

# 1 Formalization

## 1.1 Syntax

$$\begin{array}{ll} f \in \text{TRANSFORMER NAMES} & t \in \text{TYPE NAMES} \\ a, x, y, z \in \text{IDENTIFIERS} & \end{array}$$

$$\begin{array}{ll} \mathcal{Q}, \mathcal{R}, \mathcal{S} & ::= ! \mid \text{any} \mid \text{nonempty} \mid \text{empty} \mid \text{every} & \text{(type quantities)} \\ M & ::= \text{fungible} \mid \text{unique} \mid \text{immutable} \mid \text{consumable} \mid \text{asset} & \text{(type declaration modifiers)} \\ T & ::= \text{bool} \mid \text{nat} \mid \text{type } t \text{ is } \overline{M} \ T \mid \text{list } \tau \mid \{\overline{x} : \overline{\tau}\} & \text{(base types)} \\ \tau, \sigma, \pi & ::= \mathcal{Q} \ T & \text{(types)} \\ \mathcal{S} & ::= x \mid x.y \mid \text{true} \mid \text{false} \mid n \mid \text{demote}(x) \mid [x] \mid \{\overline{x} : \overline{\tau} \mapsto \overline{x}\} \mid \text{new}(t, \overline{M}, T) & \text{(sources)} \\ \mathcal{D} & ::= x \mid x.y \mid \text{var } x : T \mid \text{consume} & \text{(destinations)} \\ \text{Decl} & ::= \text{transformer } f(\overline{x} : \overline{\tau}) \rightarrow x : \tau \ \{\overline{\text{Stmt}}\} & \text{(transformers)} \\ \text{Stmt} & ::= \text{skip} \\ & \mid \mathcal{S} \rightarrow \mathcal{D} \mid \mathcal{S} \xrightarrow{x} \mathcal{D} \mid \mathcal{S} \xrightarrow{\mathcal{Q} \text{ s.t. } f(\overline{x})} \mathcal{D} \mid \mathcal{S} \rightarrow f(\overline{x}) \rightarrow \mathcal{D} \\ & \mid \text{try } \{\overline{\text{Stmt}}\} \text{ catch } \{\overline{\text{Stmt}}\} \\ \text{Prog} & ::= \overline{\text{Decl}}; \overline{\text{Stmt}} \end{array}$$

[Add rules for flow-by-variable.] [Remove bool type? Can implement the “filter” selectors another way, e.g., by using a transformer returning a pair.]

## 1.2 Statics

$\boxed{\Gamma \vdash \mathcal{S} : \tau \dashv \Delta} \quad \boxed{\Gamma \vdash \mathcal{D} : \tau \dashv \Delta}$  **Storage Typing**

A *storage* is either a source or a destination.

$$\begin{array}{c} \frac{b \in \{\text{true}, \text{false}\}}{\Gamma \vdash b : ! \text{bool} \dashv \Gamma} \text{BOOL} \qquad \frac{}{\Gamma \vdash n : ! \text{nat} \dashv \Gamma} \text{NAT} \\[10pt] \frac{}{\Gamma, x : \tau \vdash \text{demote}(x) : \text{demote}(\tau) \dashv \Gamma, x : \tau} \text{DEMOTE} \qquad \frac{\neg(\tau \text{ immutable})}{\Gamma, x : \tau \vdash x : \tau \dashv \Gamma, x : \tau} \text{VAR} \\[10pt] \frac{\Gamma \vdash x : ! T \dashv \Delta \quad \neg(T \text{ immutable}) \quad \text{fields}(T) = \overline{z} : \overline{\sigma} \quad y : \tau \in \overline{z} : \overline{\sigma}}{\Gamma \vdash x.y : \tau \dashv \Gamma} \text{FIELD} \\[10pt] \frac{}{\Gamma, x : \mathcal{Q} \ T \vdash [x] : ! \text{list } \mathcal{Q} \ T \dashv \Gamma, x : \text{empty } T} \text{SINGLE} \\[10pt] \frac{}{\Gamma, \overline{y} : \mathcal{Q} \ \overline{T} \vdash \{\overline{x} : \mathcal{Q} \ \overline{T} \mapsto \overline{y}\} : ! \{\overline{x} : \mathcal{Q} \ \overline{T}\} \dashv \Gamma, \overline{y} : \text{empty } \overline{T}} \text{RECORD} \\[10pt] \frac{}{\Gamma \vdash \text{new}(t, \overline{M}, T) : \text{every list } ! (\text{type } t \text{ is } \overline{M} \ T) \dashv \Gamma} \text{NEW} \\[10pt] \frac{}{\Gamma \vdash (\text{var } x : T) : \text{empty } T \dashv \Gamma, x : \text{empty } T} \text{VARDEF} \qquad \frac{\tau \text{ consumable}}{\Gamma \vdash \text{consume} : \tau \dashv \Gamma} \text{CONSUME} \end{array}$$

