Formalization of Dynamic Pushdown Networks in Isabelle/HOL

Peter Lammich

January 26, 2026

Abstract

We present a formalization of Dynamic Pushdown Networks (DPNs) and the automata based algorithm for computing backward reachability sets using Isabelle/HOL. Dynamic pushdown networks are an abstract model for multithreaded, interprocedural programs with dynamic thread creation that was presented by Bouajjani, Müller-Olm and Touili in 2005.

We formalize the notion of a DPN in Isabelle and describe the algorithm for computing the *pre**-set from a regular set of configurations, and prove its correctness. We first give a nondeterministic description of the algorithm, from that we then infer a deterministic one, from which we can generate executable code using Isabelle's code-generation tool.

Contents

1 String rewrite systems

theory *SRS*
imports *DPN-Setup*
begin

This formalizes systems of labelled string rewrite rules and the labelled transition systems induced by them. DPNs are special string rewrite systems.

1.1 Definitions

type-synonym $('c,'l)$ *rewrite-rule* $=$ *'c list* $\times$ *'l* $\times$ *'c list*
type-synonym $('c,'l)$ *SRS* $=$ $('c,'l)$ *rewrite-rule set*

syntax
  syn-rew-rule :: *'c list* $\Rightarrow$ *'l* $\Rightarrow$ *'c list* $\Rightarrow$ $('c,'l)$ *rewrite-rule* $(\text{-} \hookrightarrow_{\text{-}} \text{-}\ [51,51,51]\ 51)$

translations
  $s \hookrightarrow_a s' \Rightarrow (s,a,s')$

A (labelled) rewrite rule (s, a, s') consists of the left side s, the label a and the right side s'. Intuitively, it means that a substring s can be rewritten to s' by an a-step. A string rewrite system is a set of labelled rewrite rules

1.2 Induced Labelled Transition System

A string rewrite systems induces a labelled transition system on strings by rewriting substrings according to the rules

inductive-set *tr* :: $('c,'l)$ *SRS* $\Rightarrow$ $('c\ list,\ 'l)$ *LTS* **for** S
where
  rewrite: $(s \hookrightarrow_a s') \in S \Longrightarrow (ep@s@es,a,ep@s'@es) \in tr\ S$

1.3 Properties of the induced LTS

Adding characters at the start or end of a state does not influence the capability of making a transition

lemma *srs-ext-s*: $(s,a,s') \in tr\ S \Longrightarrow (wp@s@ws,a,wp@s'@ws) \in tr\ S$ $\langle proof \rangle$

lemma *srs-ext-both*: $(s,w,s')\in \mathit{trcl}\ (\mathit{tr}\ S) \Longrightarrow (\mathit{wp}@s@\mathit{ws},w,\mathit{wp}@s'@\mathit{ws})\in \mathit{trcl}\ (\mathit{tr}\ S)$
⟨*proof*⟩

corollary *srs-ext-cons*: $(s,w,s')\in \mathit{trcl}\ (\mathit{tr}\ S) \Longrightarrow (e\#s,w,e\#s')\in \mathit{trcl}\ (\mathit{tr}\ S)$ ⟨*proof*⟩
corollary *srs-ext-pre*: $(s,w,s')\in \mathit{trcl}\ (\mathit{tr}\ S) \Longrightarrow (\mathit{wp}@s,w,\mathit{wp}@s')\in \mathit{trcl}\ (\mathit{tr}\ S)$ ⟨*proof*⟩
corollary *srs-ext-post*: $(s,w,s')\in \mathit{trcl}\ (\mathit{tr}\ S) \Longrightarrow (s@\mathit{ws},w,s'@\mathit{ws})\in \mathit{trcl}\ (\mathit{tr}\ S)$ ⟨*proof*⟩

lemmas *srs-ext* = *srs-ext-both srs-ext-pre srs-ext-post*

end

2 Finite state machines

theory *FSM*
imports *DPN-Setup*
begin

This theory models nondeterministic finite state machines with explicit set of states and alphabet. ε-transitions are not supported.

2.1 Definitions

record $('s,'a)$ *FSM-rec* =
  $Q :: 's\ \mathit{set}$ — The set of states
  $\Sigma :: 'a\ \mathit{set}$ — The alphabet
  $\delta :: ('s,\ 'a)\ \mathit{LTS}$ — The transition relation
  $\mathit{s0} :: 's$ — The initial state
  $F :: 's\ \mathit{set}$ — The set of final states

locale *FSM* =
  fixes *A*
  assumes *delta-cons*: $(q,l,q')\in\delta\ A \Longrightarrow q\in Q\ A \wedge l\in\Sigma\ A \wedge q'\in Q\ A$ — The transition relation is consistent with the set of states and the alphabet
  assumes *s0-cons*: $\mathit{s0}\ A \in Q\ A$ — The initial state is a state
  assumes *F-cons*: $F\ A \subseteq Q\ A$ — The final states are states
  assumes *finite-states*: *finite* $(Q\ A)$ — The set of states is finite
  assumes *finite-alphabet*: *finite* $(\Sigma\ A)$ — The alphabet is finite

2.2 Basic properties

lemma (**in** *FSM*) *finite-delta-dom*: *finite* $(Q\ A \times \Sigma\ A \times Q\ A)$ ⟨*proof*⟩

lemma (**in** *FSM*) *finite-delta*: *finite* $(\delta\ A)$ ⟨*proof*⟩

2.3 Constructing FSMs

definition *fsm-empty* $s_0 \equiv (\!|\ Q=\{s_0\},\ \Sigma=\{\},\ \delta=\{\},\ \mathit{s0}=s_0,\ F=\{\}\ |\!)$
definition *fsm-add-F* $s\ \mathit{fsm} \equiv \mathit{fsm}(\!|\ Q:=\mathit{insert}\ s\ (Q\ \mathit{fsm}),\ F:=\mathit{insert}\ s\ (F\ \mathit{fsm})\ |\!)$

definition $\mathit{fsm\text{-}add\text{-}tr}\ q\ a\ q'\ \mathit{fsm} \equiv \mathit{fsm}(\!|\ Q{:=}\{q,q'\} \cup (Q\ \mathit{fsm}),\ \Sigma{:=}\mathit{insert}\ a\ (\Sigma\ \mathit{fsm}),\ \delta := \mathit{insert}\ (q,a,q')\ (\delta\ \mathit{fsm})\ |\!)$

lemma $\mathit{fsm\text{-}empty\text{-}invar}[\mathit{simp}]$: $\mathit{FSM}\ (\mathit{fsm\text{-}empty}\ s)$
$\langle \mathit{proof} \rangle$

lemma $\mathit{fsm\text{-}add\text{-}F\text{-}invar}[\mathit{simp}]$: **assumes** $\mathit{FSM}\,\mathit{fsm}$ **shows** $\mathit{FSM}\ (\mathit{fsm\text{-}add\text{-}F}\ s\ \mathit{fsm})$

$\langle \mathit{proof} \rangle$

lemma $\mathit{fsm\text{-}add\text{-}tr\text{-}invar}[\mathit{simp}]$: **assumes** $\mathit{FSM}\ \mathit{fsm}$ **shows** $\mathit{FSM}\ (\mathit{fsm\text{-}add\text{-}tr}\ q\ a\ q'\ \mathit{fsm})$
$\langle \mathit{proof} \rangle$

2.4 Reflexive, transitive closure of transition relation

Reflexive transitive closure on restricted domain

inductive-set $\mathit{trclAD} :: ('s,'a,'c)\ \mathit{FSM\text{-}rec\text{-}scheme} \Rightarrow ('s,'a)\ \mathit{LTS} \Rightarrow ('s,'a\ \mathit{list})\ \mathit{LTS}$
for $A\ D$
where
$\mathit{empty}[\mathit{simp}]$: $s{\in}Q\ A \Longrightarrow (s,[],s){\in}\mathit{trclAD}\ A\ D$ |
$\mathit{cons}[\mathit{simp}]$: $[\![(s,e,s'){\in}D;\ s{\in}Q\ A;\ e{\in}\Sigma\ A;\ (s',w,s''){\in}\mathit{trclAD}\ A\ D]\!] \Longrightarrow (s,e\#w,s''){\in}\mathit{trclAD}\ A\ D$

abbreviation $\mathit{trclA}\ A == \mathit{trclAD}\ A\ (\delta\ A)$

lemma $\mathit{trclAD\text{-}empty\text{-}cons}[\mathit{simp}]$: $(c,[],c'){\in}\mathit{trclAD}\ A\ D \Longrightarrow c{=}c'$ $\langle \mathit{proof} \rangle$
lemma $\mathit{trclAD\text{-}single}$: $(c,[a],c') \in \mathit{trclAD}\ A\ D \Longrightarrow (c,a,c') \in D$ $\langle \mathit{proof} \rangle$
lemma $\mathit{trclAD\text{-}elems}$: $(c,w,c'){\in}\mathit{trclAD}\ A\ D \Longrightarrow c{\in}Q\ A \wedge w{\in}\mathit{lists}\ (\Sigma\ A) \wedge c'{\in}Q\ A$ $\langle \mathit{proof} \rangle$
lemma $\mathit{trclAD\text{-}one\text{-}elem}$: $[\![c{\in}Q\ A;\ e{\in}\Sigma\ A;\ c'{\in}Q\ A;\ (c,e,c'){\in}D]\!] \Longrightarrow (c,[e],c'){\in}\mathit{trclAD}\ A\ D$ $\langle \mathit{proof} \rangle$

lemma $\mathit{trclAD\text{-}uncons}$: $(c,a\#w,c'){\in}\mathit{trclAD}\ A\ D \Longrightarrow \exists\ \mathit{ch}\ .\ (c,a,\mathit{ch}){\in}D \wedge (\mathit{ch},w,c') \in \mathit{trclAD}\ A\ D \wedge c{\in}Q\ A \wedge a{\in}\Sigma\ A$
$\langle \mathit{proof} \rangle$

lemma $\mathit{trclAD\text{-}concat}$: $!!\ c\ .\ [\![\ (c,w1,c'){\in}\mathit{trclAD}\ A\ D;\ (c',w2,c''){\in}\mathit{trclAD}\ A\ D\ ]\!] \Longrightarrow (c,w1@w2,c''){\in}\mathit{trclAD}\ A\ D$
$\langle \mathit{proof} \rangle$

lemma $\mathit{trclAD\text{-}unconcat}$: $!!\ c\ .\ (c,w1@w2,c'){\in}\mathit{trclAD}\ A\ D \Longrightarrow \exists\ \mathit{ch}\ .\ (c,w1,\mathit{ch}){\in}\mathit{trclAD}\ A\ D \wedge (\mathit{ch},w2,c'){\in}\mathit{trclAD}\ A\ D$ $\langle \mathit{proof} \rangle$

lemma $\mathit{trclAD\text{-}eq}$: $[\![Q\ A = Q\ A';\ \Sigma\ A = \Sigma\ A']\!] \Longrightarrow \mathit{trclAD}\ A\ D = \mathit{trclAD}\ A'\ D$
$\langle \mathit{proof} \rangle$

lemma *trclAD-mono*: $D{\subseteq}D' \Longrightarrow \mathit{trclAD}\ A\ D \subseteq \mathit{trclAD}\ A\ D'$
⟨*proof*⟩

lemma *trclAD-mono-adv*: $[\![D{\subseteq}D';\ Q\ A = Q\ A';\ \Sigma\ A = \Sigma\ A']\!] \Longrightarrow \mathit{trclAD}\ A\ D \subseteq \mathit{trclAD}\ A'\ D'$ ⟨*proof*⟩

2.4.1 Relation of *trclAD* and *trcl*

lemma *trclAD-by-trcl1*: $\mathit{trclAD}\ A\ D \subseteq (\mathit{trcl}\ (D \cap (Q\ A \times \Sigma\ A \times Q\ A)) \cap (Q\ A \times \mathit{lists}\ (\Sigma\ A) \times Q\ A))$
⟨*proof*⟩

lemma *trclAD-by-trcl2*: $(\mathit{trcl}\ (D \cap (Q\ A \times \Sigma\ A \times Q\ A)) \cap (Q\ A \times \mathit{lists}\ (\Sigma\ A) \times Q\ A)) \subseteq \mathit{trclAD}\ A\ D$ ⟨*proof*⟩

lemma *trclAD-by-trcl*: $\mathit{trclAD}\ A\ D = (\mathit{trcl}\ (D \cap (Q\ A \times \Sigma\ A \times Q\ A)) \cap (Q\ A \times \mathit{lists}\ (\Sigma\ A) \times Q\ A))$
⟨*proof*⟩

lemma *trclAD-by-trcl'*: $\mathit{trclAD}\ A\ D = (\mathit{trcl}\ (D \cap (Q\ A \times \Sigma\ A \times Q\ A)) \cap (Q\ A \times \mathit{UNIV} \times \mathit{UNIV}))$
⟨*proof*⟩

lemma *trclAD-by-trcl''*: $[\![\ D{\subseteq}Q\ A \times \Sigma\ A \times Q\ A\ ]\!] \Longrightarrow \mathit{trclAD}\ A\ D = \mathit{trcl}\ D \cap (Q\ A \times \mathit{UNIV} \times \mathit{UNIV})$
⟨*proof*⟩

lemma *trclAD-subset-trcl*: $\mathit{trclAD}\ A\ D \subseteq \mathit{trcl}\ (D)$ ⟨*proof*⟩

2.5 Language of a FSM

definition $\mathit{langs}\ A\ s == \{\ w\ .\ (\exists\ f{\in}(F\ A)\ .\ (s,w,f) \in \mathit{trclA}\ A)\ \}$
definition $\mathit{lang}\ A == \mathit{langs}\ A\ (s0\ A)$

lemma *langs-alt-def*: $(w{\in}\mathit{langs}\ A\ s) == (\exists f\ .\ f{\in}F\ A\ \&\ (s,w,f) \in \mathit{trclA}\ A)$ ⟨*proof*⟩

