

3.5 Soundness

In this section we prove the soundness of the inference rules with respect to the semantics. This means we ensure that if we can infer the well-typedness of a program, the execution of the program yields those kinds of values predicted by the inference rules.

3.5.1 Soundness of the Type Signature

The inference rules and the semantics for the type signatures are built in a structurally similar way. Thus, we will now show that the semantics of a phrase yields the kind of result predicted by the inference rules.

Theorem 3.1

Let Γ be a type context, $ltf \in \langle \text{list-type-fields} \rangle$, $a_i \in \mathcal{V}, T_i \in \mathcal{T}$ for $i \in \mathbb{N}_1^n$ and $n \in \mathbb{N}_0$. Assume that $\Gamma \vdash ltf : \{a_1 : T_1, \dots, a_n : T_n\}$ can be derived.

Then $\llbracket ltf \rrbracket_\Gamma = \{a_1 : T_1, \dots, a_n : T_n\}$.

Proof. Let Γ be a type context, $ltf \in \langle \text{list-type-fields} \rangle$, $a_i \in \mathcal{V}, T_i \in \mathcal{T}$ for $i \in \mathbb{N}_1^n$ and $n \in \mathbb{N}_0$. Assume $ltf : \{a_1 : T_1, \dots, a_n : T_n\}$ can be derived.

- **Case** $ltf = ""$ for $n = 0$: Then $\llbracket ltf \rrbracket = \{\}$ and therefore the conclusion holds.
- **Case** $ltf = a_1 ":" T_1 ", " ltf_1$ for $ltf_1 \in \langle \text{list-type-field} \rangle$: Then by the premise of the inference rule for ltf we can assume that $\Gamma \vdash ltf_1 : \{a_2 : T_2, \dots, a_n : T_n\}$ can be derived and by induction hypothesis $\llbracket ltf_1 \rrbracket_\Gamma = \{a_2 : T_2, \dots, a_n : T_n\}$. We can now use the semantics as describe in its definition $\llbracket ltf \rrbracket = \llbracket a_1 ":" T_1 ", " ltf_1 \rrbracket = \{a_1 : e_1, \dots, a_n : e_n\}$ for $e_i \in \text{value}_\Gamma(T_i)$ for $i \in \mathbb{N}_0^n$, thus the conclusion $\llbracket ltf \rrbracket \in \text{value}_\Gamma(\{a_1 : T_1, \dots, a_n : T_n\})$ follows.

□

Theorem 3.2

Let Γ be a type context, $lt \in \langle \text{list-type} \rangle$, $T_i \in \mathcal{T}$ for $i \in \mathbb{N}_1^n$ and $n \in \mathbb{N}_0$. Assume $\Gamma \vdash lt : (T_1, \dots, T_n)$ can be derived.

Then $\llbracket lt \rrbracket_\Gamma = (T_1, \dots, T_n)$.

Proof. See the combined proof of the conjunction of Theorem ?? and ?? below. □

Theorem 3.3

Let Γ be a type context, $t \in \langle \text{type} \rangle$ and $T \in \mathcal{T}$. Assume $\Gamma \vdash t : T$ can be derived.

Then $\llbracket t \rrbracket_\Gamma = T$.

Proof. Combined proof of Theorems ?? and ??.

We prove the conjunction of Theorem ?? and ?? by simultaneous induction over the structure of the mutually recursive grammar rules for $\langle \text{list-type} \rangle$ and $\langle \text{type} \rangle$.

Let Γ be a type context, $lt \in \langle \text{list-type} \rangle$, $T_i \in \mathcal{T}$ for $i \in \mathbb{N}_1^n$ and $n \in \mathbb{N}_0$. Assume $\Gamma \vdash lt : (T_1, \dots, T_n)$ can be derived. We show $\llbracket lt \rrbracket_\Gamma = (T_1, \dots, T_n)$.

- **Case** $lt = ""$ for $n = 0$: Then $\llbracket lt \rrbracket = ()$ and thus the conclusion holds.
- **Case** $lt = t_1 \ l_1$ for $t_1 \in \langle \text{type} \rangle$ for $l_1 \in \langle \text{list-type} \rangle$: Then from the premise of the inference rule, we assume that $\Gamma \vdash l_1 : (T_2, \dots, T_n)$ and $\Gamma \vdash t_1 : T_1$ hold. The assumption of Theorem ??, namely that $\Gamma \vdash t_1 : T_1$ can be derived, now holds. By its induction hypothesis we can therefore conclude that $\llbracket t_1 \rrbracket_\Gamma = T_1$ for $T_1 \in \mathcal{T}$. The assumption of Theorem ??, namely $\Gamma \vdash l_1 : (T_2, \dots, T_n)$, holds and therefore by the induction hypothesis of Theorem ?? we obtain $\llbracket t_1 \ l_1 \rrbracket = (t_1, t_2, \dots, t_n)$ for $\llbracket t_i \rrbracket_\Gamma = T_i$ for $t_i \in \langle \text{type} \rangle$. Thus the conclusion $\llbracket lt \rrbracket = (T_1, \dots, T_n)$ holds.

