1 Syntax

The syntax ...

2 MiniSail type system

2.1 Refinement constraint logic

$\boxed{[\![l]\!] \sim rv}$

$$\frac{}{[\![n]\!] \sim num} \quad \text{EVAL\_LIT\_NUM}$$

$$\frac{}{[\![\mathbf{T}]\!] \sim \mathbf{true}} \quad \text{EVAL\_LIT\_TRUE}$$

$$\frac{}{[\![\mathbf{F}]\!] \sim \mathbf{false}} \quad \text{EVAL\_LIT\_FALSE}$$

$$\frac{}{[\![()]\!] \sim ()} \quad \text{EVAL\_LIT\_UNIT}$$

$\boxed{i[\![v]\!] \sim rv}$

$$\frac{[\![l]\!] \sim rv}{i[\![l]\!] \sim rv} \quad \text{EVAL\_V\_LIT}$$

$$\frac{rv = i(x)}{i[\![x]\!] \sim rv} \quad \text{EVAL\_V\_VAR}$$

$$\frac{\begin{array}{c} i[\![v_1]\!] \sim rv_1 \\ i[\![v_2]\!] \sim rv_2 \end{array}}{i[\![(v_1, v_2)]\!] \sim (rv_1, rv_2)} \quad \text{EVAL\_V\_PAIR}$$

$$\frac{i[\![v]\!] \sim rv}{i[\![\dot{ctor}\; tid\; v]\!] \sim \dot{ctor}\; tid\; rv} \quad \text{EVAL\_V\_CONS}$$

$$\frac{i[\![v]\!] \sim rv}{i[\![\dot{ctor}\; tid[b]v]\!] \sim \dot{ctor}\; tid\; b\; rv} \quad \text{EVAL\_V\_CONSP}$$

$\boxed{i[\![ce]\!] \sim rv}$

$$\frac{i[\![v]\!] \sim rv}{i[\![v]\!] \sim rv} \quad \text{EVAL\_CE\_VAL}$$

$$\frac{\begin{array}{c} i[\![v_1]\!] \sim rv_1 \\ i[\![v_2]\!] \sim rv_2 \\ rv = rv_1 + rv_2 \end{array}}{i[\![v_1 + v_2]\!] \sim rv} \quad \text{EVAL\_CE\_PLUS}$$

$$\frac{\begin{array}{c} i[\![v_1]\!] \sim rv_1 \\ i[\![v_2]\!] \sim rv_2 \\ rv = rv_1 \Leftarrow rv_2 \end{array}}{i[\![va1 \leq va2]\!] \sim rv} \quad \text{EVAL\_CE\_LEQ}$$

$$\frac{i[\![v_1]\!] \sim rv_1}{i[\![\mathbf{fst}\,(v_1, v_2)]\!] \sim rv_1} \quad \text{EVAL\_CE\_FST}$$

$$\frac{i[\![v_2]\!] \sim rv_2}{i[\![\mathbf{snd}\,(v_1, v_2)]\!] \sim rv_2} \quad \text{EVAL\_CE\_SND}$$

$$\frac{i[\![v_1]\!] \sim rv_1 \quad i[\![v_2]\!] \sim rv_2 \quad rv = rv_1 @ rv_2}{i[\![v_1 @ v_2]\!] \sim rv} \quad \text{EVAL\_CE\_CONCAT}$$

$$\frac{i[\![v]\!] \sim rv' \quad rv = \mathbf{len}\, rv'}{i[\![\mathbf{len}\, v_1]\!] \sim rv} \quad \text{EVAL\_CE\_LEN}$$

$\boxed{i[\![\phi]\!] \sim rv}$

$$\frac{i[\![ce_1]\!] \sim rv_1 \quad i[\![ce_2]\!] \sim rv_2 \quad rv = (rv_1 = rv_2)}{i[\![ce_1 = ce_2]\!] \sim rv} \quad \text{EVAL\_C\_EQ}$$

$$\frac{i[\![\phi_1]\!] \sim rv_1 \quad i[\![\phi_2]\!] \sim rv_2 \quad rv = rv_1 \wedge rv_2}{i[\![\phi_1 \wedge \phi_2]\!] \sim rv} \quad \text{EVAL\_C\_AND}$$

$$\frac{i[\![\phi]\!] \sim rv' \quad rv = \sim rv'}{i[\![\neg\phi]\!] \sim rv} \quad \text{EVAL\_C\_NOT}$$

$$\frac{i[\![\phi_1]\!] \sim rv_1 \quad i[\![\phi_2]\!] \sim rv_2 \quad rv = rv_1 \Longrightarrow rv_2}{i[\![\phi_1 \Longrightarrow \phi_2]\!] \sim rv} \quad \text{EVAL\_C\_IMP}$$

$\boxed{i \models \phi}$

$$\frac{i[\![\phi]\!] \sim \mathbf{true}}{i \models \phi} \quad \text{SATIS\_CA\_CA}$$

$\boxed{i \models \Gamma}$

$$\frac{}{i \models \cdot} \quad \text{SATIS\_G\_NIL}$$

$$\frac{i \models \Gamma \quad i \models \phi}{i \models \Gamma, x : b[\phi]} \quad \text{SATIS\_G\_CONS}$$

$\boxed{\Theta \vdash_{wf} rv : b}$

$$\frac{}{\Theta \vdash_{wf} \mathit{num} : \mathbf{int}} \quad \text{WF\_RCL\_V\_INT}$$

$$\frac{}{\Theta \vdash_{wf} \mathbf{true} : \mathbf{bool}} \quad \text{WF\_RCL\_V\_TRUE}$$

$$\frac{}{\Theta \vdash_{wf} \mathbf{false} : \mathbf{bool}} \quad \text{WF\_RCL\_V\_FALSE}$$

$$\frac{}{\Theta \vdash_{wf} () : \mathbf{unit}} \quad \text{WF\_RCL\_V\_UNIT}$$

$$\frac{}{\Theta \vdash_{wf} \mathbf{bitstr} : \mathbf{bvec}} \quad \text{WF\_RCL\_V\_BVEC}$$

$$\frac{\Theta \vdash_{wf} rv_1 : b_1 \quad \Theta \vdash_{wf} rv_2 : b_2}{\Theta \vdash_{wf} (rv_1, rv_2) : b_1 * b_2} \quad \text{WF\_RCL\_V\_PAIR}$$

$$\frac{\Theta \vdash_{wf} rv : b \quad \textbf{union}\, tid = \{\, \overline{\dot{ctor}_i : \tau_i}^{\,i} \,\} \in \Theta}{\Theta \vdash_{wf} \dot{ctor}_j\; tid\; rv : tid} \quad \text{WF\_RCL\_V\_CONS}$$

$$\frac{\Theta \vdash_{wf} rv : |\tau_j|_b[b_2/\beta] \quad \textbf{union}\, tid = \forall\, \beta.\{\, \overline{\dot{ctor}_i : \tau_i}^{\,i} \,\} \in \Theta}{\Theta \vdash_{wf} \dot{ctor}_j\; tid\; b_2\; rv : \textbf{bapp}\; tid\; b_2} \quad \text{WF\_RCL\_V\_CONSP}$$

$$\frac{}{\Theta \vdash_{wf} \textbf{usort}\; rv : \beta} \quad \text{WF\_RCL\_V\_BOXED}$$

