V_n, c_n)$.
We construct $(v_{n+1}, V_{n+1}, c_{n+1})$:

• Choose $v_{n+1} \in V_n$ with $v_n < v_{n+1}$ (V_n is infinite).

Now reason as before with V_n instead of V:

• c_{n+1} is a color that colors inf. many edges $\{v_{n+1}, x\}$ with $x \in V_n$.

• $V_{n+1} = \{x \in V_n \mid f(\{v_{n+1}, x\}) = c_{n+1}\}$.

In the constructed inf. sequence, a color c occurs inf. often.

Let $V' := \{v_i \mid (v_i, V_i, c_i) \text{ with } c_i = c\} \subseteq V$.

Consider an edge $\{v_i, v_j\}$ with $v_i, v_j \in V'$.
W.l.o.g. $v_i < v_j$.

We have: $v_j \in V_{j-1} \subseteq V_i \Rightarrow f(\{v_i, v_j\}) = c_i = c$.

Hence, all edges among V' are colored by c. ■

Well-quasi orderings:

Definition:

• A quasi ordering is a reflexive and transitive relation $(A, \leq)$: (transitive: if $a \leq b$ and $b \leq c \Rightarrow a \leq c$)

$$\forall a \in A: a \leq a$$

→ Write $a > b$ for $a \geq b$ and $b \neq a$.

→ $a \geq b$ ∧ $b \geq a$ does NOT imply $a = b$ (antisymmetry is missing)

• A well quasi ordering (wqo) is a quasi ordering $(A, \leq)$ s.th.:
for every inf. sequence $(a_i)_{i \in \mathbb{N}}$ in A there are indices $i < j$ s.th. $a_i \leq a_j$.

③ in a wqo, every inf. sequence contains two comparable elements.

Example:

a) $(\mathbb{N}, \leq)$ is a wqo.

6 4 3 2 1 0 5 (with $0 \leq 5$)

b) $(\mathbb{Z}, \leq)$ is not a wqo:

6 4 3 0 -1 -2 -3 ...

Remarks:

Classical termination proofs rely on well-founded quasi orderings.

$(A, \leq)$ is well-founded if $\nexists (a_i)_{i \in \mathbb{N}} : a_0 > a_1 > a_2 > \dots$

→ Wqos are stronger: They forbid infinite antichains,

subsets $B \subseteq A$ of incomparable elements, $a \not\leq b$ $\forall a, b \in B$.

Theorem: Characterization of wqos.

Let $(A, \leq)$ be a quasi ordering. The following are equivalent:

1) $(A, \leq)$ is a wqo.

2) Every inf. sequence $(a_i)_{i \in \mathbb{N}}$ in A contains an inf. increasing subsequence $(a_{\varphi(i)})_{i \in \mathbb{N}}$ with

$$a_{\varphi(i)} \leq a_{\varphi(i+1)} \quad \forall i \in \mathbb{N}.$$

3) There is no inf. strictly decreasing subsequence and no inf. antichain in A.

Proof:

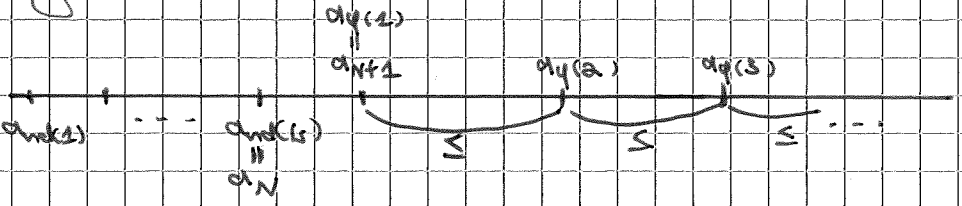
1) ⇒ 2) Let $(a_i)_{i \in \mathbb{N}}$ be an inf. sequence in A.

Consider the subsequence $(a_{nd(i)})_{i \in \mathbb{N}}$ of elts. not dominated by successors: For each $a_{nd(i)}$ $\nexists j > nd(i)$ with $a_{nd(i)} \leq a_j$.

