

# SNESL formalization

Dandan Xue

September 11, 2017

## 0 Level-0

Draft version 0.0.4: added the proof of the main correctness theorem (in process)

### 0.1 Source language syntax

(Ignore empty sequence for now)

Expressions:

$$e ::= x \mid \mathbf{let} \ x = e_1 \ \mathbf{in} \ e_2 \mid \phi(x_1, \dots, x_k) \mid \{e : x \ \mathbf{in} \ y \ \mathbf{using} \ \cdot\} \\ \phi = \mathbf{const}_n \mid \mathbf{iota} \mid \mathbf{plus}$$

Values:

$$n \in \mathbf{Z} \\ v ::= n \mid \{v_1, \dots, v_k\}$$

### 0.2 Type system

$$\tau ::= \mathbf{int} \mid \{\tau_1\}$$

Type environment  $\Gamma = [x_1 \mapsto \tau_1, \dots, x_i \mapsto \tau_i]$ .

- Expression typing rules:

Judgment  $\boxed{\Gamma \vdash e : \tau}$

$$\frac{}{\Gamma \vdash x : \tau} (\Gamma(x) = \tau) \qquad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Gamma[x \mapsto \tau_1] \vdash e_2 : \tau}{\Gamma \vdash \mathbf{let} \ x = e_1 \ \mathbf{in} \ e_2 : \tau} \\ \frac{\vdash \phi : (\tau_1, \dots, \tau_k) \rightarrow \tau}{\Gamma \vdash \phi(x_1, \dots, x_k) : \tau} ((\Gamma(x_i) = \tau_i)_{i=1}^k) \qquad \frac{[x \mapsto \tau_1] \vdash e : \tau}{\Gamma \vdash \{e : x \ \mathbf{in} \ y \ \mathbf{using} \ \cdot\} : \{\tau\}} (\Gamma(y) = \{\tau_1\})$$

- Auxiliary Judgment  $\boxed{\vdash \phi : (\tau_1, \dots, \tau_k) \rightarrow \tau}$

$$\frac{}{\vdash \mathbf{const}_n : \mathbf{int}} \qquad \frac{}{\vdash \mathbf{iota} : \mathbf{int} \rightarrow \{\mathbf{int}\}} \qquad \frac{}{\vdash \mathbf{plus} : (\mathbf{int}, \mathbf{int}) \rightarrow \mathbf{int}}$$

- Value typing rules:

Judgment  $\boxed{\vdash v : \tau}$

$$\frac{}{\vdash n : \mathbf{int}} \qquad \frac{(\vdash v_i : \tau)_{i=1}^k}{\vdash \{v_1, \dots, v_k\} : \{\tau\}}$$

### 0.3 Source language semantics

$$\rho = [x_1 \mapsto v_1, \dots, x_i \mapsto v_i]$$

- Judgment  $\boxed{\rho \vdash e \downarrow v}$

$$\frac{}{\rho \vdash x \downarrow v} (\rho(x) = v) \quad \frac{\rho \vdash e_1 \downarrow v_1 \quad \rho[x \mapsto v_1] \vdash e_2 \downarrow v}{\rho \vdash \mathbf{let} \ e_1 = x \ \mathbf{in} \ e_2 \downarrow v}$$

$$\frac{\vdash \phi(v_1, \dots, v_k) \downarrow v}{\rho \vdash \phi(x_1, \dots, x_k) \downarrow v} ((\rho(x_i) = v_i)_{i=1}^k)$$

$$\frac{([x \mapsto v_i] \vdash e \downarrow v'_i)_{i=1}^k}{\rho \vdash \{e : x \ \mathbf{in} \ y \ \mathbf{using} \ \cdot\} \downarrow \{v'_1, \dots, v'_k\}} (\rho(y) = \{v_1, \dots, v_k\})$$

- Auxiliary Judgment  $\boxed{\vdash \phi(v_1, \dots, v_k) \downarrow v}$

$$\frac{}{\vdash \mathbf{const}_n() \downarrow n} \quad \frac{}{\vdash \mathbf{iota}(n) \downarrow \{0, 1, \dots, n-1\}} (n \geq 0)$$

$$\frac{}{\vdash \mathbf{plus}(n_1, n_2) \downarrow n_3} (n_3 = n_1 + n_2)$$

### 0.4 SVCODE syntax

- (1) Stream id:

$$s \in \mathbf{SId} = \mathbf{N} = \{0, 1, 2, \dots\}$$

- (2) Stream tree:

$$\mathbf{STree} \ni st ::= s \mid (st_1, s)$$

- (3) SVCODE operations:

$$\psi ::= \mathbf{Ctrl} \mid \mathbf{Const}_a \mid \mathbf{ToFlags} \mid \mathbf{Usum} \mid \mathbf{MapTwo}_{\oplus} \mid \mathbf{ScanPlus}$$

where  $\oplus$  stands for some binary operation on  $\mathbf{int}$ .