$\boxed{\Theta; \Gamma \vdash i}$

$$\frac{}{\Theta; \cdot \vdash i} \quad \text{WF\_VAL\_EMPTY}$$

$$\frac{rv = i(x) \quad \Theta \vdash_{wf} rv : b}{\Theta; \Gamma, x : b[\phi] \vdash i} \quad \text{WF\_VAL\_CONS}$$

$\boxed{\Theta; B; \Gamma \models \phi}$

$$\frac{\Theta; B; \Gamma \vdash_{wf} \phi \quad \forall i. \Theta; \Gamma \vdash i \wedge i \models \Gamma \longrightarrow i \models \phi}{\Theta; B; \Gamma \models \phi} \quad \text{VALID\_VALID}$$

2.2 Wellformedness

$\boxed{\vdash_{wf} \Theta}$ Wellformedness for type definition context

$$\frac{}{\vdash_{wf} \cdot} \quad \text{THETA\_BEMPTY}$$

$$\frac{tid \notin \mathrm{dom}(\Theta) \quad \textbf{distinct}\; \dot{ctor}_1 \ldots \dot{ctor}_n \quad \dot{ctor}_1 \ldots \dot{ctor}_n \notin \Theta}{\vdash_{wf} \Theta, \textbf{union}\; tid = \{\dot{ctor}_1 : \tau_1, \ldots, \dot{ctor}_n : \tau_n\}} \quad \text{THETA\_BUNION}$$

$\boxed{\Theta; B \vdash_{wf} b}$ Wellformedness for base-type

$$\frac{\vdash_{wf} \Theta}{\Theta; B \vdash_{wf} \textbf{bool}} \quad \text{WF\_B\_BOOL}$$

$$\frac{\vdash_{wf} \Theta}{\Theta; B \vdash_{wf} \textbf{int}} \quad \text{WF\_B\_INT}$$

$$\frac{\vdash_{wf} \Theta}{\Theta; B \vdash_{wf} \textbf{unit}} \quad \text{WF\_B\_UNIT}$$

$$\frac{\vdash_{wf} \Theta}{\Theta; B \vdash_{wf} \textbf{bvec}} \quad \text{WF\_B\_BVEC}$$

$$\frac{\Theta; B \vdash_{wf} b_1 \quad \Theta; B \vdash_{wf} b_2}{\Theta; B \vdash_{wf} b_1 * b_2} \quad \text{WF\_B\_PAIR}$$

$$\frac{\vdash_{wf} \Theta \quad \mathbf{union}\; tid = \{\dot{ctor}_1 : \tau_1, .., \dot{ctor}_n : \tau_n\} \in \Theta}{\Theta; B \vdash_{wf} tid} \quad \text{WF\_B\_TID}$$

$$\frac{\beta \in B}{\Theta; B \vdash_{wf} \beta} \quad \text{WF\_B\_BVR}$$

$\boxed{\Theta \vdash_{wf} \Phi}$ Wellformedness for function definition context

$$\frac{f \notin \mathrm{dom}(\Phi) \quad \Theta; \cdot, \beta \vdash_{wf} b \quad \Theta; \cdot, \beta \vdash_{wf} x : b[\phi] \quad \Theta; \cdot, \beta; x : b[\phi] \vdash_{wf} \tau}{\Theta \vdash_{wf} \Phi, \mathbf{val}\, \forall\, \beta. f : (x : b[\phi]) \to \tau} \quad \text{WF\_P\_VALSPEC\_POLY}$$

$$\frac{f \notin \mathrm{dom}(\Phi) \quad \Theta; \cdot \vdash_{wf} b \quad \Theta; \cdot \vdash_{wf} x : b[\phi] \quad \Theta; \cdot; x : b[\phi] \vdash_{wf} \tau}{\Theta \vdash_{wf} \Phi, \mathbf{val}\, f : (x : b[\phi]) \to \tau} \quad \text{WF\_P\_VALSPEC}$$

$$\frac{\vdash_{wf} \Theta}{\Theta \vdash_{wf} \cdot} \quad \text{WF\_P\_EMPTY}$$

$\boxed{\Theta; B \vdash_{wf} \Gamma}$ Wellformedness for immutable variable context

$$\frac{\vdash_{wf} \Theta}{\Theta; B \vdash_{wf} \cdot} \quad \text{WF\_G\_EMPTY}$$

$$\frac{\Theta; B \vdash_{wf} \Gamma \quad \Theta; B \vdash_{wf} b \quad \Theta; B; \Gamma, x : b[\top] \vdash_{wf} \phi \quad x \notin \mathrm{dom}(\Gamma)}{\Theta; B \vdash_{wf} \Gamma, x : b[\phi]} \quad \text{WF\_G\_CONS}$$

$$\frac{\Theta; B \vdash_{wf} \Gamma \quad \Theta; B \vdash_{wf} b \quad x \notin \mathrm{dom}(\Gamma)}{\Theta; B \vdash_{wf} \Gamma, x : b[\top]} \quad \text{WF\_G\_CONS\_TRUE}$$

$$\frac{\Theta; B \vdash_{wf} \Gamma \quad \Theta; B \vdash_{wf} b \quad x \notin \mathrm{dom}(\Gamma)}{\Theta; B \vdash_{wf} \Gamma, x : b[\bot]} \quad \text{WF\_G\_CONS\_FALSE}$$

$\boxed{\Theta; B; \Gamma \vdash_{wf} \Delta}$ Wellformedness for mutable variable context

$$\frac{\Theta; B \vdash_{wf} \Gamma}{\Theta; B; \Gamma \vdash_{wf} \cdot} \quad \text{WF\_D\_EMPTY}$$

$$\frac{\begin{array}{c}\Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash_{wf} \tau \\ u \notin \mathrm{dom}(\Delta)\end{array}}{\Theta; B; \Gamma \vdash_{wf} \Delta, u : \tau} \quad \text{WF\_D\_CONS}$$

