Coverability Graphs

So far: Approximating VASS by Marking Equation

- Coverability graphs reflect the firing of transitions along markings (like reachability graphs)
- but: may abstract away exact token count with ω to indicate arbitrarily many tokens

• Generalize natural numbers to $\mathbb{N}_\omega = \mathbb{N} \cup \{\omega\}$

Extend $<$ and $+$ to $\mathbb{N}_\omega$

$$m < \omega$$

$$\omega + m := \omega =: \omega - m \qquad \text{for all } m \in \mathbb{N}$$

$$\omega - \omega \quad \text{undefined}$$

• For a Petri net $N = (S, T, W)$ a <u>generalized marking</u> is $M_\omega : S \to \mathbb{N}_\omega$

ω-marked places $\Omega(M_\omega) = \{ s \in S \mid M_\omega(s) = \omega \}$

Extend firing relation to generalized markings

$M_\omega [t\rangle$ if $M_\omega \geq W(-,t)$

$M^1_\omega [t\rangle M^2_\omega$ if $M^1_\omega [t\rangle$ and

$$M^2_\omega = M^1_\omega - W(-,t) + W(t,-)$$

- The <u>coverability graph</u> is defined by the following algorithm (modified DFS)

Input: Petri net $N = (S, T, W, \mu_0)$

Output: $Cov(N) := (V, E, \mu_0)$

$V := \{\mu_0\}$; $E = \emptyset$

$L := \mu_0$ // worklist

while $L \neq \emptyset$ {

  $\mu_\omega^1 = deq(L)$

  implies that t is enabled in μ_ω^1

  for all $t = t_1 \dots t_n \in T$ with $\mu_\omega^1 [t\rangle \mu_\omega^2$ { // process enabled transitions

    for all μ_ω on path from μ_0 to μ_ω^1 that satisfy $\mu_\omega \lneq \mu_\omega^2$ {

      $\mu_\omega^2(s) := \omega$ for all $s \in S$ with $\mu_\omega(s) < \mu_\omega^2(s)$

    }

    if $\mu_\omega^2 \notin V$ {

      $V := V \cup \{\mu_\omega^2\}$

      $L := enq(\mu_\omega^2)$

    }

    $E := E \cup \{(\mu_\omega^1, \mu_\omega^2)\}$

  }

}

→ Output is not deterministic: depends on worklist and order in which transitions are processed

→ to make it deterministic we use FIFO buffer and a fixed ordering on transitions $t_1, \dots, t_n$

<u>Lemma (Finiteness)</u> For every Petri net N the coverability graph $Cov(N)$ is finite.

→ follows due to the fact that $\leq$ on $\mathbb{N}_\omega^S$ is a well-quasi-order

<u>Lemma (N to $Cov(N)$)</u> Consider a transition sequence $\sigma \in T^*$ with $M_0 [\sigma\rangle M$. Then there is a path $M_0 \xrightarrow{\sigma} M_\omega$ in $Cov(N)$ with $M \leq M_\omega$.

→ Proof by induction on the length of σ

<u>Lemma ($Cov(N)$ to N)</u> For all $M_\omega \in Cov(N)$ and $k \in \mathbb{N}$ there is $M \in Reach(N)$ with

$$M(s) \geq k \qquad s \in \Omega(M_\omega)$$
$$M(s) = M_\omega(s) \qquad s \in S \setminus \Omega(M_\omega)$$

→ Proof by induction on shortest path to M_ω

The case where a new ω-entry is introduced needs the following observation:

Consider

$$M_0 \xrightarrow{\tau} M_\omega^1 \xrightarrow{\sigma} M_\omega^2 \quad \text{with } M_\omega^1 \lneq M_\omega^2$$

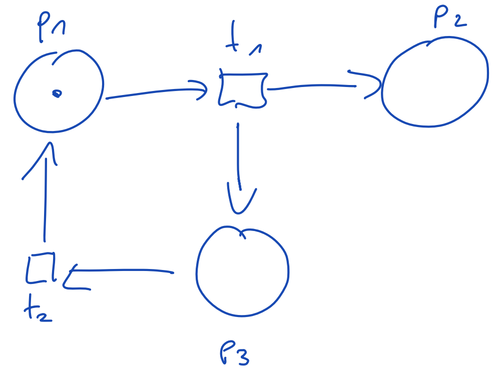
By repeating σ an arbitrary token count can be generated on the places $s \in S$ with $M_\omega^1(s) < M_\omega^2(s)$

<u>Lemma (Decision Procedure)</u> Given Petri net $N = (S, T, W, M_0)$

1. M is coverable in N if and only if there is M_ω in $Cov(N)$ with $M_\omega \geq M$
2. Place $s \in S$ is unbounded if and only if there is M_ω in $Cov(N)$ with $M_\omega(s) = \omega$

→ gives decision procedure by finiteness of $Cov(N)$

Example: Petri Net:



Coverability graph:

$$(1\,0\,0) \xrightarrow{t_1} (0\,1\,1) \xrightarrow{t_2} \begin{matrix}\cancel{(1\,1\,0)} \\ (1\,\omega\,0)\end{matrix} \underset{t_2}{\overset{t_1}{\rightleftarrows}} (0\,\omega\,1)$$

Well Quasi Orderings

A *quasi ordering (qo)* is a reflexive and transitive relation $\leq \subseteq A \times A$. We also call $(A, \leq)$ a qo. We write $a < b$ for $a \leq b$ and $b \not\leq a$

A qo $(A, \leq)$ is a *well quasi ordering (wqo)* if for every infinite sequence $(a_i)_{i \in \mathbb{N}}$ in A there are indices $i < j$ with $a_i \leq a_j$

- Exploit unavoidability of repetition for termination proofs
- traditional proofs rely on well founded relations with no strictly decreasing sequences
- wqo's additionally forbid infinite antichains

An *antichain* is a set $B \subseteq A$ of incomparable elements, $a \not\leq b$ for all $a, b \in B$

Lemma (Characterization of wqo) Consider a qo $(A, \leq)$

The following are equivalent:

1. $(A, \leq)$ is a wqo
2. Every infinite sequence $(a_i)_{i \in \mathbb{N}}$ in A contains infinite non-decreasing sub-sequence $(a_{\varphi(i)})_{i \in \mathbb{N}}$ with $a_{\varphi(i)} \leq a_{\varphi(i+1)}$ for all $i \in \mathbb{N}$
3. There is no infinite strictly decreasing sequence and no infinite antichain in A

Proof $(1) \Rightarrow (2)$. Consider sequence $(a_i)_{i \in \mathbb{N}}$

Take subsequence $(a_{nd(i)})_{i \in \mathbb{N}}$ of elements that are not dominated by some successor.

The sequence must be finite by wqo assumption.

We will find infinite non-decreasing subsequence from

$\max\{nd(i) \mid i \in \mathbb{N}\} + 1$

$(2) \Rightarrow (3)$ By definition

$(3) \Rightarrow (1)$ Consider sequence $(a_i)_{i \in \mathbb{N}}$

Assume there are no indices $i < j$ with $a_i \leq a_j$

We construct an infinite antichain: ↯

1. Construct a strictly decreasing sequence from a_0 by finding the first strictly smaller successors

$$a_0 > a_{\varphi(1)} > a_{\varphi(2)} > \dots > a_{\varphi(n_0)}$$

This sequence is finite by assumption.

2. The last element $a_{\varphi(n_0)}$ has no comparable successors (by assumption)

   Add $a_{\varphi(n_0)}$ to an antichain.

3. Repeat this for $a_{\varphi(n_0)+1}$