$\boxed{\Gamma \vdash S \text{ ok} \dashv \Delta}$  **Statement Well-formedness**

$$\frac{}{\Gamma \vdash \text{skip ok} \dashv \Gamma} \text{OK-SKIP} \quad \frac{\Gamma \vdash S : \mathcal{Q} \ T \dashv \Delta \quad \text{update}(\Delta, S, \Delta(S) \ominus Q) \vdash D : \mathcal{R} \ T \dashv \Xi}{\Gamma \vdash (S \rightarrow D) \text{ ok} \dashv \text{update}(\Xi, D, \Xi(D) \oplus Q)} \text{OK-FLOW-EVERY}$$

$$\frac{\Gamma \vdash S : \mathcal{Q} \ T \dashv \Delta \quad \Delta \vdash x : \text{demote}(\mathcal{R} \ T) \dashv \Delta \quad \text{update}(\Delta, S, \Delta(S) \ominus Q) \vdash D : S \ T \dashv \Xi}{\Gamma \vdash (S \xrightarrow{x} D) \text{ ok} \dashv \text{update}(\Xi, D, \Xi(D) \oplus \mathcal{R})} \text{OK-FLOW-VAR}$$

$$\frac{\begin{array}{c} \Gamma \vdash S : \mathcal{Q} \ T \dashv \Delta \\ \text{transformer } f(\overline{x} : \overline{\sigma}, y : \text{demote}(\text{elementype}(T))) \rightarrow z : ! \text{bool} \{ \overline{\text{Stmt}} \} \\ \forall i. \text{demote}(\Gamma(a_i)) = \sigma_i \quad \text{update}(\Delta, S, \Delta(S) \ominus Q) \vdash D : S \ T \dashv \Xi \end{array}}{\Gamma \vdash (S \xrightarrow{\mathcal{R} \text{ s.t. } f(\overline{a})} D) \text{ ok} \dashv \text{update}(\Xi, D, \Xi(D) \oplus \min(\mathcal{Q}, \mathcal{R}))} \text{OK-FLOW-FILTER}$$

$$\frac{\begin{array}{c} \Gamma \vdash S : \mathcal{Q} \ T_1 \dashv \Delta \\ \text{transformer } f(\overline{x} : \overline{\sigma}, y : \text{demote}(\text{elementype}(T_1))) \rightarrow z : \mathcal{R} \ T_2 \{ \overline{\text{Stmt}} \} \\ \forall i. \text{demote}(\Gamma(x_i)) = \sigma_i \quad \text{update}(\Delta, S, \Delta(S) \ominus Q) \vdash D : S \ T_2 \dashv \Xi \end{array}}{\Gamma \vdash (S \rightarrow f(\overline{x}) \rightarrow D) \text{ ok} \dashv \text{update}(\Xi, D, \Xi(D) \oplus Q)} \text{OK-FLOW-TRANSFORMER}$$

$$\frac{\Gamma \vdash \overline{S_1} \text{ ok} \dashv \Delta \quad \Gamma \vdash \overline{S_2} \text{ ok} \dashv \Xi}{\Gamma \vdash (\text{try } \{ \overline{S_1} \} \text{ catch } \{ \overline{S_2} \}) \text{ ok} \dashv \Delta \sqcup \Xi} \text{OK-TRY}$$

$\boxed{\vdash \text{Decl ok}}$  **Declaration Well-formedness**

$$\frac{\overline{x} : \overline{\tau} \vdash \overline{\text{Stmt}} \text{ ok} \dashv \Gamma, y : \sigma \quad \forall \pi \in \text{img}(\Gamma). \neg(\pi \text{ asset})}{\vdash (\text{transformer } f(\overline{x} : \overline{\tau}) \rightarrow y : \sigma \{ \overline{\text{Stmt}} \}) \text{ ok}} \text{OK-TRANSFORMER}$$