$\boxed{\Theta; B; \Gamma \vdash_{wf} v : b}$ WF for values

$$\frac{\begin{array}{c}\Theta; B \vdash_{wf} \Gamma \\ x : b[\phi] \in \Gamma\end{array}}{\Theta; B; \Gamma \vdash_{wf} x : b} \quad \text{WF\_V\_VAR}$$

$$\frac{\Theta; B \vdash_{wf} \Gamma}{\Theta; B; \Gamma \vdash_{wf} n : \mathbf{int}} \quad \text{WF\_V\_NUM}$$

$$\frac{\Theta; B \vdash_{wf} \Gamma}{\Theta; B; \Gamma \vdash_{wf} \mathbf{T} : \mathbf{bool}} \quad \text{WF\_V\_TRUE}$$

$$\frac{\Theta; B \vdash_{wf} \Gamma}{\Theta; B; \Gamma \vdash_{wf} \mathbf{F} : \mathbf{bool}} \quad \text{WF\_V\_FALSE}$$

$$\frac{\Theta; B \vdash_{wf} \Gamma}{\Theta; B; \Gamma \vdash_{wf} () : \mathbf{unit}} \quad \text{WF\_V\_UNIT}$$

$$\frac{\begin{array}{l}\Theta; B; \Gamma \vdash_{wf} v : |\tau_j|_b \\ \mathbf{union}\, \mathit{tid} = \{\, \overline{\dot{ctor}_i : \tau_i}^{\,i} \,\} \in \Theta\end{array}}{\Theta; B; \Gamma \vdash_{wf} \dot{ctor}_j\ \mathit{tid}\ v : \mathit{tid}} \quad \text{WF\_V\_CONS}$$

$$\frac{\begin{array}{l}\Theta; B; \Gamma \vdash_{wf} v : |\tau_j|_b[b_2/\beta] \\ \Theta; B \vdash_{wf} b_2 \\ \mathbf{union}\, \mathit{tid} = \forall\, \beta.\{\, \overline{\dot{ctor}_i : \tau_i}^{\,i} \,\} \in \Theta\end{array}}{\Theta; B; \Gamma \vdash_{wf} \dot{ctor}_j\ \mathit{tid}[b_2]v : \mathbf{bapp}\, \mathit{tid}\, b_2} \quad \text{WF\_V\_CONSP}$$

$$\frac{\begin{array}{c}\Theta; B; \Gamma \vdash_{wf} v_1 : b_1 \\ \Theta; B; \Gamma \vdash_{wf} v_2 : b_2\end{array}}{\Theta; B; \Gamma \vdash_{wf} (v_1, v_2) : b_1 * b_2} \quad \text{WF\_V\_PAIR}$$

$\boxed{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} e : b}$ WF for expressions

$$\frac{\begin{array}{l}\Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} v : b \\ \mathbf{val}\, f : (x : b[\phi]) \to \tau \in \Phi\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} f\, v : |\tau|_b} \quad \text{WF\_E\_APP}$$

$$\frac{\begin{array}{l}\Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} v : b_1[b_2/\beta] \\ \mathbf{val}\, \forall\, \beta.f : (x : b_1[\phi]) \to \tau \in \Phi\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} f[b_2]v : |\tau|_b[b_2/\beta]} \quad \text{WF\_E\_APP\_POLY}$$

$$\frac{\begin{array}{l}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash_{wf} v_1 : \mathbf{int} \\ \Theta; B; \Gamma \vdash_{wf} v_2 : \mathbf{int}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} v_1 + v_2 : \mathbf{int}} \quad \text{WF\_E\_PLUS}$$

$$\frac{\begin{array}{c}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash_{wf} v_1 : \mathbf{int} \\ \Theta; B; \Gamma \vdash_{wf} v_2 : \mathbf{int}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} v_1 \leq v_2 : \mathbf{bool}} \quad \text{WF\_E\_LEQ}$$

$$\frac{\begin{array}{c}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash_{wf} v : b_1 * b_2\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{fst}\, v : b_1} \quad \text{WF\_E\_FST}$$

$$\frac{\begin{array}{c}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash_{wf} v : b_1 * b_2\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{snd}\, v : b_2} \quad \text{WF\_E\_SND}$$

$$\frac{\begin{array}{c}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash_{wf} v : \mathbf{bvec}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{len}\, v : \mathbf{int}} \quad \text{WF\_E\_LEN}$$

$$\frac{\begin{array}{c}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash_{wf} v_1 : \mathbf{bvec} \\ \Theta; B; \Gamma \vdash_{wf} v_2 : \mathbf{bvec}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} v_1 @ v_2 : \mathbf{bvec}} \quad \text{WF\_E\_CONCAT}$$

$$\frac{\begin{array}{c}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash_{wf} v_1 : \mathbf{int} \\ \Theta; B; \Gamma \vdash_{wf} v_2 : \mathbf{bvec}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{split}\, v_1\, v_2 : \mathbf{bvec} * \mathbf{bvec}} \quad \text{WF\_E\_SPLIT}$$

$$\frac{\begin{array}{c}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ u : \tau \in \Delta\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} u : |\tau|_b} \quad \text{WF\_E\_MVAR}$$

$\boxed{\Theta; B; \Gamma \vdash_{wf} \phi}$ WF for constraints

$$\frac{\begin{array}{c}\Theta; B; \Gamma \vdash_{wf} \phi_1 \\ \Theta; B; \Gamma \vdash_{wf} \phi_2\end{array}}{\Theta; B; \Gamma \vdash_{wf} \phi_1 \wedge \phi_2} \quad \text{WF\_C\_CONJ}$$

$$\frac{\begin{array}{c}\Theta; B; \Gamma \vdash_{wf} \phi_1 \\ \Theta; B; \Gamma \vdash_{wf} \phi_2\end{array}}{\Theta; B; \Gamma \vdash_{wf} \phi_1 \Longrightarrow \phi_2} \quad \text{WF\_C\_IMP}$$

$$\frac{\begin{array}{c}\Theta; \cdot; B; \Gamma; \cdot \vdash_{wf} e_1 : b \\ \Theta; \cdot; B; \Gamma; \cdot \vdash_{wf} e_2 : b\end{array}}{\Theta; B; \Gamma \vdash_{wf} ce_1 = ce_2} \quad \text{WF\_C\_EQ}$$

$\boxed{\Theta; B; \Gamma \vdash_{wf} \tau}$ WF for types

$$\frac{\Theta; B; \Gamma, z : b[\top] \vdash_{wf} \phi}{\Theta; B; \Gamma \vdash_{wf} \{z : b | \phi\}} \quad \text{WF\_T\_TAU}$$