2.6 Example: Product automaton

definition $\mathit{prod\text{-}fsm}\ A1\ A2 == (\!|\ Q{=}Q\ A1 \times Q\ A2,\ \Sigma{=}\Sigma\ A1 \cap \Sigma\ A2,\ \delta = \{\ ((s,t),a,(s',t'))\ .\ (s,a,s'){\in}\delta\ A1 \wedge (t,a,t'){\in}\delta\ A2\ \},\ s0{=}(s0\ A1,s0\ A2),\ F = \{(s,t)\ .\ s{\in}F\ A1 \wedge t{\in}F\ A2\}\ |\!)$

lemma *prod-inter-1*: $!!\ s\ s'\ f\ f'\ .\ ((s,s'),w,(f,f')) \in \mathit{trclA}\ (\mathit{prod\text{-}fsm}\ A\ A') \Longrightarrow (s,w,f) \in \mathit{trclA}\ A \wedge (s',w,f') \in \mathit{trclA}\ A'$ ⟨*proof*⟩

lemma *prod-inter-2*: $!!\ s\ s'\ f\ f'\ .\ (s,w,f) \in \mathit{trclA}\ A \wedge (s',w,f') \in \mathit{trclA}\ A' \Longrightarrow ((s,s'),w,(f,f')) \in \mathit{trclA}\ (\mathit{prod\text{-}fsm}\ A\ A')$ ⟨*proof*⟩

lemma *prod-F*: $(a,b){\in}F\ (\mathit{prod\text{-}fsm}\ A\ B) = (a{\in}F\ A \wedge b{\in}F\ B)$ ⟨*proof*⟩

lemma *prod-FI*: $[\![a{\in}F\ A;\ b{\in}F\ B]\!] \Longrightarrow (a,b){\in}F\ (\mathit{prod\text{-}fsm}\ A\ B)$ ⟨*proof*⟩

lemma *prod-fsm-langs*: $\mathit{langs}\ (\mathit{prod\text{-}fsm}\ A\ B)\ (s,t) = \mathit{langs}\ A\ s \cap \mathit{langs}\ B\ t$ ⟨*proof*⟩

lemma *prod-FSM-intro*: $\mathit{FSM}\ A1 \Longrightarrow \mathit{FSM}\ A2 \Longrightarrow \mathit{FSM}\ (\mathit{prod\text{-}fsm}\ A1\ A2)$ ⟨*proof*⟩

end

3 Nondeterministic recursive algorithms

theory *NDET*
imports *Main*
begin

This theory models nondeterministic, recursive algorithms by means of a step relation.

An algorithm is modelled as follows:

1. Start with some state s
2. If there is no s' with $(s,s'){\in}R$, terminate with state s
3. Else set $s := s'$ and continue with step 2

Thus, R is the step relation, relating the previous with the next state. If the state is not in the domain of R, the algorithm terminates.

The relation *A-rel R* describes the non-reflexive part of the algorithm, that is all possible mappings for non-terminating initial states. We will first explore properties of this non-reflexive part, and then transfer them to the whole algorithm, that also specifies how terminating initial states are treated.

inductive-set *A-rel* :: $('s{\times}'s)\ \mathit{set} \Rightarrow ('s{\times}'s)\ \mathit{set}$ **for** R
where
  A-rel-base: $[\![(s,s'){\in}R;\ s'{\notin}\mathit{Domain}\ R]\!] \Longrightarrow (s,s'){\in}\mathit{A\text{-}rel}\ R$ |
  A-rel-step: $[\![(s,sh){\in}R;\ (sh,s'){\in}\mathit{A\text{-}rel}\ R]\!] \Longrightarrow (s,s'){\in}\mathit{A\text{-}rel}\ R$

3.1 Basic properties

The algorithm just terminates at terminating states

lemma *termstate*: $(s,s'){\in}\mathit{A\text{-}rel}\ R \Longrightarrow s'{\notin}\mathit{Domain}\ R$ ⟨*proof*⟩

lemma *dom-subset*: $\mathit{Domain}\ (\mathit{A\text{-}rel}\ R) \subseteq \mathit{Domain}\ R$ ⟨*proof*⟩

We can use invariants to reason over properties of the algorithm

definition *is-inv* $R\ s0\ P == P\ s0 \wedge (\forall\, s\ s'.\ (s,s'){\in}R \wedge P\ s \longrightarrow P\ s')$

lemma inv: $[\![(s0,sf)\in A\text{-}rel\ R;\ is\text{-}inv\ R\ s0\ P]\!] \Longrightarrow P\ sf$ $\langle \mathit{proof}\rangle$
lemma invI: $[\![P\ s0;\ !!\ s\ s'.\ [\![(s,s')\in R;\ P\ s]\!] \Longrightarrow P\ s']\!] \Longrightarrow is\text{-}inv\ R\ s0\ P$ $\langle \mathit{proof}\rangle$
lemma $\mathit{inv2}$: $[\![(s0,sf)\in A\text{-}rel\ R;\ P\ s0;\ !!\ s\ s'.\ [\![(s,s')\in R;\ P\ s]\!] \Longrightarrow P\ s']\!] \Longrightarrow P\ sf$
$\langle \mathit{proof}\rangle$

To establish new invariants, we can use already existing invariants

lemma $\mathit{inv\text{-}useI}$: $[\![P\ s0;\ !!\ s\ s'.\ [\![(s,s')\in R;\ P\ s;\ !!P'.\ is\text{-}inv\ R\ s0\ P' \Longrightarrow P'\ s\ ]\!] \Longrightarrow P\ s'\ ]\!] \Longrightarrow is\text{-}inv\ R\ s0\ (\lambda s.\ P\ s \wedge (\forall P'.\ is\text{-}inv\ R\ s0\ P' \longrightarrow P'\ s))$
$\langle \mathit{proof}\rangle$

If the inverse step relation is well-founded, the algorithm will terminate for every state in $\mathit{Domain}\ R$ ($\subseteq$-direction). The $\supseteq$-direction is from $\mathit{dom\text{-}subset}$

lemma $\mathit{wf\text{-}dom\text{-}eq}$: $wf\ (R^{-1}) \Longrightarrow Domain\ R = Domain\ (A\text{-}rel\ R)$ $\langle \mathit{proof}\rangle$

3.2 Refinement

Refinement is a simulation property between step relations.

We define refinement w.r.t. an abstraction relation α, that relates abstract to concrete states. The refining step-relation is called more concrete than the refined one.

definition $\mathit{refines} :: ('s{*}'s)\ set \Rightarrow ('r{*}'s)\ set \Rightarrow ('r{*}'r)\ set \Rightarrow bool\ (\text{-}\leq_{\text{-}}\text{-}\ [50,50,50]\ 50)$ **where**
$R \leq_{\alpha} S == \alpha\ O\ R \subseteq S\ O\ \alpha \wedge \alpha\ ``\ Domain\ S \subseteq Domain\ R$

lemma $\mathit{refinesI}$: $[\![\alpha\ O\ R \subseteq S\ O\ \alpha;\ \alpha\ ``\ Domain\ S \subseteq Domain\ R]\!] \Longrightarrow R{\leq_{\alpha}}S$ $\langle \mathit{proof}\rangle$
lemma $\mathit{refinesE}$: $R{\leq_{\alpha}}S \Longrightarrow \alpha\ O\ R \subseteq S\ O\ \alpha$
$R{\leq_{\alpha}}S \Longrightarrow \alpha\ ``\ Domain\ S \subseteq Domain\ R$
$\langle \mathit{proof}\rangle$

Intuitively, the first condition for refinement means, that for each concrete step $(c,c')\in S$ where the start state c has an abstract counterpart $(a,c)\in\alpha$, there is also an abstract counterpart of the end state $(a',c')\in\alpha$ and the step can also be done on the abstract counterparts $(a,a')\in R$.

lemma $\mathit{refines\text{-}compI}$:
assumes A: $!!\ a\ c\ c'.\ [\![\ (a,c)\in\alpha;\ (c,c')\in S\ ]\!] \Longrightarrow \exists\, a'.\ (a,a')\in R \wedge (a',c')\in\alpha$
shows $\alpha\ O\ S \subseteq R\ O\ \alpha$ $\langle \mathit{proof}\rangle$

lemma $\mathit{refines\text{-}compE}$: $[\![\alpha\ O\ S \subseteq R\ O\ \alpha;\ (a,c)\in\alpha;\ (c,c')\in S]\!] \Longrightarrow \exists\, a'.\ (a,a')\in R \wedge (a',c')\in\alpha$ $\langle \mathit{proof}\rangle$

Intuitively, the second condition for refinement means, that if there is an abstract step $(a,a')\in R$, where the start state has a concrete counterpart c, then there must also be a concrete step from c. Note that this concrete step is not required to lead to the concrete counterpart of a'. In fact, it is only important that there is such a concrete step, ensuring that the concrete algorithm will not terminate on states on that the abstract algorithm continues execution.

lemma *refines-domI*:
  assumes A: !! $a\ a'\ c.\ [\![(a,c)\in\alpha;\ (a,a')\in R\ ]\!] \Longrightarrow c\in \mathit{Domain}\ S$
  shows α *‘‘ Domain* $R \subseteq$ *Domain* S ⟨*proof*⟩

lemma *refines-domE*: $[\![\alpha$ *‘‘ Domain* $R \subseteq$ *Domain* $S;\ (a,c)\in\alpha;\ (a,a')\in R]\!] \Longrightarrow c\in \mathit{Domain}\ S$ ⟨*proof*⟩

lemma *refinesI2*:
  assumes A: !! $a\ c\ c'.\ [\![\ (a,c)\in\alpha;\ (c,c')\in S\ \ ]\!] \Longrightarrow \exists\, a'.\ (a,a')\in R \wedge (a',c')\in\alpha$
  assumes B: !! $a\ a'\ c.\ [\![(a,c)\in\alpha;\ (a,a')\in R\ ]\!] \Longrightarrow c\in \mathit{Domain}\ S$
  shows $S\leq_{\alpha}R$ ⟨*proof*⟩

lemma *refinesE2*:
  $[\![S\leq_{\alpha}R;\ (a,c)\in\alpha;\ (c,c')\in S]\!] \Longrightarrow \exists\, a'.\ (a,a')\in R \wedge (a',c')\in\alpha$
  $[\![S\leq_{\alpha}R;\ (a,c)\in\alpha;\ (a,a')\in R]\!] \Longrightarrow c\in \mathit{Domain}\ S$
  ⟨*proof*⟩

Reflexivity of identity refinement

lemma *refines-id-refl*[*intro*!, *simp*]: $R\leq_{Id}R$ ⟨*proof*⟩

Transitivity of refinement

lemma *refines-trans*: **assumes** R: $R \leq_{\alpha} S \quad S \leq_{\beta} T$ **shows** $R\leq_{\beta\ O\ \alpha}T$
⟨*proof*⟩

Property transfer lemma

lemma *refines-A-rel*[*rule-format*]:
  assumes R: $R\leq_{\alpha}S$ **and** A: $(r,r')\in$ *A-rel* R $(s,r)\in\alpha$
  shows $(\exists\, s'.\ (s',r')\in\alpha \wedge (s,s')\in$ *A-rel* $S)$
  ⟨*proof*⟩

Property transfer lemma for single-valued abstractions (i.e. abstraction functions)

lemma *refines-A-rel-sv*: $[\![R\leq_{\alpha}S;\ (r,r')\in$ *A-rel* R; *single-valued* $(\alpha^{-1});\ (s,r)\in\alpha;\ (s',r')\in\alpha]\!]$ $\Longrightarrow (s,s')\in$ *A-rel* S ⟨*proof*⟩

3.3 Extension to reflexive states

Up to now we only defined how to relate initial states to terminating states if the algorithm makes at least one step. In this section, we also add the reflexive part: Initial states for that no steps can be made are mapped to themselves.

definition
  ndet-algo R == (*A-rel* R) $\cup \{(s,s)\ |\ s.\ s\notin$ *Domain* $R\}$

lemma *ndet-algo-A-rel*: $[\![x{\in}\mathit{Domain}\ R;\ (x,y){\in}\mathit{ndet\text{-}algo}\ R]\!] \Longrightarrow (x,y){\in}\mathit{A\text{-}rel}\ R$
$\langle \mathit{proof} \rangle$

lemma *ndet-algoE*: $[\![(s,s'){\in}\mathit{ndet\text{-}algo}\ R;\ [\![(s,s'){\in}\mathit{A\text{-}rel}\ R]\!] \Longrightarrow P;\ [\![\ s{=}s';\ s{\notin}\mathit{Domain}\ R]\!] \Longrightarrow P]\!] \Longrightarrow P$ $\langle \mathit{proof} \rangle$
lemma *ndet-algoE'*: $[\![(s,s'){\in}\mathit{ndet\text{-}algo}\ R;\ [\![(s,s'){\in}\mathit{A\text{-}rel}\ R;\ s{\in}\mathit{Domain}\ R;\ s'{\notin}\mathit{Domain}\ R]\!] \Longrightarrow P;\ [\![\ s{=}s';\ s{\notin}\mathit{Domain}\ R]\!] \Longrightarrow P]\!] \Longrightarrow P$
$\langle \mathit{proof} \rangle$

ndet-algo is total (i.e. the algorithm is defined for every initial state), if R^{-1} is well founded

lemma *ndet-algo-total*: $\mathit{wf}\ (R^{-1}) \Longrightarrow \mathit{Domain}\ (\mathit{ndet\text{-}algo}\ R) = \mathit{UNIV}$
$\langle \mathit{proof} \rangle$

