7. Model checking pushdown systems (recursive programs)

Goal: Decide $P \models \varphi$ for P a pushdown system

Technically: Reachability of accepting loops

Approach:
- Compute set of all predecessors of a given set of configurations C (configurations that lead to C)
- Let $pre(C)$ = immediate predecessors of C.
  - ↳ Compute $pre^*(C)$.
  - ↳ Then $pre^*(C) = \bigcup_{i \in \mathbb{N}} X_i$ with $X_0 = C$ and $X_{i+1} = X_i \cup pre(X_i)$.

Problem:
- Finite state systems:
  Sequence $(X_i)_{i \in \mathbb{N}}$ reaches fixed point (highly inefficient)
- Infinite state systems (like PDS):
  Sequence $(X_i)_{i \in \mathbb{N}}$ usually does not converge.

Solution: Representation structures
- ↳ Finite structures that represent infinite sets of configurations
- ↳ Should have good closure properties (wishlist):
  - Closed under $\cup$ for $X_{i+1} = X_i \cup pre(X_i)$ (or generally Boolean operations)
  - Closed under pre
  - Decidable membership problem ($c \in R$ for c a configuration and R a representation)

Examples:
- Timed automata
  ⇝ sets of configurations represented by regions
- Well structured transition systems
  ⇝ upward-closed sets of configurations represented by minimal elements
- Lossy channel systems
  ⇝ sets of configurations by simple regular expressions.

Here: Pushdown systems P

↳ Configuration = pair (q, w) where q = stack
w = stack content (represented as word)

↳ Representation structure: NFA

A accepts (q, w) if stack q of A accepts w

Note:

↳ A represents sets of configurations of P

↳ A does not represent behaviour of P

Contribution

- NFAs closed under Boolean operations
- Membership is decidable

⇒ Algorithm to compute $pre^*(C)$

⇒ Exploit it for model checking PDS against LTL

↳ Construct NFA accepting all configurations that satisfy an ω-regular property

F.1 Pushdown systems and their representation structures

Idea: pushdown automata (Kellerautomat)

$(q, \boxed{\gamma}) = (q, c\,\delta a)$

↳ But not as language acceptor

↳ Interested in their configurations and configuration changes.

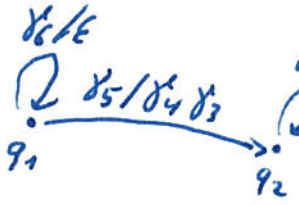
Definition (Syntax of pushdown systems)

A pushdown system (PDS) is a triple $P = (Q, \Gamma, \rightarrow)$ with

- Q = set of states
- Γ = stack alphabet
- $\rightarrow \subseteq (Q \times \Gamma) \times (Q \times \Gamma^*)$ set of transitions.

Usually write $q \xrightarrow{\gamma/\omega} q'$ instead of $((q,\gamma),(q',\omega)) \in \to$.

Example:



is $P = (\{q_1, q_2\}, \{\gamma_1, \ldots, \gamma_6\}, \to)$ with

$q_1 \xrightarrow{\gamma_6/\varepsilon} q_1$

$q_1 \xrightarrow{\gamma_5/\gamma_4\gamma_3} q_2$

$q_2 \xrightarrow{\gamma_4/\gamma_1\gamma_2} q_2$

Behaviour of pushdown system $P = (Q, \Gamma, \to)$ defined in terms of

Configurations $= (q, \omega)$ with

$q \in Q$ the state

$\omega \in \Gamma^*$ the stack content

Set of all configurations is $CF = Q \times \Gamma^*$.

Definition (Semantics of PDS)

Let $P = (Q, \Gamma, \to)$ a PDS.

It induces a transition relation $\to \subseteq CF \times CF$

between configurations by

$(q, \gamma.\omega') \to (q', \omega\omega')$ if $q \xrightarrow{\gamma/\omega} q'$ in P.

Call $(q, \gamma\omega')$ immediate predecessor of $(q', \omega\omega')$

$(q', \omega.\omega')$ immediate successor of $(q, \gamma.\omega)$

Denote reflexive and transitive closure of $\to$ by $\to^*$.

If $c \to^* c'$ with $c, c' \in CF$, call

c a predecessor of c'

c' a successor of c.

Say c' reachable from c.

Predecessor function abstracts from transitions.

Let $C \subseteq CF$ set of configurations. Then

$$pre(C) := \{ c \in CF \mid c \to c' \text{ with } c' \in C \}$$

Reflexive and transitive closure of pre is

$$pre^*(C) := \{ c \in CF \mid c \to^* c' \text{ with } c' \in C \}$$

Also have

$$pre^+(C) := pre(pre^*(C)).$$

Example (continued):

$(q_1, \gamma_6^2 \gamma_5) \in pre^*(\{(q_2, \gamma_1 \gamma_2 \gamma_3)\})$

Why?