$\boxed{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} s : b}$ WF for statements

$$\frac{\begin{array}{l}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash_{wf} v : b\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} v : b} \quad \text{WF\_S\_VAL}$$

$$\frac{\begin{array}{l}u \notin \mathrm{dom}(\Delta) \\ \Theta; B; \Gamma \vdash_{wf} v : b_1 \\ \Theta; \Phi; B; \Gamma; \Delta, u : \tau \vdash_{wf} s : b_2\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{var}\, u : \tau := v\, \mathbf{in}\, s : b_2} \quad \text{WF\_S\_VAR}$$

$$\frac{\begin{array}{l}\Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ u : \{z : b|\phi\} \in \Delta \\ \Theta; B; \Gamma \vdash_{wf} v : b\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} u := v : \mathbf{unit}} \quad \text{WF\_S\_ASSIGN}$$

$$\frac{\begin{array}{l}\Theta; B; \Gamma \vdash_{wf} v : \mathbf{bool} \\ \Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} s_1 : b \\ \Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} s_2 : b\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{if}\, v\, \mathbf{then}\, s_1\, \mathbf{else}\, s_2 : b} \quad \text{WF\_S\_IF}$$

$$\frac{\begin{array}{l}x \# \Gamma \\ \Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} e : b_1 \\ \Theta; \Phi; B; \Gamma, x : b_1[\phi]; \Delta \vdash_{wf} s : b_2\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{let}\, x = e\, \mathbf{in}\, s : b_2} \quad \text{WF\_S\_LET}$$

$$\frac{\begin{array}{l}x \# \Gamma \\ \Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} s_1 : b_1 \\ \Theta; \Phi; B; \Gamma, x : b_1[\top]; \Delta \vdash_{wf} s_2 : b_2 \\ \Theta; B; \Gamma \vdash_{wf} \{z : b_1|\phi\}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{let}\ x : \{z : b_1|\phi\} = s_1\ \mathbf{in}\ s_2 : b_2} \quad \text{WF\_S\_LET2}$$

$$\frac{\begin{array}{l}\mathbf{union}\, tid = \{\, \overline{\dot{ctor}_i : \{z_i : b_i|\phi_i\}}^{\,i}\, \} \in \Theta \\ \Theta; B; \Gamma \vdash_{wf} v : tid \\ \overline{\Theta; \Phi; B; \Gamma, x_i : b_i[v = \dot{ctor}_i\, tid\, x_i \wedge \phi_i[x_i/z_i]]; \Delta \vdash_{wf} s_i : b}^{\,i}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{match}\, v\, \mathbf{of}\, \overline{\dot{ctor}_i\, x_i \Rightarrow s_i}^{\,i} : b} \quad \text{WF\_S\_MATCH}$$

$$\frac{\begin{array}{l}\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} s_1 : \mathbf{bool} \\ \Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} s_2 : \mathbf{unit}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{while}\, (s_1)\, \mathbf{do}\, \{s_2\} : \mathbf{unit}} \quad \text{WF\_S\_WHILE}$$

$$\frac{\begin{array}{l}\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} s_1 : \mathbf{unit} \\ \Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} s_2 : b\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} s_1; s_2 : b} \quad \text{WF\_S\_SEQ}$$

$$\frac{\begin{array}{l}x \# \Gamma \\ \Theta; B; \Gamma \vdash_{wf} \phi \\ \Theta; \Phi; B; \Gamma, x : \mathbf{bool}[\phi]; \Delta \vdash_{wf} s : b\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash_{wf} \mathbf{assert}\, \phi\, \mathbf{in}\, s : b} \quad \text{WF\_S\_ASSERT}$$

$\boxed{\Theta; B \vdash \Gamma_1 \sqsubseteq \Gamma_2}$ Γ_2 is an extension of Γ_1

$$\frac{\Theta; B \vdash_{wf} \Gamma}{\Theta; B \vdash \Gamma \sqsubseteq \Gamma} \quad \text{EXTEND\_G\_REFL}$$

$$\frac{\begin{array}{l}\Theta; B \vdash \Gamma_3 \sqsubseteq \Gamma_1, \Gamma_2 \\ x \notin \mathrm{dom}(\Gamma_1, \Gamma_2) \\ \Theta; B \vdash_{wf} \Gamma, x : b[\phi]\end{array}}{\Theta; B \vdash \Gamma_3 \sqsubseteq \Gamma_1, (\Gamma_2, x : b[\phi])} \quad \text{EXTEND\_G\_INSERT}$$

$\boxed{\Theta; B; \Gamma \vdash \Delta_2 \sqsubseteq \Delta_1}$ Δ_1 is an extension of Δ_2

$$\frac{\Theta; B; \Gamma \vdash_{wf} \Delta}{\Theta; B; \Gamma \vdash \Delta \sqsubseteq \Delta} \quad \text{EXTEND\_D\_REFL}$$

$$\frac{\begin{array}{l}\Theta; B; \Gamma \vdash \Delta_3 \sqsubseteq \Delta_1, \Delta_2 \\ u \notin \mathrm{dom}(\Delta_1, \Delta_2) \\ \Theta; B; \Gamma \vdash_{wf} \tau\end{array}}{\Theta; B; \Gamma \vdash \Delta_3 \sqsubseteq \Delta_1, (\Delta_2, u : \tau)} \quad \text{EXTEND\_D\_INSERT}$$

2.3 Subtyping

$\boxed{\Theta; B; \Gamma \vdash \tau_1 \lesssim \tau_2}$ Subtyping

$$\frac{\begin{array}{l}\Theta; B; \Gamma \vdash_{wf} \{z_1 : b|\phi_1\} \\ \Theta; B; \Gamma \vdash_{wf} \{z_2 : b|\phi_2\} \\ \Theta; B; \Gamma, z_3 : b[\phi_1[z_3/z_1]] \models \phi_2[z_3/z_1]\end{array}}{\Theta; B; \Gamma \vdash \{z_1 : b|\phi_1\} \lesssim \{z_2 : b|\phi_2\}} \quad \text{SUBTYPE\_ANF\_SUBTYPE}$$

2.4 Typing

$\boxed{\vdash l \Rightarrow \tau}$ Type synthesis for literals. Infer that type of l is τ

$$\frac{}{\vdash () \Rightarrow \{z : \mathbf{unit}|z = ()\}} \quad \text{INFER\_L\_UNIT}$$

$$\frac{}{\vdash \mathbf{T} \Rightarrow \{z : \mathbf{bool}|z = \mathbf{T}\}} \quad \text{INFER\_L\_TRUE}$$

$$\frac{}{\vdash \mathbf{F} \Rightarrow \{z : \mathbf{bool}|z = \mathbf{F}\}} \quad \text{INFER\_L\_FALSE}$$

$$\frac{}{\vdash n \Rightarrow \{z : \mathbf{int}|z = n\}} \quad \text{INFER\_L\_NUM}$$

$$\frac{}{\vdash bin \Rightarrow \{z : \mathbf{bvec}|z = bin\}} \quad \text{INFER\_L\_BVEC}$$