Assume $(a_{nd(i)})_{i \in \mathbb{N}}$ is infinite. By 1) we get that some $a_{nd(i)}$ is dominated by an $a_{nd(j)}$ ↳

⇒ $(a_{nd(i)})_{i \in \mathbb{N}}$ is finite.

Let $N := nd(k)$ be the maximal index in the sequence. Then, all a_i with $i > N$ have a dominating successor. Hence, starting from $N+1$, we can find an increasing subsequence:



2) $\Rightarrow$ 3) ✓

3) $\Rightarrow$ 1) (Actually 3) $\Rightarrow$ 2) (or 2) $\Rightarrow$ 1) is easy)

We use Ramsey's Theorem.

Let $(a_i)_{i \in \mathbb{N}}$ be an inf. sequence in A.

Consider the complete graph $G = (\mathbb{N}, E)$ with, intuitively, the vertices are the elements in $(a_i)_{i \in \mathbb{N}}$.

Construct the coloring $f: E \to C := \{\leq, >, \text{incomp.}\}$ as follows

$$f(\{x,y\}) = \begin{cases} \leq, & \text{if } a_x \leq a_y \\ >, & \text{if } a_x > a_y \\ \text{incomp.}, & \text{otherwise} \end{cases}$$

By Ramsey we get an inf. complete subgraph colored by a single color c of C.

$\rightarrow$ c cannot be $>$ or incomp. since we assumed 3).

$\Rightarrow$ $c = \leq$ and we can find an inf. increasing subsequence of $(a_i)_{i \in \mathbb{N}}$. ■

Upward and downward closed sets:

Goal: Use finite set of minimal elements to represent arbitrarily large "upward closed" sets.

Definition: Minimal elements.

Let $(A, \leq)$ be a wqo and $B \subseteq A$. A set of minimal elements is a subset $\min(B) \subseteq B$ s.th.:

- for any $b \in B$ $\exists$ $m \in \min(B)$: $m \leq b$, and
- $\min(B)$ is an antichain.

⑤

Lemma:

Let $(A, \leq)$ be a wqo and let $B \subseteq A$.

There exists a finite set of minimal elements $\min(B)$.

Proof:

Assume there is no set of min. elements. Let $b_0 \in B$ arbitrary.

We construct $(b_i)_{i \in \mathbb{N}}$. For b_{i+1} choose an element from B s.th. $b_j \not\geq b_{i+1}$ $\forall j = 1, \dots, i$.

Note that b_{i+1} exists. Otherwise, we could construct a finite set of min. elements from $\{b_0, \dots, b_i\}$.

The sequence $(b_i)_{i \in \mathbb{N}}$ violates the wqo-definition ↯ ■

Remarks:

- $\min(B)$ need not be unique ⇝ missing antisymmetry.
- $\min(B)$ are good candidates to represent inf. sets.

Definition: Upward and downward closure.

Let $(A, \leq)$ be a wqo.

1) A set $I \subseteq A$ is upward closed if:

For all $x, a \in A$: $x \in I$ and $x \leq a \Rightarrow a \in I$.

→ The upward closure of a set $B \subseteq A$ is

$B\uparrow := \{a \in A \mid a \geq b \text{ for some } b \in B\}$.

2) A set $D \subseteq A$ is downward closed if:

For all $x, a \in A$: $x \in D$ and $a \leq x \Rightarrow a \in D$.

→ The downward closure of a set $B \subseteq A$ is

$B\downarrow := \{a \in A \mid a \leq b \text{ for some } b \in B\}$.

Lemma: Representation of upward closed sets.

Let $(A, \leq)$ be a wqo and $I \subseteq A$ and upward closed set.

Let $\min(I)$ be a finite set of min. elements. Then:

$$I = \min(I)\uparrow .$$

Proof: Simple.

We show that coverability in wSTS is decidable.
Termination argument of algorithm:

→ build chain of upward closed sets:
$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$

→ chain stabilizes due to wqo.

Theorem: Chains of upward closed sets.
Let $(A, \leq)$ be a quasi ordering. The following are equivalent:

1) $(A, \leq)$ is a wqo.