$\boxed{\text{Prog ok}}$  **Program Well-formedness**

$$\frac{\vdash \overline{\text{Decl}} \text{ ok} \quad \emptyset \vdash \overline{\text{Stmt}} \text{ ok} \dashv \Gamma \quad \forall \tau \in \text{img}(\Gamma). \neg(\tau \text{ asset})}{(\overline{\text{Decl}}; \overline{\text{Stmt}}) \text{ ok}} \text{OK-PROG}$$

### 1.3 Dynamics

$$V ::= \text{true} \mid \text{false} \mid n \mid \{x : \tau \mapsto V\}$$

$$\mathcal{V} ::= \overline{V}$$

[We don't strictly need the type in the records

$$\text{Stmt} ::= \dots \mid \text{put}(\mathcal{V}, D) \mid \text{revert} \mid \text{try}(\Sigma, \overline{S}, \overline{S})$$

right now, but it doesn't really hurt either, I think.]

**Definition 1.** An environment  $\Sigma$  is a tuple  $(\mu, \rho)$  where  $\mu : \text{IDENTIFIERNAMES} \rightarrow \mathbb{N}$  is the variable lookup environment, and  $\rho : \mathbb{N} \rightarrow \mathcal{V}$  is the storage environment.

$$\boxed{\langle \Sigma, \text{Stmt} \rangle \rightarrow \langle \Sigma, \text{Stmt} \rangle}$$

Note that we abbreviate  $\langle \Sigma, \cdot \rangle$  as  $\Sigma$ , which signals the end of evaluation.

The new constructs of  $\text{resolve}(\Sigma, S)$  and  $\text{put}(\mathcal{V}, D)$  are used to simplify the process of locating sources and updating destinations, respectively.

$$\frac{\langle \Sigma, S_1 \rangle \rightarrow \langle \Sigma', \overline{S_3} \rangle}{\langle \Sigma, S_1 \overline{S_2} \rangle \rightarrow \langle \Sigma', \overline{S_3} \overline{S_2} \rangle} \text{SEQ} \quad \frac{}{\langle \Sigma, (\text{revert}) \overline{S} \rangle \rightarrow \langle \Sigma, \text{revert} \rangle} \text{REVERT} \quad \frac{}{\langle \Sigma, \text{skip} \rangle \rightarrow \Sigma} \text{SKIP}$$

Here we give the rules for the new  $\text{put}(\mathcal{V}, \mathcal{D})$  statement. **[TODO: Need to finalize how  $\mathcal{V} + \mathcal{W}$  works; in particular, need to make sure that you can't overwrite things that shouldn't be overwritten (e.g., a nonfungible nat). Probably need to tag types with modifiers or something.]**