- (4) SVCODE program:

$$\begin{aligned} p ::= & \epsilon \\ & \mid s := \psi(s_1, \dots, s_i) \\ & \mid st := \mathbf{WithCtrl}(s, p) \\ & \mid p_1; p_2 \end{aligned}$$

- (5) Target language values:

$$\begin{aligned} b & \in \{\mathbf{T}, \mathbf{F}\} \\ a & ::= n \mid b \mid () \\ \vec{b} & = \langle b_1, \dots, b_i \rangle \\ \vec{a} & = \langle a_1, \dots, a_i \rangle \\ \mathbf{SVal} \ni w & ::= \vec{a} \mid (w, \vec{b}) \end{aligned}$$

- (6) Some notations and operations:

- For some  $a_0$  and  $\vec{a} = \langle a_1, \dots, a_i \rangle$ , let  $\langle a_0 | \vec{a} \rangle = \langle a_0, a_1, \dots, a_i \rangle$ .

- $++ : \mathbf{SVal} \rightarrow \mathbf{SVal} \rightarrow \mathbf{SVal}$   
 $\langle a_1, \dots, a_i \rangle ++ \langle a'_1, \dots, a'_i \rangle = \langle a_1, \dots, a_i, a'_1, \dots, a'_i \rangle$   
 $(w_1, \vec{b}_1) ++ (w_2, \vec{b}_2) = (w_1 ++ w_2, \vec{b}_1 ++ \vec{b}_2)$
- **sids** is a function that converts a  $st \in \mathbf{STree}$  to a set of  $s \in \mathbf{SId}$ :  
 $\mathbf{sids}(s) = \{s\}$   
 $\mathbf{sids}((st, s)) = \mathbf{sids}(st) \cup \{s\}$
- For some set of **SId**,  $t$ , and some  $s \in \mathbf{SId}$ , let  $t \leq s$  denote  $\forall s' \in t. s' < s$ .

## 0.5 SVCODE semantics

SVCODE runtime environment  $\sigma = [s_1 \mapsto \vec{a}_1, \dots, s_i \mapsto \vec{a}_i]$ .

We define some notations and operations related to  $\sigma$ :

(1) Let  $\sigma_1 \stackrel{\leq s}{=} \sigma_2$  denote  $\forall s' < s. \sigma_1(s') = \sigma_2(s')$ .

(2) Judgment  $\boxed{\sigma(st) = w}$

$$\frac{}{\sigma(s) = \vec{a}} \quad \frac{\sigma(st) = w \quad \overline{\sigma(s) = \vec{a}}}{\sigma((st, s)) = (w, \vec{a})}$$

**Definition 0.1.**  $\sigma_1 \stackrel{st}{\sim} \sigma_2$  iff

- (1)  $\text{dom}(\sigma_1) = \text{dom}(\sigma_2)$
- (2)  $\forall s \in (\text{dom}(\sigma_1) - \mathbf{sids}(st)). \sigma_1(s) = \sigma_2(s)$

It is easy to show that this relation  $\stackrel{st}{\sim}$  is commutative, transitive and associative.

**Definition 0.2.**  $\sigma_1 \stackrel{st}{\boxtimes} \sigma_2 = \sigma$  iff

- (1)  $\sigma_1 \stackrel{st}{\sim} \sigma_2$
- (2)  $\sigma(s) = \begin{cases} \sigma_1(s) ++ \sigma_2(s), & s \in \mathbf{sids}(st) \\ \sigma_1(s), & \text{otherwise} \end{cases}$

**Lemma 0.1.** If  $\sigma_1 \stackrel{st}{\sim} \sigma_2$ , then  $(\sigma_1 \stackrel{st}{\boxtimes} \sigma_3) \stackrel{st}{\sim} \sigma_2$ .