Let Γ be a type context, $t \in \langle \text{type} \rangle$ and $T \in \mathcal{T}$. Assume $\Gamma \vdash t : T$ can be derived. We show $\llbracket t \rrbracket_\Gamma = T$.

- **Case** $t = \text{"Bool"}$: Then $\llbracket t \rrbracket_\Gamma = \text{Bool}$ and the conclusion holds.
- **Case** $t = \text{"Int"}$: Then by the premise of the inference rule for "Int", we can assume that $\Gamma \vdash t : \text{Int}$ can be derived and therefore $\llbracket t \rrbracket_\Gamma = \text{Int}$. We see that the conclusion holds.
- **Case** $t = \text{"List" } t_2$, for $t_2 \in \langle \text{type} \rangle$: By the premise of the inference rule we assume $\Gamma \vdash t_2 : T_2$ can be derived and by induction hypothesis $\llbracket t_2 \rrbracket_\Gamma = T_2$ for given $T_2 \in \mathcal{T}$. Then $\llbracket t \rrbracket_\Gamma = [e_1, \dots, e_n]$ for $e_i \in \text{value}_\Gamma(T_2)$, $i \in \mathbb{N}_0^n$ and $n \in \mathbb{N}$. Thus the conclusion holds.
- **Case** $t = "(" \ t_1 \ , \ "t_2 \)"$, for $t_1, t_2 \in \langle \text{type} \rangle$: By the premise of the inference rule $\Gamma \vdash t_1 : T_1$ and $\Gamma \vdash t_2 : T_2$ hold for given $T_1, T_2 \in \mathcal{T}$. Then by induction hypothesis $\llbracket t_1 \rrbracket_\Gamma = T_1$ and $\llbracket t_2 \rrbracket_\Gamma = T_2$. Thus by the definition of the semantics the conclusion holds analogously to the cases above.
- **Case** $t = "{" \ ltf \ "}"$, for $ltf \in \langle \text{list-type-field} \rangle$: Then by the premise of the inference rule $\Gamma \vdash ltf : \{a_1 : T_1, \dots, a_n : T_n\}$ for $a_i \in \mathcal{V}, T_i \in \mathcal{T}, i \in \mathbb{N}_1^n$ and $n \in \mathbb{N}_0$. Thus by Theorem ?? $\llbracket ltf \rrbracket_\Gamma = T$ and therefore the conclusion holds analogously to the cases above.
- **Case** $t = t_1 \ "->" \ t_2$, for $t_1, t_2 \in \langle \text{type} \rangle$: By the premise of the inference rule $\Gamma \vdash t_1 : T_1$ and $\Gamma \vdash t_2 : T_2$ hold for given $T_1, T_2 \in \mathcal{T}$. By induction hypothesis $\llbracket t_i \rrbracket_\Gamma = T_i$ for $i \in \{1, 2\}$. Thus by the definition of the semantics the conclusion holds analogously to the cases above.

- **Case $t = c \text{ } lt$ for $lt \in \langle \text{list-type} \rangle$ and $c \in \langle \text{upper-var} \rangle$:** By the premise of the inference rule we know $(c, T') \in \Gamma$ with $T' \in \mathcal{T}$ and can assume that $\Gamma \vdash lt : (T_0, \dots, T_n)$ can be derived. Therefore, the assumption of Theorem ??, namely that $\Gamma \vdash lt : (T_0, \dots, T_n)$ can be derived, holds and by applying its induction hypothesis, we know $\llbracket lt \rrbracket_\Gamma = (T_1, \dots, T_n)$ for $T_i \in \mathcal{T}$, $i \in \mathbb{N}^n$ and $n \in \mathbb{N}_0$. Thus by the definition of the semantics the conclusion holds.
- **Case $t = a$ for $a \in \mathcal{V}$:** Then by the definition of the semantics the conclusion holds analogously to the cases above.

□

3.5.2 Soundness of the Variable Context

In our previous sections we had two different meanings for Δ . We will now define the relation between the two.

Definition 3.1: Similar Variable context

Let Γ, Δ be type contexts and Δ' a variable context.

We say Δ' is *similar to Δ with respect to Γ* iff for all $T \in \mathcal{T}$ and for all $a \in \mathcal{V}$ the following holds:

$$(a, T) \in \Delta \Rightarrow \exists e \in \text{value}_\Gamma(\bar{\Gamma}(T)). (a, e) \in \Delta'.$$

Theorem 3.4

Let Γ, Δ be type contexts and Δ' be a variable context similar to Δ with respect to Γ . Let $a \in \mathcal{V}$ and $T \in \mathcal{T}$. Let $e \in \text{value}_\Gamma(\bar{\Gamma}(T))$.

Then $\Delta' \cup \{(a, e)\}$ is similar to $\Delta \cup \{(a, \bar{\Gamma}(T))\}$ with respect to Γ .

Proof. Let Δ be a type context and Δ' be a variable context similar to Δ with respect to Γ . Let $a \in \mathcal{V}$ and $T \in \mathcal{T}$. Let $e \in \text{value}_\Gamma(\bar{\Gamma}(T))$.