2) For each sequence $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ of upward closed sets, there is a $k \in \mathbb{N}$: $I_k = I_{k+1}$.

3) For each sequence $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ of upward closed sets, there is an $l \in \mathbb{N}$: $I_l = I_{l+1} = I_{l+2} = \dots$.

Proof:

1) ⇒ 2)
Assume the chain $I_0 \subseteq I_1 \subseteq \dots$ does not stabilize at a k.
Then, there are elements

$a_0 \in I_1 \setminus I_0$, $a_1 \in I_2 \setminus I_1$, $a_2 \in I_3 \setminus I_2$, ...

Since all I_i are upward closed, we get that $a_i \not\leq a_j$ for each $i < j$ (Otherwise $a_j \geq a_i \overset{\in I_{i+1}}{\Rightarrow} a_j \in I_{i+1} \subseteq I_j$ ↯).
But then, $(a_i)_{i \in \mathbb{N}}$ contradicts the wqo definition. ↯

2) ⇒ 3)
Assume 3) does not hold. Then, there is a sequence
$I_0 \subseteq I_1 \subseteq \dots$ so that: $\forall k_0 \in \mathbb{N}, \exists k_1$:
$k_0 < k_1$ and $I_{k_0} \subsetneq I_{k_1}$.
For k_1, $\exists k_2$: $k_1 < k_2$ and $I_{k_1} \subsetneq I_{k_2}$.

We get an inf. sequence

$$I_{k_0} \subsetneq I_{k_1} \subsetneq I_{k_2} \subsetneq \dots \quad \text{↯2)}$$

3) ⇒ 1).

Let $(a_i)_{i\in\mathbb{N}}$ be an inf. sequence in A.

Define a sequence of upward closed sets:

$$I_0 := \{a_0\}\uparrow, \quad I_1 := \{a_0, a_1\}\uparrow, \quad I_2 = \{a_0, a_1, a_2\}\uparrow, \dots$$

$\Rightarrow I_0 \subseteq I_1 \subseteq \dots$

By 3) $\exists$ (smallest) $l \in \mathbb{N}$: $I_l = I_{l+1} = \dots$.

$I_l = \{a_0, \dots, a_l\}\uparrow$ $\quad I_{l+1} = \{a_0, \dots, a_l, \underline{a_{l+1}}\}\uparrow$

$\Rightarrow \exists\, j < l+1$ s.th. $a_j \le a_{l+1} \Rightarrow$ wqo. ■

Constructing Well quasi orderings:

Importance of WSTS comes from the fact that many sets are wqo.

- Reason: wqos can be composed to new wqos.
- Algebraic toolkit to derive wqos.

Lemma: If A is finite, $(A, =)$ is a wqo.

Moreover, $(\mathbb{N}, \le)$ is a wqo.

Lemma: Closed under product

If $(A, \le_A)$ and $(B, \le_B)$ are wqos, then

$(A \times B, \le)$ is a wqo, where

$$(a_1, b_1) \le (a_2, b_2) \text{ iff } a_1 \le_A a_2 \text{ and } b_1 \le_B b_2.$$

Proof:

Let $(a_i, b_i)_{i\in\mathbb{N}} \subseteq A \times B$ be an inf. sequence.

Then $(a_i)_{i\in\mathbb{N}}$ is an inf. sequence in A.

Since $(A, \le_A)$ is a wqo: there is an inf. increasing subsequence

$(a_{\varphi(i)})_{i\in\mathbb{N}}$ with $a_{\varphi(i)} \le_A a_{\varphi(i+1)}$ $\forall i \in \mathbb{N}$.

Now consider $(a_{\varphi(i)}, b_{\varphi(i)})_{i\in\mathbb{N}}$, subsequence of $(a_i, b_i)_{i\in\mathbb{N}}$.

Then, $(b_{\varphi(i)})_{i\in\mathbb{N}}$ is an inf. sequence in B.