**Lemma 0.2** (?! wrong). If  $\sigma_1 \stackrel{st_1}{\sim} \sigma'_1$ ,  $\sigma_2 \stackrel{st_2}{\sim} \sigma'_2$ ,  $\sigma_1 \stackrel{\leq s}{=} \sigma_2$ , and  $\sigma'_1 \stackrel{\leq s}{=} \sigma'_2$  then  $\sigma_1 \stackrel{st_1}{\boxtimes} \sigma'_1 \stackrel{\leq s}{=} \sigma_2 \stackrel{st_2}{\boxtimes} \sigma'_2$ .

SVCODE operational semantics:

- Judgment  $\boxed{\langle p, \sigma \rangle \downarrow^{\vec{a}_c} \sigma'}$

$\vec{a}_c$  is the control stream.

$$\frac{}{\langle \epsilon, \sigma \rangle \downarrow^{\vec{a}_c} \sigma} \quad \frac{\psi(\vec{a}_1, \dots, \vec{a}_k) \downarrow^{\vec{a}_c} \vec{a}}{\langle s := \psi(s_1, \dots, s_k), \sigma \rangle \downarrow^{\vec{a}_c} \sigma[s \mapsto \vec{a}]} ((\sigma(s_i) = \vec{a}_i)_{i=1}^k)$$

$$\frac{}{\langle st := \text{WithCtrl}(s, p), \sigma \rangle \downarrow^{\vec{a}_c} \sigma[s_1 \mapsto \langle \rangle, \dots, s_i \mapsto \langle \rangle]} (\sigma(s) = \langle \rangle, \mathbf{sids}(st) = \{s_1, \dots, s_i\})$$

$$\frac{\langle p, \sigma \rangle \downarrow^{\vec{a}_s} \sigma''}{\langle st := \text{WithCtrl}(s, p), \sigma \rangle \downarrow^{\vec{a}_c} \sigma[s_1 \mapsto \sigma''(s_1), \dots, s_i \mapsto \sigma''(s_i)]} \left( \begin{array}{l} \sigma(s) = \vec{a}_s = \langle a_0 | \vec{a} \rangle \\ \mathbf{sids}(st) = \{s_1, \dots, s_i\} \end{array} \right)$$

$$\frac{\langle p_1, \sigma \rangle \downarrow^{\vec{a}_c} \sigma'' \quad \langle p_2, \sigma'' \rangle \downarrow^{\vec{a}_c} \sigma'}{\langle p_1; p_2, \sigma \rangle \downarrow^{\vec{a}_c} \sigma'}$$

- *Transducer semantics*:

$$\text{Judgment } \boxed{\psi(\vec{a}_1, \dots, \vec{a}_k) \downarrow^{\vec{a}_c} \vec{a}}$$

$$\frac{\psi(\vec{a}_{11}, \dots, \vec{a}_{k1}) \downarrow \vec{a}_1 \quad \psi(\vec{a}_{12}, \dots, \vec{a}_{k2}) \downarrow^{\vec{a}_c} \vec{a}_2}{\psi(\vec{a}_{11} ++ \vec{a}_{12}, \dots, \vec{a}_{k1} ++ \vec{a}_{k2}) \downarrow^{\langle a_0 | \vec{a}_c \rangle} \vec{a}} \quad (\vec{a} = \vec{a}_1 ++ \vec{a}_2)$$

$$\overline{\psi(\vec{a}_1, \dots, \vec{a}_k) \downarrow^{\langle \rangle} \langle \rangle}$$

- *Transducer block semantics*:

$$\text{Judgment } \boxed{\psi(\vec{a}_1, \dots, \vec{a}_k) \Downarrow \vec{a}}$$

$$\overline{\text{Const}_a \Downarrow \langle a \rangle} \quad \overline{\text{ToFlags}(\langle n \rangle) \Downarrow \langle F_1, \dots, F_n, T \rangle} \quad \overline{\text{MapTwo}_{\oplus}(\langle n_1 \rangle, \langle n_2 \rangle) \Downarrow \langle n_3 \rangle} \quad (n_3 = n_1 \oplus n_2)$$

$$\frac{\psi(\langle F \rangle, \dots, \vec{a}_{k1}) \Downarrow \vec{a}_1 \quad \psi(\vec{a}_{12}, \dots, \vec{a}_{k2}) \Downarrow \vec{a}_2}{\psi(\langle F \rangle ++ \vec{a}_{12}, \dots, \vec{a}_{k1} ++ \vec{a}_{k2}) \Downarrow \vec{a}} \quad (\vec{a} = \vec{a}_1 ++ \vec{a}_2)$$

$$\frac{\psi(\langle T \rangle, \dots, \vec{a}_k) \Downarrow \vec{a}}{\psi(\langle T \rangle, \dots, \vec{a}_k) \Downarrow \vec{a}}$$

