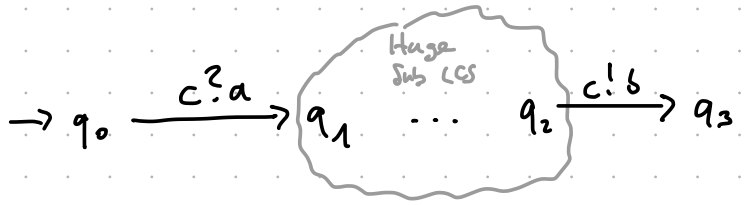
Coverability Forwards

Recall the coverability problem for WSTS:

> Given: WSTS $W = (Q, \leq, Q_0, \to)$ and $q_f \in Q$
> Decide: Is there a run $q_0, q_1, \dots, q_k$ with $q_0 \in Q_0$ and $q_k \geq q_f$?

Consider the following LCS



To decide whether $(q_3, c \mapsto b)$ is coverable Abdulla's backwards search explores the huge part of the LCS.

However, a forward would terminate immediately because no transition because no transition is enabled from $(q_0, c \mapsto \varepsilon)$

Goal: Forward algorithm for coverability

Remember: Abdulla's backward search represents states by upcl. sets

Idea: Forward search overapproximates reachable states by dwcl. sets

↳ if a state is coverable from q then it is also coverable from any state $q' \geq q$.
Thus adding smaller states in a forward search is sound

Phrased differently q_f is coverable from q_0 if

$q_f \in \downarrow post^*(Q_0)$ with $post(S) = \{s' \in Q \mid \exists s \in S.\ s \to s'\}$

$\underbrace{post^*(S)}_{=: reach(S)} = \bigcup_{i \in \mathbb{N}} post^i(S)$

while Abdulla decides $q_0 \in \uparrow pre^*(\uparrow\{q_f\})$ for some $q_0 \in Q_0$

Algorithm: run two semi-algorithms in parallel:

(1) Enumerate runs $q_0 \to q_1 \to \dots q_k$ and return YES if $q_k \geq q_f$
(2) Enumerate dwcl. sets D and return NO if

(2.1) $Q_0 \subseteq D$
(2.2) $\downarrow post(D) \subseteq D$
(2.3) $q_f \notin D$

} D is an inductive invariant wrt. $\downarrow post$

Assume all steps are computable.
The algorithm decides coverability for WSTS.

Soundness: If YES is returned, then q_f is coverable by construction.

If NO is returned, one can show

$$post^*(Q_0) \subseteq D$$

by induction. Then $\downarrow post^*(Q_0) \subseteq \downarrow D = D$ and since $q_f \notin D$ this implies $q_f \notin \downarrow post^*(Q_0)$

Termination: If q_f is coverable, then (1) will eventually enumerate a witness and return YES.

If q_f is not coverable, then (2) will eventually enumerate $D = \downarrow post^*(Q_0)$ which satisfies (2.1)-(2.3):

$$Q_0 \subseteq \downarrow post^*(Q_0) \quad \text{// by definition}$$

$$\downarrow post(\downarrow post^*(Q_0)) = \downarrow post(post^*(Q_0)) \quad \text{// by monotony}$$

$$\subseteq \downarrow post^*(Q_0)$$

$$q_f \notin \downarrow post^*(Q_0) \quad \text{// } q_f \text{ not coverable}$$

Problem: The steps in the algorithm are not computable in general

Main problem: How do we finitely represent dwcl. sets?

Remember: Upcl. sets are represented by finitely minimal elements (exist by wqo)

Idea: Represent dwcl. sets by maximal elements.
However maximal elements do not exist in general
→ Thus we introduce limit elements

Example: For Petri nets we will use generalized markings $(\underbrace{\mathbb{N} \cup \{\omega\}}_{:= \mathbb{N}_\omega})^S$

$(1, \omega) = \{(1,0), (1,1), (1,2), \dots\}$

↑ limit element representing the set on the rhs

Represent Dwd Sets by Ideals ← ideals will be our limit elements

Let $(Q, \leq)$ be a quasi order. A set $S \subseteq Q$ is

directed if $\forall x, y \in S.\ \exists z \in S.\ x \leq z$ and $y \leq z$

an ideal if it is dwd. and directed.