$\boxed{\Theta; B; \Gamma \vdash v \Rightarrow \tau}$ Type synthesis. Infer that type of v is τ

$$\frac{\begin{array}{l}z\#\Gamma \\ \Theta; B \vdash_{wf} \Gamma \\ x : b[\phi] \in \Gamma\end{array}}{\Theta; B; \Gamma \vdash x \Rightarrow \{z : b|z = x\}} \quad \text{INFER\_V\_ANF\_VAR}$$

$$\frac{\begin{array}{l}\vdash l \Rightarrow \tau \\ \Theta; B \vdash_{wf} \Gamma\end{array}}{\Theta; B; \Gamma \vdash l \Rightarrow \tau} \quad \text{INFER\_V\_ANF\_LIT}$$

$$\frac{\begin{array}{l} z\#\Gamma \\ \Theta; B; \Gamma \vdash v_1 \Rightarrow \{z_1 : b_1 | \phi_1\} \\ \Theta; B; \Gamma \vdash v_2 \Rightarrow \{z_2 : b_2 | \phi_2\} \end{array}}{\Theta; B; \Gamma \vdash (v_1, v_2) \Rightarrow \{z : b_1 * b_2 | z = (v_1, v_2)\}} \quad \text{INFER\_V\_ANF\_PAIR}$$

$$\frac{\begin{array}{l} z\#\Gamma \\ \textbf{union}\; tid = \{\; \overline{\dot{ctor}_i : \tau_i}^{\,i} \;\} \in \Theta \\ \Theta; B; \Gamma \vdash v \Leftarrow \tau \end{array}}{\Theta; B; \Gamma \vdash \dot{ctor}_j\; tid\; v \Rightarrow \{z : tid | z = \dot{ctor}_j\; tid\; v\}} \quad \text{INFER\_V\_ANF\_DATA\_CONS}$$

$$\frac{\begin{array}{l} z\#\Gamma \\ \textbf{union}\; tid = \forall\, \beta.\{\; \overline{\dot{ctor}_i : \tau_i}^{\,i} \;\} \in \Theta \\ \Theta; B; \Gamma \vdash v \Leftarrow \tau[b/\beta] \end{array}}{\Theta; B; \Gamma \vdash \dot{ctor}_j\; tid[b] v \Rightarrow \{z : tid | z = \dot{ctor}_j\; tid[b] v\}} \quad \text{INFER\_V\_ANF\_DATA\_CONS\_POLY}$$

$\boxed{\Theta; B; \Gamma \vdash v \Leftarrow \tau}$ Check that type of v is τ

$$\frac{\begin{array}{l} \Theta; B; \Gamma \vdash v \Rightarrow \{z_2 : b | \phi_2\} \\ \Theta; B; \Gamma \vdash \{z_2 : b | \phi_2\} \lesssim \{z_1 : b | \phi_1\} \end{array}}{\Theta; B; \Gamma \vdash v \Leftarrow \{z_1 : b | \phi_1\}} \quad \text{CHECK\_V\_ANF\_VAL}$$

$\boxed{\Theta; \Phi; B; \Gamma; \Delta \vdash e \Rightarrow \tau}$ Infer that type of e is τ

$$\frac{\begin{array}{l} z_3\#\Gamma \\ \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash v_1 \Rightarrow \{z_1 : \textbf{int} | \phi_1\} \\ \Theta; B; \Gamma \vdash v_2 \Rightarrow \{z_2 : \textbf{int} | \phi_2\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash v_1 + v_2 \Rightarrow \{z_3 : \textbf{int} | z_3 = v_1 + v_2\}} \quad \text{INFER\_E\_ANF\_PLUS}$$

$$\frac{\begin{array}{l} z_3\#\Gamma \\ \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash v_1 \Rightarrow \{z_1 : \textbf{int} | \phi_1\} \\ \Theta; B; \Gamma \vdash v_2 \Rightarrow \{z_2 : \textbf{int} | \phi_2\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash v_1 \leq v_2 \Rightarrow \{z_3 : \textbf{bool} | z_3 = va1 \leq va2\}} \quad \text{INFER\_E\_ANF\_LEQ}$$

$$\frac{\begin{array}{l} \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \textbf{val}\, f : (x : b[\phi]) \to \tau \in \Phi \\ \Theta; B; \Gamma \vdash v \Leftarrow \{z : b | \phi\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash f\, v \Rightarrow \tau[v/x]} \quad \text{INFER\_E\_ANF\_APP}$$

$$\frac{\begin{array}{l} \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \textbf{val} \forall\, \beta.f : (x : b[\phi]) \to \tau \in \Phi \\ \Theta; B; \Gamma \vdash v \Leftarrow \{z : b[b_2/\beta] | \phi\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash f[b_2] v \Rightarrow \tau[b_2/\beta][v/x]} \quad \text{INFER\_E\_ANF\_APP\_POLY}$$

$$\frac{\begin{array}{l} z\#\Gamma \\ \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash v \Rightarrow \{z : b_1 * b_2 | \phi\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \textbf{fst}\, v \Rightarrow \{z : b_1 | z = \textbf{fst}\, v\}} \quad \text{INFER\_E\_ANF\_FST}$$

$$\frac{\begin{array}{l} z\#\Gamma \\ \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash v \Rightarrow \{z : b_1 * b_2 | \phi\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{snd}\, v \Rightarrow \{z : b_2 | z = \mathbf{snd}\, v\}} \quad \text{INFER\_E\_ANF\_SND}$$

$$\frac{\begin{array}{l} z\#\Gamma \\ \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash v_1 \Rightarrow \{z_1 : \mathbf{bvec} | \phi_1\} \\ \Theta; B; \Gamma \vdash v_2 \Rightarrow \{z_2 : \mathbf{bvec} | \phi_2\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash v_1 @ v_2 \Rightarrow \{z : \mathbf{bvec} | z = v_1 @ v_2\}} \quad \text{INFER\_E\_ANF\_CONCAT}$$

$$\frac{\begin{array}{l} z\#\Gamma \\ \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash v_1 \Rightarrow \{z_1 : \mathbf{int} | \phi_1\} \\ \Theta; B; \Gamma \vdash v_2 \Rightarrow \{z_2 : \mathbf{bvec} | \phi_2\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{split}\, v_1\, v_2 \Rightarrow \{z : \mathbf{bvec} | v_2 = \mathbf{fst}\, z @ \mathbf{snd}\, z \wedge v_1 = \mathbf{len}\,(\mathbf{fst}\, z)\}} \quad \text{INFER\_E\_ANF\_SPLIT}$$

$$\frac{\begin{array}{l} z\#\Gamma \\ \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash v \Rightarrow \{z : \mathbf{bvec} | \phi\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{snd}\, v \Rightarrow \{z : b_2 | z = \mathbf{len}\, v\}} \quad \text{INFER\_E\_ANF\_LEN}$$

$$\frac{\begin{array}{l} \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ u : \tau \in \Delta \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash u \Rightarrow \tau} \quad \text{INFER\_E\_ANF\_MVAR}$$

