4 Liquid Types

4.1 Notion of Liquid Types

So-called *refinement types* exclude values from existing types by using a predicate (in this context also called a *refinement*). The definition of such a refinement can be chosen quite freely, but it is important to note that one will also need to provide an algorithm to validate such refinements. This motivates the use of SMT solvers and refinements tailored to the capabilities of specific solvers. Such a set of refinement types are for example *liquid types* (**l**ogically **qu**al**i**fie**d** data types). We will now specify a version of liquid types. Note that definitions of liquid types vary dependent on the capability of the underlying SMT solver. In our case we will use a very modest definition that should be usable with an arbitrary solver.

We start by defining the syntax and semantic of valid refinements.

Definition 4.1: Logical Qualifier Expressions

We define the set of logical qualifier expressions $\mathcal{Q}$ as follows:

$$\begin{aligned}
\mathit{IntExp} ::=\ & \mathbb{Z} \\
|\ & \mathit{IntExp} + \mathit{IntExp} \\
|\ & \mathit{IntExp} * \mathbb{Z} \\
|\ & \mathcal{V} \\
\\
\mathcal{Q} ::=\ & \mathit{True} \\
|\ & \mathit{False} \\
|\ & \mathit{IntExp} < \mathcal{V} \\
|\ & \mathcal{V} < \mathit{IntExp} \\
|\ & \mathcal{V} = \mathit{IntExp} \\
|\ & \mathcal{Q} \wedge \mathcal{Q} \\
|\ & \mathcal{Q} \vee \mathcal{Q} \\
|\ & \neg \mathcal{Q}
\end{aligned}$$

Definition 4.2: Well-Formed Logical Qualifier Expressions

Let $e \in \mathcal{Q}$. Let $\Theta : \mathcal{V} \nrightarrow \mathbb{N}$.

—

We say e is *well formed* with respect to Θ iff for all variables v in e, $\Theta(v)$ is well-defined, meaning $\exists n \in \mathbb{N}.(v, n) \in \Theta$.

Definition 4.3: Semantics of Logical Qualifier Expressions

We define the semantic of arithmetic expressions *IntExp* as follows.

$$\begin{aligned}
[\![\cdot]\!]_{\cdot} : \mathit{IntExp} \to (\mathcal{V} \nrightarrow \mathbb{N}) \to \mathbb{N} \\
[\![n]\!]_{\Theta} =& n \\
[\![i + j]\!]_{\Theta} =& [\![i]\!]_{\Theta} + [\![j]\!]_{\Theta} \\
[\![i \cdot n]\!]_{\Theta} =& [\![i]\!]_{\Theta} \cdot n \\
[\![a]\!]_{\Theta} =& \Theta(a)
\end{aligned}$$

Note that we assume that the given expression is well-formed with respect to Θ.

We also define the semantic of logical qualifier expressions $\mathcal{Q}$ as follows:

$$\begin{aligned}
[\![\cdot]\!]_{\cdot} : \mathcal{Q} \to (\mathcal{V} \nrightarrow \mathbb{N}) \to \mathit{Bool} \\
[\![\mathit{True}]\!]_{\Theta} =& \mathit{True} \\
[\![\mathit{False}]\!]_{\Theta} =& \mathit{False} \\
[\![i < a]\!]_{\Theta} =& ([\![i]\!]_{\Theta} < [\![a]\!]_{\Theta}) \\
[\![a < i]\!]_{\Theta} =& ([\![a]\!]_{\Theta} < [\![i]\!]_{\Theta}) \\
[\![a = i]\!]_{\Theta} =& ([\![a]\!]_{\Theta} = [\![i]\!]_{\Theta}) \\
[\![p \wedge q]\!]_{\Theta} =& ([\![p]\!]_{\Theta} \wedge [\![q]\!]_{\Theta}) \\
[\![p \vee q]\!]_{\Theta} =& ([\![p]\!]_{\Theta} \vee [\![q]\!]_{\Theta}) \\
[\![\neg p]\!]_{\Theta} =& (\neg [\![p]\!]_{\Theta})
\end{aligned}$$

We will now extend our previous definition of types (see Definition) with the notion of refinement types. This extension is not very interesting, as refinement types don't behave differently from their underlying type.