Since $(B, \leq_B)$ is a wqo, there are $i<j$: $b_{\varphi(i)} \leq_B b_{\varphi(j)}$

Then we have $\varphi(i) < \varphi(j)$ and:

$a_{\varphi(i)} \leq_A a_{\varphi(j)}$, and $b_{\varphi(i)} \leq_B b_{\varphi(j)}$.

$\Rightarrow (a_{\varphi(i)}, b_{\varphi(i)}) \leq (a_{\varphi(j)}, b_{\varphi(j)})$. ■

We lift the statement to words.
→ Unbounded cartesian products.

Definition:

Let $(A, \leq)$ be a wqo and $u, v \in A^*$. We define

$u \leq^* v$ iff $u = a_1 \cdots a_m$, $v = b_1 \cdots b_n$ and

there are $1 \leq i_1 < \cdots < i_m \leq n$: $a_j \leq b_{i_j}$ $\forall j = 1, \ldots, m$.

→ We can embedd the word u into v.

Lemma: Higman - 1952.

If $(A, \leq)$ is a wqo, then $(A^*, \leq^*)$ is a wqo.

Proof:

Assume $(A^*, \leq^*)$ is not a wqo. Then there are bad sequences.

These are sequences in A^* that do not contain comparable elements.

By induction, we construct a particularly small bad sequence $(u_i)_{i\in\mathbb{N}}$ that derives a contradiction.

IB: Select the (a) shortest word u_0 that starts a bad sequence.

IS: Assume we constructed $u_0, \ldots, u_n$.

Select the shortest word u_{n+1} such that $u_0, \ldots, u_n, u_{n+1}$ is a prefix of a bad sequence.

→ Note that u_{n+1} exists!

The resulting sequence $(v_i)_{i\in\mathbb{N}}$ is bad.

(otherwise $\exists i<j: v_i \leq^* v_j$. But $v_0, \dots, v_j$ is prefix of bad sequence ↯)

Let $v_i = a_i . w_i$, $a_i \in A$, $w_i \in A^*$.

Since $(A, \leq)$ is a wqo, $(a_i)_{i\in\mathbb{N}}$ contains an increasing subsequence $(a_{\varphi(i)})_{i\in\mathbb{N}}$.

Now consider the sequence

$$v_0, v_1, \dots, v_{\varphi(0)-1}, v_{\varphi(0)}, v_{\varphi(1)}, \dots$$

The word $v_{\varphi(0)}$ is shorter than $v_{\varphi(0)}$. Hence, the sequence has to be good. Otherwise, we would have selected $v_{\varphi(0)}$ instead of $v_{\varphi(0)}$.

⇒ The sequence contains comparable elements.

- Cannot be among $v_0, \dots, v_{\varphi(0)-1}$. Otherwise $(v_i)_{i\in\mathbb{N}}$ would be good. ↯
- Cannot be between $v_i \leq^* v_{\varphi(j)}$. Otherwise, $v_i \leq^* v_{\varphi(j)} \leq^* a_{\varphi(j)} . w_{\varphi(j)} = v_{\varphi(j)}$. So $(v_i)_{i\in\mathbb{N}}$ would be good. ↯
- We have: $v_{\varphi(i)} \leq^* v_{\varphi(j)}$ for an $i<j$.
  Since $a_{\varphi(i)} \leq a_{\varphi(j)} \Rightarrow \underbrace{a_{\varphi(i)} . w_{\varphi(i)}}_{v_{\varphi(i)}} \leq^* \underbrace{a_{\varphi(j)} . w_{\varphi(j)}}_{v_{\varphi(j)}}$ ↯

⇒ Bad sequences do not exist. ∎

Well Structured Transition Systems:

- Frameworks for automatic verification of inf. state systems.
- Found when trying to generalize results for other models. By Finkel and Abdulla.

Definition:

- A **transition system** is a tuple $TS = (\Gamma, \gamma_0, \to)$ with
  - Γ a (typically infinite) set of configurations,
  - $\gamma_0 \in \Gamma$ an initial configuration,
  - $\to \subseteq \Gamma \times \Gamma$ a transition relation.