- *Transducer unary semantics*:

$$\text{Judgment } \boxed{\psi(\langle b \rangle, \dots, \vec{a}_k) \Downarrow \vec{a}}$$

$$\overline{\text{Usum}(\langle F \rangle) \Downarrow \langle () \rangle} \quad \overline{\text{Usum}(\langle T \rangle) \Downarrow \langle \rangle}$$

- *Semantics of transducer block with accumulator*:

$$\text{Judgment } \boxed{\psi_n(\vec{a}_1, \dots, \vec{a}_k) \Downarrow \vec{a}}$$

$$\frac{\psi_{n_0}(\langle F \rangle, \dots, \vec{a}_{k1}) \Downarrow^{n'_0} \langle n_1 \rangle \quad \psi_{n'_0}(\vec{a}_{12}, \dots, \vec{a}_{k2}) \Downarrow \vec{a}_2}{\psi_{n_0}(\langle F \rangle ++ \vec{a}_{12}, \dots, \vec{a}_{k1} ++ \vec{a}_{k2}) \Downarrow \langle n_1 \rangle ++ \vec{a}_2}$$

$$\frac{\psi_{n_0}(\langle T \rangle, \dots, \vec{a}_k) \Downarrow \langle n_1 \rangle}{\psi_{n_0}(\langle T \rangle, \dots, \vec{a}_k) \Downarrow \langle n_1 \rangle}$$

- *Semantics of transducer unary with accumulator*:

$$\text{Judgment } \boxed{\psi_n(\langle F \rangle, \dots, \vec{a}_k) \Downarrow^{n'} \vec{a}}$$

$$\overline{\text{ScanPlus}_{n_0}(\langle F \rangle, \langle n \rangle) \Downarrow^{n_0+n} \langle n_0 \rangle}$$

$$\text{Judgment } \boxed{\psi_n(\langle T \rangle, \dots, \vec{a}_k) \Downarrow \vec{a}}$$

$$\overline{\text{ScanPlus}_{n_0}(\langle T \rangle, \langle \rangle) \Downarrow \langle n_0 \rangle}$$

**Theorem 0.1** (SVCODE determinism). *If  $\langle p, \sigma \rangle \downarrow^{\vec{a}_c} \sigma'$  and  $\langle p, \sigma \rangle \downarrow^{\vec{a}_c} \sigma''$ , then  $\sigma' = \sigma''$ .*

**Lemma 0.3** (??). If  $\sigma_1 \stackrel{st}{\sim} \sigma_2$ , (!!should have:  $\text{import}(p) = st$ )  $\langle p, \sigma_1 \rangle \downarrow^{\vec{a}_1} \sigma'_1$ ,  $\langle p, \sigma_2 \rangle \downarrow^{\vec{a}_2} \sigma'_2$ , then  $\langle p, \sigma_1 \bowtie \sigma_2 \rangle \downarrow^{\vec{a}_1 ++ \vec{a}_2} \sigma'_1 \bowtie \sigma'_2$

**Definition 0.3.**  $\vec{a}$  is a prefix of  $\vec{a}'$  if  $\vec{a} \sqsubseteq \vec{a}'$ .

$$\text{Judgment } \boxed{\vec{a} \sqsubseteq \vec{a}'}$$

$$\frac{}{\langle \rangle \sqsubseteq \vec{a}} \quad \frac{\vec{a} \sqsubseteq \vec{a}'}{\langle a_0 | \vec{a} \rangle \sqsubseteq \langle a_0 | \vec{a}' \rangle}$$

**Lemma 0.4.** If

- (i)  $(\vec{a}'_i \sqsubseteq \vec{a}_i)_{i=1}^k$  and  $\psi(\vec{a}'_1, \dots, \vec{a}'_k) \downarrow \vec{a}'$ ,
- (ii)  $(\vec{a}''_i \sqsubseteq \vec{a}_i)_{i=1}^k$  and  $\psi(\vec{a}''_1, \dots, \vec{a}''_k) \downarrow \vec{a}''$

then

- (i)  $(\vec{a}'_i = \vec{a}''_i)_{i=1}^k$
- (ii)  $\vec{a}' = \vec{a}''$ .

