B Stack Extension Theorem

Definition 12.

$$classe(z,s,h) = \{s',h \mid [s' \mid z \to 42] = [s \mid z \to 42]\}$$

May be it's more clear to say that
$s\restriction_{dom(s)\setminus\{z\}}, h \in classe(z,s,h)$
$\forall v.[s \mid z \to v], h \in classe(z,s,h)$.

This is the $classe(z,s,h)$ is the set of states containing s,h and all states similar to s,h for everything but for z.

Definition 13. *For $z \in Var$, $X \in \mathcal{P}(S \times H)$,*

$$nodep(z,X) \triangleq True \text{ iff } \forall s,h \in X.classe(z,s,h) \subseteq X$$

We extend this definition to environnements:

$$nodep(z,\rho) \triangleq True \text{ iff } (\forall X_v \in dom(\rho).nodep(z,\rho(X_v)))$$

Notice that we have $\forall z.nodep(z,\emptyset)$

Theorem 4. *If* - $nodep(z,\rho)$ - $FV_v(P) \in dom(\rho)$ - $z \notin FV(P)$ - $[\![P]\!]_\rho$ *exists* *then* $nodep(z,[\![P]\!]_\rho)$.

Corollary 4. *If* - $z \notin FV(P)$ - $[\![P]\!]$ *exists* *then* $nodep(z,[\![P]\!])$.

The idea of the theorem would be, if P is v-closed, z does not occur free in P, then $\forall v.$ $(s,h \in [\![P]\!]$ iff $[s \mid z \to v], h \in [\![P]\!])$.

We could say it as, if z does not occur free in a v-closed formula, then set of states satisfying the formula does not have any particular values for z.

Proof (Cor. 4). Direct from Th. 4.□

Proof (Th. 4). THE PROOF IS ONLY MADE IF ALL THE lfp and gpf are for MONOTONIC FUNCTIONS. But this is the case for the *wlp* and *sp* formulas and for the example in the paper.

First notice that if $z \notin Var(E).[\![E]\!]^s = [\![E]\!]^{[s|z\to v]}$.
$[\![x]\!]^s = s(x) = [\![x]\!]^{[s|z\to v]}$
$[\![42]\!]^s = 42 = [\![42]\!]^{[s|z\to v]}$
$[\![True]\!]^s = true = [\![x]\!]^{[s|z\to v]}$
$[\![E_1 op E_2]\!]^s = [\![E_1]\!]^s op [\![E_2]\!]^s = [\![E_1]\!]^{[s|z\to v]} op [\![E_2]\!]^{[s|z\to v]} = [\![x]\!]^{[s|z\to v]}$

We proceed by induction on P. We do not write down when we use induction to have the conditions for $z \notin FV(...)$.