The result of the algorithm is always a terminating state

lemma *termstate-ndet-algo*: $(s,s'){\in}\mathit{ndet\text{-}algo}\ R \Longrightarrow s'{\notin}\mathit{Domain}\ R$ $\langle \mathit{proof} \rangle$

Property transfer lemma for *ndet-algo*

lemma *refines-ndet-algo*[*rule-format*]:
assumes R: $S{\le_\alpha}R$ **and** A: $(c,c'){\in}\mathit{ndet\text{-}algo}\ S$
shows $\forall\, a.\ (a,c){\in}\alpha \longrightarrow (\exists\, a'.\ (a',c'){\in}\alpha \wedge (a,a'){\in}\mathit{ndet\text{-}algo}\ R)$
$\langle \mathit{proof} \rangle$

Property transfer lemma for single-valued abstractions (i.e. Abstraction functions)

lemma *refines-ndet-algo-sv*: $[\![S{\le_\alpha}R;\ (c,c'){\in}\mathit{ndet\text{-}algo}\ S;\ \mathit{single\text{-}valued}\ (\alpha^{-1});\ (a,c){\in}\alpha;\ (a',c'){\in}\alpha]\!] \Longrightarrow (a,a'){\in}\mathit{ndet\text{-}algo}\ R$ $\langle \mathit{proof} \rangle$

3.4 Well-foundedness

lemma *wf-imp-minimal*: $[\![\mathit{wf}\ S;\ x{\in}Q]\!] \Longrightarrow \exists\, z{\in}Q.\ (\forall\, x.\ (x,z){\in}S \longrightarrow x{\notin}Q)$ $\langle \mathit{proof} \rangle$

This lemma allows to show well-foundedness of a refining relation by providing a well-founded refined relation for each element in the domain of the refining relation.

lemma *refines-wf*:
assumes A: $!!r.\ [\![\ r{\in}\mathit{Domain}\ R\ ]\!] \Longrightarrow (s\ r,r){\in}\alpha\ r \wedge R{\le_{\alpha\ r}}\ S\ r \wedge \mathit{wf}\ ((S\ r)^{-1})$
shows $\mathit{wf}\ (R^{-1})$
$\langle \mathit{proof} \rangle$

3.4.1 The relations $>$ and $\supset$ on finite domains

definition $\mathit{greaterN}\ N == \{(i,j)\ .\ j{<}i\ \&\ i{\le}(N{::}\mathit{nat})\}$
definition $\mathit{greaterS}\ S == \{(a,b)\ .\ b{\subset}a\ \&\ a{\subseteq}(S{::}'a\ \mathit{set})\}$

$>$ on initial segment of nat is well founded

lemma *wf-greaterN*: $\mathit{wf}\ (\mathit{greaterN}\ N)$

$\langle proof \rangle$

Strict version of *card-mono*

lemma *card-mono-strict*: $[\![finite\ B;\ A \subset B]\!] \Longrightarrow card\ A < card\ B$ $\langle proof \rangle$

$\supset$ on finite sets is well founded

This is shown here by embedding the $\supset$ relation into the $>$ relation, using cardinality

lemma *wf-greaterS*: $finite\ S \Longrightarrow wf\ (greaterS\ S)$ $\langle proof \rangle$

This lemma shows well-foundedness of saturation algorithms, where in each step some set is increased, and this set remains below some finite upper bound

lemma *sat-wf*:
  assumes *subset*: $!!r\ r'.\ (r,r') \in R \Longrightarrow \alpha\ r \subset \alpha\ r' \wedge \alpha\ r' \subseteq U$
  assumes *finite*: $finite\ U$
  shows $wf\ (R^{-1})$
$\langle proof \rangle$

3.5 Implementation

The first step to implement a nondeterministic algorithm specified by a relation R is to provide a deterministic refinement w.r.t. the identity abstraction *Id*. We can describe such a deterministic refinement as the graph of a partial function *sel*. We call this function a selector function, because it selects the next state from the possible states specified by R.

In order to get a working implementation, we must prove termination. That is, we have to show that $(graph\ sel)^{-1}$ is well-founded. If we already know that R^{-1} is well-founded, this property transfers to $(graph\ sel)^{-1}$.

Once obtained well-foundedness, we can use the selector function to implement the following recursive function:

$algo\ s = case\ sel\ s\ of\ None \Rightarrow s \mid Some\ s' \Rightarrow algo\ s'$

And we can show, that *algo* is consistent with *ndet-algo R*, that is $(s,algo\ s) \in ndet\text{-}algo\ R$.

3.5.1 Graphs of functions

The graph of a (partial) function is the relation of arguments and function values

definition $graph\ f == \{(x,x')\ .\ f\ x = Some\ x'\}$

lemma *graphI*[*intro*]: $f\ x = Some\ x' \Longrightarrow (x,x') \in graph\ f$ $\langle proof \rangle$
lemma *graphD*[*dest*]: $(x,x') \in graph\ f \Longrightarrow f\ x = Some\ x'$ $\langle proof \rangle$
lemma *graph-dom-iff1*: $(x \notin Domain\ (graph\ f)) = (f\ x = None)$ $\langle proof \rangle$
lemma *graph-dom-iff2*: $(x \in Domain\ (graph\ f)) = (f\ x \neq None)$ $\langle proof \rangle$

3.5.2 Deterministic refinement w.r.t. the identity abstraction

lemma *detRef-eq*: $(graph\ sel \leq_{Id}\ R) = ((\forall\, s\ s'.\ sel\ s = Some\ s' \longrightarrow (s,s') \in R) \wedge (\forall\, s.\ sel\ s = None \longrightarrow s \notin Domain\ R))$
⟨*proof*⟩

lemma *detRef-wf-transfer*: $[\![wf\ (R^{-1});\ graph\ sel \leq_{Id}\ R\ ]\!] \Longrightarrow wf\ ((graph\ sel)^{-1})$
⟨*proof*⟩

3.5.3 Recursive characterization

locale *detRef-impl* =
fixes *algo* **and** *sel* **and** *R*
assumes *detRef*: $graph\ sel \leq_{Id}\ R$
assumes *algo-rec*[*simp*]: $!!\ s\ s'.\ sel\ s = Some\ s' \Longrightarrow algo\ s = algo\ s'$ **and** *algo-term*[*simp*]: $!!\ s.\ sel\ s = None \Longrightarrow algo\ s = s$
assumes *wf*: $wf\ ((graph\ sel)^{-1})$

lemma (**in** *detRef-impl*) *sel-cons*:
$sel\ s = Some\ s' \Longrightarrow (s,s') \in R$
$sel\ s = None \Longrightarrow s \notin Domain\ R$
$s \in Domain\ R \Longrightarrow \exists\, s'.\ sel\ s = Some\ s'$
$s \notin Domain\ R \Longrightarrow sel\ s = None$
⟨*proof*⟩

lemma (**in** *detRef-impl*) *algo-correct*: $(s,algo\ s) \in ndet\text{-}algo\ R$ ⟨*proof*⟩

end

4 Dynamic pushdown networks

theory *DPN*
imports *DPN-Setup SRS FSM NDET*
begin

Dynamic pushdown networks (DPNs) are a model for parallel, context free processes where processes can create new processes.

They have been introduced in [1]. In this theory we formalize DPNs and the automata based algorithm for calculating a representation of the (regular) set of backward reachable configurations, starting at a regular set of configurations.

We describe the algorithm nondeterministically, and prove its termination and correctness.

4.1 Dynamic pushdown networks

4.1.1 Definition

record $('c,'l)$ *DPN-rec* =
  csyms :: $'c$ *set*
  ssyms :: $'c$ *set*
  sep :: $'c$
  labels :: $'l$ *set*
  rules :: $('c,'l)$ *SRS*

A dynamic pushdown network consists of a finite set of control symbols, a finite set of stack symbols, a separator symbol[1], a finite set of labels and a finite set of labelled string rewrite rules.

The set of control and stack symbols are disjoint, and both do not contain the separator. A string rewrite rule is either of the form $[p,\gamma] \hookrightarrow_a p1\#w1$ or $[p,\gamma] \hookrightarrow_a p1\#w1@\sharp\#p2\#w2$ where p,$p1$,$p2$ are control symbols, $w1$,$w2$ are sequences of stack symbols, a is a label and $\sharp$ is the separator.

locale *DPN* =
  fixes M
  fixes *separator* ($\sharp$)
  defines *sep-def*: $\sharp$ == *sep* M
  assumes *sym-finite*: *finite* (*csyms* M) *finite* (*ssyms* M)
  assumes *sym-disjoint*: *csyms* M ∩ *ssyms* M = {} $\sharp$ ∉ *csyms* M ∪ *ssyms* M
  assumes *lab-finite*: *finite* (*labels* M)
  assumes *rules-finite*: *finite* (*rules* M)
  assumes *rule-fmt*: $r \in$ *rules* $M \Longrightarrow$
    $(\exists\, p\ \gamma\ a\ p'\ w.\ p \in csyms\ M \wedge \gamma \in ssyms\ M \wedge p' \in csyms\ M \wedge w \in lists\ (ssyms\ M) \wedge a \in labels\ M \wedge r = p\#[\gamma] \hookrightarrow_a p'\#w)$
  $\vee\ (\exists\, p\ \gamma\ a\ p1\ w1\ p2\ w2.\ p \in csyms\ M \wedge \gamma \in ssyms\ M \wedge p1 \in csyms\ M \wedge w1 \in lists\ (ssyms\ M) \wedge p2 \in csyms\ M \wedge w2 \in lists\ (ssyms\ M) \wedge a \in labels\ M \wedge r = p\#[\gamma] \hookrightarrow_a p1\#w1@\sharp\#p2\#w2)$

lemma (**in** *DPN*) *sep-fold*: *sep* M == $\sharp$ ⟨*proof*⟩

lemma (**in** *DPN*) *sym-disjoint'*: *sep* M ∉ *csyms* M ∪ *ssyms* M ⟨*proof*⟩

4.1.2 Basic properties

lemma (**in** *DPN*) *syms-part*: $x \in csyms\ M \Longrightarrow x \notin ssyms\ M$ $x \in ssyms\ M \Longrightarrow x \notin csyms\ M$ ⟨*proof*⟩
lemma (**in** *DPN*) *syms-sep*: $\sharp \notin csyms\ M$ $\sharp \notin ssyms\ M$ ⟨*proof*⟩
lemma (**in** *DPN*) *syms-sep'*: $sep\ M \notin csyms\ M$ $sep\ M \notin ssyms\ M$ ⟨*proof*⟩

lemma (**in** *DPN*) *rule-cases*[*consumes 1*, *case-names no-spawn spawn*]:
  assumes *A*: $r \in rules\ M$

[1] In the final version of [1], no separator symbols are used. We use them here because we think it simplifies formalization of the proofs.

assumes *NOSPAWN*: !! *p* γ *a p′ w*. ⟦*p*∈*csyms M*; γ∈*ssyms M*; *p′*∈*csyms M*; *w*∈*lists* (*ssyms M*); *a*∈*labels M*; *r*=*p*#[γ] $\hookrightarrow_a$ *p′*#*w*⟧ ⟹ *P*
assumes *SPAWN*: !! *p* γ *a p1 w1 p2 w2*. ⟦*p*∈*csyms M*; γ∈*ssyms M*; *p1*∈*csyms M*; *w1*∈*lists* (*ssyms M*); *p2*∈*csyms M*; *w2*∈*lists* (*ssyms M*); *a*∈*labels M*; *r*=*p*#[γ] $\hookrightarrow_a$ *p1*#*w1*@♯#*p2*#*w2*⟧ ⟹ *P*
shows *P*
⟨*proof*⟩

lemma (**in** *DPN*) *rule-cases′*:
⟦*r*∈*rules M*;
!! *p* γ *a p′ w*. ⟦*p*∈*csyms M*; γ∈*ssyms M*; *p′*∈*csyms M*; *w*∈*lists* (*ssyms M*); *a*∈*labels M*; *r*=*p*#[γ] $\hookrightarrow_a$ *p′*#*w*⟧ ⟹ *P*;
!! *p* γ *a p1 w1 p2 w2*. ⟦*p*∈*csyms M*; γ∈*ssyms M*; *p1*∈*csyms M*; *w1*∈*lists* (*ssyms M*); *p2*∈*csyms M*; *w2*∈*lists* (*ssyms M*); *a*∈*labels M*; *r*=*p*#[γ] $\hookrightarrow_a$ *p1*#*w1*@(*sep M*)#*p2*#*w2*⟧ ⟹ *P*⟧
⟹ *P* ⟨*proof*⟩

lemma (**in** *DPN*) *rule-prem-fmt*: *r*∈*rules M* ⟹ ∃ *p* γ *a c′*. *p*∈*csyms M* ∧ γ∈*ssyms M* ∧ *a*∈*labels M* ∧ *set c′* ⊆ *csyms M* ∪ *ssyms M* ∪ {♯} ∧ *r*=(*p*#[γ] $\hookrightarrow_a$ *c′*)
⟨*proof*⟩

lemma (**in** *DPN*) *rule-prem-fmt′*: *r*∈*rules M* ⟹ ∃ *p* γ *a c′*. *p*∈*csyms M* ∧ γ∈*ssyms M* ∧ *a*∈*labels M* ∧ *set c′* ⊆ *csyms M* ∪ *ssyms M* ∪ {*sep M*} ∧ *r*=(*p*#[γ] $\hookrightarrow_a$ *c′*) ⟨*proof*⟩

lemma (**in** *DPN*) *rule-prem-fmt2*: [*p*,γ]$\hookrightarrow_a$ *c′* ∈ *rules M* ⟹ *p*∈*csyms M* ∧ γ∈*ssyms M* ∧ *a*∈*labels M* ∧ *set c′* ⊆ *csyms M* ∪ *ssyms M* ∪ {♯} ⟨*proof*⟩
lemma (**in** *DPN*) *rule-prem-fmt2′*: [*p*,γ]$\hookrightarrow_a$ *c′* ∈ *rules M* ⟹ *p*∈*csyms M* ∧ γ∈*ssyms M* ∧ *a*∈*labels M* ∧ *set c′* ⊆ *csyms M* ∪ *ssyms M* ∪ {*sep M*} ⟨*proof*⟩

lemma (**in** *DPN*) *rule-fmt-fs*: [*p*,γ]$\hookrightarrow_a$ *p′*#*c′* ∈ *rules M* ⟹ *p*∈*csyms M* ∧ γ∈*ssyms M* ∧ *a*∈*labels M* ∧ *p′*∈*csyms M* ∧ *set c′* ⊆ *csyms M* ∪ *ssyms M* ∪ {♯}
⟨*proof*⟩