$\boxed{\Theta; \Phi; B; \Gamma; \Delta \vdash e \Leftarrow \tau}$ Check that type of e is τ

$$\frac{\begin{array}{c} \Theta; \Phi; B; \Gamma; \Delta \vdash e \Rightarrow \{z_2 : b | \phi_2\} \\ \Theta; B; \Gamma \vdash \{z_2 : b | \phi_2\} \lesssim \{z_1 : b | \phi_1\} \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash e \Leftarrow \{z_1 : b | \phi_1\}} \quad \text{CHECK\_E\_ANF\_EXPR}$$

$\boxed{\Theta; \Phi; B; \Gamma; \Delta \vdash s \Leftarrow \tau}$ Check that type of s is τ

$$\frac{\begin{array}{l} \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ \Theta; B; \Gamma \vdash v \Leftarrow \tau \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash v \Leftarrow \tau} \quad \text{CHECK\_S\_VAL}$$

$$\frac{\begin{array}{l} u \notin \mathrm{dom}(\Delta) \\ \Theta; B; \Gamma \vdash v \Leftarrow \tau \\ \Theta; \Phi; B; \Gamma; \Delta, u : \tau \vdash s \Leftarrow \tau_2 \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{var}\, u : \tau := v\, \mathbf{in}\, s \Leftarrow \tau_2} \quad \text{CHECK\_S\_VAR}$$

$$\frac{\begin{array}{l} \Theta \vdash_{wf} \Phi \\ \Theta; B; \Gamma \vdash_{wf} \Delta \\ u : \tau \in \Delta \\ \Theta; B; \Gamma \vdash v \Leftarrow \tau \end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash u := v \Leftarrow \{z : \mathbf{unit} | \top\}} \quad \text{CHECK\_S\_ASSIGN}$$

$$\frac{\begin{array}{l}\Theta; B; \Gamma \vdash v \Rightarrow \{z : \mathbf{bool} | \phi_1\} \\ \Theta; \Phi; B; \Gamma; \Delta \vdash s_1 \Leftarrow \{z_1 : b | v = \mathbf{T} \implies \phi[z_1/z]\} \\ \Theta; \Phi; B; \Gamma; \Delta \vdash s_2 \Leftarrow \{z_2 : b | v = \mathbf{F} \implies \phi[z_2/z]\}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{if}\, v\, \mathbf{then}\, s_1\, \mathbf{else}\, s_2 \Leftarrow \{z : b | \phi\}} \quad \text{CHECK\_S\_IF}$$

$$\frac{\begin{array}{l}x \# \Gamma \\ \Theta; \Phi; B; \Gamma; \Delta \vdash e \Rightarrow \{z : b | \phi\} \\ \Theta; \Phi; B; \Gamma, x : b[\phi[x/z]]; \Delta \vdash s \Leftarrow \tau\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{let}\, x = e\, \mathbf{in}\, s \Leftarrow \tau} \quad \text{CHECK\_S\_LET}$$

$$\frac{\begin{array}{l}x \# \Gamma \\ \Theta; \Phi; B; \Gamma, x : \mathbf{bool}[\phi]; \Delta \vdash s \Leftarrow \tau\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{assert}\, \phi\, \mathbf{in}\, s \Leftarrow \tau} \quad \text{CHECK\_S\_ASSERT}$$

$$\frac{\begin{array}{l}x \# \Gamma \\ \Theta; \Phi; B; \Gamma; \Delta \vdash s_1 \Leftarrow \{z : b | \phi\} \\ \Theta; \Phi; B; \Gamma, x : b[\phi[x/z]]; \Delta \vdash s_2 \Leftarrow \tau\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{let}\ x : \{z : b | \phi\} = s_1\ \mathbf{in}\ s_2 \Leftarrow \tau} \quad \text{CHECK\_S\_LET2}$$

$$\frac{\begin{array}{l}\mathbf{union}\, tid = \{\, \overline{\dot{ctor}_i : \{z_i : b_i | \phi_i\}}^{\,i}\ \} \in \Theta \\ \Theta; B; \Gamma \vdash v \Rightarrow \{z : tid | \phi\} \\ \overline{\Theta; \Phi; B; \Gamma, x_i : b_i[v = \dot{ctor}_i\, tid\, x_i \wedge \phi_i[x_i/z_i]]; \Delta \vdash s_i \Leftarrow \tau}^{\,i}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{match}\, v\, \mathbf{of}\, \overline{\dot{ctor}_i\, x_i \Rightarrow s_i}^{\,i} \Leftarrow \tau} \quad \text{CHECK\_S\_MATCH}$$

$$\frac{\begin{array}{l}\Theta; \Phi; B; \Gamma; \Delta \vdash s_1 \Leftarrow \{z : \mathbf{bool} | \top\} \\ \Theta; \Phi; B; \Gamma; \Delta \vdash s_2 \Leftarrow \{z : \mathbf{unit} | \top\}\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{while}\, (s_1)\, \mathbf{do}\, \{s_2\} \Leftarrow \{z : \mathbf{unit} | \top\}} \quad \text{CHECK\_S\_WHILE}$$

$$\frac{\begin{array}{l}\Theta; \Phi; B; \Gamma; \Delta \vdash s_1 \Leftarrow \{z : \mathbf{unit} | \top\} \\ \Theta; \Phi; B; \Gamma; \Delta \vdash s_2 \Leftarrow \tau\end{array}}{\Theta; \Phi; B; \Gamma; \Delta \vdash s_1 ; s_2 \Leftarrow \tau} \quad \text{CHECK\_S\_SEQ}$$

$$\frac{}{\Theta; \Phi; B; \Gamma; \Delta \vdash \mathbf{abort} \Leftarrow \tau} \quad \text{CHECK\_S\_ABORT}$$

$\boxed{\Theta_1; \Phi_1 \vdash def_1 \mathinner{..} def_n \rightsquigarrow \Theta_2; \Phi_2}$

$$\frac{\begin{array}{c}\mathbf{val}\, f : (x : b[\phi]) \to \tau \in \Phi \\ \Theta; \Phi; \cdot; x : b[\phi]; \cdot \vdash s \Leftarrow \tau\end{array}}{\Theta; \Phi \vdash \mathbf{function}\, f(x) = s \rightsquigarrow \Theta; \Phi, \mathbf{function}\, f(x) = s} \quad \text{CHECK\_DEFS\_ANF\_FUNDEF}$$

$$\frac{\begin{array}{c}\mathbf{val}\, \forall\, \beta . f : (x : b[\phi]) \to \tau \in \Phi \\ \Theta; \Phi; \cdot, \beta; x : b[\phi]; \cdot \vdash s \Leftarrow \tau\end{array}}{\Theta; \Phi \vdash \mathbf{function}\, f(x) = s \rightsquigarrow \Theta; \Phi, \mathbf{function}\, f(x) = s} \quad \text{CHECK\_DEFS\_ANF\_FUNDEF\_POLY}$$

