Formalized Theorems from the Paper “A Coalgebraic Decision Procedure for WS1S”

Dmitriy Traytel

January 20, 2015

lemma
  fixes I :: *interp*
  and $x\ y\ X$ :: *nat*
  and $\varphi\ \psi$ :: *formula*
  shows
  $I \Vdash T \longleftrightarrow \mathit{True}$
  $I \Vdash F \longleftrightarrow \mathit{False}$
  $I \Vdash (\mathit{FO}\ x) \longleftrightarrow I[x]_1 \neq \{\}$
  $I \Vdash (x < y) \longleftrightarrow \mathit{Min}\ (I[x]_1) < \mathit{Min}\ (I[y]_1) \wedge I[x]_1 \neq \{\} \wedge I[y]_1 \neq \{\}$
  $I \Vdash (x \in X) \longleftrightarrow \mathit{Min}\ (I[x]_1) \in I[X]_2 \wedge I[x]_1 \neq \{\} \wedge \mathit{finite}\ (I[X]_2)$
  $I \Vdash (\neg\ \varphi) \longleftrightarrow \neg\ (I \Vdash \varphi)$
  $I \Vdash (\varphi \vee \psi) \longleftrightarrow (I \Vdash \varphi \vee I \Vdash \psi)$
  $I \Vdash (\mathit{FAnd}\ \varphi\ \psi) \longleftrightarrow (I \Vdash \varphi \wedge I \Vdash \psi)$
  $I \Vdash (\exists_1\ \varphi) \longleftrightarrow (\exists P.\ \mathit{finite}\ P \wedge P{::}_{1as2}I \Vdash \varphi)$
  $I \Vdash (\exists_2\ \varphi) \longleftrightarrow (\exists P.\ \mathit{finite}\ P \wedge P{::}_{2}I \Vdash \varphi)$
  ⟨*proof*⟩

lemma
  fixes I :: *interp*
  and $x\ y\ X$ :: *nat*
  and $\varphi\ \psi$ :: *formula*
  shows
  $I \Vdash_< T \longleftrightarrow \mathit{True}$
  $I \Vdash_< F \longleftrightarrow \mathit{False}$
  $I \Vdash_< (\mathit{FO}\ x) \longleftrightarrow I[x]_1 \neq \{\}$
  $I \Vdash_< (x < y) \longleftrightarrow \mathit{Min}\ (I[x]_1) < \mathit{Min}\ (I[y]_1) \wedge I[x]_1 \neq \{\} \wedge I[y]_1 \neq \{\}$
  $I \Vdash_< (x \in X) \longleftrightarrow \mathit{Min}\ (I[x]_1) \in I[X]_2 \wedge I[x]_1 \neq \{\} \wedge \mathit{finite}\ (I[X]_2)$
  $I \Vdash_< (\neg\ \varphi) \longleftrightarrow \neg\ (I \Vdash_< \varphi)$
  $I \Vdash_< (\varphi \vee \psi) \longleftrightarrow (I \Vdash_< \varphi \vee I \Vdash_< \psi)$
  $I \Vdash_< (\mathit{FAnd}\ \varphi\ \psi) \longleftrightarrow (I \Vdash_< \varphi \wedge I \Vdash_< \psi)$
  $I \Vdash_< (\exists_1\ \varphi) \longleftrightarrow (\exists P.\ (\forall p \in P.\ p <\#\ I) \wedge P{::}_{1as2}I \Vdash_< \varphi)$
  $I \Vdash_< (\exists_2\ \varphi) \longleftrightarrow (\exists P.\ (\forall p \in P.\ p <\#\ I) \wedge P{::}_{2}I \Vdash_< \varphi)$
  ⟨*proof*⟩

lemma
  fixes I :: *interp*
  and $x\ y\ X$ :: *nat*
  and $\varphi\ \psi$ :: *formula*
  shows
  $I \models T \longleftrightarrow \mathit{True}$
  $I \models F \longleftrightarrow \mathit{False}$
  $I \models (\mathit{FO}\ x) \longleftrightarrow I[x]_1 \neq \{\}$
  $I \models (x < y) \longleftrightarrow \mathit{Min}\ (I[x]_1) < \mathit{Min}\ (I[y]_1) \wedge I[x]_1 \neq \{\} \wedge I[y]_1 \neq \{\}$
  $I \models (x \in X) \longleftrightarrow \mathit{Min}\ (I[x]_1) \in I[X]_2 \wedge I[x]_1 \neq \{\} \wedge \mathit{finite}\ (I[X]_2)$
  $I \models (\neg\ \varphi) \longleftrightarrow \neg\ (I \models \varphi)$