We know Δ is similar to Δ' with respect to Γ , meaning for all $T' \in \mathcal{T}$ and for all $a' \in \mathcal{V}$ the following holds:

$$(a', T') \in \Delta \Rightarrow \exists d \in \text{value}_\Gamma(\bar{\Gamma}(T')) \text{ such that } (a', d) \in \Delta'.$$

Let $a' \in \mathcal{V}$ and $T' \in \mathcal{T}$ such that $(a', T') \in \Delta \cup \{(a, \bar{\Gamma}(T))\}$.

- **Case $(a', T') \in \Delta$:** Because Δ is similar to Δ' we can directly conclude $\exists d \in \text{value}_\Gamma(\bar{\Gamma}(T'))$ such that $(a', d) \in \Delta' \cup \{(a, e)\}$.
- **Case $(a', T') = (a, \bar{\Gamma}(T))$:** We know $e \in \text{value}_\Gamma(\bar{\Gamma}(T))$ and $(a, e) \in \Delta' \cup \{(a, e)\}$. By $a' = a$ we therefore conclude $(a', e) \in \Delta' \cup \{(a, e)\}$.

□

Types in Δ are all most generalized types. Instead of proving this, we show that the semantic only produces values of most generalized types. This is a weaker statement but strong enough for our purposes.

3.5.3 Soundness of the Expression Semantics

We can now use the definition of well-formed variable contexts, to prove the soundness of the expression semantics.

Theorem 3.5

Let $b \in \langle \text{bool} \rangle$.

—

Then $\llbracket b \rrbracket \in \text{value}_\emptyset(\text{Bool})$.

Proof. Let $b \in \langle \text{bool} \rangle$.

- **Case** $b = \text{"True"}$: Then $\llbracket b \rrbracket = \text{True}$. Thus the conclusion holds.
- **Case** $b = \text{"False"}$: Then $\llbracket b \rrbracket = \text{False}$. Thus the conclusion holds.

□

Theorem 3.6

Let $i \in \langle \text{int} \rangle$.

—

Then $\llbracket i \rrbracket \in \text{value}_\emptyset(\text{Int})$.

Proof. Let $i \in \langle \text{int} \rangle$.

- **Case** $i = \text{"0"}$: Then $\llbracket i \rrbracket = 0$. Thus the conclusion holds.
- **Case** $i = n$ for $n \in \mathbb{N}$: Then $\llbracket i \rrbracket = \text{Succ}^n 0$. Thus the conclusion holds.
- **Case** $i = \text{"-"} n$ for $n \in \mathbb{N}$: Then $\llbracket i \rrbracket = \text{Neg Succ}^n 0$. Thus the conclusion holds.

□

Theorem 3.7

Let Γ, Δ be type contexts, Δ' be a variable context similar to Δ with respect to Γ and $lef \in \langle \text{list-exp-field} \rangle$. Assume $\Gamma, \Delta \vdash lef : T$ can be derived for $T = \{a_1 : T_1, \dots, a_n : T_n\} \in \mathcal{T}$, $a_i \in \mathcal{V}$, $T_i \in \mathcal{T}$, for all $i \in \mathbb{N}_1^n$, and $n \in \mathbb{N}_0$.

—

Then $\llbracket lef \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T))$.

Proof. See the combined proof of the conjunction of Theorem ??, ?? and ?? below. \square

Theorem 3.8

Let Γ, Δ be type contexts, Δ' be a variable context similar to Δ with respect to Γ and $le \in \langle \text{list-exp} \rangle$. Assume $\Gamma, \Delta \vdash le : \text{List } T$ can be derived for $T \in \mathcal{T}$.

Then $\llbracket le \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(\text{List } T))$.

Proof. See the combined proof of the conjunction of Theorem ??, ?? and ?? below. \square

Theorem 3.9

Let Γ, Δ be type contexts, Δ' be a variable context similar to Δ with respect to Γ . Let $e \in \langle \text{exp} \rangle$ and $T \in \mathcal{T}$. Assume $\Delta, \Gamma \vdash e : T$ can be derived.

Then $\llbracket e \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T))$.

Proof. We prove the conjunction of Theorem ??, ?? and ?? by simultaneous induction over the structure of the mutually recursive grammar rules for $\langle \text{list-exp-field} \rangle$, $\langle \text{list-exp} \rangle$ and $\langle \text{exp} \rangle$.

Let Γ, Δ be type contexts, Δ' be a variable context similar to Δ with respect to Γ and $lef \in \langle \text{list-exp-field} \rangle$. Assume the judgment $\Gamma, \Delta \vdash lef : T$ can be derived for $T = \{a_1 : T_1, \dots, a_n : T_n\} \in \mathcal{T}$, $a_i \in \mathcal{V}$, $T_i \in \mathcal{T}$, for all $i \in \mathbb{N}_1^n$ and given $n \in \mathbb{N}_0$. We show $\llbracket lef \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T))$.