$$\frac{\Theta \vdash_{wf} \mathbf{val}\, f : (x : b[\phi]) \to \tau}{\Theta; \Phi \vdash \mathbf{val}\, f : (x : b[\phi]) \to \tau \rightsquigarrow \Theta; \Phi, \mathbf{val}\, f : (x : b[\phi]) \to \tau} \quad \text{CHECK\_DEFS\_ANF\_VALSPEC}$$

$$\frac{\Theta \vdash_{wf} \mathbf{val}\, \forall\, \beta . f : (x : b[\phi]) \to \tau}{\Theta; \Phi \vdash \mathbf{val}\, \forall\, \beta . f : (x : b[\phi]) \to \tau \rightsquigarrow \Theta; \Phi, \mathbf{val}\, \forall\, \beta . f : (x : b[\phi]) \to \tau} \quad \text{CHECK\_DEFS\_ANF\_VALSPEC\_POLY}$$

$$\frac{}{\Theta; \Phi \vdash \mathbf{union}\, tid = \{\, \overline{\dot{ctor}_i : \tau_i}^{\,i}\ \} \rightsquigarrow \Theta, \mathbf{union}\, tid = \{\, \overline{\dot{ctor}_i : \tau_i}^{\,i}\ \}; \Phi} \quad \text{CHECK\_DEFS\_ANF\_UNIONDEF}$$

$$\frac{\begin{array}{c}\Theta_1; \Phi_1 \vdash def \rightsquigarrow \Theta_2; \Phi_2 \\ \Theta_2; \Phi_2 \vdash def_1 \mathinner{..} def_n \rightsquigarrow \Theta_3; \Phi_3\end{array}}{\Theta_1; \Phi_1 \vdash def\, def_1 \mathinner{..} def_n \rightsquigarrow \Theta_3; \Phi_3} \quad \text{CHECK\_DEFS\_ANF\_DEFS}$$

$\boxed{\vdash p}$

$$\frac{\cdot;\cdot \vdash def_1 \mathrel{..} def_n \rightsquigarrow \Theta_2;\Phi_2 \qquad \Theta_2;\Phi_2;\cdot;\cdot;\cdot \vdash s \Leftarrow \{z : \mathbf{int}|\top\}}{\vdash def_1; \mathrel{..}; def_n;; s} \quad \text{CHECK\_PROGRAM\_PROG}$$

$\boxed{\Theta \vdash \Delta \sim \delta}$

$$\frac{\delta = u_1 \to v_1, \mathrel{..}, u_n \to v_n \qquad \Delta = u_1 : \tau_1, \mathrel{..}, u_n : \tau_n \qquad \Theta;\cdot;\cdot \vdash v_1 \Leftarrow \tau_1 \quad .. \quad \Theta;\cdot;\cdot \vdash v_n \Leftarrow \tau_n}{\Theta \vdash \Delta \sim \delta} \quad \text{DSIM\_DSIM}$$

$\boxed{\Theta;\Phi;\Delta \vdash (\delta, s) \Leftarrow \tau}$ Program state typing judgement

$$\frac{\Theta \vdash \Delta \sim \delta \qquad \Theta;\Phi;\cdot;\cdot;\Delta \vdash s \Leftarrow \tau}{\Theta;\Phi;\Delta \vdash (\delta, s) \Leftarrow \tau} \quad \text{CHECK\_REDEX\_STMT}$$

2.5 Operational semantics

$\boxed{\Phi \vdash \langle \delta, s_1 \rangle \to \langle \delta', s_2 \rangle}$ One step reduction

$$\frac{}{\Phi \vdash \langle \delta, \mathbf{if}\ \mathbf{T}\ \mathbf{then}\ s_1\ \mathbf{else}\ s_2 \rangle \to \langle \delta, s_1 \rangle} \quad \text{REDUCE\_IF\_TRUE}$$

$$\frac{}{\Phi \vdash \langle \delta, \mathbf{if}\ \mathbf{F}\ \mathbf{then}\ s_1\ \mathbf{else}\ s_2 \rangle \to \langle \delta, s_2 \rangle} \quad \text{REDUCE\_IF\_FALSE}$$

$$\frac{}{\Phi \vdash \langle \delta, \mathbf{let}\ x = v\ \mathbf{in}\ s \rangle \to \langle \delta, s[v/x] \rangle} \quad \text{REDUCE\_LET\_VALUE}$$

$$\frac{v_1 + v_2 = v}{\Phi \vdash \langle \delta, \mathbf{let}\ x = v_1 + v_2\ \mathbf{in}\ s \rangle \to \langle \delta, \mathbf{let}\ x = v\ \mathbf{in}\ s \rangle} \quad \text{REDUCE\_LET\_PLUS}$$

$$\frac{v_1 \le v_2 = v}{\Phi \vdash \langle \delta, \mathbf{let}\ x = v_1 \le v_2\ \mathbf{in}\ s \rangle \to \langle \delta, \mathbf{let}\ x = v\ \mathbf{in}\ s \rangle} \quad \text{REDUCE\_LET\_LEQ}$$

$$\frac{\mathbf{val}\ f : (x : b[\phi]) \to \tau \in \Phi \qquad \mathbf{function}\ f(x) = s_1 \in \Phi}{\Phi \vdash \langle \delta, \mathbf{let}\ y = f\ v\ \mathbf{in}\ s_2 \rangle \to \langle \delta, \mathbf{let}\ \ y : \tau[v/x] = s_1[v/x]\ \ \mathbf{in}\ \ s_2 \rangle} \quad \text{REDUCE\_LET\_APP}$$

$$\frac{\mathbf{val}\ \forall\,\beta.f : (x : b[\phi]) \to \tau \in \Phi \qquad \mathbf{function}\ f(x) = s_1 \in \Phi}{\Phi \vdash \langle \delta, \mathbf{let}\ y = f[b_1]v\ \mathbf{in}\ s_2 \rangle \to \langle \delta, \mathbf{let}\ \ y : \tau[v/x][b_1/\beta] = s_1[v/x][b_1/\beta]\ \ \mathbf{in}\ \ s_2 \rangle} \quad \text{REDUCE\_LET\_APP\_POLY}$$

$$\frac{}{\Phi \vdash \langle \delta, \mathbf{let}\ x = \mathbf{fst}\ (v_1, v_2)\ \mathbf{in}\ s \rangle \to \langle \delta, \mathbf{let}\ x = v_1\ \mathbf{in}\ s \rangle} \quad \text{REDUCE\_LET\_FST}$$

$$\frac{}{\Phi \vdash \langle \delta, \mathbf{let}\ x = \mathbf{snd}\ (v_1, v_2)\ \mathbf{in}\ s \rangle \to \langle \delta, \mathbf{let}\ x = v_2\ \mathbf{in}\ s \rangle} \quad \text{REDUCE\_LET\_SND}$$