$I \models (\varphi \lor \psi) \longleftrightarrow (I \models \varphi \lor I \models \psi)$
$I \models (\mathit{FAnd}\ \varphi\ \psi) \longleftrightarrow (I \models \varphi \land I \models \psi)$
$I \models (\exists_1\ \varphi) \longleftrightarrow (\exists p.\ p{::}_1 I \models \varphi)$
$I \models (\exists_2\ \varphi) \longleftrightarrow (\exists P.\ \mathit{finite}\ P \land P{::}_2 I \models \varphi)$
$\langle \mathit{proof} \rangle$

lemma
fixes $I :: \mathit{interp}$
and $x\ y\ X :: \mathit{nat}$
and $\varphi\ \psi :: \mathit{formula}$
shows
$I \models_< T \longleftrightarrow \mathit{True}$
$I \models_< F \longleftrightarrow \mathit{False}$
$I \models_< (\mathit{FO}\ x) \longleftrightarrow I[x]_1 \neq \{\}$
$I \models_< (x < y) \longleftrightarrow \mathit{Min}\ (I[x]_1) < \mathit{Min}\ (I[y]_1) \land I[x]_1 \neq \{\} \land I[y]_1 \neq \{\}$
$I \models_< (x \in X) \longleftrightarrow \mathit{Min}\ (I[x]_1) \in I[X]_2 \land I[x]_1 \neq \{\} \land \mathit{finite}\ (I[X]_2)$
$I \models_< (\neg\ \varphi) \longleftrightarrow \neg\ (I \models_< \varphi)$
$I \models_< (\varphi \lor \psi) \longleftrightarrow (I \models_< \varphi \lor I \models_< \psi)$
$I \models_< (\exists_1\ \varphi) \longleftrightarrow (\exists p <\#\ I.\ p{::}_1 I \models_< \varphi)$
$I \models_< (\exists_2\ \varphi) \longleftrightarrow (\exists P.\ (\forall p \in P.\ p <\#\ I) \land P{::}_2 I \models_< \varphi)$
$\langle \mathit{proof} \rangle$

abbreviation *bisimilar* (**infix** $\sim$ *65*) **where**
$L \sim K \equiv (\exists R.\ R\ L\ K \land (\forall L'\ K'.\ R\ L'\ K' \longrightarrow$
$(([] \in L' \longleftrightarrow [] \in K') \land (\forall a.\ R\ (L')_a\ (K')_a))))$

theorem *Theorem1*:
fixes $L\ K :: {'a}\ \mathit{language}$
shows $L \sim K \Longrightarrow L = K$
$\langle \mathit{proof} \rangle$

lemma *Theorem2*:
fixes $\Sigma :: {'a}\ \mathit{list}$
and $L :: {'t} \Rightarrow {'a}\ \mathit{language}$
and $L' :: {'s} \Rightarrow {'a}\ \mathit{language}$
and $\iota :: {'s} \Rightarrow {'t}$
and $\delta :: {'a} \Rightarrow {'t} \Rightarrow {'t}$
and $\mathrm{o} :: {'t} \Rightarrow \mathit{bool}$
and $\mathit{wf} :: {'t} \Rightarrow \mathit{bool}$
assumes $\bigwedge s\ w.\ \mathit{wf}\ s \Longrightarrow w \in L\ s \Longrightarrow w \in \Sigma^*$
and $\bigwedge t.\ L\ (\iota\ t) = L'\ t$
and $\bigwedge s\ a.\ \mathit{wf}\ s \Longrightarrow a \in \mathit{set}\ \Sigma \Longrightarrow \mathit{wf}\ (\delta\ a\ s)$
and $\bigwedge s\ a.\ \mathit{wf}\ s \Longrightarrow a \in \mathit{set}\ \Sigma \Longrightarrow L\ (\delta\ a\ s) = (L\ s)_a$
and $\bigwedge s.\ \mathit{wf}\ s \Longrightarrow \mathrm{o}\ s \longleftrightarrow [] \in L\ s$
and $\bigwedge s.\ \mathit{wf}\ s \Longrightarrow \mathit{finite}\ \{\mathit{fold}\ \delta\ w\ s\ |w.\ w \in \Sigma^*\}$
and $\mathit{wf}\ (\iota\ s)\ \mathit{wf}\ (\iota\ s')$
shows $\mathit{bisim}\ \mathit{wf}\ \Sigma\ \iota\ \delta\ \mathrm{o}\ s\ s' \longleftrightarrow L'\ s = L'\ s'$
$\langle \mathit{proof} \rangle$

lemma *Theorem3*:
fixes $\varphi :: \mathit{formula}$
and $I :: \mathit{interp}$
and $a :: \mathit{bool\ list} \times \mathit{bool\ list}$
assumes $\mathit{wf}\ (\#_V\ I)\ \varphi$
and $\#_V\ I = |a|$
shows $I \models \delta\ a\ \varphi \longleftrightarrow \mathit{CONS}\ a\ I \models \varphi$
and $I \models_< \delta\ a\ \varphi \longleftrightarrow \mathit{CONS}\ a\ I \models_< \varphi$
$\langle \mathit{proof} \rangle$