- **Case** $lef = a_1 \text{ "=" } e_1$ for $e_1 \in \langle \text{exp} \rangle$ and $n = 1$: Then by the premise of the inference rule we assume $\Gamma, \Delta \vdash e_1 : T_1$ can be derived and therefore the assumption of Theorem ?? holds. By applying said theorem we can therefore conclude $\llbracket e_1 \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T_1))$. Then $\llbracket lef \rrbracket_{\Gamma, \Delta'} = \{a_1 = e_1\}$ and therefore the conclusion holds.
- **Case** $lef = a_1 \text{ "=" } e_1 \text{ ", " } lef_0$ for $e_1 \in \langle \text{exp} \rangle$ and $lef_0 \in \langle \text{list-exp-field} \rangle$: Then by the premise of the inference rule we assume $\Gamma, \Delta \vdash lef_0 : \{a_2 : T_2, \dots, a_n : T_n\}$ and $\Gamma, \Delta \vdash e_1 : T_1$ can both be derived. Thus the assumption of Theorem ?? holds and by the induction hypothesis of said theorem $\llbracket e_1 \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T_1))$. By $\Gamma, \Delta \vdash lef_0 : T$ the assumption for the induction hypothesis of Theorem ?? holds and therefore by applying the theorem we obtain $\llbracket lef_0 \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(\{a_2 : T_2, \dots, a_n : T_n\}))$. Then $\llbracket lef \rrbracket_{\Gamma, \Delta'} = \{a_1 = e_1, \dots, a_n = e_n\}$ for $e_i \in \text{value}_{\Gamma}(\bar{\Gamma}(T_i))$ and thus the conclusion holds.

Let Γ, Δ be type contexts, Δ' be a variable context similar to Δ with respect to Γ and $le \in \langle \text{list-exp} \rangle$. Assume $\Gamma, \Delta \vdash le : \text{List } T$ can be derived for given $T \in \mathcal{T}$. We show $\llbracket le \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\text{List } T)$.

- **Case** $le = ""$: Then $\llbracket "" \rrbracket_{\Gamma, \Delta'} = \text{Empty}$ and thus the conclusion holds.
- **Case** $le = e, le_1$ for $e \in \langle \text{exp} \rangle$ and $le_1 \in \langle \text{list-exp} \rangle$: Then by the premise of the inference rule we assume $\Gamma, \Delta \vdash e : T$ and $\Gamma, \Delta \vdash le_1 : \text{List } T$ can be derived. The assumption of Theorem ??, namely that $\Gamma, \Delta \vdash e : T$ can be derived, holds and by applying that theorem $\llbracket e \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T))$. The assumption of Theorem ??, namely that $\Gamma, \Delta \vdash le_1 : T$ can be derived, also holds and by applying said theorem we conclude $\llbracket le_1 \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(\text{List } T))$. By using the definition of the semantics $\llbracket le \rrbracket_{\Gamma, \Delta'} = \text{Cons } e \llbracket le_1 \rrbracket_{\Gamma, \Delta'}$ and therefore the conclusion holds.

Let Γ, Δ be type contexts, Δ' be a variable context similar to Δ with respect to Γ . Let $e \in \langle \text{exp} \rangle$ and $T \in \mathcal{T}$. Assume $\Delta, \Gamma \vdash e : T$ can be derived.

- **Case** $e = \text{"foldl"}$: Then $T = \forall a. \forall b. (a \rightarrow b \rightarrow b) \rightarrow b \rightarrow \text{List } a \rightarrow b$ and

$$\llbracket \text{"foldl"} \rrbracket_{\Gamma, \Delta'} = \lambda f. \lambda e_1. \lambda l_1. \begin{cases} e_1 & \text{if } [] = l_1 \\ f(e_2, s(f, e_1, l_2)) & \text{if } \text{Cons } e_2 \ l_2 = l_1 \end{cases}$$

where $e_1 \in \text{value}_{\Gamma}(T_1), e_2 \in \text{value}_{\Gamma}(T_2)$ and $l_1, l_2 \in \text{value}_{\Gamma}(\text{List } T_2)$ and $f \in \text{value}_{\Gamma}(T_2 \rightarrow T_1 \rightarrow T_1)$ for $T_1, T_2 \in \mathcal{T}$ and thus the conclusion holds.

- **Case** $e = \text{"(::)"}$: Then $T = \forall a. a \rightarrow \text{List } a \rightarrow \text{List } a$ and $\llbracket \text{"(::)" } \rrbracket_{\Gamma, \Delta'} = \lambda e. \lambda l. \text{Cons } e \ l$ where $e \in \text{value}_{\Gamma}(T')$ and $l \in \text{value}_{\Gamma}(\text{List } T')$ for $T' \in \mathcal{T}$ and thus the conclusion holds.
- **Case** $e = \text{"(+)}"$: Then $T = \text{Int} \rightarrow \text{Int} \rightarrow \text{Int}$ and $\llbracket \text{"(+)"} \rrbracket_{\Gamma, \Delta'} = \lambda n. \lambda m. n + m$ where $n, m \in \mathbb{Z}$ and thus the conclusion holds.
- **Case** $e = \text{"(-)"}$: Then $T = \text{Int} \rightarrow \text{Int} \rightarrow \text{Int}$ and $\llbracket \text{"(-)"} \rrbracket_{\Gamma, \Delta'} = \lambda n. \lambda m. n - m$ where $n, m \in \mathbb{Z}$ and thus the conclusion holds.
- **Case** $e = \text{"(*)}"$: Then $T = \text{Int} \rightarrow \text{Int} \rightarrow \text{Int}$ and $\llbracket \text{"(*)"} \rrbracket_{\Gamma, \Delta'} = \lambda n. \lambda m. n * m$ where $n, m \in \mathbb{Z}$ and thus the conclusion holds.
- **Case** $e = \text{"(//)"}$: Then $T = \text{Int} \rightarrow \text{Int} \rightarrow \text{Int}$ and

$$\llbracket \text{"(//)"} \rrbracket_{\Gamma, \Delta'} = s : \Leftrightarrow \begin{cases} s = \lambda n. \lambda m. \lfloor \frac{n}{m} \rfloor & \text{if } m \neq 0 \\ 0 & \text{else} \end{cases}$$

where $n, m \in \mathbb{Z}$ and thus the conclusion holds.