$$\begin{array}{c}
\frac{}{\langle \Sigma, \text{put}(\mathcal{V}, \text{consume}) \rangle \rightarrow \Sigma} \text{PUT-CONSUME} \qquad \frac{}{\langle \Sigma, \text{put}(\mathcal{V}, x) \rangle \rightarrow \langle \Sigma, \text{put}(\mathcal{V}, \mu(x)) \rangle} \text{PUT-VAR} \\
\\
\frac{\rho(\mu(X)) = \overline{\{x : \tau \mapsto \ell\}} \quad (y : \sigma \mapsto k) \in \overline{x : \tau \mapsto \ell}}{\langle \Sigma, \text{put}(\mathcal{V}, x.y) \rangle \rightarrow \langle \Sigma, \text{put}(\mathcal{V}, k) \rangle} \text{PUT-FIELD} \\
\\
\frac{\rho(\ell) = \mathcal{W} \quad \mathcal{W} + \mathcal{V} \neq \text{revert}}{\langle \Sigma, \text{put}(\mathcal{V}, \ell) \rangle \rightarrow \Sigma[\rho \mapsto \rho[\ell \mapsto \mathcal{W} + \mathcal{V}]]} \text{PUT-LOC} \qquad \frac{\rho(\ell) = \mathcal{W} \quad \mathcal{W} + \mathcal{V} = \text{revert}}{\langle \Sigma, \text{put}(\mathcal{V}, \ell) \rangle \rightarrow \langle \Sigma, \text{revert} \rangle} \text{PUT-LOC-FAIL} \\
\\
\frac{\ell \notin \text{dom}(\rho)}{\langle \Sigma, \text{put}(\mathcal{V}, \text{var } A : T) \rangle \rightarrow \Sigma[\mu \mapsto \mu[A \mapsto \ell], \rho \mapsto \rho[\ell \mapsto \mathcal{V}]]} \text{PUT-VARDEF} \\
\\
\frac{\text{resolve}(\Sigma, \mathcal{S}) = (\Sigma', \ell)}{\langle \Sigma, \mathcal{S} \rightarrow \mathcal{D} \rangle \rightarrow \langle \Sigma'[\rho \mapsto \rho'[\ell \mapsto []]], \text{put}(\rho'(\ell), \mathcal{D}) \rangle} \text{FLOW-EVERY} \\
\\
\frac{\text{resolve}(\Sigma, \mathcal{S}) = (\Sigma', \ell) \quad \rho'(\ell) = \mathcal{V} \quad \rho'(\mu'(x)) = \mathcal{W} \quad \mathcal{W} \leq \mathcal{V}}{\langle \Sigma, \mathcal{S} \xrightarrow{x} \mathcal{D} \rangle \rightarrow \langle \Sigma'[\rho \mapsto \rho'[\ell \mapsto \mathcal{V} - \mathcal{W}]], \text{put}(\mathcal{W}, \mathcal{D}) \rangle} \text{FLOW-VAR} \\
\\
\frac{\text{resolve}(\Sigma, \mathcal{S}) = (\Sigma', \ell) \quad \rho'(\ell) = \mathcal{V} \quad \rho'(\mu'(x)) = \mathcal{W} \quad \mathcal{W} \not\leq \mathcal{V}}{\langle \Sigma, \mathcal{S} \xrightarrow{x} \mathcal{D} \rangle \rightarrow \langle \Sigma', \text{revert} \rangle} \text{FLOW-VAR-FAIL} \\
\\
\frac{\text{resolve}(\Sigma, \mathcal{S}) = (\Sigma', \ell) \quad \rho'(\ell) = \mathcal{V} \quad \mathcal{U} = [v \in \mathcal{V} \mid \langle \Sigma', f(\bar{x}, v) \rangle \rightarrow^* \langle \Sigma'', k \rangle \text{ and } \rho''(k) = \text{true}] \quad \text{compat}(|\mathcal{U}|, |\mathcal{V}|, \mathcal{Q})}{\left\langle \Sigma, (\mathcal{S} \xrightarrow{\mathcal{Q} \text{ s.t. } f(\bar{x})} \mathcal{D}) \right\rangle \rightarrow \langle \Sigma'[\rho' \mapsto \rho'[\ell \mapsto \rho'(\ell) - \mathcal{U}]], \text{put}(\mathcal{U}, \mathcal{D}) \rangle} \text{FLOW-FILTER} \\
\\
\frac{\text{resolve}(\Sigma, \mathcal{S}) = (\Sigma', \ell) \quad \rho'(\ell) = \mathcal{V} \quad \mathcal{U} = [v \in \mathcal{V} \mid \langle \Sigma', f(\bar{x}, v) \rangle \rightarrow^* \langle \Sigma'', k \rangle \text{ and } \rho''(k) = \text{true}] \quad \neg \text{compat}(|\mathcal{U}|, |\mathcal{V}|, \mathcal{Q})}{\left\langle \Sigma, (\mathcal{S} \xrightarrow{\mathcal{Q} \text{ s.t. } f(\bar{x})} \mathcal{D}) \right\rangle \rightarrow \langle \Sigma', \text{revert} \rangle} \text{FLOW-FILTER-FAIL} \\
\\
\frac{\text{resolve}(\Sigma, \mathcal{S}) = (\Sigma', \ell) \quad \rho'(\ell) = v, \mathcal{V} \quad \langle \Sigma'[\rho \mapsto \rho'[\ell \mapsto \mathcal{V}]], f(\bar{x}, v) \rangle \rightarrow^* \langle \Sigma'', k \rangle}{\langle \Sigma, \mathcal{S} \rightarrow f(\bar{x}) \rightarrow \mathcal{D} \rangle \rightarrow \langle (\mu', \rho''), \text{put}(\rho''(k), \mathcal{D}) (\mathcal{S} \rightarrow f(\bar{x}) \rightarrow \mathcal{D}) \rangle} \text{FLOW-TRANSFORMER} \\
\\
\frac{\text{resolve}(\Sigma, \mathcal{S}) = (\Sigma', \ell) \quad \rho'(\ell) = []}{\langle \Sigma, \mathcal{S} \rightarrow f(\bar{x}) \rightarrow \mathcal{D} \rangle \rightarrow \Sigma} \text{FLOW-TRANSFORMER-DONE} \\
\\
\frac{\ell \notin \text{dom}(\rho) \quad \text{transformer } f(\bar{y} : \tau) \rightarrow z : \sigma \{ \bar{S} \} \quad \mu' = \overline{y \mapsto \mu(x)}, z \mapsto \ell}{\langle \Sigma, f(\bar{x}) \rangle \rightarrow \langle (\mu', \rho[\ell \mapsto []]), \bar{S} \ell \rangle} \text{CALL}
\end{array}$$