Lemma Let $(Q, \leq)$ be a wqo. Then any seq. $D_0 \supsetneq D_1 \supsetneq \dots$ of dwd. sets is finite.

Proof: Consider seq. $\overline{D_0} \subsetneq \overline{D_1} \subsetneq \dots$ of upd. sets.
This seq. is finite by Lemma from previous lecture.

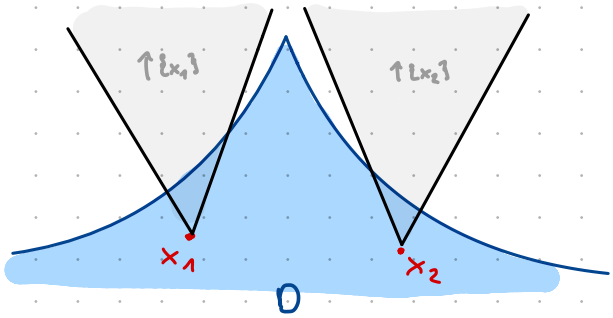
Lemma Let $(Q, \leq)$ be a wqo.
Every dwd. set $D \subseteq Q$ is a finite union of ideals.

Proof. Towards a contradiction let $D \subseteq Q$ dwd. set that is not a finite union of ideals.

Moreover let D be minimal wrt. set inclusion (*)

↳ possible because a sequence $D_0 \supsetneq D_1 \supsetneq \dots$ of dwd. sets is finite by previous lemma

Then D itself is not directed, i.e. there are $x_1, x_2 \in D$ so that no $x \in D$ exists with $x_1, x_2 \leq x$. (otherwise D would already be an ideal)



Note that
$D \cap \uparrow\{x_1\} \cap \uparrow\{x_2\} = \emptyset$
(otherwise there would be $x \in D.\ x_1, x_2 \leq x$)

Then $D = D \setminus \uparrow\{x_1\} \cup D \setminus \uparrow\{x_2\} \cup \underbrace{D \cap \uparrow\{x_1\} \cap \uparrow\{x_2\}}_{\emptyset}$

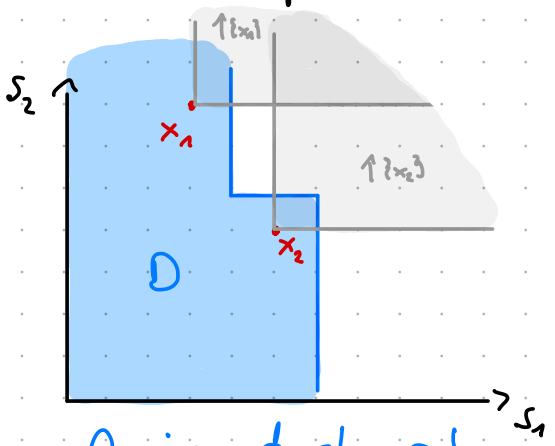
$= \underbrace{D \setminus \uparrow\{x_1\}}_{\text{both sets are}} \cup \underbrace{D \setminus \uparrow\{x_2\}}_{\text{both sets are}}$

both sets are
- dwd. (Complement of wcd is dwd. + intersection of dwd. is dwd.)
- a proper subset of D

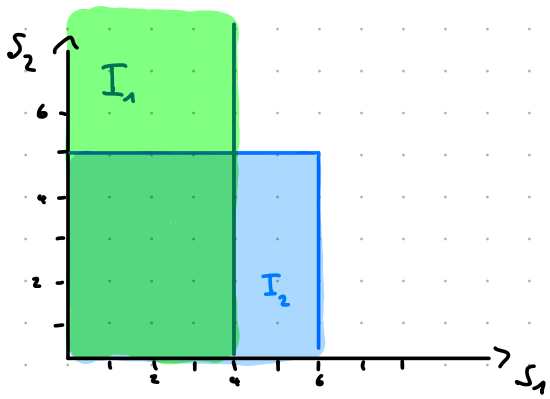
minimality of D (*) $\Rightarrow$ $D \setminus \uparrow\{x_1\}$ and $D \setminus \uparrow\{x_2\}$ are finite union of ideals

$\Rightarrow$ D is finite union of ideals.