## 0.6 Translation

$$\delta = [x_1 \mapsto st_1, \dots, x_i \mapsto st_i]$$

- Judgment  $\boxed{\delta \vdash e \xRightarrow[s_1]{s_0} (p, st)}$

$$\frac{}{\delta \vdash x \xRightarrow[s_0]{s_0} (\epsilon, st)} \quad \frac{\delta \vdash e_1 \xRightarrow[s'_0]{s_0} (p_1, st_1) \quad \delta[x \mapsto st_1] \vdash e_2 \xRightarrow[s_1]{s'_0} (p_2, st)}{\delta \vdash \text{let } x = e_1 \text{ in } e_2 \xRightarrow[s_1]{s_0} (p_1; p_2, st)}$$

$$\frac{\vdash \phi(st_1, \dots, st_k) \xRightarrow[s_1]{s_0} (p, st)}{\delta \vdash \phi(x_1, \dots, x_k) \xRightarrow[s_1]{s_0} (p, st)} \quad ((\delta(x_i) = st_i)_{i=1}^k)$$

$$\frac{[x \mapsto st_1] \vdash e \xRightarrow[s_1]{s_0+1} (p, st)}{\delta \vdash \{e : x \text{ in } y \text{ using } \cdot\} \xRightarrow[s_1]{s_0} (s_0 := \text{Usum}(s_2); st := \text{WithCtrl}(s_0, p), (st, s_2))} \quad (\delta(y) = (st_1, s_2))$$

- Auxiliary Judgment  $\boxed{\vdash \phi(st_1, \dots, st_k) \xRightarrow[s_1]{s_0} (p, st)}$

$$\frac{}{\text{const}_a() \xRightarrow[s_0]{s_0+1} (s_0 := \text{Const}_a, s_0)}$$

$$\frac{\text{iota}(s) \xRightarrow[s_0]{s_4} (p, (s_3, s_0))}{\left( \begin{array}{l} s_{i+1} = s_i + 1 \\ p = s_0 := \text{ToFlags}(s); \\ s_1 := \text{Usum}(s_0); \\ s_2 := \text{WithCtrl}(s_1, s_2 := \text{Const}_1); \\ s_3 := \text{ScanPlus}(s_0, s_2) \end{array} \right)}$$

$$\frac{}{\text{plus}(s_1, s_2) \xRightarrow[s_0]{s_0+1} (s_0 := \text{MapTwo}_+(s_1, s_2), s_0)}$$

## 0.7 Value representation

- Judgment  $\boxed{v \triangleright_{\tau} w}$

$$\frac{}{n \triangleright_{\text{int}} \langle n \rangle} \quad \frac{(v_i \triangleright_{\tau} w_i)_{i=1}^k}{\{v_1, \dots, v_k\} \triangleright_{\{\tau\}} (w, \langle \mathbf{F}_1, \dots, \mathbf{F}_k, \mathbf{T} \rangle)} (w = w_1 ++ w_2 ++ \dots ++ w_k)$$

**Lemma 0.5.** *If  $v \triangleright_{\tau} w$ ,  $v' \triangleright_{\tau} w$ , then  $v = v'$ .*

## 0.8 Correctness proof

**Lemma 0.6** (???). *If  $\Gamma \vdash e : \{\tau\}$ ,  $\rho \vdash e \downarrow \{v_1, \dots, v_k\}$ , and  $\delta \vdash e \xrightarrow[s_1]{s_0} (p, (st, s))$ , then  $s \notin \mathbf{sids}(st)$ .*

**Lemma 0.7.** *If*

$$(i) \vdash \phi : (\tau_1, \dots, \tau_k) \rightarrow \tau$$

$$(ii) \vdash \phi(v_1, \dots, v_k) \downarrow v$$

$$(iii) \vdash \phi(st_1, \dots, st_k) \xrightarrow[s_1]{s_0} (p, st)$$

$$(iv) (v_i \triangleright_{\tau_i} st_i)_{i=1}^k$$

$$(v) \bigcup_{i=1}^k \mathbf{sids}(st_i) \leq s_0$$

*then*

$$(i) \langle p, \sigma \rangle \downarrow^{\vec{a}_c} \sigma' \text{ (by } \mathcal{P} \text{)}$$

$$(ii) v \triangleright_{\tau} \sigma'(st) \text{ (by } \mathcal{V} \text{)}$$

$$(iii) \sigma' \xrightarrow{s_0} \sigma$$

$$(iv) s_0 \leq s_1$$

$$(v) \mathbf{sids}(st) \leq s_1$$

**Theorem 0.2.** *If*

$$(i) \Gamma \vdash e : \tau \text{ (by some derivation } \mathcal{T} \text{)}$$

$$(ii) \rho \vdash e \downarrow v \text{ (by } \mathcal{E} \text{)}$$

$$(iii) \delta \vdash e \xrightarrow[s_1]{s_0} (p, st) \text{ (by } \mathcal{C} \text{)}$$

$$(iv) \forall x \in \text{dom}(\Gamma). \vdash \rho(x) : \Gamma(x) \wedge \mathbf{sids}(\delta(x)) \leq s_0 \wedge \rho(x) \triangleright_{\Gamma(x)} \sigma(\delta(x))$$