We introduce a new statement,  $\text{try}(\Sigma, \overline{S_1}, \overline{S_2})$ , to implement the try-catch statement, which keeps track of the environment that we begin execution in so that we can revert to the original environment in the case of a `revert`.

$$\begin{array}{c}
\overline{\langle \Sigma, \text{try } \{\overline{S_1}\} \text{ catch } \{\overline{S_2}\} \rangle} \rightarrow \overline{\langle \Sigma, \text{try}(\Sigma, \overline{S_1}, \overline{S_2}) \rangle} \quad \text{TRY-START} \\
\\
\frac{\langle \Sigma, \overline{S_1} \rangle \rightarrow \langle \Sigma'', \overline{S'_1} \rangle}{\overline{\langle \Sigma, \text{try}(\Sigma', \overline{S_1}, \overline{S_2}) \rangle} \rightarrow \overline{\langle \Sigma'', \text{try}(\Sigma', \overline{S'_1}, \overline{S_2}) \rangle}} \quad \text{TRY-STEP} \\
\\
\overline{\langle \Sigma, \text{try}(\Sigma', \text{revert}, \overline{S_2}) \rangle} \rightarrow \overline{\langle \Sigma', \overline{S_2} \rangle} \quad \text{TRY-REVERT} \qquad \overline{\langle \Sigma, \text{try}(\Sigma', \cdot, \overline{S_2}) \rangle} \rightarrow \Sigma \quad \text{TRY-DONE}
\end{array}$$

[Need to handle fungible specially (or maybe only after adding nats, I'm not sure it really has any meaning without them)]

$\text{resolve}(\Sigma, S) = (\Sigma', \ell)$  **Storage Resolution**

We use  $\text{resolve}(\Sigma, S)$  to get the location storing the values of  $S$ , which returns an environment because it may need to allocate new memory (e.g., in the case of creating a new record value).

$$\begin{array}{c}
\frac{\mu(S) = \ell}{\text{resolve}(\Sigma, S) = (\Sigma, \ell)} \quad \text{RESOLVE-VAR} \qquad \frac{\rho(\mu(x)) = \overline{\{z : \tau \mapsto \ell\}} \quad (y : \sigma \mapsto k) \in \overline{\{z : \tau \mapsto \ell\}}}{\text{resolve}(\Sigma, x.y) = (\Sigma, k)} \quad \text{RESOLVE-FIELD} \\
\\
\frac{\ell \notin \text{dom}(\rho)}{\text{resolve}(\Sigma, [x]) = (\Sigma[\rho \mapsto \rho[\ell \mapsto \rho(\mu(x)), \mu(x) \mapsto []]], \ell)} \quad \text{RESOLVE-SINGLE} \\
\\
\frac{\ell \notin \text{dom}(\rho) \quad k \notin \text{dom}(\rho) \cup \overline{\ell} \quad \Sigma' = \Sigma[\rho \mapsto \rho[\mu(y) \mapsto [], \ell \mapsto \rho(\mu(y)), k \mapsto \overline{\{x : \tau \mapsto \ell\}}]]}{\text{resolve}(\Sigma, \{x : \tau \mapsto \overline{y}\}) = (\Sigma', k)} \quad \text{RESOLVE-RECORD} \\
\\
\frac{b \in \{\text{true}, \text{false}\} \quad \ell \notin \text{dom}(\rho)}{\text{resolve}(\Sigma, b) = (\Sigma[\rho \mapsto \rho[\ell \mapsto b]], \ell)} \quad \text{RESOLVE-BOOL} \\
\\
\frac{\mu(t) = \ell}{\text{resolve}(\Sigma, \text{new}(t, \overline{M}, T)) = (\Sigma, \ell)} \quad \text{RESOLVE-SOURCE} \\
\\
\frac{t \notin \text{dom}(\mu) \quad \ell \notin \text{dom}(\rho)}{\text{resolve}(\Sigma, \text{new}(t, \overline{M}, T)) = (\Sigma'[\rho \mapsto \rho[\ell \mapsto \text{values}(T)], \mu \mapsto \mu[t \mapsto \ell]], \ell)} \quad \text{RESOLVE-NEW-SOURCE}
\end{array}$$