Example: Consider a Petri net $\mathcal{N} = (S, T, W)$ with two places $S = \{s_1, s_2\}$



D is dwcl set
D is not directed



I_1 is an ideal
I_2 is an ideal
$\rightarrow D = I_1 \cup I_2$

For a Petri net (S, T, W) we represent ideals by generalized markings.

A generalized marking is $\mathbb{N}_\omega^S$ where $\mathbb{N}_\omega := \mathbb{N} \cup \{\omega\}$. The natural order $\leq$ is extended to $\mathbb{N}_\omega$ by setting $n \leq \omega$ for all $n \in \mathbb{N}$

Then $I_1 = \downarrow(4, \omega)$ and $I_2 = \downarrow(6, 5)$.

Effective ideals

Now we can represent a dwcl set by a finite union of ideals

However we still need an effective representation of ideals!

↑ Like generalized markings for Petri nets

A WSTS is ideal-effective if

- ideals are recursive enumerable
- $I_1 \subseteq I_2$ is decidable for ideals I_1, I_2
- $\downarrow \text{port}(I)$ is computable for ideal I

(*) Remark: In ideal-effective WSTS $D_1 \subseteq D_2$ is decidable for dwcl sets $D_1, D_2 \subseteq Q$ given by finite union of ideals. This is a consequence of the following lemma.

Lemma Let $(Q, \leq)$ be wqo, $I \subseteq Q$ ideal and $D_1, D_2 \subseteq Q$ dwcl sets. Then $I \subseteq D_1 \cup D_2$ implies $I \subseteq D_1$ or $I \subseteq D_2$

Proof: Homework.

Theorem Let $(Q, \leq, Q_0, \to)$ be a ideal-effective WSTS with
- enumerable runs
- $\leq$ decidable
- $\downarrow Q_0$ is given as finite union of ideals

Then coverability is decidable by the Karp algorithm.

Proof: By assumption runs are enumerable. Then (1) is computable because $\leq$ is decidable.

For (2) we enumerate decl. sets by enumerating finite unions of ideals $D = I_1 \cup \dots \cup I_k$.

It remains to show that (2.1) - (2.3) are decidable.

(2.1) $\downarrow Q_0$ is give by finite union of ideals by assumption. Decidable by $Q_0 \leq D \iff \downarrow Q_0 \leq D$ and (*)

(2.2) Decidable by $\downarrow post(D) = \underbrace{\downarrow post(I_1) \cup \dots \cup \downarrow post(I_k)}_{\text{finite union of ideals}}$ computable and (*)

(2.3) Decidable by $q_\varepsilon \notin D \iff \downarrow \{q_\varepsilon\} \not\subseteq D$ and (*)

Coverability graphs for Petri nets (aka. Karp-Miller trees)

Previous lecture: A forward algorithm for coverability in WSTS.

→ this algorithm essentially guesses the invariant $\downarrow post^*(Q_0)$ and checks it.

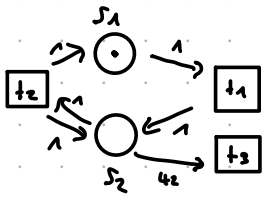
Now: We consider Petri nets which have more structure than general WSTS.

Goal: Compute $\downarrow post^*(Q_0)$ directly

Idea: Compute reachability graph and introduce limit elements/ideals if a loop with strictly positive effect occurs

↳ we call this acceleration.

Example: Acceleration



$\binom{1}{0} \xrightarrow{t_1} \binom{0}{1} \xrightarrow{t_2} \binom{1}{1}$ and $\binom{1}{1} > \binom{1}{0}$. So we can repeat $t_1 t_2$ to increase the token count in s_2:

$$\binom{1}{0} \xrightarrow{t_1t_2} \binom{1}{1} \xrightarrow{t_1t_2} \binom{1}{2} \xrightarrow{t_1t_2} \binom{1}{3} \xrightarrow{t_1t_2} \cdots$$

→ We introduce limit elements $\binom{1}{0} \xrightarrow{t_1} \binom{0}{1} \xrightarrow{t_2} \binom{1}{\omega}$ and continue exploring from $\binom{1}{\omega} \xrightarrow{t_3} \binom{1}{\omega}$

→ intuitively ω means: don't know but unbounded many tokens

Formally: Let $N = (S, T, W)$ Petri net. Recall that ideals are represented by generalized markings $\mathbb{N}_\omega^S$.