$$\frac{v_1 @ v_2 = v_3}{\Phi \vdash \langle \delta, \mathbf{let}\ x = v_1 @ v_2\ \mathbf{in}\ s \rangle \to \langle \delta, \mathbf{let}\ x = v_3\ \mathbf{in}\ s \rangle} \quad \text{REDUCE\_LET\_CONCAT}$$

$$\frac{v_1 =\ \mathbf{split}\ v_2\ v_3}{\Phi \vdash \langle \delta, \mathbf{let}\ x = \mathbf{split}\ v_2\ v_3\ \mathbf{in}\ s \rangle \to \langle \delta, \mathbf{let}\ x = v_1\ \mathbf{in}\ s \rangle} \quad \text{REDUCE\_LET\_SPLIT}$$

$$\frac{\mathbf{len}\ v_1 = v_2}{\Phi \vdash \langle \delta, \mathbf{let}\ x = \mathbf{len}\ v_1\ \mathbf{in}\ s \rangle \to \langle \delta, \mathbf{let}\ x = v_2\ \mathbf{in}\ s \rangle} \quad \text{REDUCE\_LET\_LEN}$$

$$\frac{v = \delta(u)}{\Phi \vdash \langle \delta, \mathbf{let}\, x = u\, \mathbf{in}\, s \rangle \to \langle \delta, \mathbf{let}\, x = v\, \mathbf{in}\, s \rangle} \quad \text{REDUCE\_LET\_MVAR}$$

$$\frac{u \notin \mathrm{dom}(\delta)}{\Phi \vdash \langle \delta, \mathbf{var}\, u : \tau := v\, \mathbf{in}\, s \rangle \to \langle \delta[u \mapsto v], s \rangle} \quad \text{REDUCE\_MVAR\_DECL}$$

$$\frac{\delta' = \delta[u \mapsto v]}{\Phi \vdash \langle \delta, u := v \rangle \to \langle \delta', () \rangle} \quad \text{REDUCE\_MVAR\_ASSIGN}$$

$$\frac{\Phi \vdash \langle \delta, s_1 \rangle \to \langle \delta', s_3 \rangle}{\Phi \vdash \langle \delta, s_1; s \rangle \to \langle \delta', s_3; s \rangle} \quad \text{REDUCE\_SEQ1}$$

$$\frac{}{\Phi \vdash \langle \delta, (); s \rangle \to \langle \delta, s \rangle} \quad \text{REDUCE\_SEQ2}$$

$$\frac{}{\Phi \vdash \langle \delta, \mathbf{let}\ x : \tau = v\ \mathbf{in}\ s_2 \rangle \to \langle \delta, s_2[v/x] \rangle} \quad \text{REDUCE\_LET2\_VAL}$$

$$\frac{\Phi \vdash \langle \delta, s_1 \rangle \to \langle \delta', s_3 \rangle}{\Phi \vdash \langle \delta, \mathbf{let}\ x : \tau = s_1\ \mathbf{in}\ s_2 \rangle \to \langle \delta', \mathbf{let}\ x : \tau = s_3\ \mathbf{in}\ s_2 \rangle} \quad \text{REDUCE\_LET2\_STMT}$$

$$\frac{}{\Phi \vdash \langle \delta, \mathbf{match}\, (\dot{ctor}_j\ tid\ v)\, \mathbf{of}\, \overline{\dot{ctor}_i\, x_i \Rightarrow s_i}^{\,i} \rangle \to \langle \delta, s_j[v/x_j] \rangle} \quad \text{REDUCE\_MATCH}$$

$$\frac{x\ \mathbf{fresh}}{\Phi \vdash \langle \delta, \mathbf{while}\, (s_1)\, \mathbf{do}\, \{s_2\} \rangle \to \langle \delta, \mathbf{let}\ x : \{z : \mathbf{bool} | \top\} = s_1\ \mathbf{in}\ \mathbf{if}\, x\, \mathbf{then}\, (s_2; \mathbf{while}\, (s_1)\, \mathbf{do}\, \{s_2\})\, \mathbf{else}\, () \rangle} \quad \text{REDUC}$$

$$\frac{}{\Phi \vdash \langle \delta, \mathbf{assert}\, \phi\, \mathbf{in}\, v \rangle \to \langle \delta, v \rangle} \quad \text{REDUCE\_ASSERT1}$$

$$\frac{\Phi \vdash \langle \delta, s_1 \rangle \to \langle \delta', s_2 \rangle}{\Phi \vdash \langle \delta, \mathbf{assert}\, \phi\, \mathbf{in}\, s_1 \rangle \to \langle \delta', \mathbf{assert}\, \phi\, \mathbf{in}\, s_2 \rangle} \quad \text{REDUCE\_ASSERT2}$$

$\boxed{\Phi \vdash \langle \delta_1, s_1 \rangle \xrightarrow{*} \langle \delta_2, s_2 \rangle}$ Multi-step reduction

$$\frac{\Phi \vdash \langle \delta_1, s_1 \rangle \to \langle \delta_2, s_2 \rangle}{\Phi \vdash \langle \delta_1, s_1 \rangle \xrightarrow{*} \langle \delta_2, s_2 \rangle} \quad \text{REDUCE\_MANY\_SINGLE\_STEP}$$

$$\frac{\begin{array}{c}\Phi \vdash \langle \delta_1, s_1 \rangle \to \langle \delta_2, s_2 \rangle \\ \Phi \vdash \langle \delta_2, s_2 \rangle \xrightarrow{*} \langle \delta_3, s_3 \rangle\end{array}}{\Phi \vdash \langle \delta_1, s_1 \rangle \xrightarrow{*} \langle \delta_3, s_3 \rangle} \quad \text{REDUCE\_MANY\_MANY\_STEP}$$

2.6 Machine configuration check

$\boxed{\Theta \vdash \delta \sim \Delta}$

$$\frac{}{\Theta \vdash \cdot \sim \cdot} \quad \text{CHECK\_STORE\_EMPTY}$$

$$\frac{\begin{array}{c}u \notin \mathrm{dom}(\Delta) \\ \Theta \vdash \delta \sim \Delta \\ \Theta; \cdot; \cdot \vdash v \Leftarrow \tau\end{array}}{\Theta \vdash \delta[u \mapsto v] \sim \Delta, u : \tau} \quad \text{CHECK\_STORE\_CONS}$$

$\boxed{\Theta; \Phi; \Delta \vdash (\delta, s) \Leftarrow \tau}$

$$\frac{\begin{array}{c}\Theta \vdash \delta \sim \Delta \\ \Theta; \Phi; \cdot; \cdot; \Delta \vdash s \Leftarrow \tau\end{array}}{\Theta; \Phi; \Delta \vdash (\delta, s) \Leftarrow \tau} \quad \text{CHECK\_CONFIG\_CONFIG}$$

```
Definition rules:        160 good    0 bad
Definition rule clauses: 465 good    0 bad
```