4.1.3 Building DPNs

Sanity check: we can create valid DPNs by adding rules to an empty DPN

definition *dpn-empty C S s* ≡ ⦇
csyms = *C*,
ssyms = *S*,
sep = *s*,
labels = {},
rules = {}
⦈

definition *dpn-add-local-rule p* γ *a* p_1 w_1 *D* ≡ *D*⦇ *labels* := *insert a* (*labels D*), *rules* := *insert* ([*p*,γ],*a*,p_1#w_1) (*rules D*) ⦈
definition *dpn-add-spawn-rule p* γ *a* p_1 w_1 p_2 w_2 *D* ≡ *D*⦇ *labels* := *insert a* (*labels D*), *rules* := *insert* ([*p*,γ],*a*,p_1#w_1@*sep D*#p_2#w_2) (*rules D*) ⦈

lemma *dpn-empty-invar*[*simp*]: $[\![$*finite C*; *finite S*; $C \cap S = \{\}$; $s \notin C \cup S]\!] \Longrightarrow$ *DPN* (*dpn-empty C S s*)
  ⟨*proof*⟩

lemma *dpn-add-local-rule-invar*[*simp*]:
  assumes *A*: $\{p, p_1\} \subseteq$ *csyms D insert* γ (*set* w_1) $\subseteq$ *ssyms D* **and** *DPN D*
  shows *DPN* (*dpn-add-local-rule p* γ *a* p_1 w_1 *D*)
⟨*proof*⟩

lemma *dpn-add-spawn-rule-invar*[*simp*]:
  assumes *A*: $\{p, p_1, p_2\} \subseteq$ *csyms D insert* γ (*set* $w_1 \cup$ *set* w_2) $\subseteq$ *ssyms D* **and** *DPN D*
  shows *DPN* (*dpn-add-spawn-rule p* γ *a* p_1 w_1 p_2 w_2 *D*)
⟨*proof*⟩

4.2 M-automata

We are interested in calculating the predecessor sets of regular sets of configurations. For this purpose, the regular sets of configurations are represented as finite state machines, that conform to certain constraints, depending on the underlying DPN. These FSMs are called M-automata.

4.2.1 Definition

record ('*s*,'*c*) *MFSM-rec* = ('*s*,'*c*) *FSM-rec* +
  sstates :: '*s set*
  cstates :: '*s set*
  sp :: '*s* ⇒ '*c* ⇒ '*s*

M-automata are FSMs whose states are partioned into control and stack states. For each control state *s* and control symbol *p*, there is a unique and distinguished stack state *sp A s p*, and a transition (*s*,*p*,*sp A s p*)$\in\delta$. The initial state is a control state, and the final states are all stack states. Moreover, the transitions are restricted: The only incoming transitions of control states are separator transitions from stack states. The only outgoing transitions are the (*s*,*p*,*sp A s p*)$\in\delta$ transitions mentioned above. The *sp A s p*-states have no other incoming transitions.

locale *MFSM* = *DPN M* + *FSM A*
  for *M A* +

  assumes *alpha-cons*: Σ *A* = *csyms M* $\cup$ *ssyms M* $\cup$ $\{\sharp\}$
  assumes *states-part*: *sstates A* $\cap$ *cstates A* = {} *Q A* = *sstates A* $\cup$ *cstates A*
  assumes *uniqueSp*: $[\![$*s*$\in$*cstates A*; *p*$\in$*csyms M*$]\!] \Longrightarrow$ *sp A s p* $\in$ *sstates A* $[\![$*p*$\in$*csyms M*; *p*'$\in$*csyms M*; *s*$\in$*cstates A*; *s*'$\in$*cstates A*; *sp A s p* = *sp A s' p'*$]\!] \Longrightarrow$ *s*=*s*' $\wedge$ *p*=*p*'

assumes *delta-fmt*: $\delta\ A \subseteq (\mathit{sstates}\ A \times \mathit{ssyms}\ M \times (\mathit{sstates}\ A - \{\mathit{sp}\ A\ s\ p \mid s\ p\ .\ s{\in}\mathit{cstates}\ A \wedge p{\in}\mathit{csyms}\ M\})) \cup (\mathit{sstates}\ A \times \{\sharp\} \times \mathit{cstates}\ A) \cup \{(s,p,\mathit{sp}\ A\ s\ p) \mid s\ p\ .\ s{\in}\mathit{cstates}\ A \wedge p{\in}\mathit{csyms}\ M\}$
$\delta\ A \supseteq \{(s,p,\mathit{sp}\ A\ s\ p) \mid s\ p\ .\ s{\in}\mathit{cstates}\ A \wedge p{\in}\mathit{csyms}\ M\}$
assumes *s0-fmt*: $\mathit{s0}\ A \in \mathit{cstates}\ A$
assumes *F-fmt*: $F\ A{\subseteq}\mathit{sstates}\ A$ — This deviates slightly from [1], as we cannot represent the empty configuration here. However, this restriction is harmless, since the only predecessor of the empty configuration is the empty configuration itself.
constrains $M{::}('c,'l,'e1)$ *DPN-rec-scheme*
constrains $A{::}('s,'c,'e2)$ *MFSM-rec-scheme*

lemma (**in** *MFSM*) *alpha-cons′*: $\Sigma\ A = \mathit{csyms}\ M \cup \mathit{ssyms}\ M \cup \{\mathit{sep}\ M\}$ ⟨*proof*⟩
lemma (**in** *MFSM*) *delta-fmt′*: $\delta\ A \subseteq (\mathit{sstates}\ A \times \mathit{ssyms}\ M \times (\mathit{sstates}\ A - \{\mathit{sp}\ A\ s\ p \mid s\ p\ .\ s{\in}\mathit{cstates}\ A \wedge p{\in}\mathit{csyms}\ M\})) \cup (\mathit{sstates}\ A \times \{\mathit{sep}\ M\} \times \mathit{cstates}\ A) \cup \{(s,p,\mathit{sp}\ A\ s\ p) \mid s\ p\ .\ s{\in}\mathit{cstates}\ A \wedge p{\in}\mathit{csyms}\ M\}$
$\delta\ A \supseteq \{(s,p,\mathit{sp}\ A\ s\ p) \mid s\ p\ .\ s{\in}\mathit{cstates}\ A \wedge p{\in}\mathit{csyms}\ M\}$ ⟨*proof*⟩

4.2.2 Basic properties

lemma (**in** *MFSM*) *finite-cs-states*: $\mathit{finite}\ (\mathit{sstates}\ A)$ $\mathit{finite}\ (\mathit{cstates}\ A)$
⟨*proof*⟩

lemma (**in** *MFSM*) *sep-out-syms*: $x{\in}\mathit{csyms}\ M \Longrightarrow x \neq \sharp$ $x{\in}\mathit{ssyms}\ M \Longrightarrow x \neq \sharp$
⟨*proof*⟩
lemma (**in** *MFSM*) *sepI*: $[\![x{\in}\Sigma\ A;x{\notin}\mathit{csyms}\ M;\ x{\notin}\mathit{ssyms}\ M]\!] \Longrightarrow x{=}\sharp$ ⟨*proof*⟩
lemma (**in** *MFSM*) *sep-out-syms′*: $x{\in}\mathit{csyms}\ M \Longrightarrow x \neq \mathit{sep}\ M$ $x{\in}\mathit{ssyms}\ M \Longrightarrow x \neq \mathit{sep}\ M$ ⟨*proof*⟩
lemma (**in** *MFSM*) *sepI′*: $[\![x{\in}\Sigma\ A;x{\notin}\mathit{csyms}\ M;\ x{\notin}\mathit{ssyms}\ M]\!] \Longrightarrow x{=}\mathit{sep}\ M$ ⟨*proof*⟩

lemma (**in** *MFSM*) *states-partI1*: $x{\in}\mathit{sstates}\ A \Longrightarrow \neg x{\in}\mathit{cstates}\ A$ ⟨*proof*⟩
lemma (**in** *MFSM*) *states-partI2*: $x{\in}\mathit{cstates}\ A \Longrightarrow \neg x{\in}\mathit{sstates}\ A$ ⟨*proof*⟩
lemma (**in** *MFSM*) *states-part-elim*[*elim*]: $[\![q{\in}Q\ A;\ q{\in}\mathit{sstates}\ A \Longrightarrow P;\ q{\in}\mathit{cstates}\ A \Longrightarrow P]\!] \Longrightarrow P$ ⟨*proof*⟩

lemmas (**in** *MFSM*) *mfsm-cons* = *sep-out-syms sepI sep-out-syms′ sepI′ states-partI1 states-partI2 syms-part syms-sep uniqueSp*
lemmas (**in** *MFSM*) *mfsm-cons′* = *sep-out-syms sepI sep-out-syms′ sepI′ states-partI1 states-partI2 syms-part uniqueSp*

lemma (**in** *MFSM*) *delta-cases*: $[\![(q,p,q'){\in}\delta\ A;\ q{\in}\mathit{sstates}\ A \wedge p{\in}\mathit{ssyms}\ M \wedge q'{\in}\mathit{sstates}\ A \wedge q'{\notin}\{\mathit{sp}\ A\ s\ p \mid s\ p\ .\ s{\in}\mathit{cstates}\ A \wedge p{\in}\mathit{csyms}\ M\} \Longrightarrow P;$
$q{\in}\mathit{sstates}\ A \wedge p{=}\sharp \wedge q'{\in}\mathit{cstates}\ A \Longrightarrow P;$
$q{\in}\mathit{cstates}\ A \wedge p{\in}\mathit{csyms}\ M \wedge q'{=}\mathit{sp}\ A\ q\ p \Longrightarrow P]\!] \Longrightarrow P$
⟨*proof*⟩

lemma (**in** *MFSM*) *delta-elems*: $(q,p,q')\in\delta\ A \Longrightarrow q\in \mathit{sstates}\ A \land ((p\in \mathit{ssyms}\ M \land q'\in \mathit{sstates}\ A \land (q'\notin\{\mathit{sp}\ A\ s\ p \mid s\ p\ .\ s\in \mathit{cstates}\ A \land p\in \mathit{csyms}\ M\})) \lor (p=\sharp \land q'\in \mathit{cstates}\ A)) \lor (q\in \mathit{cstates}\ A \land p\in \mathit{csyms}\ M \land q'=\mathit{sp}\ A\ q\ p)$
⟨*proof*⟩

lemma (**in** *MFSM*) *delta-cases'*: $[\![(q,p,q')\in\delta\ A;\ q\in \mathit{sstates}\ A \land p\in \mathit{ssyms}\ M \land q'\in \mathit{sstates}\ A \land q'\notin\{\mathit{sp}\ A\ s\ p \mid s\ p\ .\ s\in \mathit{cstates}\ A \land p\in \mathit{csyms}\ M\} \Longrightarrow P;$
$q\in \mathit{sstates}\ A \land p=\mathit{sep}\ M \land q'\in \mathit{cstates}\ A \Longrightarrow P;$
$q\in \mathit{cstates}\ A \land p\in \mathit{csyms}\ M \land q'=\mathit{sp}\ A\ q\ p \Longrightarrow P]\!] \Longrightarrow P$
⟨*proof*⟩

lemma (**in** *MFSM*) *delta-elems'*: $(q,p,q')\in\delta\ A \Longrightarrow q\in \mathit{sstates}\ A \land ((p\in \mathit{ssyms}\ M \land q'\in \mathit{sstates}\ A \land (q'\notin\{\mathit{sp}\ A\ s\ p \mid s\ p\ .\ s\in \mathit{cstates}\ A \land p\in \mathit{csyms}\ M\})) \lor (p=\mathit{sep}\ M \land q'\in \mathit{cstates}\ A)) \lor (q\in \mathit{cstates}\ A \land p\in \mathit{csyms}\ M \land q'=\mathit{sp}\ A\ q\ p)$
⟨*proof*⟩

4.2.3 Some implications of the M-automata conditions

This list of properties is taken almost literally from [1].

