4 Soundness

We will now show that the extension is sound. To do so we first will show the soundness of the new semantic with respect to the inference rules.

Theorem 4.1

Let $iet \in$ <int-exp-type> and $exp \in \mathit{IntExp}$. Assume $iet : exp$ can be derived.

—

Then $[\![iet]\!] = exp$.

Proof. Let $iet \in$ <int-exp-type> and $exp \in \mathit{IntExp}$. Assume $iet : exp$ can be derived.

- **Case** $iet = i$ for $i \in \mathit{Int}$: Then $[\![iet]\!] = i$ and therefore the conclusion holds.
- **Case** $iet = iet_1$ + iet_2 for $iet_1, iet_2 \in$ <int-exp-type>: From the premise of the inference rule, we assume that $iet_1 : exp_1$ and $iet_2 : exp_2$ hold. By induction hypothesis $[\![iet_1]\!] = exp_1$ and $[\![iet_2]\!] = exp_2$. Thus $[\![iet]\!] = exp_1 + exp_2$ and therefore the conclusion holds.
- **Case** $iet = iet_1$ * i for $iet_1 \in$ <int-exp-type> and $i \in \mathit{Int}$: From the premise of the inference rule, we assume that $iet_1 : exp_1$ holds. By induction hypothesis $[\![iet_1]\!] = exp_1$. Thus $[\![iet]\!] = exp_1 \cdot i$ and therefore the conclusion holds.
- **Case** $iet = a$ for $a \in \mathcal{A}$: Then $[\![a]\!] = a$ and therefore the conclusion holds.

□

Theorem 4.2

Let $qt \in$ <qualifier-type> and $q \in \mathcal{Q}$. Assume $qt : q$ can be derived.

—

Then $[\![qt]\!] = q$.

Proof. Let $qt \in$ <qualifier-type> and $q \in \mathcal{Q}$. Assume $qt : q$ can be derived.

- **Case** $qt =$ `True`: Then $[\![qt]\!] = \mathit{True}$ and therefore the conclusion holds.
- **Case** $qt =$ `False`: Then $[\![qt]\!] = \mathit{False}$ and therefore the conclusion holds.
- **Case** $qt =$ `(<)` iet `v`: From the premise of the inference rule, we assume that $iet : exp$. By Theorem 4.1 $[\![iet]\!] = exp$ for $exp \in \mathit{IntExp}$. Then $[\![qt]\!] = exp < \nu$ and therefore the conclusion holds.
- **Case** $qt =$ `(<)` `v` iet: From the premise of the inference rule, we assume that $iet : exp$. By Theorem 4.1 $[\![iet]\!] = exp$ for $exp \in \mathit{IntExp}$. Then $[\![qt]\!] = \nu < exp$ and therefore the conclusion holds.

- **Case** $qt =$ `(=) v` iet: From the premise of the inference rule, we assume that $iet : exp$. By Theorem 4.1 $[\![iet]\!] = exp$ for $exp \in IntExp$. Then $[\![qt]\!] = (\nu = exp)$ and therefore the conclusion holds.

- **Case** $qt =$ `(&&)` qt_1 qt_2 for $qt_1, qt_2 \in$ `<qualifier-type>`: From the premise of the inference rule, we assume that $qt_1 : q_1$ and $qt_2 : q_2$ hold for $q_1, q_2 \in \mathcal{Q}$. By induction hypothesis $[\![qt_1]\!] = q_1$ and $[\![qt_2]\!] = q_2$. Thus $[\![qt]\!] = q_1 \wedge q_2$ and therefore the conclusion holds.

- **Case** $qt =$ `(||)` qt_1 qt_2 for $qt_1, qt_2 \in$ `<qualifier-type>`: From the premise of the inference rule, we assume that $qt_1 : q_1$ and $qt_2 : q_2$ hold for $q_1, q_2 \in \mathcal{Q}$. By induction hypothesis $[\![qt_1]\!] = q_1$ and $[\![qt_2]\!] = q_2$. Thus $[\![qt]\!] = q_1 \vee q_2$ and therefore the conclusion holds.

- **Case** $qt =$ `not` qt_1 for $qt_1 \in$ `<qualifier-type>`: From the premise of the inference rule, we assume that $qt_1 : q_1$ holds for $q_1 \in \mathcal{Q}$. By induction hypothesis $[\![qt_1]\!] = q_1$. Thus $[\![qt]\!] = \neg\, q_1$ and therefore the conclusion holds.

□

Theorem 4.3

Let $\Theta : \mathcal{V} \nrightarrow \mathcal{T}$. Let $lt \in$ `<liquid-type>` and $\hat{T} \in \mathcal{T}$. Assume $lt :_\Theta \hat{T}$ can be derived.