lemma *Theorem4*:
  fixes φ :: *formula*
  shows *finite* $\{\ |fold\ \delta\ xs\ \varphi|_{ACI} \mid xs.\ True\}$
  ⟨*proof*⟩

lemma *Example1*:
  shows $|\delta\ ([False], [])\ (Ex_2\ (0 \in 0))|_{ACI} = Ex_2\ (0\ \in 0)$
  and $|\delta\ ([True], [])\ (Ex_2\ (0 \in 0))|_{ACI} = Ex_2\ (F \vee T)$
  and $|\delta\ ([False], [])\ (Ex_2\ (F \vee T))|_{ACI} = Ex_2\ (F \vee T)$
  and $|\delta\ ([True], [])\ (Ex_2\ (F \vee T))|_{ACI} = Ex_2\ (F \vee T)$
  ⟨*proof*⟩

lemma *Theorem5*:
  fixes φ :: *formula*
  shows *finite* $\{\ |fold\ \varrho\ xs\ \varphi|_{ACI} \mid xs.\ True\}$
  ⟨*proof*⟩

lemma *Theorem6*:
  fixes φ :: *formula*
  and I :: *interp*
  and a :: *bool list* $\times$ *bool list*
  assumes $wf\ (\#_V\ I)\ \varphi$
  and $\#_V\ I = |a|$
  shows $I \models_< \varrho\ a\ \varphi \longleftrightarrow SNOC\ a\ I \models_< \varphi$
  ⟨*proof*⟩

lemma *Theorem71*:
  fixes φ :: *formula*
  and I :: *interp*
  assumes $wf\ (\#_V\ I)\ \varphi$
  and $\#I = 0$
  shows $o_<\ \varphi \longleftrightarrow I \models_< \varphi$
  ⟨*proof*⟩

lemma *Theorem72*:
  fixes φ :: *formula*
  and I :: *interp*
  assumes $wf\ (\#_V\ I)\ \varphi$
  shows $I \models_< futurize\ (\#_V\ I)\ \varphi \longleftrightarrow$
    $(\exists k.\ (SNOC\ (zero\ (\#_V\ I))\ \hat{}\hat{}\ k)\ I \models_< \varphi)$
  ⟨*proof*⟩

lemma *Theorem73*:
  fixes φ :: *formula*
  and I :: *interp*
  assumes $wf\ (\#_V\ I)\ \varphi$
  shows $I \models_< \lfloor\varphi\rfloor_{(\#_V\ I)} \longleftrightarrow I \models \varphi$
  ⟨*proof*⟩

lemma *Theorem74*:
  fixes φ :: *formula*
  and I :: *interp*
  assumes $wf\ (\#_V\ I)\ \varphi$
  and $\#I = 0$
  shows $o\ (\#_V\ I)\ \varphi \longleftrightarrow I \models \varphi$
  ⟨*proof*⟩

lemma *language_def*:

$L\ n\ \varphi = \{enc\ I \mid I.\ I \Vdash \varphi \wedge \#_V\ I = n\}$
$L_<\ n\ \varphi = \{enc\ I \mid I.\ I \Vdash_< \varphi \wedge \#_V\ I = n\}$
$\mathcal{L}\ n\ \varphi = \{enc\ I \mid I.\ I \models \varphi \wedge (\forall x{\in}FOV\ \varphi.\ I[x]_1 \neq \{\}) \wedge \#_V\ I = n\}$
$\mathcal{L}_<\ n\ \varphi = \{enc\ I \mid I.\ I \models_< \varphi \wedge (\forall x{\in}FOV\ \varphi.\ I[x]_1 \neq \{\}) \wedge \#_V\ I = n\}$
$\langle proof \rangle$

lemma *Theorem8*:
$L\ n\ (RESTRICT\ \varphi) = \mathcal{L}\ n\ \varphi$
$L_<\ n\ (RESTRICT\ \varphi) = \mathcal{L}_<\ n\ \varphi$
$\langle proof \rangle$

lemma *Theorem9*:
fixes $\varphi\ \psi$ :: *formula*
and n :: *interp_size*
shows $eqv\ n\ \varphi\ \psi \Longrightarrow \mathcal{L}\ n\ \varphi = \mathcal{L}\ n\ \psi$
and $eqv_<\ n\ \varphi\ \psi \Longrightarrow \mathcal{L}_<\ n\ \varphi = \mathcal{L}_<\ n\ \psi$
$\langle proof \rangle$

lemma *Example2*:
shows $eqv\ \langle 1,\ 0 \rangle\ (Ex_2\ (0 \in 0))\ (FO\ 0)$
$\langle proof \rangle$