Each control state s has $\mathit{sp}\ A\ s\ p$ as its unique p-successor

lemma (**in** *MFSM*) *cstate-succ-ex*: $[\![p\in \mathit{csyms}\ M;\ s\in \mathit{cstates}\ A]\!] \Longrightarrow (s,p,\mathit{sp}\ A\ s\ p) \in \delta\ A$
⟨*proof*⟩

lemma (**in** *MFSM*) *cstate-succ-ex'*: $[\![p\in \mathit{csyms}\ M;\ s\in \mathit{cstates}\ A;\ \delta\ A \subseteq D]\!] \Longrightarrow (s,p,\mathit{sp}\ A\ s\ p) \in D$ ⟨*proof*⟩

lemma (**in** *MFSM*) *cstate-succ-unique*: $[\![s\in \mathit{cstates}\ A;\ (s,p,x)\in\delta\ A]\!] \Longrightarrow p\in \mathit{csyms}\ M \land x=\mathit{sp}\ A\ s\ p$ ⟨*proof*⟩

Transitions labeled with control symbols only leave from control states

lemma (**in** *MFSM*) *csym-from-cstate*: $[\![(s,p,s')\in\delta\ A;\ p\in \mathit{csyms}\ M]\!] \Longrightarrow s\in \mathit{cstates}\ A$ ⟨*proof*⟩

s is the only predecessor of $\mathit{sp}\ A\ s\ p$

lemma (**in** *MFSM*) *sp-pred-ex*: $[\![s\in \mathit{cstates}\ A;\ p\in \mathit{csyms}\ M]\!] \Longrightarrow (s,p,\mathit{sp}\ A\ s\ p)\in\delta\ A$ ⟨*proof*⟩
lemma (**in** *MFSM*) *sp-pred-unique*: $[\![s\in \mathit{cstates}\ A;\ p\in \mathit{csyms}\ M;\ (s',p',\mathit{sp}\ A\ s\ p)\in\delta\ A]\!] \Longrightarrow s'=s \land p'=p \land s'\in \mathit{cstates}\ A \land p'\in \mathit{csyms}\ M$ ⟨*proof*⟩

Only separators lead from stack states to control states

lemma (**in** *MFSM*) *sep-in-between*: $[\![s\in \mathit{sstates}\ A;\ s'\in \mathit{cstates}\ A;\ (s,p,s')\in\delta\ A]\!] \Longrightarrow p=\sharp$ ⟨*proof*⟩
lemma (**in** *MFSM*) *sep-to-cstate*: $[\![(s,\sharp,s')\in\delta\ A]\!] \Longrightarrow s\in \mathit{sstates}\ A \land s'\in \mathit{cstates}\ A$ ⟨*proof*⟩

Stack states do not have successors labelled with control symbols

lemma (**in** *MFSM*) *sstate-succ*: ⟦*s*∈*sstates A*; (*s*,γ,*s'*)∈δ *A*⟧ ⟹ γ ∉ *csyms M* ⟨*proof*⟩
lemma (**in** *MFSM*) *sstate-succ2*: ⟦*s*∈*sstates A*; (*s*,γ,*s'*)∈δ *A*; γ≠♯⟧ ⟹ γ∈*ssyms M* ∧ *s'*∈*sstates A* ⟨*proof*⟩

M-automata do not accept the empty word

lemma (**in** *MFSM*) *not-empty*[*iff*]: []∉*lang A*
⟨*proof*⟩

The paths through an M-automata have a very special form: Paths starting at a stack state are either labelled entirely with stack symbols, or have a prefix labelled with stack symbols followed by a separator

lemma (**in** *MFSM*) *path-from-sstate*: !!*s* . ⟦*s*∈*sstates A*; (*s*,*w*,*f*)∈*trclA A*⟧ ⟹ (*f*∈*sstates A* ∧ *w*∈*lists* (*ssyms M*)) ∨ (∃ *w1 w2 t*. *w*=*w1*@♯#*w2* ∧ *w1*∈*lists* (*ssyms M*) ∧ *t*∈*sstates A* ∧ (*s*,*w1*,*t*)∈*trclA A* ∧ (*t*,♯#*w2*,*f*)∈*trclA A*)
⟨*proof*⟩

Using *MFSM.path-from-sstate*, we can describe the format of paths from control states, too. A path from a control state *s* to some final state starts with a transition (*s*, *p*, *sp A s p*) for some control symbol *p*. It then continues with a sequence of transitions labelled by stack symbols. It then either ends or continues with a separator transition, bringing it to a control state again, and some further transitions from there on.

lemma (**in** *MFSM*) *path-from-cstate*:
assumes *A*: *s*∈*cstates A* (*s*,*c*,*f*)∈*trclA A f*∈*sstates A*
assumes *SINGLE*: !! *p w* . ⟦*c*=*p*#*w*; *p*∈*csyms M*; *w*∈*lists* (*ssyms M*); (*s*,*p*,*sp A s p*)∈δ *A*; (*sp A s p*,*w*,*f*)∈*trclA A*⟧ ⟹ *P*
assumes *CONC*: !! *p w cr t s'* . ⟦*c*=*p*#*w*@♯#*cr*; *p*∈*csyms M*; *w*∈*lists* (*ssyms M*); *t*∈*sstates A*; *s'*∈*cstates A*; (*s*,*p*,*sp A s p*)∈δ *A*; (*sp A s p*,*w*,*t*)∈*trclA A*; (*t*,♯,*s'*)∈δ *A*; (*s'*,*cr*,*f*)∈*trclA A*⟧ ⟹ *P*
shows *P*
⟨*proof*⟩

4.3 *pre**-sets of regular sets of configurations

Given a regular set *L* of configurations and a set Δ of string rewrite rules, *pre** Δ *L* is the set of configurations that can be rewritten to some configuration in *L*, using rules from Δ arbitrarily often.

We first define this set inductively based on rewrite steps, and then provide the characterization described above as a lemma.

inductive-set *pre-star* :: (*'c*,*'l*) *SRS* ⇒ (*'s*,*'c*,*'e*) *FSM-rec-scheme* ⇒ *'c list set* (*pre**)
for Δ *L*
where
pre-refl: *c*∈*lang L* ⟹ *c*∈*pre** Δ *L* |
pre-step: ⟦*c'*∈*pre** Δ *L*; (*c*,*a*,*c'*)∈*tr* Δ⟧ ⟹ *c*∈*pre** Δ *L*

Alternative characterization of $\mathit{pre}^*\ \Delta\ L$

lemma *pre-star-alt*: $\mathit{pre}^*\ \Delta\ L = \{c\ .\ \exists\, c'{\in}\mathit{lang}\ L\ .\ \exists\, \mathit{as}\ .\ (c,\mathit{as},c'){\in}\mathit{trcl}\ (\mathit{tr}\ \Delta)\}$ $\langle \mathit{proof}\rangle$

lemma *pre-star-altI*: $[\![c'{\in}\mathit{lang}\ L;\ c{\hookrightarrow}_{as}\ c'{\in}\mathit{trcl}\ (\mathit{tr}\ \Delta)]\!] \Longrightarrow c{\in}\mathit{pre}^*\ \Delta\ L\ \langle \mathit{proof}\rangle$
lemma *pre-star-altE*: $[\![c{\in}\mathit{pre}^*\ \Delta\ L;\ !!c'\ \mathit{as}.\ [\![c'{\in}\mathit{lang}\ L;\ c{\hookrightarrow}_{as}\ c'{\in}\mathit{trcl}\ (\mathit{tr}\ \Delta)]\!] \Longrightarrow P]\!] \Longrightarrow P\ \langle \mathit{proof}\rangle$

4.4 Nondeterministic algorithm for pre*

In this section, we formalize the saturation algorithm for computing $\mathit{pre}^*\ \Delta\ L$ from [1]. Roughly, the algorithm works as follows:

1. Set $D = \delta\ A$

2. Choose a rule $([p,\ \gamma],\ a,\ c') \in \mathit{rules}\ M$ and states $q{,}q'{\in}Q\ A$, such that D can read the configuration c' from state q and end in state q' (i.e. $(q,\ c',\ q') \in \mathit{trclAD}\ A\ D$) and such that $(\mathit{sp}\ A\ q\ p,\ \gamma,\ q') \notin D$. If this is not possible, terminate.

3. Add the transition $(\mathit{sp}\ A\ q\ p,\ \gamma,\ q') \notin D$ to D and continue with step 2

Intuitively, the behaviour of this algorithm can be explained as follows: If there is a configuration $c_1\ @\ c'\ @\ c_2 \in \mathit{pre}^*\ \Delta\ L$, and a rule $(p\ \#\ \gamma,\ a,\ c') \in \Delta$, then we also have $c_1\ @\ p\ \#\ \gamma\ @\ c_2 \in \mathit{pre}^*\ \Delta\ L$. The effect of step 3 is exactly adding these configurations $c_1\ @\ p\ \#\ \gamma\ @\ c_2\mathit{2}$ to the regular set of configurations.

We describe the algorithm nondeterministically by its step relation *ps-R*. Each step describes the addition of one transition.

In this approach, we directly restrict the domain of the step-relation to transition relations below some upper bound *ps-upper*. We will later show, that the initial transition relation of an M-automata is below this upper bound, and that the step-relation preserves the property of being below this upper bound.

We define *ps-upper M A* as a finite set, and show that the initial transition relation $\delta\ A$ of an M-automata is below *ps-upper M A*, and that *ps-R M A* preserves the property of being below the finite set *ps-upper M A*. Note that we use the more fine-grained *ps-upper M A* as upper bound for the termination proof rather than $Q\ A \times \Sigma\ A \times Q\ A$, as $\mathit{sp}\ A\ q\ p$ is only specified for control states q and control symbols p. Hence we need the finer structure of *ps-upper M A* to guarantee that *sp* is only applied to arguments it is specified for. Anyway, the fine-grained *ps-upper M A* bound is also needed for the correctness proof.

definition $\textit{ps-upper} :: ('c,'l,'e1)\ \textit{DPN-rec-scheme} \Rightarrow ('s,'c,'e2)\ \textit{MFSM-rec-scheme} \Rightarrow ('s,'c)\ \textit{LTS}$ **where**
$\textit{ps-upper}\ M\ A == (\textit{sstates}\ A \times \textit{ssyms}\ M \times \textit{sstates}\ A) \cup (\textit{sstates}\ A \times \{\textit{sep}\ M\} \times \textit{cstates}\ A) \cup \{(s,p,\textit{sp}\ A\ s\ p) \mid s\ p\ .\ s{\in}\textit{cstates}\ A \wedge p{\in}\textit{csyms}\ M\}$

inductive-set $\textit{ps-R} :: ('c,'l,'e1)\ \textit{DPN-rec-scheme} \Rightarrow ('s,'c,'e2)\ \textit{MFSM-rec-scheme} \Rightarrow (('s,'c)\ \textit{LTS} * ('s,'c)\ \textit{LTS})\ \textit{set}$ **for** $M\ A$
where
$[\![[p,\gamma]{\hookrightarrow}_a\ c' \in \textit{rules}\ M;\ (q,c',q'){\in}\textit{trclAD}\ A\ D;\ (\textit{sp}\ A\ q\ p,\gamma,q'){\notin}D;\ D{\subseteq}\textit{ps-upper}\ M\ A]\!] \Longrightarrow (D,\textit{insert}\ (\textit{sp}\ A\ q\ p,\gamma,q')\ D){\in}\textit{ps-R}\ M\ A$

lemma $\textit{ps-R-dom-below}$: $(D,D'){\in}\textit{ps-R}\ M\ A \Longrightarrow D{\subseteq}\textit{ps-upper}\ M\ A\ \langle \textit{proof}\rangle$

4.4.1 Termination

Termination of our algorithm is equivalent to well-foundedness of its (converse) step relation, that is, we have to show $\textit{wf}\ ((\textit{ps-R}\ M\ A)^{-1})$.

In the following, we also establich some properties of transition relations below $\textit{ps-upper}\ M\ A$, that will be used later in the correctness proof.

lemma (**in** $\textit{MFSM}$) $\textit{ps-upper-cases}$: $[\![(s,e,s'){\in}\textit{ps-upper}\ M\ A;$
$[\![s{\in}\textit{sstates}\ A;\ e{\in}\textit{ssyms}\ M;\ s'{\in}\textit{sstates}\ A]\!] \Longrightarrow P;$
$[\![s{\in}\textit{sstates}\ A;\ e{=}\sharp;\ s'{\in}\textit{cstates}\ A]\!] \Longrightarrow P;$
$[\![s{\in}\textit{cstates}\ A;\ e{\in}\textit{csyms}\ M;\ s'{=}\textit{sp}\ A\ s\ e]\!] \Longrightarrow P$
$]\!] \Longrightarrow P$
$\langle \textit{proof}\rangle$

lemma (**in** $\textit{MFSM}$) $\textit{ps-upper-cases}'$: $[\![(s,e,s'){\in}\textit{ps-upper}\ M\ A;$
$[\![s{\in}\textit{sstates}\ A;\ e{\in}\textit{ssyms}\ M;\ s'{\in}\textit{sstates}\ A]\!] \Longrightarrow P;$
$[\![s{\in}\textit{sstates}\ A;\ e{=}\textit{sep}\ M;\ s'{\in}\textit{cstates}\ A]\!] \Longrightarrow P;$
$[\![s{\in}\textit{cstates}\ A;\ e{\in}\textit{csyms}\ M;\ s'{=}\textit{sp}\ A\ s\ e]\!] \Longrightarrow P$
$]\!] \Longrightarrow P$
$\langle \textit{proof}\rangle$

lemma (**in** $\textit{MFSM}$) $\textit{ps-upper-below-trivial}$: $\textit{ps-upper}\ M\ A \subseteq Q\ A \times \Sigma\ A \times Q\ A$ $\langle \textit{proof}\rangle$

lemma (**in** $\textit{MFSM}$) $\textit{ps-upper-finite}$: $\textit{finite}\ (\textit{ps-upper}\ M\ A)\ \langle \textit{proof}\rangle$

The initial transition relation of the M-automaton is below $\textit{ps-upper}\ M\ A$

lemma (**in** $\textit{MFSM}$) $\textit{initial-delta-below}$: $\delta\ A \subseteq \textit{ps-upper}\ M\ A\ \langle \textit{proof}\rangle$