**then**

$$(v) \langle p, \sigma \rangle \downarrow^{(\cdot)} \sigma' \text{ (by } \mathcal{P} \text{)}$$

$$(vi) v \triangleright_{\tau} \sigma'(st) \text{ (by } \mathcal{V} \text{)}$$

$$(vii) \sigma' \xrightarrow{s_0} \sigma$$

$$(viii) s_0 \leq s_1$$

$$(ix) \mathbf{sids}(st) \leq s_1$$

*Proof.* By induction on the syntax of  $e$ .

- Case  $e = \{e_1 : x \text{ in } y \text{ using } \cdot\}$ .

We must have:

$$\begin{aligned}
\text{(i)} \quad \mathcal{T} &= \frac{\mathcal{T}_1}{\Gamma \vdash \{e_1 : x \text{ in } y \text{ using } \cdot\} : \{\tau_2\}} (\Gamma(y) = \{\tau_1\}) \\
\text{(ii)} \quad \mathcal{E} &= \frac{\mathcal{E}_i}{\rho \vdash \{e_1 : x \text{ in } y \text{ using } \cdot\} \downarrow \{v'_1, \dots, v'_k\}} (\rho(y) = \{v_1, \dots, v_k\}) \\
\text{(iii)} \quad \mathcal{C} &= \frac{\mathcal{C}_1}{\delta \vdash \{e_1 : x \text{ in } y \text{ using } \cdot\} \xrightarrow[s_1]{s_0} (s_0 := \text{Usum}(s_2); st_2 := \text{WithCtrl}(s_0, p_1), (st_2, s_2))} (\delta(y) = (st_1, s_2))
\end{aligned}$$

So  $p = (s_0 := \text{Usum}(s_2); st_2 := \text{WithCtrl}(s_0, p_1))$ ,  $\tau = \{\tau_2\}$ ,  $v = \{v'_1, \dots, v'_k\}$ ,  $st = (st_2, s_2)$ .

(iv)  $\vdash \rho(y) : \Gamma(y)$  gives us  $\vdash \{v_1, \dots, v_k\} : \{\tau_1\}$ , which must have the derivation:

$$\frac{(\vdash v_i : \tau_1)_{i=1}^k}{\vdash \{v_1, \dots, v_k\} : \{\tau_1\}} \quad (1)$$

$\text{sids}(\delta(y)) \leq s_0$  gives us

$$\text{sids}(\delta(y)) = \text{sids}((st_1, s_2)) = \text{sids}(st_1) \cup \{s_2\} \leq s_0 \quad (2)$$

$\rho(y) \triangleright_{\Gamma(y)} \sigma(\delta(y)) = \{v_1, \dots, v_k\} \triangleright_{\{\tau_1\}} \sigma((st_1, s_2))$  must have the derivation:

$$\frac{\mathcal{V}_i}{\{v_1, \dots, v_k\} \triangleright_{\{\tau_1\}} \sigma((st_1, s_2))} \quad (3)$$

where

$$\sigma(st_1) = w = w_1 ++ w_2 ++ \dots ++ w_k \quad (4)$$

and

$$\sigma(s_2) = \langle \mathbf{F}_1, \dots, \mathbf{F}_k, \mathbf{T} \rangle. \quad (5)$$

First we shall show:

- (v)  $\langle s_0 := \text{Usum}(s_2); st_2 := \text{WithCtrl}(s_0, p_1), \sigma \rangle \downarrow^{\langle () \rangle} \sigma'$
- (vi)  $\{v'_1, \dots, v'_k\} \triangleright_{\{\tau_2\}} \sigma'((st_2, s_2))$  by  $\mathcal{V}$ .