- TS is **well-structured** if there is $\leq \subseteq \Gamma \times \Gamma$ s.th.
  - $\leq$ is a wqo,
  - $\leq$ is a simulation relation.

- A **simulation relation** $\leq \subseteq \Gamma \times \Gamma$ satisfies:

$\forall \gamma_1, \gamma_2, \gamma_3 \in \Gamma$:

$\gamma_3 \; \vee \; \gamma_1 \to \gamma_2$ there is a $\gamma_4 \in \Gamma$: $\gamma_3 \to \gamma_4$ and $\gamma_2 \leq \gamma_4$.

We write $TS = (\Gamma, \gamma_0, \to, \leq)$ for a WSTS.

Abdulla's Backward Search:

Goal: Decide coverability in WSTS:

- Can we reach a config. $\gamma_0 \to^* \gamma'$ that covers a target config γ: $\gamma' \geq \gamma$?
- Reformulate to: can we reach an element in $\{\gamma\}\uparrow$?
- So, we show how to decide the following problem:

Given: A WSTS $TS = (\Gamma, \gamma_0, \to, \leq)$ and an upward closed set $I \subseteq \Gamma$.

Question: Is there a $\gamma \in I$: $\gamma_0 \to^* \gamma$?

Idea: Check it backwards!

- Start with $I_0 = I$.
- Compute I_1 = configs that reach I_0 in at most one step.
- Compute I_2 = config. that reach I_0 in at most two steps.
- ⋮

Then I is reachable from $\gamma_0 \iff \gamma_0 \in \bigcup_{j \in \mathbb{N}} I_j$.

→ The sets I_j can be shown to be upward closed

⇒ we get a chain of upw. closed sets

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

Thm.: ⇒ $\exists\, k$: $I_k = I_{k+1} = \dots$

Hence $\bigcup_{j \in \mathbb{N}} I_j = I_k$.

Algorithm:

1) Generate chain $I_0 \subseteq I_1 \subseteq \dots$

2) Check for stabilization $I_k = I_{k+1}$

3) If stabilized, check if $\gamma_0 \in I_k$.

Problem:

How to check $I_k = I_{k+1}$ and $\gamma_0 \in I_k$?

→ The I_j are infinite.

Solution:

Represent the I_j by their minimal elements μ_j:

$$I_j = \mu_j\uparrow$$

→ Then we can work with finite sets.

Overview:

I is reachable from γ_0 $\Leftrightarrow$ $\gamma_0 \in I_k$ with $I_k = I_{k+1}$

$\Leftrightarrow$ $\gamma_0 \geq \gamma$ for a $\gamma \in \mu_k$ and $\mu_k\uparrow = \mu_{k+1}\uparrow$.

PART 1: I is reachable from γ_0 $\Leftrightarrow$ $\gamma_0 \in I_k$: $I_k = I_{k+1}$.

Definition: Let $(\Gamma, \gamma_0, \to, \leq)$ be a WSTS and $B \subseteq \Gamma$. Then the predecessors of B are in the set $\mathrm{pre}(B) = \{\gamma \in \Gamma \mid \gamma \to \gamma' \text{ for a } \gamma' \in B\} \subseteq \Gamma$.

→ ~~Tabring~~

→ Upward closed sets are closed under taking predecessors.

Lemma: $\uparrow pre(I)$ is upw. closed.

Consider a transition system $TS = (\Gamma, \gamma_0, \to)$ and $\leq \subseteq \Gamma \times \Gamma$ a relation. Then:

$\leq$ is a simulation relation $\iff$ for each upward closed set $I \subseteq \Gamma$, $pre(I)$ is upward closed.

Proof: Exercise. ■

Definition: Chain of sets I_j.

Let $TS = (\Gamma, \gamma_0, \to, \leq)$ be a WSTS, ~~Then we se~~ and $I \subseteq \Gamma$ upward closed. We construct:

$I_0 := I$ and $I_{j+1} := I_0 \cup pre(I_j)$ $\forall j \in \mathbb{N}$.

→ By construction: $I_j = \bigcup_{l=0}^{j} pre^l(I)$.