Some lemmas about structure of transition relations below $\textit{ps-upper}\ M\ A$

lemma (**in** $\textit{MFSM}$) $\textit{cstate-succ-unique}'$: $[\![s{\in}\textit{cstates}\ A;\ (s,p,x){\in}D;\ D{\subseteq}\textit{ps-upper}\ M\ A]\!] \Longrightarrow p{\in}\textit{csyms}\ M \wedge x{=}\textit{sp}\ A\ s\ p\ \langle \textit{proof}\rangle$
lemma (**in** $\textit{MFSM}$) $\textit{csym-from-cstate}'$: $[\![(s,p,s'){\in}D;\ D{\subseteq}\textit{ps-upper}\ M\ A;\ p{\in}\textit{csyms}\ M]\!] \Longrightarrow s{\in}\textit{cstates}\ A\ \langle \textit{proof}\rangle$

The only way to end up in a control state is after executing a separator.

lemma (**in** *MFSM*) *ctrl-after-sep*: **assumes** *BELOW*: $D \subseteq$ *ps-upper M A*
  assumes *A*: $(q,c',q') \in$*trclAD A D* $c' \neq []$
  shows $q' \in$*cstates A* = (*last* $c' = \sharp$)
⟨*proof*⟩

When applying a rules right hand side to a control state, we will get to a stack state

lemma (**in** *MFSM*) *ctrl-rule*: **assumes** *BELOW*: $D \subseteq$ *ps-upper M A*
  assumes *A*: $([p,\gamma],a,c') \in$*rules M* **and** *B*: $q \in$*cstates A* $(q,c',q') \in$*trclAD A D*
  shows $q' \in$*sstates A*
⟨*proof*⟩

ps-R M A preserves the property of being below *ps-upper M A*, and the transition relation becomes strictly greater in each step

lemma (**in** *MFSM*) *ps-R-below*: **assumes** *E*: $(D,D') \in$*ps-R M A*
  shows $D \subset D' \wedge D' \subseteq$ *ps-upper M A*
⟨*proof*⟩

As a result of this section, we get the well-foundedness of *ps-R M A*, and that the transition relations that occur during the saturation algorithm stay above the initial transition relation δ *A* and below *ps-upper M A*

theorem (**in** *MFSM*) *ps-R-wf*: *wf* ((*ps-R M A*)$^{-1}$) ⟨*proof*⟩

theorem (**in** *MFSM*) *ps-R-above-inv*: *is-inv* (*ps-R M A*) (δ *A*) ($\lambda D.\ \delta\ A \subseteq D$)
⟨*proof*⟩

theorem (**in** *MFSM*) *ps-R-below-inv*: *is-inv* (*ps-R M A*) (δ *A*) ($\lambda D.\ D \subseteq$*ps-upper M A*) ⟨*proof*⟩

We can also show that the algorithm is defined for every possible initial automata

theorem (**in** *MFSM*) *total*: $\exists D.$ (δ *A*, *D*)$\in$*ndet-algo*(*ps-R M A*) ⟨*proof*⟩

4.4.2 Soundness

The soundness (over-approximation) proof works by induction over the definition of *pre**.

In the reflexive case, a configuration from the original language is also in the saturated language, because no transitions are killed during saturation.

In the step case, we assume that a configuration c' is in the saturated language, and show for a rewriting step $c \hookrightarrow_a c'$ that also c is in the saturated language.

theorem (**in** *MFSM*) *sound*: $[\![c \in$*pre-star* (*rules M*) *A*; (δ *A*,s')$\in$*ndet-algo* (*ps-R M A*)$]\!] \Longrightarrow c \in$*lang* (*A*(| δ:=s' |))
⟨*proof*⟩

4.4.3 Precision

In this section we show the precision of the algorithm, that is we show that the saturated language is below the backwards reachable set.

The following induction scheme makes an induction over the number of occurences of a certain transition in words accepted by a FSM:
To prove a proposition for all words from state *qs* to state *qf* in FSM *A* that has a transition rule $(s,\ a,\ s') \in \delta\ A$, we have to show the following:

- Show, that the proposition is valid for words that do not use the transition rule $(s,\ a,\ s') \in \delta\ A$ at all
- Assuming that there is a prefix *wp* from *qs* to *s* and a suffix *ws* from s' to *qf*, and that *wp* does not use the new rule, and further assuming that for all prefixes *wh* from *qs* to s', the proposition holds for *wh* @ *ws*, show that the proposition also holds for *wp* @ *a* # *ws*.

We actually do use *D* here instead of $\delta\ A$, for use with *trclAD*.

lemma *ins-trans-induct*[*consumes 1*, *case-names base step*]:
fixes *qs* **and** *qf*
assumes *A*: $(qs,w,qf) \in trclAD\ A\ (insert\ (s,a,s')\ D)$
assumes *BASE-CASE*: !! w . $(qs,w,qf) \in trclAD\ A\ D \Longrightarrow P\ w$
assumes *STEP-CASE*: !! $wp\ ws$. $[\![(qs,wp,s) \in trclAD\ A\ D;\ (s',ws,qf) \in trclAD\ A\ (insert\ (s,a,s')\ D);$!! wh . $(qs,wh,s') \in trclAD\ A\ D \Longrightarrow P\ (wh@ws)]\!] \Longrightarrow P\ (wp@a\#ws)$
shows $P\ w$
⟨*proof*⟩

The following lemma is a stronger elimination rule than *ps-R.cases*. It makes a more fine-grained distinction. In words: A step of the algorithm adds a transition $(sp\ A\ q\ p,\ \gamma,\ s')$, if there is a rule $([p,\ \gamma],\ a,\ p'\ \#\ c')$, and a transition sequence $(q,\ p'\ \#\ c',\ s') \in trclAD\ A\ D$. That is, if we have $(sp\ A\ q\ p',\ c',\ s') \in trclAD\ A\ D$.

lemma (**in** *MFSM*) *ps-R-elims-adv*:
assumes $(D,D') \in ps\text{-}R\ M\ A$
obtains $\gamma\ s'\ a\ p'\ c'\ p\ q$ **where**
$D' = insert\ (sp\ A\ q\ p,\gamma,s')\ D$ $(sp\ A\ q\ p,\gamma,s') \notin D$ $[p,\gamma] \hookrightarrow_a p'\#c' \in rules\ M$ $(q,p'\#c',s') \in trclAD\ A\ D$
$p \in csyms\ M$ $\gamma \in ssyms\ M$ $q \in cstates\ A$ $p' \in csyms\ M$ $a \in labels\ M$ $(q,p',sp\ A\ q\ p') \in D$ $(sp\ A\ q\ p',c',s') \in trclAD\ A\ D$
⟨*proof*⟩

Now follows a helper lemma to establish the precision result. In the original paper [1] it is called the *crucial point* of the precision proof.

It states that for transition relations that occur during the execution of the algorithm, for each word *w* that leads from the start state to a state *sp A q*

p, there is a word ws @ $[p]$ that leads to $\mathit{sp}\ A\ q\ p$ in the initial automaton and w can be rewritten to ws @ $[p]$.

In the initial transition relation, a state of the form $\mathit{sp}\ A\ q\ p$ has only one incoming edge labelled p (*MFSM.sp-pred-ex MFSM.sp-pred-unique*). Intuitively, this lemma explains why it is correct to add further incoming edges to $\mathit{sp}\ A\ q\ p$: All words using such edges can be rewritten to a word using the original edge.

lemma (**in** *MFSM*) *sp-property*:
shows $\mathit{is\text{-}inv}\ (\mathit{ps\text{-}R}\ M\ A)\ (\delta\ A)\ (\lambda D.$
$(\forall\ w\ .\ \forall p{\in}\mathit{csyms}\ M.\ \forall q{\in}\mathit{cstates}\ A.\ (\mathit{s0}\ A,w,\mathit{sp}\ A\ q\ p){\in}\mathit{trclAD}\ A\ D \longrightarrow (\exists\,\mathit{ws}\ \mathit{as}.\ (\mathit{s0}\ A,\mathit{ws},q){\in}\mathit{trclA}\ A \wedge (w,\mathit{as},\mathit{ws}@[p]){\in}\mathit{trcl}\ (\mathit{tr}\ (\mathit{rules}\ M)))) \wedge$
$(\forall P'.\ \mathit{is\text{-}inv}\ (\mathit{ps\text{-}R}\ M\ A)\ (\delta\ A)\ P' \longrightarrow P'\ D))$
— We show the thesis by proving that it is an invariant of the saturation procedure
⟨*proof*⟩

Helper lemma to clarify some subgoal in the precision proof:

lemma *trclAD-delta-update-inv*: $\mathit{trclAD}\ (A(\!|\delta{:=}X|\!))\ D = \mathit{trclAD}\ A\ D$ ⟨*proof*⟩

The precision is proved as an invariant of the saturation algorithm:

theorem (**in** *MFSM*) *precise-inv*:
shows $\mathit{is\text{-}inv}\ (\mathit{ps\text{-}R}\ M\ A)\ (\delta\ A)\ (\lambda D.\ (\mathit{lang}\ (A(\!|\delta{:=}D|\!)) \subseteq \mathit{pre}^*\ (\mathit{rules}\ M)\ A) \wedge (\forall P'.\ \mathit{is\text{-}inv}\ (\mathit{ps\text{-}R}\ M\ A)\ (\delta\ A)\ P' \longrightarrow P'\ D))$
⟨*proof*⟩

As precision is an invariant of the saturation algorithm, and is trivial for the case of an already saturated initial automata, the result of the saturation algorithm is precise

corollary (**in** *MFSM*) *precise*: $[\![(\delta\ A,D){\in}\mathit{ndet\text{-}algo}\ (\mathit{ps\text{-}R}\ M\ A);\ x{\in}\mathit{lang}\ (A(\!|\ \delta{:=}D\ |\!))]\!] \Longrightarrow x{\in}\mathit{pre\text{-}star}\ (\mathit{rules}\ M)\ A$
⟨*proof*⟩

And finally we get correctness of the algorithm, with no restrictions on valid states

theorem (**in** *MFSM*) *correct*: $[\![(\delta\ A,D){\in}\mathit{ndet\text{-}algo}\ (\mathit{ps\text{-}R}\ M\ A)]\!] \Longrightarrow \mathit{lang}\ (A(\!|\ \delta{:=}D\ |\!)) = \mathit{pre\text{-}star}\ (\mathit{rules}\ M)\ A$ ⟨*proof*⟩

So the main results of this theory are, that the algorithm is defined for every possible initial automata

$\mathit{MFSM}\ ?M\ ?A \Longrightarrow \exists\, D.\ (\delta\ ?A,\ D) \in \mathit{ndet\text{-}algo}\ (\mathit{ps\text{-}R}\ ?M\ ?A)$

and returns the correct result

$[\![\mathit{MFSM}\ ?M\ ?A;\ (\delta\ ?A,\ ?D) \in \mathit{ndet\text{-}algo}\ (\mathit{ps\text{-}R}\ ?M\ ?A)]\!] \Longrightarrow \mathit{lang}\ (?A(\!|\delta := ?D|\!)) = \mathit{pre}^*\ (\mathit{rules}\ ?M)\ ?A$

We could also prove determination, i.e. the terminating state is uniquely determined by the initial state (though there may be many ways to get there). This is not really needed here, because for correctness, we do not look at the structure of the final automaton, but just at its language. The language of the final automaton is determined, as implied by *MFSM.correct*.

end

5 Non-executable implementation of the DPN pre*-algorithm

theory *DPN-impl*
imports *DPN*
begin

This theory is to explore how to prove the correctness of straightforward implementations of the DPN pre* algorithm. It does not provide an executable specification, but uses set-datatype and the SOME-operator to describe a deterministic refinement of the nondeterministic pre*-algorithm. This refinement is then characterized as a recursive function, using recdef.

This proof uses the same techniques to get the recursive function and prove its correctness as are used for the straightforward executable implementation in DPN_implEx. Differences from the executable specification are:

- The state of the algorithm contains the transition relation that is saturated, thus making the refinement abstraction just a projection onto this component. The executable specification, however, uses list representation of sets, thus making the refinement abstraction more complex.
- The termination proof is easier: In this approach, we only do recursion if our state contains a valid M-automata and a consistent transition relation. Using this property, we can infer termination easily from the termination of *ps-R*. The executable implementation does not check wether the state is valid, and thus may also do recursion for invalid states. Thus, the termination argument must also regard those invalid states, and hence must be more general.

