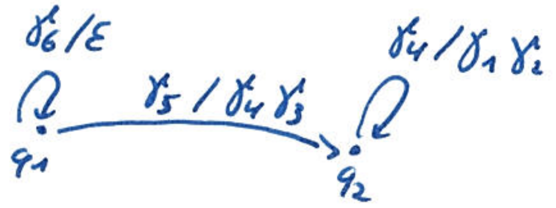
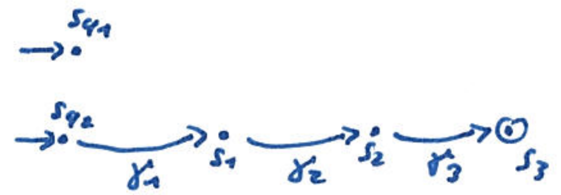
Example (continued):

PDS P:



P-NFA A:



Goal:

Compute $pre^*(CF(A)) = \{c \in CF \mid c \to^* c' \in CF(A)\}$

Idea:

Sequence of sets of configurations

$Y_0 \subseteq Y_1 \subseteq \dots$

that satisfies

(Term) there is $i \in \mathbb{N}$ with $Y_{i+1} = Y_i$

(Compl) $X_i \subseteq Y_i$ f.a. $i \in \mathbb{N}$

(Sound) $Y_i \subseteq \bigcup_{j \in \mathbb{N}} X_j$ f.a. $i \in \mathbb{N}$.

Construction:

Y_i = set of configurations accepted by a P-NFA A_i.

$$\begin{array}{ccccc} CF(A_0) & \subseteq & CF(A_1) & \subseteq & CF(A_2) \subseteq \dots \\ \shortparallel & & \shortparallel & & \shortparallel \\ Y_0 & & Y_1 & & Y_2 \end{array}$$

From A_i to A_{i+1}:

- only add transitions
  - ↳ that start from initial states
- never change the states.

Consequence:

(Term) holds, at most $|S|^2 |\Gamma|$ transitions can be added.

Definition ($(\mathcal{A}_i)_{i \in \mathbb{N}}$ and $\mathcal{A}_{pre^*}$):

Let $\mathcal{P} = (Q, \Gamma, \to)$ a PDS and $C = CF(\mathcal{A})$ a regular set of configurations.

Let $\mathcal{A} = (S, S_I, \to, S_F)$. (Recall that for P-NFA $S_I = \{s_q \mid q \in Q\}$)

Then

$$\mathcal{A}_0 := \mathcal{A}.$$

Let $\mathcal{A}_i = (S, S_I, \to_i, S_F)$.

Set

$$\mathcal{A}_{i+1} := (S, S_I, \underbrace{\to_i \cup \to'}_{=: \to_{i+1}}, S_F)$$

with

$$s_{q_1} \xrightarrow{\gamma}{}' s \quad \text{if} \quad s_{q_2} \xrightarrow{w}_i s \quad \text{and} \quad q_1 \xrightarrow{\gamma / w} q_2 .$$

Define

$$\mathcal{A}_{pre^*} = \mathcal{A}_i \quad \text{with} \quad \mathcal{A}_i = \mathcal{A}_{i+1}.$$

Intuition:

- $(q_1, \gamma w')$ immediate predecessor of $(q_2, w.w')$ wrt. transition $q_1 \xrightarrow{\gamma / w} q_2$.
- So if $w.w'$ is accepted from s_{q_2}