Definition 4.4: Extended Types

We define the following

T is a *mono type* $:\Leftrightarrow$

$$\begin{aligned}
& T \text{ is a type variable} \\
\vee\ & T \text{ is a type application} \\
\vee\ & T \text{ is a algebraic type} \\
\vee\ & T \text{ is a product type} \\
\vee\ & T \text{ is a function type} \\
\vee\ & T \text{ is a liquid type}
\end{aligned}$$

T is a *poly type* $:\Leftrightarrow$

$$\begin{aligned}
& T = \forall a.T' \\
& \text{where } T' \text{ is a mono type} \\
& \text{or poly type and } a \text{ is a symbol.}
\end{aligned}$$

T is a *type*:$\Leftrightarrow$

$$\begin{aligned}&T \text{ is a mono type}\\ \vee\ &T \text{ is a poly type.}\end{aligned}$$

by using the predicates:

$$\begin{aligned}
T \text{ is a } \textit{type variable} :&\Leftrightarrow T \text{ is a symbol.}\\
T \text{ is a } \textit{type application} :&\Leftrightarrow T \text{ is of form } C\ T_1 \dots T_n\\
&\quad \text{where } n \in \mathbb{N}, C \text{ is a symbol and the } T_i \text{ are mono}\\
&\quad \text{types for all } i \in \mathbb{N}_1^n.\\
T \text{ is a } \textit{algebraic type} :&\Leftrightarrow T \text{ is of form}\\
&\quad \mu C.C_1\ T_{1,1} \dots T_{1,k(1)} \mid \dots \mid C_n\ T_{n,1} \dots T_{n,k(n)}\\
&\quad \text{such that } \exists i \in \mathbb{N}.\forall j \in \mathbb{N}_1^{k(i)}.T_{i,j} \neq C\\
&\quad \text{where } n \in \mathbb{N}, k \in \mathbb{N}_1^n \to \mathbb{N}_0, C \text{ is a symbol and}\\
&\quad T_{i,k(j)} \text{ is a mono type}\\
&\quad \text{ or } T_{i,k(j)} = C \text{ for all } i \in \mathbb{N}_1^n \text{ and } j \in \mathbb{N}_1^{k(i)}.\\
T \text{ is a } \textit{product type} :&\Leftrightarrow T \text{ is of form } \{l_1 : T_1, \dots, l_n : T_n\}\\
&\quad \text{where } n \in \mathbb{N}_0 \text{ and } l_i \text{ are symbols and } T_i \text{ are mono}\\
&\quad \text{types for all } i \in \mathbb{N}_1^n.\\
T \text{ is a } \textit{function type} :&\Leftrightarrow T \text{ is of form } T_1 \to T_2\\
&\quad \text{where } T_1 \text{ and } T_2 \text{ are mono types.}\\
T \text{ is a } \textit{liquid type} :&\Leftrightarrow T \text{ is of form } \{a : \textit{Int} \mid r\}\\
&\quad \text{where } T_0 \text{ is a type}, a \text{ is a symbol, } r \in \mathcal{Q},\\
&\quad \textit{Nat} := \mu C.1 \mid \textit{Succ}\ C\\
&\quad \text{and } \textit{Int} := \mu_.0 \mid \textit{Pos Nat} \mid \textit{Neg Nat}.\\
&\vee\ T \text{ is of form } a : \hat{T}_1 \to \hat{T}_2\\
&\quad \text{where } a \text{ is a symbol}, \hat{T}_2 \text{ and } \hat{T}_1 \text{ are liquid types}
\end{aligned}$$

Note that we mark a liquid type with a hat: $\hat{T}$ to distinguish it from a regular type T.

We will also need to redefine the definition of free variables and type substitution. The only change is the trival addition of refinement types.

Definition 4.5: Bound, Free, Set of free variables

Let $r \in \mathcal{Q}$, $n \in \mathbb{N}_0$, a be a type variable, T be a type, C be a symbol, $k \in \mathbb{N}_1^n \to \mathbb{N}_0$, T_i be a type, $T_{i,k(j)}$ be a type or a symbol and C_i be a symbol for all $i \in \mathbb{N}_1^n$ and $j \in \mathbb{N}_1^n$. Let $\textit{Nat} := \mu C.1 \mid \textit{Succ}\ C$ and $\textit{Int} := \mu\_.0 \mid \textit{Pos Nat} \mid \textit{Neg Nat}$.