- **Case** $e = \text{"(<)"}$: Then $T = \text{Int} \rightarrow \text{Int} \rightarrow \text{Bool}$ and $\llbracket \text{"(<)" } \rrbracket_{\Gamma, \Delta'} = \lambda n. \lambda m. n < m$ where $n, m \in \mathbb{Z}$ and thus the conclusion holds.
- **Case** $e = \text{"(==)"}$: Then $T = \text{Int} \rightarrow \text{Int} \rightarrow \text{Bool}$ and $\llbracket \text{"(==)" } \rrbracket_{\Gamma, \Delta'} = \lambda n. \lambda m. (n = m)$ where $n, m \in \mathbb{Z}$ and thus the conclusion holds.
- **Case** $e = \text{"not"}$: Then $T = \text{Bool} \rightarrow \text{Bool}$ and $\llbracket \text{"not"} \rrbracket_{\Gamma, \Delta'} = \lambda b. \neg b$ where $b \in \text{value}_{\Gamma}(\text{Bool})$ and thus the conclusion holds.

- **Case** $e = "(\&\&)":$ Then $T = Bool \rightarrow Bool \rightarrow Bool$ and $\llbracket "(\&\&)" \rrbracket_{\Gamma, \Delta'} = \lambda b_1. \lambda b_2. b_1 \wedge b_2$ where $b_1, b_2 \in \text{value}_{\Gamma}(Bool)$ and thus the conclusion holds.
- **Case** $e = "(||)":$ Then $T = Bool \rightarrow Bool \rightarrow Bool$ and $\llbracket "(||)" \rrbracket_{\Gamma, \Delta'} = \lambda b_1. \lambda b_2. b_1 \vee b_2$ where $b_1, b_2 \in \text{value}_{\Gamma}(Bool)$ and thus the conclusion holds.
- **Case** $e = e_1 "|>" e_2$ for given $e_1, e_2 \in \langle \text{exp} \rangle$: By the premise of the inference rule we assume $\Gamma, \Delta \vdash e_1 : T_1$ and $\Gamma, \Delta \vdash e_2 : T_1 \rightarrow T$ for $T_1 \in \mathcal{T}$ can be derived and by induction hypothesis of Theorem ?? $\llbracket e_1 \rrbracket_{\Gamma, \Delta'} \in \text{value}(\bar{\Gamma}(T_1))$ and $\llbracket e_2 \rrbracket_{\Gamma, \Delta'} \in \text{value}(\bar{\Gamma}(T_1 \rightarrow T))$. Then $\llbracket e_1 "|>" e_2 \rrbracket_{\Gamma, \Delta'} = \llbracket e_2 \rrbracket_{\Gamma, \Delta'}(\llbracket e_1 \rrbracket_{\Gamma, \Delta'})$ and thus the conclusion holds.
- **Case** $e = e_1 ">>" e_2$ for given $e_1, e_2 \in \langle \text{exp} \rangle$: Then $T = T_1 \rightarrow T_3$ for $T_1, T_3 \in \mathcal{T}$. By the premise of the inference rule we assume $\Gamma, \Delta \vdash e_1 : T_1 \rightarrow T_2$ for $T_2 \in \mathcal{T}$ and $\Gamma, \Delta \vdash e_2 : T_2 \rightarrow T_3$ can be derived. Then by induction hypothesis of Theorem ?? we know $\llbracket e_1 \rrbracket_{\Gamma, \Delta'} \in \text{value}(\bar{\Gamma}(T_1 \rightarrow T_2))$ and $\llbracket e_2 \rrbracket_{\Gamma, \Delta'} \in \text{value}(\bar{\Gamma}(T_2 \rightarrow T_3))$. Thus, by the definition of the semantics the conclusion holds analogously to the cases above.