—

Then $[\![lt]\!] = \hat{T}$.

Proof. Let $\Theta : \mathcal{V} \nrightarrow \mathcal{T}$. Let $lt \in$ `<liquid-type>` and $\hat{T} \in \mathcal{T}$. Assume $lt :_\Theta \hat{T}$ can be derived.

- **Case** $lt =$ `"{v:Int|"` qt `"}"` for $qt \in$ `<qualifier-type>`: From the premise of the inference rule, we assume that $qt : q$ for $q \in \mathcal{Q}$ holds. By Theorem 4.2 $[\![qt]\!] = q$. Then $[\![lt]\!] = \{\nu : Int|\ q\}$ and therefore the conclusion holds.

- **Case** $lt = a$ `":"` `"{v:Int|"` qt `"}"` `"->"` lt_2 for $a \in \mathcal{V}$, $qt \in$ `<qualifier-type>` and $lt \in$ `<liquid-type>`: From the premise of the inference rule, we assume that `"{v:Int|"` qt `"}"` $:_\Theta \hat{T}_1$ and $lt_2 :_{\Theta \cup \{(a, \hat{T}_1)\}} \hat{T}_2$ for liquid types $\hat{T}_1, \hat{T}_2$. By induction hypothesis $[\![lt_2]\!] = \hat{T}_2$. Then $[\![lt]\!] = a : \hat{T}_1 \to \hat{T}_2$ and therefore the conclusion holds.

□

We can now again prove the soundness of the semantic of type annotations.

Theorem 4.4

Let Γ be a type context, $t \in$ `<type>` and $T \in \mathcal{T}$. Assume $\Gamma \vdash t : T$ can be derived.

—

Then $[\![t]\!]_\Gamma = T$.

Proof. Let Γ be a type context, $t \in$ `<type>` and $T \in \mathcal{T}$. Assume $\Gamma \vdash t : T$ can be derived.

- **Case** $t = lt$ for $lt \in$ `<liquid-type>`: From the premise of the inference rule, we assume that $lt :_\Theta \hat{T}$ for liquid type $\hat{T}$ holds. By Theorem 4.3 $[\![lt]\!] = \hat{T}$. Then $[\![t]\!] = \hat{T}$ and therefore the conclusion holds.

All other cases have been proven in Theorem ??. □

What is left is to prove the soundness of the semantic of expressions. This is by the definition of refinement types trivially true, as the set values of a refinement type is always a subtype of the set of values of the base type.

Theorem 4.5

Let Γ, Δ be type contexts, Δ' be a variable context similar to Δ with respect to Γ. Let $\Lambda \subset \mathcal{Q}$ and $\Theta : \mathcal{V} \nrightarrow \mathcal{T}$. Let $e \in$ `<exp>` and $T \in \mathcal{T}$. Assume $\Gamma, \Delta, \Theta, \Lambda \vdash e : T$ can be derived.

—

Then $[\![e]\!]_{\Gamma,\Delta'} \in \text{value}_\Gamma(\overline{\Gamma}(T))$.

Proof. Let Γ, Δ be type contexts, Δ' be a variable context similar to Δ with respect to Γ. Let $\Lambda \subset \mathcal{Q}$ and $\Theta : \mathcal{V} \nrightarrow \mathcal{T}$. Let $e \in$ `<exp>` and $T \in \mathcal{T}$. Assume $\Gamma, \Delta, \Theta, \Lambda \vdash e : T$ can be derived.

- **Case** $e =$ `"(+)"`: Then $T = a : Int \to b : Int \to \{\nu : Int \mid \nu = a + b\}$ and $[\![\texttt{"(+)"}]\!]_{\Gamma,\Delta'} = \lambda n.\lambda m.n + m$ where $n, m \in \mathbb{Z}$ and thus the conclusion holds.

- **Case** $e =$ `"(-)"`: Then $T = a : Int \to b : Int \to \{\nu : Int \mid \nu = a + (-b)\}$ and $[\![\texttt{"(-)"}]\!]_{\Gamma,\Delta'} = \lambda n.\lambda m.n - m$ where $n, m \in \mathbb{Z}$ and thus by $n - m = n + (-m)$ the conclusion holds.

- **Case** $e =$ `"(*)"`: Then $T = a : Int \to b : Int \to \{\nu : Int \mid \nu = a * b\}$ and $[\![\texttt{"(*)"}]\!]_{\Gamma,\Delta'} = \lambda n.\lambda m.n * m$ where $n, m \in \mathbb{Z}$ and thus the conclusion holds.