5.1 Definitions

type-synonym (*'c,'l,'s,'m1,'m2*) *pss-state* = (((*'c,'l,'m1*) *DPN-rec-scheme* ∗ (*'s,'c,'m2*) *MFSM-rec-scheme*) ∗ (*'s,'c*) *LTS*)

Function to select next transition to be added

definition *pss-isNext* :: (*'c,'l,'m1*) *DPN-rec-scheme* ⇒ (*'s,'c,'m2*) *MFSM-rec-scheme* ⇒ (*'s,'c*) *LTS* ⇒ (*'s*∗*'c*∗*'s*) ⇒ *bool* **where**
pss-isNext M A D t == $t \notin D \land (\exists\, q\ p\ \gamma\ q'\ a\ c'.\ t=(sp\ A\ q\ p,\gamma,q') \land [p,\gamma] \hookrightarrow_a c' \in rules\ M \land (q,c',q') \in trclAD\ A\ D)$

definition *pss-next M A D == if* (∃ *t. pss-isNext M A D t*) *then Some* (*SOME t. pss-isNext M A D t*) *else None*

Next state selector function

definition
pss-next-state S == case S of ((*M*,*A*),*D*) ⇒ *if MFSM M A* ∧ *D*⊆*ps-upper M A then* (*case pss-next M A D of None* ⇒ *None* | *Some t* ⇒ *Some* ((*M*,*A*),*insert t D*)) *else None*

Relation describing the deterministic algorithm

definition
pss-R == graph pss-next-state

lemma *pss-nextE1*: *pss-next M A D = Some t* ⟹ *t*∉*D* ∧ (∃ *q p* γ *q′ a c′. t*=(*sp A q p*,γ,*q′*) ∧ $[p,\gamma]\hookrightarrow_a c'$ ∈ *rules M* ∧ (*q*,*c′*,*q′*)∈*trclAD A D*)
⟨*proof*⟩

lemma *pss-nextE2*: *pss-next M A D = None* ⟹ ¬(∃ *q p* γ *q′ a c′ t. t*∉*D* ∧ *t*=(*sp A q p*,γ,*q′*) ∧ $[p,\gamma]\hookrightarrow_a c'$ ∈ *rules M* ∧ (*q*,*c′*,*q′*)∈*trclAD A D*)
⟨*proof*⟩

lemmas (**in** *MFSM*) *pss-nextE = pss-nextE1 pss-nextE2*

The relation of the deterministic algorithm is also the recursion relation of the recursive characterization of the algorithm

lemma *pss-R-alt*[*termination-simp*]: *pss-R ==* {(((*M*,*A*),*D*),((*M*,*A*),*insert t D*)) | *M A D t. MFSM M A* ∧ *D*⊆*ps-upper M A* ∧ *pss-next M A D = Some t*}
⟨*proof*⟩

5.2 Refining *ps-R*

We first show that the next-step relation refines *ps-R M A*. From this, we will get both termination and correctness

Abstraction relation to project on the second component of a tuple, with fixed first component

definition α*snd f ==* { (*s*,(*f*,*s*)) | *s. True* }
lemma α*snd-comp-simp*: *R O* α*snd f =* {(*s*,(*f*,*s′*))| *s s′*. (*s*,*s′*)∈*R*} ⟨*proof*⟩

lemma α*sndI*[*simp*]: (*s*,(*f*,*s*))∈α*snd f* ⟨*proof*⟩
lemma α*sndE*: (*s*,(*f*,*s′*))∈α*snd f′* ⟹ *f*=*f′* ∧ *s*=*s′* ⟨*proof*⟩

Relation of *pss-next* and *ps-R M A*

lemma (**in** *MFSM*) *pss-cons1*: ⟦*pss-next M A D = Some t*; *D*⊆*ps-upper M A*⟧ ⟹ (*D*,*insert t D*)∈*ps-R M A* ⟨*proof*⟩
lemma (**in** *MFSM*) *pss-cons2*: *pss-next M A D = None* ⟹ *D*∉*Domain* (*ps-R M A*) ⟨*proof*⟩

lemma (**in** *MFSM*) *pss-cons1-rev*: ⟦*D*⊆*ps-upper M A*; *D*∉*Domain* (*ps-R M A*)⟧ ⟹ *pss-next M A D* = *None* ⟨*proof*⟩
lemma (**in** *MFSM*) *pss-cons2-rev*: ⟦*D*∈*Domain* (*ps-R M A*)⟧ ⟹ ∃ *t*. *pss-next M A D* = *Some t* ∧ (*D*,*insert t D*)∈*ps-R M A*
⟨*proof*⟩

The refinement result

theorem (**in** *MFSM*) *pss-refines*: *pss-R* $\leq_{\alpha snd\ (M,A)}$ (*ps-R M A*) ⟨*proof*⟩

5.3 Termination

We can infer termination directly from the well-foundedness of *ps-R* and *MFSM.pss-refines*

theorem *pss-R-wf*: *wf* (*pss-R*$^{-1}$)
⟨*proof*⟩

5.4 Recursive characterization

Having proved termination, we can characterize our algorithm as a recursive function

function *pss-algo-rec* :: ((*'c*,*'l*,*'s*,*'m1*,*'m2*) *pss-state*) ⇒ ((*'c*,*'l*,*'s*,*'m1*,*'m2*) *pss-state*)
where
pss-algo-rec ((*M*,*A*),*D*) = (*if* (*MFSM M A* ∧ *D*⊆*ps-upper M A*) *then* (*case* (*pss-next M A D*) *of None* ⇒ ((*M*,*A*),*D*) | (*Some t*) ⇒ *pss-algo-rec* ((*M*,*A*),*insert t D*)) *else* ((*M*,*A*),*D*))
⟨*proof*⟩

termination
⟨*proof*⟩

lemma *pss-algo-rec-newsimps*[*simp*]:
⟦*MFSM M A*; *D*⊆*ps-upper M A*; *pss-next M A D* = *None*⟧ ⟹ *pss-algo-rec* ((*M*,*A*),*D*) = ((*M*,*A*),*D*)
⟦*MFSM M A*; *D*⊆*ps-upper M A*; *pss-next M A D* = *Some t*⟧ ⟹ *pss-algo-rec* ((*M*,*A*),*D*) = *pss-algo-rec* ((*M*,*A*),*insert t D*)
¬*MFSM M A* ⟹ *pss-algo-rec* ((*M*,*A*),*D*) = ((*M*,*A*),*D*)
¬(*D* ⊆ *ps-upper M A*) ⟹ *pss-algo-rec* ((*M*,*A*),*D*) = ((*M*,*A*),*D*)
⟨*proof*⟩

declare *pss-algo-rec.simps*[*simp del*]

5.5 Correctness

The correctness of the recursive version of our algorithm can be inferred using the results from the locale *detRef-impl*

interpretation *det-impl*: *detRef-impl pss-algo-rec pss-next-state pss-R*

⟨*proof*⟩

theorem (**in** *MFSM*) *pss-correct*: *lang* (*A*⦇ *δ*:=*snd* (*pss-algo-rec* ((*M*,*A*),(*δ A*))) ⦈) = *pre-star* (*rules M*) *A*
⟨*proof*⟩

end

6 Tools for executable specifications

theory *ImplHelper*
imports *Main*
begin

6.1 Searching in Lists

Given a function *f* and a list *l*, return the result of the first element *e* ∈ *set l* with *f e* ≠ *None*. The functional code snippet *first-that f l* corresponds to the imperative code snippet: *for e in l do { if f e ≠ None then return Some (f e) }; return None*

primrec *first-that* :: (*'s* ⇒ *'a option*) ⇒ *'s list* ⇒ *'a option* **where**
  first-that f [] = *None*
| *first-that f* (*e#w*) = (*case f e of None* ⇒ *first-that f w* | *Some a* ⇒ *Some a*)

lemma *first-thatE1*: *first-that f l* = *Some a* ⟹ ∃ *e*∈*set l*. *f e* = *Some a*
  ⟨*proof*⟩

lemma *first-thatE2*: *first-that f l* = *None* ⟹ ∀ *e*∈*set l*. *f e* = *None*
  ⟨*proof*⟩

lemmas *first-thatE* = *first-thatE1 first-thatE2*

lemma *first-thatI1*: *e*∈*set l* ∧ *f e* = *Some a* ⟹ ∃ *a'*. *first-that f l* = *Some a'*
  ⟨*proof*⟩

lemma *first-thatI2*: ∀ *e*∈*set l*. *f e* = *None* ⟹ *first-that f l* = *None*
  ⟨*proof*⟩

lemmas *first-thatI* = *first-thatI1 first-thatI2*

end

7 Executable algorithms for finite state machines

theory *FSM-ex*
imports *FSM ImplHelper*
begin

The transition relation of a finite state machine is represented as a list of labeled edges

type-synonym $('s,'a)\ \mathit{delta} = ('s \times 'a \times 's)\ \mathit{list}$

7.1 Word lookup operation

Operation that finds some state q' that is reachable from state q with word w and has additional property P.

primrec $\mathit{lookup} :: ('s \Rightarrow \mathit{bool}) \Rightarrow ('s,'a)\ \mathit{delta} \Rightarrow 's \Rightarrow 'a\ \mathit{list} \Rightarrow 's\ \mathit{option}$ **where**
$\mathit{lookup}\ P\ d\ q\ [] = (\mathit{if}\ P\ q\ \mathit{then}\ \mathit{Some}\ q\ \mathit{else}\ \mathit{None})$
$|\ \mathit{lookup}\ P\ d\ q\ (e\#w) = \mathit{first\text{-}that}\ (\lambda t.\ \mathit{let}\ (qs,es,q')=t\ \mathit{in}\ \mathit{if}\ q{=}qs \wedge e{=}es\ \mathit{then}\ \mathit{lookup}\ P\ d\ q'\ w\ \mathit{else}\ \mathit{None})\ d$

lemma $\mathit{lookupE1}$: $!!q.\ \mathit{lookup}\ P\ d\ q\ w = \mathit{Some}\ q' \Longrightarrow P\ q' \wedge (q,w,q') \in \mathit{trcl}\ (\mathit{set}\ d)$
$\langle \mathit{proof} \rangle$

lemma $\mathit{lookupE2}$: $!!q.\ \mathit{lookup}\ P\ d\ q\ w = \mathit{None} \Longrightarrow \neg(\exists\, q'.\ (P\ q') \wedge (q,w,q') \in \mathit{trcl}\ (\mathit{set}\ d))$ $\langle \mathit{proof} \rangle$

lemma $\mathit{lookupI1}$: $[\![P\ q';\ (q,w,q'){\in}\mathit{trcl}\ (\mathit{set}\ d)]\!] \Longrightarrow \exists\, q'.\ \mathit{lookup}\ P\ d\ q\ w = \mathit{Some}\ q'$
$\langle \mathit{proof} \rangle$

lemma $\mathit{lookupI2}$: $\neg(\exists\, q'.\ P\ q' \wedge (q,w,q'){\in}\mathit{trcl}\ (\mathit{set}\ d)) \Longrightarrow \mathit{lookup}\ P\ d\ q\ w = \mathit{None}$
$\langle \mathit{proof} \rangle$

lemmas $\mathit{lookupE} = \mathit{lookupE1}\ \mathit{lookupE2}$
lemmas $\mathit{lookupI} = \mathit{lookupI1}\ \mathit{lookupI2}$

lemma $\mathit{lookup\text{-}trclAD\text{-}E1}$:
assumes map: $\mathit{set}\ d = D$ **and** start: $q{\in}Q\ A$ **and** cons: $D \subseteq Q\ A \times \Sigma\ A \times Q\ A$
assumes A: $\mathit{lookup}\ P\ d\ q\ w = \mathit{Some}\ q'$
shows $P\ q' \wedge (q,w,q'){\in}\mathit{trclAD}\ A\ D$
$\langle \mathit{proof} \rangle$

lemma $\mathit{lookup\text{-}trclAD\text{-}E2}$:
assumes map: $\mathit{set}\ d = D$
assumes A: $\mathit{lookup}\ P\ d\ q\ w = \mathit{None}$
shows $\neg\ (\exists\, q'.\ P\ q' \wedge (q,w,q'){\in}\mathit{trclAD}\ A\ D)$
$\langle \mathit{proof} \rangle$

lemma $\mathit{lookup\text{-}trclAD\text{-}I1}$: $[\![\mathit{set}\ d = D;\ (q,w,q'){\in}\mathit{trclAD}\ A\ D;\ P\ q']\!] \Longrightarrow \exists\, q'.\ \mathit{lookup}\ P\ d\ q\ w = \mathit{Some}\ q'$
$\langle \mathit{proof} \rangle$

lemma $\mathit{lookup\text{-}trclAD\text{-}I2}$: $[\![\mathit{set}\ d = D;\ q{\in}Q\ A;\ D \subseteq Q\ A \times \Sigma\ A \times Q\ A;\ \neg(\exists\, q'.\ P\ q' \wedge (q,w,q'){\in}\mathit{trclAD}\ A\ D)]\!] \Longrightarrow \mathit{lookup}\ P\ d\ q\ w = \mathit{None}$
$\langle \mathit{proof} \rangle$

lemmas *lookup-trclAD-E* = *lookup-trclAD-E1 lookup-trclAD-E2*
lemmas *lookup-trclAD-I* = *lookup-trclAD-I1 lookup-trclAD-I2*

7.2 Reachable states and alphabet inferred from transition relation

definition $states\ d == fst\ ‘\ (set\ d) \cup (snd{\circ}snd)\ ‘\ (set\ d)$
definition $alpha\ d == (fst{\circ}snd)\ ‘\ (set\ d)$

lemma *statesAlphaI*: $(q,a,q')\in set\ d \Longrightarrow q\in states\ d \wedge q'\in states\ d \wedge a\in alpha\ d$ $\langle proof\rangle$
lemma *statesE*: $q\in states\ d \Longrightarrow \exists\, a\ q'.\ ((q,a,q')\in set\ d \vee (q',a,q)\in set\ d)$ $\langle proof\rangle$
lemma *alphaE*: $a\in alpha\ d \Longrightarrow \exists\, q\ q'.\ (q,a,q')\in set\ d$ $\langle proof\rangle$

lemma *states-finite*: $finite\ (states\ d)$ $\langle proof\rangle$
lemma *alpha-finite*: $finite\ (alpha\ d)$ $\langle proof\rangle$

lemma *statesAlpha-subset*: $set\ d \subseteq states\ d \times alpha\ d \times states\ d$ $\langle proof\rangle$

lemma *states-mono*: $set\ d \subseteq set\ d' \Longrightarrow states\ d \subseteq states\ d'$ $\langle proof\rangle$
lemma *alpha-mono*: $set\ d \subseteq set\ d' \Longrightarrow alpha\ d \subseteq alpha\ d'$ $\langle proof\rangle$

lemma *statesAlpha-insert*: $set\ d' = insert\ (q,a,q')\ (set\ d) \Longrightarrow states\ d' = states\ d \cup \{q,q'\} \wedge alpha\ d' = insert\ a\ (alpha\ d)$
  $\langle proof\rangle$

lemma *statesAlpha-inv*: $[\![q\in states\ d;\ a\in alpha\ d;\ q'\in states\ d;\ set\ d'{=}insert\ (q,a,q')\ (set\ d)]\!] \Longrightarrow states\ d = states\ d' \wedge alpha\ d = alpha\ d'$
  $\langle proof\rangle$

export-code *lookup* **checking** *SML*

end

8 Implementation of DPN pre*-algorithm

theory *DPN-implEx*
imports *DPN FSM-ex*
begin

In this section, we provide a straightforward executable specification of the DPN-algorithm. It has a polynomial complexity, but is far from having optimal complexity.