We extend $\leq, <, +$ to $M_1, M_2 \in \mathbb{N}_\omega^S$:

- $M_1 \leq M_2$ if $M_1(s) \leq M_2(s)$ for all $s \in S$.
- $M_1 < M_2$ if $M_1 \leq M_2$, $\exists s \in S.\ M_1(s) < M_2(s)$
- $\omega + n := \omega$, $\omega - n := \omega$ for $n \in \mathbb{N}$
- $\omega + \omega := \omega$, $\omega - \omega$ is undefined.

We also extend the firing relation to $|\cdot\rangle \subseteq \mathbb{N}_\omega^S \times \mathbb{N}_\omega^S$:

- $M_1 |t\rangle$ if $M_1 \geq \omega(-, t)$
- $M_1 |t\rangle M_2$ if $M_1 |t\rangle$ and $M_2 = M_1 - \omega(-, t) + \omega(t, -)$

Algorithm: Input: Petri net $N = (S, T, W)$ and $M_0 \in \mathbb{N}_\omega^S$

Output: $Cov(N, M_0) = (V, E, M_0)$

$V := \{M_0\}$; $E := \emptyset$

Worklist := M_0

while worklist $\neq \emptyset$ {

  M_1 = worklist.dequeue()

  for all $t \in T$ with $M_1 [t\rangle M_2$ { (t is enabled in M_1)

    for all M on path from M_0 to M_1 in $Cov(N)$ so that $M \leq M_2$ {

      $M_2(s) := \omega$ for all $s \in S$ with $M(s) < M_2(s)$

    }

    if $M_2 \notin V$ {

      $V := V \cup \{M_2\}$

      Worklist.enqueue(M_2)

    }

    $E := E \cup \{(M_1, M_2)\}$

  }

}

The coverability graph $Cov(N, M_0)$ for a Petri net N from a marking M_0 is defined by the algorithm.

To make the outcome deterministic / independet on processing order of markings / transitions we use

- a FIFO worklist
- and a fixed ordering on T

We show that the algorithm terminates and thus that $Cov(N, M_0)$ is finite.

Termination: Towards a contradiction, assume that the algorithm does not terminate. Then V is infinite (each while iteration dequeues, a non-terminating execution must infinitely enqueue, before enqueue we add new node to V).
Since all nodes in V are reachable from M_0 there is an infinite spanning tree of $Cov(N, M_0)$ with root M_0.
The spanning tree has (finite) outdegree $\leq |T|$ (each transition is considered once for each marking)
König's Lemma gives an infinite path from M_0.
Since $\mathbb{N}_\omega^S$ is a wqo there is an infinite increasing sequence

$$M_0 \leq M_1 \leq M_2 \leq \dots$$

where M_{i+1} occurs later on path than M_i.
Since the spanning tree has no cycles the sequence is strict:

$$M_0 \lneq M_1 \lneq M_2 \lneq \dots$$

By choosing an (infinite) subsequence we may assume that M_i was added earlier to V than M_j for all $i < j$.
Then, acceleration ensures that M_{i+1} has strictly more ω-entries than M_i.
Since a marking can have at most $|S|$ ω-entries we conclude that $M_1 \lneq M_2 \lneq \dots$ is finite ↯

We show that $Cov(N, M_0)$ is a finite representation of $\downarrow post^*(M_0)$.
The next two lemmas show (both directions of)

$$\downarrow post^*(M_0) = \downarrow V \cap \mathbb{N}^S \quad \text{where } Cov(N, M_0) = (V, E, M_0)$$

Lemma $M_0 \mid \sigma \rangle M$ implies $M_0 \xrightarrow{\sigma}_E M' \geq M$ (path in $Cov(N, M_0)$)

→ Every coverable marking is represented by $Cov(N, M_0)$

Lemma Every $M \in \downarrow V \cap \mathbb{N}^S$ is coverable in N.

→ Every marking represented by $Cov(N, M_0)$ is coverable.

Proof first Lemma: Induction on length of σ.