- **Case** $e =$ `"(//)"`: Then $T = Int \to \{\nu : Int \mid \neg(\nu = 0)\} \to Int$ and

$$[\![\texttt{"(//)"}]\!]_{\Gamma,\Delta'} = s :\Leftrightarrow s = \lambda n.\lambda m. \begin{cases} \left\lfloor \frac{n}{m} \right\rfloor & \text{if } m \neq 0 \\ 0 & \text{else} \end{cases}$$

  where $n, m \in \mathbb{Z}$. Wee see that the "else"-case is dead and the $m \neq 0$-case is well formed. Thus the conclusion holds

- **Case** $e =$ `"if"` e_1 `"then"` e_2 `"else"` e_3 for $e_1, e_2, e_3 \in$ `<exp>`: By the premise of the inference rule we assume $\Gamma, \Delta, \Theta, \vdash e_1 : Bool$, $\Gamma, \Delta, \Theta, \Lambda \cup \{e'_1\} \vdash e_2 : \hat{T}$ and $\Gamma, \Delta, \Theta, \Lambda \cup \{\neg e'_1\} \vdash e_3 : \hat{T}$ as well as $e_1 : e'_1$ can be derived for $e'_1 \in \mathcal{Q}$. By induction hypothesis $[\![e_1]\!]_{\Gamma,\Delta'} \in \text{value}(Bool)$, $[\![e_2]\!]_{\Gamma,\Delta'} \in \text{value}(T)$ and

$[\![e_3]\!]_{\Gamma,\Delta'} \in \text{value}(T)$. Thus, by the definition of the semantics the conclusion holds analogously to the cases above.

- **Case** $e = e_1\ e_2$ for $e_1, e_2 \in$ `<exp>`: By the premise of the inference rule we assume $\Gamma, \Delta, \Theta, \Lambda \vdash e_1 : (a : \hat{T}_1 \to \hat{T}_2)$ and $\Gamma, \Delta, \Theta, \Lambda \vdash e_2 : \hat{T}_1$ as well as $[\hat{T}_2]_{a \leftarrow e_2'} = T$ and $e_2 : e_2'$ can be derived for $e_2' \in \mathcal{Q}$ and $a \in \mathcal{V}$. Therefore, by the induction hypothesis we know, $[\![e_1]\!]_{\Gamma,\Delta'} \in \text{value}_\Gamma(\overline{\Gamma}(\hat{T}_1 \to \hat{T}_2))$ and $[\![e_1]\!]_{\Gamma,\Delta'} \in \text{value}_\Gamma(\overline{\Gamma}(\hat{T}_1))$. Thus $[\![e]\!] \in \text{value}([\hat{T}_2]_{a \leftarrow e_2'})$ and thus the semantics the conclusion holds analogously to the cases above.
- **Case** $e =$ `"\"` a `"->"` e for $a \in \mathcal{V}, e \in$ `<exp>`: Then $T = b : \hat{T}_1 \to \hat{T}_2$ for liquid types $\hat{T}_1, \hat{T}_2$ and $b \in \mathcal{V}$. By the premise of the inference rule we assume $\Gamma, \Delta \cup \{(a, \hat{T}_1)\}, \Theta \cup \{(a, \hat{T}_1)\}, \Lambda \vdash e : \hat{T}_2$ can be derived. We now need to show that $[\![e]\!]_{\Gamma,\Delta'} \in \text{value}_\Gamma(\hat{T}_1 \to \hat{T}_2)$. We know $[\![e]\!]_{\Gamma,\Delta'} = \lambda b.[\![e]\!]_{\Gamma,\Delta\cup\{(a,b)\}}$ for $b \in \mathcal{V}$. We will therefore by the definition of the abstraction in the lambda expression let $b \in \text{value}_\Gamma(\overline{\Gamma}(\hat{T}_1))$ and show $[\![e]\!]_{\Gamma,\Delta'\cup\{(a,b)\}} \in \text{value}_\Gamma(\hat{T}_2)$. By Theorem **??** $\Delta' \cup \{(a, b)\}$ is similar to $\Delta \cup \{(a, \overline{\Gamma}(\hat{T}_1))\}$ and therefore by induction hypothesis we conclude $[\![e]\!]_{\Gamma,\Delta'\cup\{(a,b)\}} \in \text{value}_\Gamma(\hat{T}_2)$. Thus the conclusion holds.
- **Case** $e = a$ for $a \in \mathcal{V}$: By the premise of the inference rule we assume $(c, T) \in \Delta$. The semantic requires that there exists an $e \in \text{value}_\Gamma(\overline{\Gamma}(T))$ such that $(c, e) \in \Delta'$. Δ' is similar to Δ and therefore this is a valid assumption. Thus, the semantic is sound and by its definition the conclusion holds analogously to the cases above.

All other cases have been proven in Theorem **??**. $\square$