—

We say

- a is *free* in $T :\Leftrightarrow a \in \mathit{free}(T)$
- a is *bound* in $T :\Leftrightarrow a \notin \mathit{free}(T)$ and a occurs in T.

where

$$
\begin{aligned}
\mathrm{free}(a) :=& \{a\}\\
\mathrm{free}(C\ T_1 \dots T_n) :=& \bigcup_{i \in \mathbb{N}_1^n} \mathrm{free}(T_i)\\
\mathrm{free}\begin{pmatrix} \mu C. \\ C_1\ T_{1,1} \dots\ T_{1,k(1)} \\ | \dots \\ |\ C_n\ T_{n,1} \dots\ T_{n,k(n)} \end{pmatrix} :=& \bigcup_{i \in \mathbb{N}_0^n} \bigcup_{j \in \mathbb{N}_0^{k_i}} \begin{cases} \varnothing & \text{if } T_{i,j} = C \\ \mathrm{free}(T_{i,j}) & \text{else} \end{cases}\\
\mathrm{free}(\{\_ : T_1, \dots, \_ : T_n\}) :=& \bigcup_{i \in \mathbb{N}_1^n} \mathrm{free}(T_i)\\
\mathrm{free}(T_1 \to T_2) :=& \mathrm{free}(T_1) \cup \mathrm{free}(T_2)\\
\mathrm{free}(\forall a.T) :=& \mathrm{free}(T) \backslash \{a\}\\
\mathrm{free}(\{a : \mathit{Int} \mid r\}) :=& \{\}\\
\mathrm{free}(a : \hat{T}_1 \to \hat{T}_2) :=& \mathrm{free}(\hat{T}_1) \cup \mathrm{free}(\hat{T}_2)
\end{aligned}
$$

Definition 4.6: Type substitution

Let $r \in \mathcal{Q}$, $n \in \mathbb{N}$, $\Theta : \mathcal{V} \nrightarrow \{t \in \mathcal{T} | t \text{ is a mono type}\}$, $a \in \mathcal{V}$. Let $T, T_1, T_2 \in \mathcal{T}$, $k : \mathbb{N}_1^n \to \mathbb{N}_0$ and $T_{i,k(j)} \in \mathcal{T}$ for all $i \in \mathbb{N}_1^n$ and $j \in \mathbb{N}_1^n$. Let $\hat{T}$ be a liquid type.

—

We define the substitute of a type $[.]_\Theta : \mathcal{T} \to \mathcal{T}$ as

$$
\begin{aligned}
[a]_\Theta :=& \begin{cases} S & \text{if } (a, S) \in \Theta \\ a & \text{else} \end{cases}\\
\begin{bmatrix} \mu C. \\ C_1\ T_{1,1} \dots\ T_{1,k(1)} \\ | \dots \\ |\ C_n\ T_{n,1} \dots\ T_{n,k(n)} \end{bmatrix}_\Theta :=& \begin{matrix} \mu C. \\ C_1\ [T_{1,1}]_{\Theta \backslash \{C,\_\}} \dots [T_{1,k_1}]_{\Theta \backslash \{C,\_\}} \\ | \dots \\ |\ C_n\ [T_{n,1}]_{\Theta \backslash \{C,\_\}} \dots [T_{n,k_n}]_{\Theta \backslash \{C,\_\}} \end{matrix}\\
[\{l_1 : T_1, \dots, l_n : T_n\}]_\Theta :=& \{l_1 : [T_1]_\Theta, \dots, l_n : [T_n]_\Theta\}\\
[T_1 \to T_2]_\Theta :=& [T_1]_\Theta \to [T_2]_\Theta\\
[\forall b.T]_\Theta :=& \begin{cases} [T]_\Theta & \text{if } \exists (b, S) \in \Theta \wedge S \notin \mathcal{V} \\ \forall S.[T]_\Theta & \text{if } \exists (b, S) \in \Theta \wedge S \in \mathcal{V} \\ \forall b.[T]_\Theta & \text{else.} \end{cases}\\
[\{a : \mathit{Int} \mid r\}]_\Theta :=& \{a : \mathit{Int} \mid r\}\\
[a : \hat{T}_1 \to \hat{T}_2]_\Theta :=& a : [\hat{T}_1]_\Theta \to [\hat{T}_2]_\Theta
\end{aligned}
$$

Θ is called the set of substitutions.

We will now redefine the notion of values. As mentioned before, liquid types exclude values that do not ensure a specific refinement.

Definition 4.7: Values

Let $r \in \mathcal{Q}$, $\mathcal{S}$ the class of all finite sets, $n \in \mathbb{N}$, $a \in \mathcal{V}$, $T, T_1, T_2, S \in \mathcal{T}$, $k \in \mathbb{N}_1^n \to \mathbb{N}_0$ and $T_{i,k(j)} \in \mathcal{T}$ for all $i \in \mathbb{N}_1^n$ and $j \in \mathbb{N}_1^n$. Let Γ be a type context. Let $\hat{T}$ be a liquid type.