Induction step: Consider

$$M_0 \,|\, \sigma \rangle M_1 \,|\, t \rangle M$$

- By IH $M_0 \xrightarrow{\sigma}_E M_1' \geq M_1$ holds
- By monotonicity of the firing relation t is enabled in M_1'

$$M_1' = M_1 + (M_1' - M_1) \,|\, t \rangle M + (M_1' - M_1)$$

Thus $M_1' \xrightarrow{t}_E M'$ with $M' \geq M + \underbrace{(M_1' - M_1)}_{\geq 0} \geq M$

(M' may be accelerated)

$\Rightarrow$ Together we have

$$M_0 \xrightarrow{\sigma}_E M_1' \xrightarrow{t}_E M' \geq M$$

Proof second Lemma: Induction on the length of the shortest path to $M_V \in V$ so that $M \leq M_V$.

Induction step: Consider $M \in \downarrow V_1 \setminus N^S$

$$M_0 \xrightarrow{\sigma} M_1' \xrightarrow{t} M_2' \geq M$$

so that $\sigma.t$ is a shortest path to some $M_V \geq M$.

- Consider acceleration in last step $M_1 \xrightarrow{t} M_2'$.
  Let $M_1' \,|\, t \rangle M_2$. If no acceleration then $M_2 = M_2'$
  Otherwise $M_2 \lneq M_2'$ and there is $\sigma_2 \in T^*$ and $i \in \mathbb{N}$ so that

$$M_2 \,|\, \sigma_2^i \rangle M_2 + i \cdot (M_2' - M_2) \geq M$$

↳ Effect of σ_2 on $s \in S$ is

> 0 if $M_2'(s) = \omega$ and $M_2(s) \neq \omega$

$= 0$ if $M_2'(s) = M_2(s) \neq \omega$

arbitrary if $M_2'(s) = M_2(s) = \omega$

$\Rightarrow$ Thus there is $M_1 \leq M_1'$ so that

$$M_1 \,|\, t.\sigma_2^i \rangle M' \geq M$$

- By IH and $M_0 \xrightarrow{\sigma} M_1' \geq M_1$ we know that M_1 is coverable. Let $M_0 [\sigma_1\rangle M_1'' \geq M_1$.

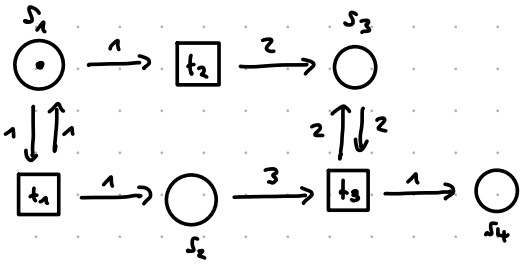
- By monotonicity of firing relation $[t.\sigma_2 i\rangle$ is enabled in M_1''

$$M_1'' = M_1 + (M_1'' - M_1) \,[t.\sigma_2 i\rangle\, M' + (M_1'' - M_1)$$

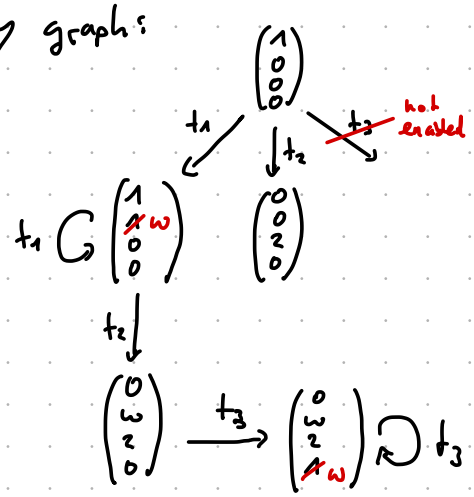
$\Rightarrow$ Together we have

$$M_0 [\sigma_1\rangle M_1'' [t.\sigma_2 i\rangle M' + \underbrace{(M_1'' - M_1)}_{\geq 0} \geq M$$

Example:



Coverability graph:



Ideal decomposition of $\downarrow post^*\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$:

$$\downarrow post^*\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$= \downarrow \left\{ \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\\omega\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\2\\0\end{pmatrix}, \begin{pmatrix}0\\\omega\\2\\0\end{pmatrix}, \begin{pmatrix}0\\\omega\\2\\\omega\end{pmatrix} \right\}$$

$$= \downarrow \left\{ \begin{pmatrix}1\\\omega\\0\\0\end{pmatrix} \right\} \cup \downarrow \left\{ \begin{pmatrix}0\\\omega\\2\\\omega\end{pmatrix} \right\}$$