- (vii)  $\sigma' \xrightarrow{\leq s_0} \sigma$

**??TODO: proof of MP0**

Assume we already have  $\mathcal{P}_0$  of  $\langle s_0 := \text{Usum}(s_2), \sigma \rangle \downarrow^{\langle () \rangle} \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle]$

Then  $\mathcal{P}$  must have the shape:

$$\frac{\mathcal{P}_0 \quad \mathcal{P}_1}{\langle s_0 := \text{Usum}(s_2), \sigma \rangle \downarrow^{\langle () \rangle} \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle] \quad \langle st_2 := \text{WithCtrl}(s_0, p_1), \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle] \rangle \downarrow^{\langle () \rangle} \sigma'} \langle s_0 := \text{Usum}(s_2); st_2 := \text{WithCtrl}(s_0, p_1), \sigma \rangle \downarrow^{\langle () \rangle} \sigma'$$

Since we have

$$\begin{aligned}
\mathcal{T}_1 &= [x \mapsto \tau_1] \vdash e_1 : \tau_2 \\
\mathcal{E}_i &= [x \mapsto v_i] \vdash e_1 \downarrow v'_i
\end{aligned}$$

for  $i = 1, \dots, k$ , and

$$\mathcal{C}_1 = [x \mapsto st_1] \vdash e_1 \xrightarrow[s_1]{s_0+1} (p_1, st_2)$$

Let  $\Gamma_1 = [x \mapsto \tau_1]$ ,  $\rho_i = [x \mapsto v_i]$  and  $\delta_1 = [x \mapsto st_1]$ .  
From (1) and (2) it is clear that

$$\forall z \in \text{dom}(\Gamma_1). \vdash \rho_i(z) : \Gamma_1(z) \wedge \mathbf{sids}(\delta_1(z)) \leq s_0.$$

Let  $i$  range from 1 to  $k$ : we take  $\sigma_i \stackrel{st_1}{\sim} \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle]$  such that  $\sigma_i(st_1) = w_i$ .  
From  $\mathcal{V}_i$  in (3) we know that

$$\forall z \in \text{dom}(\Gamma_1). \rho_i(z) \triangleright_{\Gamma_1(z)} \sigma_i(\delta_1(z)).$$

Then by IH ( $k$  times) on  $\mathcal{T}_1$  with  $\mathcal{E}_i, \mathcal{C}_1$  we obtain the following result:

$$\langle \langle p_1, \sigma_i \rangle \downarrow^{()_i} \sigma'_i \rangle_{i=1}^k \tag{6}$$

$$(v'_i \triangleright_{\tau_2} \sigma'_i(st_2))_{i=1}^k \tag{7}$$

$$(\sigma'_i \stackrel{\leq s_0+1}{=} \sigma_i)_{i=1}^k \tag{8}$$

$$s_0 + 1 \leq s_1 \tag{9}$$

$$\mathbf{sids}(st_2) \leq s_1 \tag{10}$$

Assume  $\mathbf{sids}(st_2) = \{s'_1, \dots, s'_j\}$ .

Then there are two possibilities:

- Subcase  $k = 0$ , that is  $\sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle](s_0) = \langle \rangle$ .  
Then

$$\mathcal{P}_1 = \frac{\langle st_2 := \mathbf{WithCtrl}(s_0, p_1), \sigma \rangle \downarrow^{()_0} \sigma[s_0 \mapsto \langle \rangle, s'_1 \mapsto \langle \rangle, \dots, s'_j \mapsto \langle \rangle]}{\quad},$$

thus in this subcase

$$\sigma' = \sigma[s_0 \mapsto \langle \rangle, s'_1 \mapsto \langle \rangle, \dots, s'_j \mapsto \langle \rangle].$$

Since  $k = 0$ , then  $v = \{\}$ ,  $\sigma(s_2) = \langle \mathbf{T} \rangle$  (from (5)), and

$$\begin{aligned} \sigma'(s_2) &= \sigma(s_2) = \langle \mathbf{T} \rangle \text{ (?? not correct if } s_2 \in \mathbf{sids}(st_2)/\mathbf{sids}(st_1)), \\ \sigma'(st_2) &= \sigma[s_0 \mapsto \langle \rangle, s'_1 \mapsto \langle \rangle, \dots, s'_j \mapsto \langle \rangle](st_2) = (\dots((\langle \rangle, \langle \rangle)_1, \langle \rangle)_2, \dots)_{j-1}. \end{aligned}$$

Therefore  $\sigma'((st_2, s_2)) = (\sigma'(st_2), \sigma'(s_2))$ , with which we construct

$$\mathcal{V} = \overline{\{\} \triangleright_{\{\tau_2\}} ((\dots((\langle \rangle, \langle \rangle)_1, \dots)_{j-1}, \langle \mathbf{T} \rangle))}$$

as required.