—

We define

$$\begin{aligned}
\mathrm{values}_\Gamma &: \mathcal{V} \to \mathcal{S} \\
\mathrm{values}_\Gamma(a) &:= \mathrm{values}_\Gamma(\Gamma(a)) \\
\mathrm{values}_\Gamma(C\ T_1\ \dots\ T_n) &:= \mathrm{values}_\Gamma(\overline{\Gamma(C)}(T_1, \dots, T_n)) \\
\mathrm{values}_\Gamma\begin{pmatrix} \mu C. \\ |C_1\ T_{1,1} \dots\ T_{1,k(1)} \\ | \dots \\ |\ C_n\ T_{n,1} \dots\ T_{n,k(n)} \end{pmatrix} &:= \bigcup_{i \in \mathbb{N}_0} \mathrm{rvalues}_\Gamma\left(i,\ \begin{matrix} \mu C. \\ |\ C_1\ T_{1,1} \dots\ T_{1,k(1)} \\ | \dots \\ |\ C_n\ T_{n,1} \dots\ T_{n,k(n)} \end{matrix}\right) \\
\mathrm{values}_\Gamma(\{l_1 : T_1, \dots, l_n : T_n\}) &:= \Big\{\{l_1 = t_1, \dots, l_n = t_n\} \\
&\qquad \mid \forall i \in \mathbb{N}_1^n . t_i \in \mathrm{values}_\Gamma(T_i)\Big\} \\
\mathrm{values}_\Gamma(T_1 \to T_2) &:= \{f \mid f \in \mathrm{values}_\Gamma(T_1) \to \mathrm{values}_\Gamma(T_2)\} \\
\mathrm{values}_\Gamma(\forall a.T) &:= \lambda b.\mathrm{values}_{\{(a,b)\} \cup \Gamma}(T) \text{ where the symbol } b \text{ does} \\
&\qquad \text{not occur in } T. \\
\mathrm{values}_\Gamma(\{a : \mathit{Int} \mid r\}) &:= \mathrm{refinedValues}_{\{\}}(\{a : \mathit{Int} \mid r\}) \\
\mathrm{values}_\Gamma(a : \hat{T}_1 \to \hat{T}_2) &:= \mathrm{refinedValues}_{\{\}}(a : \hat{T}_1 \to \hat{T}_2)
\end{aligned}$$

using the following helper functions.

Let $l \in \mathbb{N}, T := \mu C.\ |\ C_1\ T_{1,1} \dots\ T_{1,k(1)}\ | \dots\ |\ C_n\ T_{n,1} \dots\ T_{n,k(n)}$. We define:

$$\mathrm{rvalues}_\Gamma(0, T) := \left\{ C_i\ v_1 \dots v_n \ \middle|\ \begin{matrix} i \in \mathbb{N}_1^n \\ \wedge \forall j \in \mathbb{N}_1^{k(i)} . T_{i,j} \neq C \wedge v_j \in \mathrm{values}_\Gamma(T_{i,j}) \end{matrix} \right\}$$

$$\mathrm{rvalues}_\Gamma(l+1, T) := \left\{ C_i\ v_1 \dots v_n \ \middle|\ \begin{matrix} i \in \mathbb{N}_1^n \\ \wedge \forall j \in \mathbb{N}_1^{k(i)} . v_j \in \begin{cases} \mathrm{rvalues}_\Gamma(l, T) & \text{if } T_{i,j} = C \\ \mathrm{values}_\Gamma(T_{i,j}) & \text{else} \end{cases} \end{matrix} \right\}$$

Let $\Theta : \mathcal{V} \nrightarrow \mathbb{N}$. We define:

$$\begin{aligned}
&\mathrm{refinedValues}_\Theta(\{a : \mathit{Int} \mid r\}) := \\
&\qquad \{n \in \mathrm{values}_{\{\}}(\mathit{Int}) | \\
&\qquad r \text{ is well formed with respect to } \Theta \cup \{(a, n)\} \wedge [\![r]\!]_{\Theta \cup \{(a,n)\}}\}
\end{aligned}$$

$$
\begin{aligned}
&\text{refinedValues}_\Theta(a : \hat{T}_1 \to \hat{T}_2) := \\
&\qquad \{b \in \text{values}_{\{\}}(\hat{T}_1 \to \hat{T}_2) | \\
&\qquad \forall n \in \text{values}_{\{\}}(\hat{T}_1).b(n) \in \text{refinedValues}_{\Theta \cup \{(a,n)\}}(\hat{T}_2)\}
\end{aligned}
$$