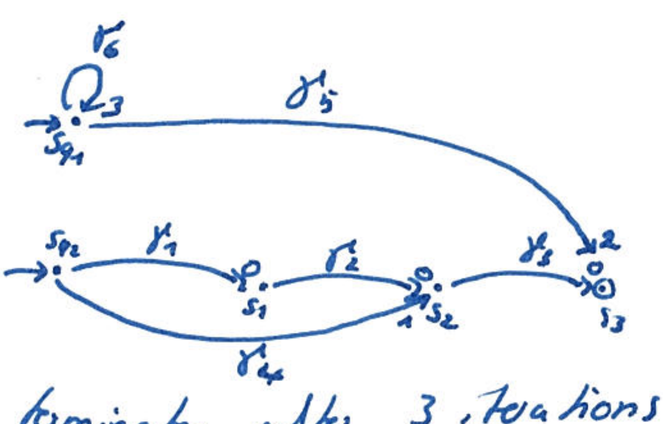
$$s_{q_2} \xrightarrow{w}_i s \xrightarrow{w'} s_F \in S_F$$

then the new transition accepts $\gamma w'$ from s_{q_1}:

$$s_{q_1} \xrightarrow{\gamma}{}' s \xrightarrow{w'} s_F \in S_F .$$

Example:

$\mathcal{A}_{pre^*}$



lazy: only add if new transition leads to final state

eager: add γ_6 in first step would also work.

Construction terminates after 3 iterations:

$$\mathcal{A}_{pre^*} = \mathcal{A}_3 \; (= \mathcal{A}_4 = \mathcal{A}_5 = \dots)$$

· We have

$$pre^*(C) = \{(q_1, \gamma_6^k \cdot \gamma_5) \mid k \in \mathbb{N}\} \cup \{(q_2, \gamma_1\gamma_2\gamma_3), (q_2, \gamma_4\gamma_3)\}.$$

· Moreover

↪ $X_1 = Y_1$ and $X_2 = Y_2$

↳ But $X_3 \subsetneq Y_3$:

After $s_{q_1} \xrightarrow{\gamma_6}_3 s_{q_1}$ has been added, we have

$$\{(q_1, \gamma_6^k \cdot \gamma_5) \mid k \in \mathbb{N}\} \subseteq Y_3.$$

but only

$$(q_1, \gamma_6 \gamma_5) \in X_3.$$

Although $(q_1, \gamma_6^k \cdot \gamma_5) \notin X_3$ for $k > 1$,

we have $(q_1, \gamma_6^k \gamma_5) \in pre^*(C)$ because

$$(q_1, \gamma_6^k \gamma_5) \in X_{k+2}.$$

<u>Theorem (Bouajjani, Esparza, Maler '97)</u>

Given a PDS P and a set of configurations accepted by a P-NFA A.

We can construct (in polynomial time) a P-NFA A_{pre^*} with

$$CF(A_{pre^*}) = pre^*(CF(A)).$$

Follows from (Compl) and (Sound) for sequence $(Y_i)_{i \in \mathbb{N}}$

(we still need to prove these two):

„$\supseteq$" $\quad pre^*(CF(A)) = \bigcup_{i \in \mathbb{N}} X_i \underset{(Compl)}{\subseteq} \bigcup_{i \in \mathbb{N}} Y_i = Y_k$ for Y_k with

$$A_k = A_{k+1} = A_{pre^*}.$$

So

$$Y_k = CF(A_{pre^*}).$$

„$\subseteq$" $\quad CF(A_{pre^*}) = Y_k \overset{(Sound)}{\subseteq} \bigcup_{i \in \mathbb{N}} X_i = pre^*(CF(A)).$

for some $k \in \mathbb{N}$.

Lemma (Completeness):

$X_i \subseteq Y_i$ f.a. $i \in \mathbb{N}$.

Proof:

By induction on i.

IB: $X_0 := C =: Y_0$

IS: Assume inclusion $X_i \subseteq Y_i$ holds.

Let

$(q_1, \gamma w') \in X_{i+1}$ (and not in X_i, otherwise IH).

Then there is a transition $q_1 \xrightarrow{\gamma / w} q_2$ and

$(q_2, w.w') \in X_i$.

By the hypothesis, $X_i \subseteq Y_i$.