$(q_1, \gamma_6^2 \gamma_5) \to (q_1, \gamma_6 \gamma_5) \to (q_1, \gamma_5) \to (q_2, \gamma_4 \gamma_3) \to (q_2, \gamma_1 \gamma_2 \gamma_3)$

But:

$(q_2, \gamma_4 \gamma_2) \notin pre^*(\{(q_2, \gamma_1 \gamma_2 \gamma_3)\})$

Why:

$(q_2, \gamma_4 \gamma_2) \to (q_2, \gamma_1 \gamma_3 \gamma_2) \not\to$

Main algorithm:

Given a (regular) set of configurations
(will be made precise in a few seconds)

Then

$pre^*(C)$ can be finitely represented by an NFA.

Definition (P-NFA):

Let $P = (Q, \Gamma, \to)$. A P-NFA is an NFA

$A = (S, S_I, \to, S_F)$ over Γ

where

$S_I := \{ s_q \mid q \in Q \}$.

So for every state of P there is an initial state of $\mathcal{A}$.

- To relate $\mathcal{A}$ and P, define

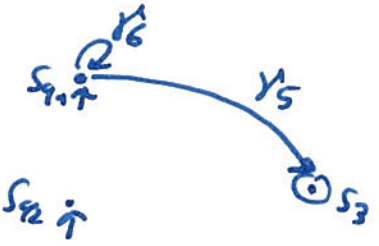
  $\mathcal{A}$ accepts configuration (q,w) if $s_q \xrightarrow{w} s_F$ with $s_F \in S_F$.

- Set of all configurations accepted by $\mathcal{A}$ is $CF(\mathcal{A})$.

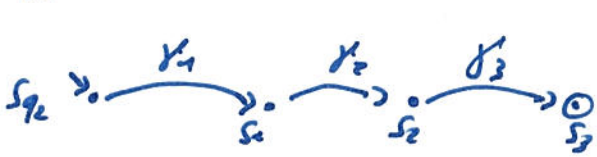
- A set of configurations $C \subseteq CF$ is regular if $C = CF(\mathcal{A})$ for some P-NFA $\mathcal{A}$.

Example (continued):

For P as before we have

$\mathcal{A}_1 =$ 

accepts $\{(q_1, \gamma_6^k \gamma_5) \mid k \in \mathbb{N}\}$.
So $\{(q_1, \gamma_6^k \gamma_5) \mid k \in \mathbb{N}\}$ is a regular set of configurations

$\mathcal{A} =$ 

accepts $\{(q_1, \gamma_1\gamma_2\gamma_3)\}$.
Also a regular set.

7.2 Computing $pre^*(C)$ (and deciding reachability)

Given: • PDS $P = (Q, \Gamma, \rightarrow)$
• Regular set of configurations $C = CF(\mathcal{A})$ for some P-NFA $\mathcal{A}$.

Compute: Another P-NFA $\mathcal{A}_{pre^*}$ so that

$$CF(\mathcal{A}_{pre^*}) = pre^*(CF(\mathcal{A})).$$

Approach:

- $pre^*(C) = \bigcup_{i \in \mathbb{N}} X_i$ with $X_0 = C$
  $X_{i+1} = X_i \cup pre(X_i)$.

- So we intend to construct this sequence

$$X_0 \subseteq X_1 \subseteq X_2 \ldots \quad \text{until} \quad X_{i+1} = X_i \text{ for some } i \in \mathbb{N}.$$

Then

$$pre^*(C) = X_i.$$

Problem:

Existence of such a fixed point not guaranteed.

Example:

and $C = \{(q, \varepsilon)\}$.

Then

$$X_i = \{(q, \varepsilon), (q, a), \ldots, (q, a^i)\}.$$

Thus

$$X_i \neq X_{i+1} \text{ for all } i \in \mathbb{N}.$$

Solution:

- Compute $pre^*(C)$ as limit of a different sequence

$$Y_0 \subseteq Y_1 \subseteq \ldots$$

of sets of configurations.

- Will satisfy three conditions:

(Term) There is $i \in \mathbb{N}$ so that $Y_i = Y_{i+1}$.

(Compl) $X_i \subseteq Y_i$ for all $i \in \mathbb{N}$.

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

Idea of construction:

Y_i = set of configurations accepted by P-NFA A_i:

$$CF(A_0) \subseteq CF(A_1) \subseteq CF(A_2) \subseteq \ldots$$
$$\| \qquad \| \qquad \|$$
$$Y_0 \qquad Y_1 \qquad Y_2$$