- **Case** $e = \text{"if" } e_1 \text{"then" } e_2 \text{"else" } e_3$ for $e_1, e_2, e_3 \in \langle \text{exp} \rangle$: By the premise of the inference rule we assume $\Gamma, \Delta \vdash e_1 : Bool$, $\Gamma, \Delta \vdash e_2 : T$ and $\Gamma, \Delta \vdash e_3 : T$ can be derived. By induction hypothesis of Theorem ?? we know $\llbracket e_1 \rrbracket_{\Gamma, \Delta'} \in \text{value}(Bool)$, $\llbracket e_2 \rrbracket_{\Gamma, \Delta'} \in \text{value}(\bar{\Gamma}(T))$ and $\llbracket e_3 \rrbracket_{\Gamma, \Delta'} \in \text{value}(\bar{\Gamma}(T))$. Thus, by the definition of the semantics the conclusion holds analogously to the cases above.
- **Case** $e = \{"lef\}$ for $lef \in \langle \text{list-exp-field} \rangle$: Then $T = \{a_1 : T_1, \dots, a_n : T_n\}$ for given $a_i \in \mathcal{V}, T_i \in \mathcal{T}$ for $i \in \mathbb{N}_0^n$ and $n \in \mathbb{N}$. By the premise of the inference rule, we assume $\Gamma, \Delta \vdash lef : \{a_1 : T_1, \dots, a_n : T_n\}$ can be derived. By induction hypothesis Theorem ?? we can therefore conclude $\llbracket lef \rrbracket_{\Gamma, \Delta'} = \{a_1 : T_1, \dots, a_n : T_n\}$. Thus, by the definition of the semantics the conclusion holds analogously to the cases above.
- **Case** $e = \{\}$: Then $T = \{\}$ and $\llbracket \{\} \rrbracket_{\Gamma, \Delta'} = \{\}$. Thus the conclusion holds.
- **Case** $e = \{"a" | lef\}$ for $a \in \mathcal{V}$ and $lef \in \langle \text{list-exp-field} \rangle$: Then $T = \{a_1 : T_1, \dots, a_n : T_n, \dots\}$ for given $a_i \in \mathcal{V}, T_i \in \mathcal{T}$ for $i \in \mathbb{N}_0^n$ and $n \in \mathbb{N}$. By the premise of the inference rule, we assume $(a, \{a_1 : T_1, \dots, a_n : T_n, \dots\}) \in \Delta$ and $\Gamma, \Delta \vdash lef : \{a_1 : T_1, \dots, a_n : T_n\}$ can be derived. By induction hypothesis Theorem ?? we can therefore conclude $\llbracket lef \rrbracket_{\Gamma, \Delta'} = \{a_1 : T_1, \dots, a_n : T_n\}$. The semantic requires that there exists an $e \in \text{value}_{\Gamma}(\bar{\Gamma}(\{a_1 : T_1, \dots, a_n : T_n\}))$ such that $(a, e) \in \Delta'$. We know 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.
- **Case** $e = a_0 "." a_1$ for $a_0, a_1 \in \mathcal{V}$: By the premise of the inference rule we assume $(a_0, \{a_1 : T, \dots\}) \in \Delta$. The semantic requires that there exists an $e \in \text{value}_{\Gamma}(\bar{\Gamma}(\{a_1 : T, \dots\}))$ such that $(a_0, e) \in \Delta'$. We know 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.
- **Case** $e = \text{"let" } mes \text{ } a = e_1 \text{ "in" } e_2$ for $mes \in \langle \text{maybe-exp-sign} \rangle, a \in \mathcal{V}, e_1, e_2 \in \langle \text{exp} \rangle$: By the premise of the inference rule we assume $\Gamma, \Delta \vdash e_1 : T_1$