Lemma: Consider a WSTS $TS = (\Gamma, \gamma_0, \to, \leq)$ and $I \subseteq \Gamma$, ~~upward~~ upward closed, $n \in \mathbb{N}$. Then,

I is reachable from γ in at most n steps $\iff \gamma \in I_n$.

Proof: By construction of the I_j. ■

A consequence is: I is reachable from $\gamma_0 \iff \gamma_0 \in \bigcup_{j \in \mathbb{N}} I_j = pre^*(I)$.

But it is even better:

Theorem:

Let $TS = (\Gamma, \gamma_0, \to, \leq)$ be a WSTS and $I \subseteq \Gamma$ upw. closed.

Then:

I is reachable from $\gamma_0 \iff \gamma_0 \in pre^*(I) = \bigcup_{j \in \mathbb{N}} I_j = I_{l_s}$ with $I_{l_s} = I_{l_s+1}$ and l_s is the first such index.

Proof:

We only need to show that $\bigcup_{j \in \mathbb{N}} I_j = I_k$.

By the construction of the I_j we get a chain

$I_0 \subseteq I_1 \subseteq \dots$

Moreover, each I_j is upward closed (pre is upw. closed + union).

Thm $\Rightarrow$ there is a first $k \in \mathbb{N}$: $I_k = I_{k+1}$.

By construction of the I_j we then get $I_k = I_{k+1} = I_{k+2} = \dots$

Hence, $\bigcup_{j \in \mathbb{N}} I_j = I_k$. ∎

PART 2: $x_0 \in I_k : I_k = I_{k+1} \iff x_0 \geq x : x \in \mu_k$ and $\mu_k\uparrow = \mu_{k+1}\uparrow$.

→ Define with the I_j, a sequence of minimal elements μ_j.

Definition: Minimal elements of I_j

Let $TS = (T, x_0, \to, \leq)$ be a WSTS and I_j the sets of PART 1.

$$\mu_0 := \min(I), \quad \mu_{j+1} := \min\left(\mu_0 \cup \bigcup_{x \in \mu_j} \text{minpre}(x)\right) \quad \forall j \in \mathbb{N}.$$

The function minpre returns a set of min. elements

$\text{minpre}(x) = \min(\text{pre}(\uparrow x\uparrow))$ for the predecessors of $\uparrow x\uparrow$.

Remarks:

→ That minpre(·) is computable has to be shown for every instantiation of the WSTS-framework! We do not get this from the WSTS definition.

→ Suppose minpre(·) is computable and $\min(I) = \mu_0$ is known. Then μ_{j+1} is computable! $\min(\underbrace{\quad}_{\text{finite set}})$.

We say a WSTS has computable minimal predecessors if minpre(x) is computable $\forall x \in T$.

Lemma: $I_j = \mu_j\uparrow \quad \forall j \in \mathbb{N}$.

Proof: Proceed by induction.

IB: $I_0 = I \underset{uc}{=} \min(I)\uparrow \underset{def}{=} \mu_0\uparrow$.

IS: Assume we have $I_j = \mu_j\uparrow$. Then:

$$I_{j+1} = I \cup pre(I_j) \overset{IH}{=} I \cup pre(\mu_j\uparrow)$$

$$= I \cup pre\Big(\bigcup_{x \in \mu_j} \{x\}\uparrow\Big)$$

$$= I \cup \bigcup_{x \in \mu_j} \underbrace{pre(\{x\}\uparrow)}_{u.c.}$$

$$= I_0\uparrow \cup \bigcup_{x \in \mu_j} \min(pre(\{x\}\uparrow))\uparrow$$

$$= \Big(\mu_0 \cup \bigcup_{x \in \mu_j} \min(pre(\{x\}\uparrow))\Big)\uparrow$$

$\cup\uparrow = \min(\cup)\uparrow$

$$= \min\Big(\mu_0 \cup \bigcup_{x \in \mu_j} minpre(x)\Big)\uparrow = \mu_{j+1}\uparrow. \quad \blacksquare$$

Remarks:

The def. of μ_j is independent of I_j. But we have $I_j = \mu_j\uparrow$.