Since  $k = 0$ , from (4) we know  $\forall s' \in \mathbf{sids}(st_1). \sigma(s') = \langle \rangle$ . For any  $s' \in \mathbf{sids}(st_2)$  and  $s' < s_0$ , it must have  $s' \in \mathbf{sids}(st_1)$  (because  $\text{codom}(\delta_1) = \{st_1\}$ ), hence  $\sigma(s') = \langle \rangle = \sigma'(s')$ . Therefore,

$$\sigma' \stackrel{\leq s_0}{=} \sigma.$$

- Subcase  $k > 0$ , that is  $\sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle] = \langle ()|\vec{a} \rangle$  for some  $\vec{a}$ .  
Then  $\mathcal{P}_1 =$

$$\frac{\langle p_1, \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle] \rangle \downarrow^{()_1, \dots, ()_k} \sigma''}{\langle st_2 := \mathbf{WithCtrl}(s_0, p_1), \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle] \rangle \downarrow^{()_0} \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle, s'_1 \mapsto \sigma''(s'_1), \dots, s'_j \mapsto \sigma''(s'_j)]}$$

So in this subcase

$$\sigma' = \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle, s'_1 \mapsto \sigma''(s'_1), \dots, s'_j \mapsto \sigma''(s'_j)].$$

Using Lemma 0.3 ( $k-1$ ) times on (6) gives us

$$\langle p_1, (\boxtimes_{i=1}^{st_1} \sigma_i)_{i=1}^k \rangle \downarrow^{()_1, \dots, ()_k} (\boxtimes_{i=1}^{st_2} \sigma'_i)_{i=1}^k$$



By Lemma 0.1 we can obtain

$$(\overset{st_1}{\boxtimes} \sigma_i)_{i=1}^k = \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle]. \quad (11)$$

Then by Theorem 0.1, we get

$$(\overset{st_2}{\boxtimes} \sigma'_i)_{i=1}^k = \sigma'' \quad (12)$$

Therefore,  $\sigma''(st_2) = \sigma'_1(st_2) ++ \dots ++ \sigma'_k(st_2)$  by Definition 0.2.

Let  $\sigma'_i(st_2) = w'_i$  and  $\sigma''(st_2) = w'$ , then  $w' = w'_1 ++ \dots ++ w'_k$ .

Since  $\sigma'(st_2) = \sigma''(st_2) = w'$ , and  $\sigma'(s_2) = \sigma(s_2) = \langle \mathbf{F}_1, \dots, \mathbf{F}_k, \mathbf{T} \rangle$ , (same problem) we now have  $\sigma'((st_2, s_2)) = (\sigma'(st_2), \sigma'(s_2)) = (w', \langle \mathbf{F}_1, \dots, \mathbf{F}_k, \mathbf{T} \rangle)$ , and we can construct

$$\mathcal{V} = \frac{(v'_i \triangleright_{\tau_2} w'_i)_{i=1}^k}{\{v'_1, \dots, v'_k\} \triangleright_{\{\tau_2\}} (w', \langle \mathbf{F}_1, \dots, \mathbf{F}_k, \mathbf{T} \rangle)}$$

as required.

From (11) we have  $\sigma_i \overset{st_1}{\sim} \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle]$ , and from (12)  $\sigma'_i \overset{st_2}{\sim} \sigma''$ .  
(8) implies

$$(\sigma'_i \overset{\leq s_0}{=} \sigma_i)_{i=1}^k$$

Using Lemma 0.2 (k-1) times, we obtain

$$\sigma'' \overset{\leq s_0}{=} \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle].$$

Therefore,  $\sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle, st_2 \mapsto \sigma''(st_2)] \overset{\leq s_0}{=} \sigma[s_0 \mapsto \langle ()_1, \dots, ()_k \rangle] \overset{\leq s_0}{=} \sigma$ .

(viii) TS:  $s_0 \leq s_1$

From (9) we immediately get  $s_0 \leq s_1 - 1 < s_1$ .

(ix) TS:  $\mathbf{sids}((st_2, s_2)) \leq s_1$

From (2) we know  $s_2 < s_0$ , thus  $s_2 < s_0 \leq s_1$ . And we already have (10). Therefore,

$$\mathbf{sids}((st_2, s_2)) = \mathbf{sids}(st_2) \cup \{s_2\} \leq s_1.$$

- Case  $e = x$ .
- Case  $e = \mathbf{let } x = e_1 \mathbf{ in } e_2$
- Case  $e = \phi(x_1, \dots, x_k)$

□