and $\Gamma, \Delta \cup \{(a, \bar{\Gamma}(T_1))\} \vdash e_2 : T_2$ can be derived. Then, by induction hypothesis of Theorem ?? we know $\llbracket e_1 \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T_1))$. Therefore, by Theorem ?? we know $\Delta' \cup \{(a, \llbracket e_1 \rrbracket_{\Gamma, \Delta'})\}$ is similar to $\Delta \cup \{(a, \bar{\Gamma}(T_1))\}$. By induction hypothesis of Theorem ?? we also know $\llbracket e_2 \rrbracket_{\Gamma, \Delta' \cup \{(a, \llbracket e_1 \rrbracket_{\Gamma, \Delta'})\}} \in \text{value}_{\Gamma}(\bar{\Gamma}(T_2))$ and thus by the definition of the semantics the conclusion holds analogously to the cases above.

- **Case $e = e_1 \ e_2$ for $e_1, e_2 \in \langle \text{exp} \rangle$:** By the premise of the inference rule we assume $\Gamma, \Delta \vdash e_1 : T_1 \rightarrow T$ and $\Gamma, \Delta \vdash e_2 : T_1$ can be derived. Therefore, by the induction hypothesis of Theorem ?? we know, $\llbracket e_1 \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T_1 \rightarrow T))$ and $\llbracket e_2 \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T_1))$. Then by the definition of the semantics the conclusion holds analogously to the cases above.
- **Case $e = b$ for $b \in \langle \text{bool} \rangle$:** Then $T = \text{Bool}$. By the premise of the inference rule we assume $b : T$ can be derived and by Theorem ?? the conclusion holds.
- **Case $e = i$ for $i \in \langle \text{int} \rangle$:** Then $T = \text{Int}$. By the premise of the inference rule we assume $b : T$ can be derived and by Theorem ?? the conclusion holds.
- **Case $e = "[\text{le}]"$ for $i \in \langle \text{list-exp} \rangle$:** Then $T = \text{List } T_1$ for $T_1 \in \mathcal{T}$. By the premise of the inference rule we assume $\Gamma, \Delta \vdash \text{le} : T$ can be derived and by induction hypothesis Theorem ?? the conclusion holds.
- **Case $e = "(\ e_1 \ , \ e_2)"$ for $e_1, e_2 \in \langle \text{exp} \rangle$:** Then $T = (T_1, T_2)$ for $T_1, T_2 \in \mathcal{T}$. By the premise of the inference rule we assume $\Gamma, \Delta \vdash e_1 : T_1$ and $\Gamma, \Delta \vdash e_2 : T_2$. Therefore, by the induction hypothesis of Theorem ?? we know $\llbracket e_1 \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T_1))$ and $\llbracket e_2 \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(\bar{\Gamma}(T_2))$. Then by the definition of the semantics the conclusion holds analogously to the cases above.
- **Case $e = "\backslash a \rightarrow" e$ for $a \in \mathcal{V}, e \in \langle \text{exp} \rangle$:** Then $T = T_1 \rightarrow T_2$ for $T_1, T_2 \in \mathcal{T}$. By the premise of the inference rule we assume $\Gamma, \Delta' \cup \{(a, \bar{\Gamma}(T_1))\} \vdash e : T_2$ can be derived. We now need to show that $\llbracket e \rrbracket_{\Gamma, \Delta'} \in \text{value}_{\Gamma}(T_1 \rightarrow T_2)$. We know $\llbracket e \rrbracket_{\Gamma, \Delta'} = \lambda b. \llbracket e \rrbracket_{\Gamma, \Delta \cup \{(a, b)\}}$ for $b \in \mathcal{V}$. We will therefore by the definition of the abstraction in the lambda expression let $b \in \text{value}_{\Gamma}(\bar{\Gamma}(T_1))$ and show $\llbracket e \rrbracket_{\Gamma, \Delta' \cup \{(a, b)\}} \in \text{value}_{\Gamma}(T_2)$. By Theorem ?? $\Delta' \cup \{(a, b)\}$ is similar to $\Delta \cup \{(a, \bar{\Gamma}(T_1))\}$ and therefore by induction hypothesis of Theorem ?? we conclude $\llbracket e \rrbracket_{\Gamma, \Delta' \cup \{(a, b)\}} \in \text{value}_{\Gamma}(T_2)$. Thus the conclusion holds.
- **Case $\Gamma, \Delta \vdash c : T$ for $c \in \mathcal{V}$:** By the premise of the inference rule we assume $(c, T) \in \Delta$. The semantic requires that there exists an $e \in \text{value}_{\Gamma}(\bar{\Gamma}(T))$ 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.

□

3.5.4 Soundness of the Statement Semantics

Statements are modelled as operations on either the type context or the variable context. We will now show that their semantics conforms to the result of the inference rules.

Theorem 3.10

Let $lsv \in \langle \text{list-statement-var} \rangle$, $a_i \in \mathbb{N}_1^n$ for $n \in \mathbb{N}_0$. Assume $lsv : (a_1, \dots, a_n)$ can be derived.

Then $\llbracket lsv \rrbracket \in \mathcal{V}^*$.

Proof. Let $lsv \in \langle \text{list-statement-var} \rangle$, $a_i \in \mathbb{N}_1^n$ for $n \in \mathbb{N}_0$. Assume $lsv : (a_1, \dots, a_n)$ can be derived.

- **Case** $lsv = ""$ and $n = 0$: Then $\llbracket lsv \rrbracket = ()$ and thus the conclusion holds.
- **Case** $lsv = a_1 \ lsv_1$ for $lsv_1 \in \langle \text{list-statement-var} \rangle$: Then by the inference rule of lsv , we assume that $lsv_1 : (a_2, \dots, a_n)$ can be derived. Then by induction hypothesis $\llbracket lsv_1 \rrbracket = (a_2, \dots, a_n)$, and therefore $\llbracket lsv \rrbracket = (a_1, \dots, a_n)$. Thus the conclusion holds.

□

Theorem 3.11

Let $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ be type contexts and Δ'_1 be a variable context similar to Δ_1 respectively with respect to Γ . Let $s \in \langle \text{statement} \rangle$ and assume $\Gamma_1, \Delta_1, s \vdash \Gamma_2, \Delta_2$ can be derived.

Then $\llbracket s \rrbracket(\Gamma_1, \Delta'_1) = (\Gamma_2, \Delta'_2)$ for a variable context Δ'_2 similar to Δ_2 with respect to Γ .

Proof. Let $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ be type contexts and Δ'_1, Δ'_2 be a variable context similar to Δ_1, Δ_2 respectively with respect to Γ_1, Δ_2 respectively. Let $s \in \langle \text{statement} \rangle$ and assume $\Gamma_1, \Delta_1, s \vdash \Gamma_2, \Delta_2$ can be derived.