Now we have: $x_0 \in I_k : I_k = I_{k+1}$ iff $x_0 \in \mu_k\uparrow : \mu_k\uparrow = \mu_{k+1}\uparrow$

PART 3: Decidability

Theorem: (Abdulla 1996)

Let $(\Pi, x_0, \rightarrow, \leq)$ be a WSTS with

- computable minimal predecessors and
- decidable $\leq$.

Given an upw. closed set I with $\min(I)$, it is decidable whether I is reachable from x_0.

Proof: Algorithm:

- Compute sequence of μ_j. (minpre computable).
- Test if $\mu_k\uparrow = \mu_{k+1}\uparrow$ (decidable since $\leq$ is decidable).
- If so, test whether $x_0 \geq x$, $x \in \mu_k$ (μ_k finite + $\leq$ decidable).

$\blacksquare$

(15) Coverability in Lossy Channel Systems:

Goal:

- Introduce Lossy Channel Systems (LCS) as a model for network protocols.
- Show that coverability is decidable, by applying WSTS.

Idea:

LCS are finite state programs communicating via unbounded FIFO channels.

→ Channel ≅ tape of TM ⇒ undecidable, need restriction.

Network protocols work even with package loss.
⇒ simulate by lossy channels.

Definition: A lossy channel system (LCS) is a tuple $L = (Q, q_0, C, M, \to)$ where:

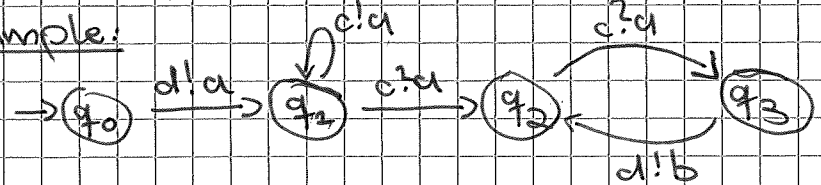
- Q is a finite set of states,
- $q_0 \in Q$ is the initial state,
- C is a finite set of channels,
- M is a finite set of messages.
- $\to \subseteq Q \times OP \times Q$, with operations $OP = C \times \{!, ?\} \times M$

Remark:

$op = c!a$ appends message a to the content in channel c (send).

$op = c?b$ removes message b from the head of channel c (receive).

Example:



To define the semantics of LCS, we need configurations:

Definition: Let $L = (Q, q_0, C, M, \to)$ be a LCS.

- A configuration of L is a pair $\gamma = (q, w) \in Q \times (M^*)^C$.
- w holds the current content in each channel.
- The initial configuration is $\gamma_0 = (q_0, \varepsilon)$.

To manipulate configurations, we use updates that reflect the lossiness of the channels with the subword ordering.

Definition:

Let $w \in (M^*)^C$, $c \in C$, and $x \in M$.

- An update $w[c:=x]$ yields a new word in $(M^*)^C$ with:

$$w[c:=x](c') = w(c') \quad \text{, if } c' \neq c$$

$$w[c:=x](c) = x.$$

- Let $(q_1, w_1), (q_2, w_2) \in Q \times (M^*)^C$ be configurations.

We define an ordering by:

$$(q_1, w_1) \leq (q_2, w_2) \iff q_1 = q_2 \text{ and } w_1(c) \leq^* w_2(c) \ \forall c \in C$$

($\leq^*$: subword order)

Note: $\leq$ is a wqo!

Definition: Transition relation among configurations.

LCS L induces a transition relation $\rightarrow \subseteq (Q \times M^{*C}) \times (Q \times M^{*C})$:

- $(q_1, w) \longrightarrow (q_2, w[c:=w(c).m])$
  if $q_1 \xrightarrow{c!m} q_2$

- $(q_1, w[c=m.w(c)]) \longrightarrow (q_2, w)$
  if $q_1 \xrightarrow{c?m} q_2$

- $\gamma_1' \longrightarrow \gamma_2'$ if $\gamma_1' \geq \gamma_1 \longrightarrow \gamma_2 \geq \gamma_2'$ for some $\gamma_1, \gamma_2 \in Q \times M^{*C}$ } Lossiness of system.