8.1 Representation of DPN and M-automata

type-synonym $'c\ rule\text{-}ex = 'c{\times}'c{\times}'c{\times}'c\ list$

type-synonym *'c DPN-ex = 'c rule-ex list*

definition *rule-repr* == { $((p,\gamma,p',c'),(p\#[\gamma],a,p'\#c'))$ | $p\ \gamma\ p'\ c'\ a$. *True* }
definition *rules-repr* == { (l,l') . *rule-repr* ‘‘ *set* $l = l'$ }

lemma *rules-repr-cons*: ⟦ $(R,S)\in$*rules-repr* ⟧ $\Longrightarrow$ $((p,\gamma,p',c')\in$*set* $R) = (\exists\, a.\ (p\#[\gamma] \hookrightarrow_a p'\#c') \in S)$
⟨*proof*⟩

We define the mapping to sp-states explicitely, well-knowing that it makes the algorithm even more inefficient

definition *find-sp d s p == first-that (λt. let (sh,ph,qh)=t in if s=sh ∧ p=ph then Some qh else None) d*

This locale describes an M-automata together with its representation used in the implementation

locale *MFSM-ex = MFSM +*
fixes *R* **and** *D*
assumes *rules-repr*: *(R,rules M)∈rules-repr*
assumes *D-above*: *δ A ⊆ set D* **and** *D-below*: *set D ⊆ ps-upper M A*

This lemma exports the additional conditions of locale MFSM_ex to locale MFSM

lemma (**in** *MFSM*) *MFSM-ex-alt*: *MFSM-ex M A R D ⟷ (R,rules M)∈rules-repr ∧ δ A ⊆ set D ∧ set D ⊆ ps-upper M A*
⟨*proof*⟩

lemmas (**in** *MFSM-ex*) *D-between = D-above D-below*

The representation of the sp-states behaves as expected

lemma (**in** *MFSM-ex*) *find-sp-cons*:
assumes *A*: *s∈cstates A p∈csyms M*
shows *find-sp D s p = Some (sp A s p)*
⟨*proof*⟩

8.2 Next-element selection

The implementation goes straightforward by implementing a function to return the next transition to be added to the transition relation of the automata being saturated

```
definition sel-next:: 'c DPN-ex ⇒ ('s,'c) delta ⇒ ('s × 'c × 's) option where
  sel-next R D ==
    first-that (λr. let (p,γ,p',c') = r in
      first-that (λt. let (q,pp',sp') = t in
        if pp'=p' then
          case find-sp D q p of
            Some spt ⇒ (case lookup (λq'. (spt,γ,q') ∉ set D) D sp' c' of
          Some q′ ⇒ Some (spt,γ,q′) |
          None ⇒ None
        ) | - ⇒ None
      else None
    ) D
  ) R
```

The state of our algorithm consists of a representation of the DPN-rules and a representation of the transition relations of the automata being saturated

type-synonym *('c,'s) seln-state = 'c DPN-ex × ('s,'c) delta*

As long as the next-element function returns elements, these are added to the transition relation and the algorithm is applied recursively. *sel-next-state* describes the next-state selector function, and *seln-R* describes the corresponding recursion relation.

definition
sel-next-state S == let (R,D)=S in case sel-next R D of None ⇒ None | Some t ⇒ Some (R,t#D)

definition
seln-R == graph sel-next-state

lemma *seln-R-alt*: *seln-R == {((R,D),(R,t#D)) | R D t. sel-next R D = Some t}*
⟨*proof*⟩

8.3 Termination

8.3.1 Saturation upper bound

Before we can define the algorithm as recursive function, we have to prove termination, that is well-foundedness of the corresponding recursion relation *seln-R*

We start by defining a trivial finite upper bound for the saturation, simply as the set of all possible transitions in the automata. Intuitively, this bound is valid because the saturation algorithm only adds transitions, but never states to the automata

definition
seln-triv-upper R D == states D × ((fst∘snd) ‘ (set R) ∪ alpha D) × states D

lemma *seln-triv-upper-finite*: *finite (seln-triv-upper R D)* ⟨*proof*⟩

lemma *D-below-triv-upper*: *set D ⊆ seln-triv-upper R D* ⟨*proof*⟩

lemma *seln-triv-upper-subset-preserve*: *set D ⊆ seln-triv-upper A D′ ⟹ seln-triv-upper A D ⊆ seln-triv-upper A D′*
⟨*proof*⟩

lemma *seln-triv-upper-mono*: *set D ⊆ set D′ ⟹ seln-triv-upper R D ⊆ seln-triv-upper R D′*
⟨*proof*⟩

lemma *seln-triv-upper-mono-list*: *seln-triv-upper R D ⊆ seln-triv-upper R* (*t#D*) ⟨*proof*⟩
lemma *seln-triv-upper-mono-list′*: *x∈seln-triv-upper R D ⟹ x∈seln-triv-upper R* (*t#D*) ⟨*proof*⟩

The trivial upper bound is not changed by inserting a transition to the automata that was already below the upper bound

lemma *seln-triv-upper-inv*: ⟦*t∈seln-triv-upper R D*; *set D′ = insert t* (*set D*)⟧ ⟹ *seln-triv-upper R D = seln-triv-upper R D′*
⟨*proof*⟩

States returned by *find-sp* are valid states of the underlying automaton

lemma *find-sp-in-states*: *find-sp D s p = Some qh ⟹ qh∈states D* ⟨*proof*⟩

The next-element selection function returns a new transition, that is below the trivial upper bound

lemma *sel-next-below*:
assumes *A*: *sel-next R D = Some t*
shows *t∉set D ∧ t∈seln-triv-upper R D*
⟨*proof*⟩

Hence, it does not change the upper bound

corollary *sel-next-upper-preserve*: ⟦*sel-next R D = Some t*⟧ ⟹ *seln-triv-upper R D = seln-triv-upper R* (*t#D*) ⟨*proof*⟩

8.3.2 Well-foundedness of recursion relation

lemma *seln-R-wf*: *wf* ($seln\text{-}R^{-1}$) ⟨*proof*⟩

8.3.3 Definition of recursive function

function *pss-algo-rec* :: (*′c*,*′s*) *seln-state* ⇒ (*′c*,*′s*) *seln-state*
where *pss-algo-rec* (*R*,*D*) = (*case sel-next R D of Some t* ⇒ *pss-algo-rec* (*R*,*t#D*) | *None* ⇒ (*R*,*D*))
⟨*proof*⟩

termination
⟨*proof*⟩

lemma *pss-algo-rec-newsimps*[*simp*]:
⟦*sel-next R D = None*⟧ ⟹ *pss-algo-rec* (*R*,*D*) = (*R*,*D*)
⟦*sel-next R D = Some t*⟧ ⟹ *pss-algo-rec* (*R*,*D*) = *pss-algo-rec* (*R*,*t#D*)
⟨*proof*⟩

declare *pss-algo-rec.simps*[*simp del*]

8.4 Correctness

8.4.1 seln_R refines ps_R

We show that *seln-R* refines *ps-R*, that is that every step made by our implementation corresponds to a step in the nondeterministic algorithm, that we already have proved correct in theory DPN.

lemma (**in** *MFSM-ex*) *sel-nextE1*:
  assumes *A*: $\mathit{sel\text{-}next}\ R\ D = \mathit{Some}\ (s,\gamma,q')$
  shows $(s,\gamma,q') \notin \mathit{set}\ D \wedge (\exists\ q\ p\ a\ c'.\ s{=}\mathit{sp}\ A\ q\ p \wedge [p,\gamma] \hookrightarrow_a c' \in \mathit{rules}\ M \wedge (q,c',q') \in \mathit{trclAD}\ A\ (\mathit{set}\ D))$
⟨*proof*⟩

lemma (**in** *MFSM-ex*) *sel-nextE2*:
  assumes *A*: $\mathit{sel\text{-}next}\ R\ D = \mathit{None}$
  shows $\neg(\exists\ q\ p\ \gamma\ q'\ a\ c'\ t.\ t \notin \mathit{set}\ D \wedge t{=}(\mathit{sp}\ A\ q\ p,\gamma,q') \wedge [p,\gamma] \hookrightarrow_a c' \in \mathit{rules}\ M \wedge (q,c',q') \in \mathit{trclAD}\ A\ (\mathit{set}\ D))$
⟨*proof*⟩

lemmas (**in** *MFSM-ex*) *sel-nextE* = *sel-nextE1 sel-nextE2*

lemma (**in** *MFSM-ex*) *seln-cons1*: $[\![\mathit{sel\text{-}next}\ R\ D = \mathit{Some}\ t]\!] \Longrightarrow (\mathit{set}\ D,\mathit{insert}\ t\ (\mathit{set}\ D)) \in \mathit{ps\text{-}R}\ M\ A$ ⟨*proof*⟩
lemma (**in** *MFSM-ex*) *seln-cons2*: $\mathit{sel\text{-}next}\ R\ D = \mathit{None} \Longrightarrow \mathit{set}\ D \notin \mathit{Domain}\ (\mathit{ps\text{-}R}\ M\ A)$ ⟨*proof*⟩

lemma (**in** *MFSM-ex*) *seln-cons1-rev*: $[\![\mathit{set}\ D \notin \mathit{Domain}\ (\mathit{ps\text{-}R}\ M\ A)]\!] \Longrightarrow \mathit{sel\text{-}next}\ R\ D = \mathit{None}$ ⟨*proof*⟩
lemma (**in** *MFSM-ex*) *seln-cons2-rev*: $[\![\mathit{set}\ D \in \mathit{Domain}\ (\mathit{ps\text{-}R}\ M\ A)]\!] \Longrightarrow \exists\, t.\ \mathit{sel\text{-}next}\ R\ D = \mathit{Some}\ t \wedge (\mathit{set}\ D,\mathit{insert}\ t\ (\mathit{set}\ D)) \in \mathit{ps\text{-}R}\ M\ A$
  ⟨*proof*⟩

DPN-specific abstraction relation, to associate states of deterministic algorithm with states of *ps-R*

definition $\alpha\mathit{seln}\ M\ A == \{\ (\mathit{set}\ D,\ (R,D))\ |\ D\ R.\ \mathit{MFSM\text{-}ex}\ M\ A\ R\ D\}$

lemma *αselnI*: $[\![S{=}\mathit{set}\ D;\ \mathit{MFSM\text{-}ex}\ M\ A\ R\ D]\!] \Longrightarrow (S,(R,D)) \in \alpha\mathit{seln}\ M\ A$
  ⟨*proof*⟩

lemma *αselnD*: $(S,(R,D)) \in \alpha\mathit{seln}\ M\ A \Longrightarrow S{=}\mathit{set}\ D \wedge \mathit{MFSM\text{-}ex}\ M\ A\ R\ D$
  ⟨*proof*⟩

lemma *αselnD'*: $(S,C) \in \alpha\mathit{seln}\ M\ A \Longrightarrow S{=}\mathit{set}\ (\mathit{snd}\ C) \wedge \mathit{MFSM\text{-}ex}\ M\ A\ (\mathit{fst}\ C)\ (\mathit{snd}\ C)$ ⟨*proof*⟩

lemma *αseln-single-valued*: $\mathit{single\text{-}valued}\ ((\alpha\mathit{seln}\ M\ A)^{-1})$
  ⟨*proof*⟩

theorem (**in** *MFSM*) *seln-refines*: *seln-R* $\leq_{\alpha seln\ M\ A}$ (*ps-R M A*) ⟨*proof*⟩

8.4.2 Computing transitions only

definition *pss-algo* :: *'c DPN-ex* ⇒ (*'s*,*'c*) *delta* ⇒ (*'s*,*'c*) *delta* **where** *pss-algo R D* ≡ *snd* (*pss-algo-rec* (*R*,*D*))

8.4.3 Correctness

We have to show that the next-state selector function's graph refines *seln-R*. This is trivial because we defined *seln-R* to be that graph

lemma *sns-refines*: *graph sel-next-state* $\leq_{Id}$ *seln-R* ⟨*proof*⟩

interpretation *det-impl*: *detRef-impl pss-algo-rec sel-next-state seln-R*
⟨*proof*⟩

And then infer correctness of the deterministic algorithm

theorem (**in** *MFSM-ex*) *pss-correct*:
assumes *D-init*: *set D* = *δ A*
shows *lang* (*A*⦇ *δ*:=*set* (*pss-algo R D*) ⦈) = *pre-star* (*rules M*) *A*
⟨*proof*⟩

corollary (**in** *MFSM*) *pss-correct*:
assumes *repr*: *set D* = *δ A* (*R*,*rules M*)∈*rules-repr*
shows *lang* (*A*⦇ *δ*:=*set* (*pss-algo R D*) ⦈) = *pre-star* (*rules M*) *A*
⟨*proof*⟩

Generate executable code

export-code *pss-algo* **checking** *SML*

end

References

[1] A. Bouajjani, M. Müller-Olm, and T. Touili. Regular symbolic analysis of dynamic networks of pushdown systems. In *Proc. of CONCUR'05*. Springer, 2005.