So configuration $(q_2, w.w')$ accepted by A_i:

$$s_{q_2} \xrightarrow{w}_i s \xrightarrow{w'}_i s_F \in S_F.$$

By definition of A_{i+1}, we get

$$s_{q_1} \xrightarrow{\gamma}_{i+1} s \xrightarrow{w'}_{i+1} s_F \in S_F.$$

So

$$(q_1, \gamma.w') \in CF(A_{i+1}) = Y_{i+1}.$$

For soundness, we require a technical lemma. $\square$

Lemma:

If $s_q \xrightarrow{w}_i s$ then $(q, w) \rightarrow^* (q', v)$ for some q', v so that $s_{q'} \xrightarrow{v}_0 s$.

// If (q, w) is accepted in ith iteration,
then it leads to a configuration (q', v)
that is accepted initially.

This is the intuition.

Lemma (Soundness):

$Y_i \subseteq pre^*(C)$ f.a. $i \in \mathbb{N}$.

Proof:

Let $(q,w) \in Y_i$.

By definition of A_i:

$$s_q \xrightarrow{w}_i s_F \quad \text{for } s_F \in S_F.$$

By technical lemma

$$(q,w) \to^* (q',v) \text{ for some } q', v \text{ with } s_{q'} \xrightarrow{v}_0 s_F.$$

So

$$(q',v) \in CF(A_0) = CF(A) = C.$$

Thus,

$$(q,w) \in pre^*(C).$$

$\square$

7.3 Model checking LTL

- To interpret LTL, pick $\Sigma = \mathbb{P}(\mathcal{P})$ for $\mathcal{P}$ finite set of propositions.
- To define

$$P \models \varphi \quad \text{with } P = (Q, \Gamma, \to) \text{ a PDS and } \varphi \in LTL,$$

assign propositions to states

$$\lambda : Q \to \Sigma.$$

Goal:

Compute all configurations $c \in CF$ so that every run starting from c satisfies φ.

Model checking:

Is an initial configuration in this set?

- Do not make this formal.
- Instead: Rely on automata-theoretic approach and assume we have

$$P \,\|\, A_{\overline{\varphi}}.$$

Definition (Büchi-pushdown system):

A Büchi-pushdown system (BPDS) is a tuple

$BP = (Q, \Gamma, \to, Q_F)$

with

- $(Q, \Gamma, \to)$ a PDS and
- $Q_F \subseteq Q$ set of final states.

Semantics in terms of runs

$r = (q_0, w_0) \to (q_1, w_1) \to \dots$

Run is accepting if

$q_i \in Q_F$ for infinitely many configurations (q_i, w_i).

Goal:

Compute set of all configurations c of BP so that BP has an accepting run from c.

Following proposition reduces this problem to reachability:

Proposition:

Consider a BPDS BP.

Then BP has an accepting run from $c \in CF$ if and only if there are configurations

$(q, \gamma), (q_F, u), (q, \gamma.v)$ with $q_F \in Q_F$

so that

(1) $c \to^* (q, \gamma w)$ for some $w \in \Gamma^*$ and

(2) $(q, \gamma) \to^+ (q_F, u) \to^* (q, \gamma.v)$.

Defer proof for a moment.

Algorithm:

Reformulate conditions (1) and (2) as

(1') $c \in pre^*(\{q\} \times \gamma\Gamma^*)$

(2') $(q, \gamma) \in pre^+((Q_F \times \Gamma^*) \cap pre^*(\{q\} \times \gamma\Gamma^*))$

- Find all configurations (q, γ) for which (2') holds (finitely many).
- Construct P-NFAs for

  $pre^*(\{q\} \times \gamma\Gamma^*)$
- Take union of all those sets.

To see that one can find (q, γ), note that

$Q_F \times \Gamma^*$ and $pre^*(\{q\} \times \gamma\Gamma^*)$

are regular.

Then their intersection is regular.

So

$pre^*((Q_F \times \Gamma^*) \cap pre^*(\{q\} \times \gamma\Gamma^*))$

is again regular

(requires construction for single pre).