Remarks:

The question whether γ is reachable from γ_0 is equivalent to the question whether γ is coverable (from γ_0).

~~Definition~~

We want to apply the backward search to decide coverability.

Lemma: Let $L = (Q, q_0, C, M, \rightarrow)$ be a LCS. The transition system $(Q \times M^{*C}, \gamma_0, \longrightarrow, \leq)$ is a WSTS.

(17) Proof:

$\leq$ is a wqo and a simulation relation. ■

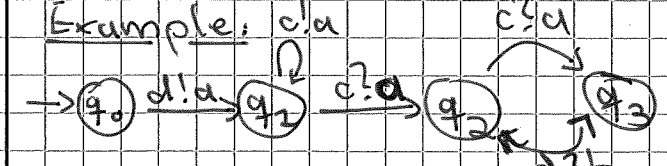
To use the backward search, we need a computable minpre(-) function and a decidable $\leq$.

Definition: Let $L=(Q, q_0, C, M, \rightarrow)$ be a LCS and $(q_2, w_2) \in Q \times M^{*C}$. We define $\text{minpre}((q_2, w_2)) := \min(T)$, where T is the smallest set so that

- $(q_1, w_1) \in T$ if $q_1 \xrightarrow{c!m} q_2$ and $w_2 = w_1[c := w_1(c).m]$ // m removed
- $(q_1, w_2) \in T$ if $q_1 \xrightarrow{c!m} q_2$ and the last element of $w_2(c) \neq m$ (or $w_2(c) = \varepsilon$). // m got lost
- $(q_1, w_1) \in T$ if $q_1 \xrightarrow{c?m} q_2$ and $w_1 = w_2[c := m.w_2(c)]$ // add m

Lemma: $\text{minpre}(\gamma) = \min(\text{pre}(\{\gamma\}\uparrow))$ and $\text{minpre}(\gamma)$ is computable.

Example:



Is (q_3, ε) reachable from $\gamma_0 = (q_0, \varepsilon)$?

$M_0 = \min\{I\} = \{(q_3, \varepsilon)\}$.

$M_1 = \min(M_0 \cup \text{minpre}((q_3, \varepsilon)))$

$= \min\{(q_3, \varepsilon), (q_2, \binom{a}{\varepsilon}), (q_2, \binom{\varepsilon}{b})\}$

$M_2 = \min(M_0 \cup \text{minpre}(q_3, \varepsilon) \cup \text{minpre}(q_2, \binom{a}{\varepsilon}) \cup \text{minpre}(q_2, \binom{\varepsilon}{b}))$

$= \min\{(q_3, \varepsilon), (q_2, \binom{a}{\varepsilon}), (q_2, \binom{\varepsilon}{b}), (q_1, \binom{aa}{\varepsilon}), (q_1, \binom{a}{b})\}$

$$\mu_3 = \underbrace{\min(\mu_0 \cup \text{minpre}(q_0, \binom{a}{\varepsilon})) \cup \text{minpre}(q_2, \binom{\varepsilon}{b})) \cup}_{\text{minpre}(q_2, \binom{aa}{\varepsilon})) \cup \text{minpre}(q_{4,} \binom{a}{b}))}$$

$$= \mu_2 \cup \{ (q_0, \binom{aa}{\varepsilon})) \cup (q_0, \binom{a}{b})) \cup (q_4, \binom{a}{\varepsilon})) \cup (q_1, \binom{\varepsilon}{b})) \}$$

$$\mu_4 = \mu_3 \cup \{ (q_0, \binom{a}{\varepsilon})), (q_4, \varepsilon), (q_0, \binom{\varepsilon}{b})) \}$$

$$\mu_5 = \mu_4 \cup \{ (q_0, \varepsilon) \}$$

$\mu_6 = \mu_5$ and $\gamma_0 \in \mu_5 \Rightarrow (q_3, \varepsilon)$ is reachable from $(q_0, \varepsilon) = \gamma_0$. ∎