- $s, h \in [\![E_1 = E_2]\!]$
  iff $[\![E_1]\!]^s = [\![E_2]\!]^s$
  iff $[\![E_1]\!]^{[s|z \to v]} = [\![E_2]\!]^{[s|z \to v]})\}$
  iff $[s \mid z \to v], h \in [\![E_1 = E_2]\!]$
- $s, h \in [\![E \mapsto E_1, E_2]\!]$
  iff $dom(h) = \{[\![E]\!]^s\}$
  and $h([\![E]\!]^s) = \langle [\![E_1]\!]^s, [\![E_2]\!]^s \rangle$
  iff $dom(h) = \{[\![E]\!]^{[s|z \to v]}\}$
  and $h([\![E]\!]^{[s|z \to v]}) = \langle [\![E_1]\!]^{[s|z \to v]}, [\![E_2]\!]^{[s|z \to v]} \rangle$
  iff $[s \mid z \to v], h \in [\![E \mapsto E_1, E_2]\!]$
- $s, h \in [\![\texttt{false}]\!]$
  iff $s, h \in \emptyset$
  iff $[s \mid z \to v], h \in \emptyset$
  iff $[s \mid z \to v], h \in [\![\texttt{false}]\!]$
- $s, h \in [\![P \Rightarrow Q]\!]_\rho$
  iff $s, h \in (\top \setminus [\![P]\!]_\rho) \cup [\![Q]\!]_\rho$
  iff $[s \mid z \to v], h \in (\top \setminus \{s, h \mid [\![P]\!]_\rho) \cup [\![Q]\!]_\rho$ (ind.)
  iff $[s \mid z \to v], h \in [\![P \Rightarrow Q]\!]_\rho$
- $s, h \in [\![\exists x.P]\!]_\rho$ when $x \neq z$
  iff $\exists v'.[s \mid x \mapsto v'], h \in [\![P]\!]_\rho$
  iff $\exists v'.[s \mid x \mapsto v' \mid z \mapsto v], h \in [\![P]\!]_\rho$ (ind.)
  iff $\exists v'.[s \mid z \mapsto v \mid x \mapsto v'], h \in [\![P]\!]_\rho$
  iff $[s \mid z \to v], h \in [\![\exists x.P]\!]_\rho$
- $s, h \in [\![\exists z.P]\!]_\rho$
  iff $\exists v'.[s \mid z \mapsto v'], h \in [\![P]\!]_\rho$
  iff $\exists v'.[s \mid z \mapsto v \mid z \mapsto v'], h \in [\![P]\!]_\rho$
  iff $[s \mid z \to v], h \in [\![\exists z.P]\!]_\rho$
- $s, h \in [\![\texttt{emp}]\!]$
  iff $h = []$
  iff $[s \mid z \to v], h \in [\![\texttt{emp}]\!]$
- $s, h \in [\![P * Q]\!]_\rho$
  iff $\exists h_0, h_1.h_0 \sharp h_1, h = h_0 \cdot h_1$
  $s, h_0 \in [\![P]\!]_\rho$ and $s, h_1 [\![Q]\!]_\rho$
  iff $\exists h_0, h_1.h_0 \sharp h_1, h = h_0 \cdot h_1$
  $[s \mid z \to v], h_0 \in [\![P]\!]_\rho$ and $[s \mid z \to v], h_1 [\![Q]\!]_\rho$ (ind.)
  iff $[s \mid z \to v], h \in [\![P * Q]\!]_\rho$
- $s, h \in [\![P -\!\!* Q]\!]_\rho$
  iff $\forall h'., h_1.h' \sharp h.$ if $s, h \in [\![P]\!]_\rho$
  then $s, h \cdot h' \in [\![Q]\!]_\rho$
  iff $\forall h'., h_1.h' \sharp h.$ if $[s \mid z \to v], h \in [\![P]\!]_\rho$
  then $[s \mid z \to v], h \cdot h' \in [\![Q]\!]_\rho$ (ind.)
  iff $[s \mid z \to v], h \in [\![P -\!\!* Q]\!]_\rho$
- $s, h \in [\![X_v]\!]_\rho$
  iff $s, h \in \rho(X_v)$
  iff $[s \mid z \mapsto v], h \in \rho(X_v)$ (hyp.)
  iff $[s \mid z \mapsto v], h \in [\![X_v]\!]_\rho$

- $s, h \in [\![P[E/x]]\!]_\rho$
  iff $[s \mid x \to [\![E]\!]^s], h \in [\![P]\!]_\rho$
  iff $[s \mid x \to [\![E]\!]^s \mid z \mapsto v], h \in [\![P]\!]_\rho$ (ind.)
  iff $[s \mid z \mapsto v \mid x \to [\![E]\!]^s], h \in [\![P]\!]_\rho$ (hyp. $z \neq x$)
  iff $[s \mid z \mapsto v \mid x \to [\![E]\!]^{[s|z \mapsto v]}], h \in [\![P]\!]_\rho$ (hyp. $z \notin Var(E)$)
  iff $[s \mid z \mapsto v], h \in [\![P[E/x]]\!]_\rho$
- $s, h \in [\![\mu X_v.P]\!]_\rho$
  iff $s, h \in \mathrm{lfp}^{\subseteq}_{\emptyset} \lambda X.\ [\![P]\!]_{[\rho|X_v \to X]}$
  iff $[s \mid z \mapsto v], h \in \mathrm{lfp}^{\subseteq}_{\emptyset} \lambda X.\ [\![P]\!]_{[\rho|X_v \to X]}$ (proof below)
  iff $[s \mid z \mapsto v], h \in [\![\mu X_v.P]\!]_\rho$