- **Case** $s = mss \ a \ "=" \ e$ for $mss \in \langle \text{maybe-statement-sort} \rangle$, $a \in \mathcal{V}$, $e \in \langle \text{exp} \rangle$, $\Gamma_1 = \Gamma_2$ and $\Delta_2 = \Delta_1 \cup \{(a, \overline{\Gamma_1}(T))\}$ for $T \in \mathcal{T}$: Then from the premise of the inference rule, we assume that $\Gamma_1, mss \vdash e : T$ and $\Gamma_1, \Delta_2 \vdash e : T$ can both be derived. By Theorem ??, we know $\llbracket e \rrbracket_{\Gamma_1, \Delta'_1} \in \text{value}_{\Gamma_1}(\overline{\Gamma_1}(T))$. Let $\Delta'_2 = \Delta'_1 \cup \{(a, \llbracket e \rrbracket_{\Gamma_1, \Delta'_1})\}$. Then $\llbracket s \rrbracket(\Gamma_1, \Delta'_1) = (\Gamma_2, \Delta'_2)$. By Theorem ?? Δ'_2 is similar to Δ_2 .
- **Case** $s = \text{"type alias"} \ c \ lsv \ "=" \ t$ for $lsv \in \langle \text{list-statement-variable} \rangle$, $c \in \mathcal{V}$ such that $\Delta_1 = \Delta_2$ and $(c, _) \notin \Gamma_1$: Let $\Delta'_1 = \Delta'_2$. From $\llbracket s \rrbracket(\Gamma_1, \Delta'_1) = (\Gamma_2, \Delta'_2)$ the conclusion trivially holds.

□

Theorem 3.12

Let $\Gamma_1, \Delta_1, \Gamma_2, \Delta_2$ be type contexts and Δ'_1 , be a variable context similar to

Δ_1 with respect to Γ . Let $ls \in \langle \text{list-statement} \rangle$ such that $\Gamma_1, \Delta_1, ls \vdash \Gamma_2, \Delta_2$ can be derived.

Then $\llbracket ls \rrbracket(\Gamma_1, \Delta'_1) = (\Gamma_2, \Delta'_2)$ for a variable context Δ'_2 similar to Δ_2 with respect to Γ .

Proof. $\Gamma_1, \Delta_1, \Gamma_2, \Delta_2$ be type contexts and Δ'_1 , be a variable context similar to Δ_1 with respect to Γ . Let $ls \in \langle \text{list-statement} \rangle$ such that $\Gamma_1, \Delta_1, ls \vdash \Gamma_2, \Delta_2$ can be derived.

- **Case** $ls = ""$ for $\Gamma_1 = \Gamma_2$ and $\Delta_1 = \Delta_2$: Let $\Delta'_1 = \Delta'_2$. Then $\llbracket ls \rrbracket = id$ and therefore the conclusion holds.
- **Case** $ls = s ";" ls_1$ for $s \in \langle \text{statement} \rangle$ and $ls_1 \in \langle \text{statement-list} \rangle$: From the premise of the inference rule, we assume $\Gamma_1, \Delta_1, s \vdash \Gamma_3, \Delta_3$ and $\Gamma_3, \Delta_3, ls_1 \vdash \Gamma_2, \Delta_2$ for some type contexts Γ_2, Δ_2 . We know by Theorem ?? that $\llbracket s \rrbracket(\Gamma_1, \Delta'_1) = (\Gamma_3, \Delta'_3)$ for a given variable context Δ'_3 similar to Δ_3 with respect to Γ . Also, by induction hypothesis we know $\llbracket ls_1 \rrbracket(\Gamma_3, \Delta'_3) = (\Gamma_2, \Delta'_2)$ for a given Δ'_2 similar to Δ_2 with respect to Γ . Thus $\llbracket ls \rrbracket = \llbracket s \rrbracket \circ \llbracket ls_1 \rrbracket$ and therefore the conclusion holds.

□

3.5.5 Soundness of the Program Semantic

A program is a sequence of statements. Starting with an empty type context, and an empty variable context, one statement at the time will be applied, resulting in a value e , a type T and a type context Γ such that $e \in \text{value}_\Gamma(T)$.

Theorem 3.13

Let $p \in \langle \text{program} \rangle$ and $T \in \mathcal{T}$. Assume $p : T$ can be derived.

Then there exist type contexts Γ and Δ such that $\llbracket p \rrbracket \in \text{value}_\Gamma(\bar{\Gamma}(T))$.

Proof. Let ls mms "main=" $e \in \langle \text{program} \rangle$, $ls \in \langle \text{list-statement} \rangle$, $mms \in \langle \text{maybe-main-sign} \rangle$ and $e \in \langle \text{exp} \rangle$. Assume $p : T$ for $T \in \mathcal{T}$, $\emptyset, \emptyset, ls \vdash \Gamma, \Delta$ and $\Gamma, \Delta \vdash e : T$ can be derived for type contexts Γ and Δ .

The assumption of Theorem ??, namely that $\emptyset, \emptyset, ls \vdash \Gamma, \Delta$ can be derived, holds. By applying said theorem we obtain $\llbracket ls \rrbracket(\emptyset, \emptyset) = (\Gamma, \Delta')$ for a variable context Δ' similar to Δ with respect to Γ . Therefore, $\llbracket p \rrbracket = \llbracket e \rrbracket_{\Gamma, \Delta'}$. We know $\Gamma, \Delta \vdash e : T$ and thus by Theorem ?? we know that $\llbracket e \rrbracket_{\Gamma, \Delta'} \in \text{value}_\Gamma(\bar{\Gamma}(T))$ and therefore the conclusion holds. □