  Let $A \triangleq \mathrm{lfp}^{\subseteq}_{\emptyset} \lambda X.\ [\![P]\!]_{[\rho|X_v \to X]}$, we want to prove *nodep*(z, A), we proceed by contradiction. Let $B \triangleq \{s, h \in A \mid [s \mid z \mapsto v], h \notin A\} \cup \{[s \mid z \mapsto v], h \in A \mid s, h \notin A\}$,
  Let $C \triangleq A \setminus B$, by construction is the biggest set such that *nodep*(z, C) and $C \subseteq A$
  since *nodep*(z, ρ) we then have *nodep*$(z, [\rho \mid X_v \to C])$, then by induction we have *nodep*$(z, [\![P]\!]_{[\rho|X_v \to C]})$.
  Let $F \triangleq \lambda X.\ [\![P]\!]_{[\rho|X_v \to X]}$, we have *nodep*$(z, F(C))$.
  ....
  If F is monotonic, then since $C \subseteq A$ we have $F(C) \subseteq F(A)$ and so $F(C) \subseteq A$, since by construction, C is the biggest set X such that $X \subseteq A$ and *nodep*(z, X), we have $F(C) \subseteq C$, then since A is the $\mathrm{lfp}^{\subseteq}_{\emptyset} F$, by Tarsky $A = \sqcap\{X \mid F(X) \subseteq X\}$, so we have $A \subseteq C$ and so $A = C$ and then *nodep*(z, A) as expected.
- $s, h \in [\![\nu X_v.P]\!]_\rho$
  iff $s, h \in \mathrm{gfp}^{\subseteq}_{\emptyset} \lambda X.\ [\![P]\!]_{[\rho|X_v \to X]}$
  iff $[s \mid z \mapsto v], h \in \mathrm{gfp}^{\subseteq}_{\emptyset} \lambda X.\ [\![P]\!]_{[\rho|X_v \to X]}$ (proof below)
  iff $[s \mid z \mapsto v], h \in [\![\nu X_v.P]\!]_\rho$

  Let $A \triangleq \mathrm{gfp}^{\subseteq}_{\emptyset} \lambda X.\ [\![P]\!]_{[\rho|X_v \to X]}$, we want to prove *nodep*(z, A), we proceed by contradiction. Let $C \triangleq \{s, h \mid \exists s', h \in A.[s' \mid z \mapsto 42] = [s \mid z \mapsto 42]\}$, by construction C is the smallest set such that *nodep*(z, C) and $A \subseteq C$
  since *nodep*(z, ρ) we then have *nodep*$(z, [\rho \mid X_v \to C])$, then by induction we have *nodep*$(z, [\![P]\!]_{[\rho|X_v \to C]})$.
  Let $F \triangleq \lambda X.\ [\![P]\!]_{[\rho|X_v \to X]}$, we have *nodep*$(z, F(C))$.
  ....
  If F is monotonic, then since $A \subseteq C$ we have $F(A) \subseteq F(C)$ and so $A \subseteq F(C)$, since by construction, C is the smallest set X such that $X \subseteq A$ and *nodep*(z, X), we have $C \subseteq F(C)$, then since A is the $\mathrm{gfp}^{\subseteq}_{\emptyset} F$, by Tarsky $A = \sqcup\{X \mid X \subseteq F(X)\}$, so we have $C \subseteq A$ and so $A = C$ and then *nodep*(z, A) as expected.

□