[TODO: Need to be sure to handle uniqueness correctly; could do this in RESOLVE-NEW-SOURCE, or in the various flow rules.]

## 1.4 Auxiliaries

**Definition 2.** Define  $\text{Quant} = \{\text{empty}, \text{any}, !, \text{nonempty}, \text{every}\}$ , and call any  $Q \in \text{Quant}$  a type quantity. Define  $\text{empty} < \text{any} < ! < \text{nonempty} < \text{every}$ .

$\tau$  asset **Asset Types**

$$\begin{aligned}
(Q \ T) \text{ asset} &\Leftrightarrow Q \neq \text{empty} \text{ and } (\text{asset} \in \text{modifiers}(T) \text{ or} \\
&\quad (T = \mathcal{C} \ \tau \text{ and } \tau \text{ asset}) \text{ or} \\
&\quad (T = \{\overline{y:\sigma}\} \text{ and } \exists x : \tau \in \overline{y:\sigma}.(\tau \text{ asset})))
\end{aligned}$$

$\tau$  consumable **Consumable Types**

$$\begin{aligned}
(Q \ T) \text{ consumable} &\Leftrightarrow \text{consumable} \in \text{modifiers}(T) \text{ or} \\
&\quad \neg((Q \ T) \text{ asset}) \text{ or} \\
&\quad (T = \mathcal{C} \ \tau \text{ and } \tau \text{ consumable}) \text{ or} \\
&\quad (T = \{\overline{y:\sigma}\} \text{ and } \forall x : \tau \in \overline{y:\sigma}.(\sigma \text{ consumable}))
\end{aligned}$$

$Q \oplus \mathcal{R}$  represents the quantity present when flowing  $\mathcal{R}$  of something to a storage already containing  $Q$ .  $Q \ominus \mathcal{R}$  represents the quantity left over after flowing  $\mathcal{R}$  from a storage containing  $Q$ .

**Definition 3.** Let  $Q, \mathcal{R} \in \mathbf{Quant}$ . Define the commutative operator  $\oplus$ , called combine, as the unique function  $\mathbf{Quant}^2 \rightarrow \mathbf{Quant}$  such that

$$\begin{aligned}
Q \oplus \text{empty} &= Q \\
Q \oplus \text{every} &= \text{every} \\
\text{nonempty} \oplus \mathcal{R} &= \text{nonempty} \quad \text{if } \text{empty} < \mathcal{R} < \text{every} \\
! \oplus \mathcal{R} &= \text{nonempty} \quad \text{if } \text{empty} < \mathcal{R} < \text{every} \\
\text{any} \oplus \text{any} &= \text{any}
\end{aligned}$$

Define the operator  $\ominus$ , called split, as the unique function  $\mathbf{Quant}^2 \rightarrow \mathbf{Quant}$  such that

$$\begin{aligned}
Q \ominus \text{empty} &= Q \\
\text{empty} \ominus \mathcal{R} &= \text{empty} \\
Q \ominus \text{every} &= \text{empty} \\
\text{every} \ominus \mathcal{R} &= \text{every} \quad \text{if } \mathcal{R} < \text{every} \\
\text{nonempty} - \mathcal{R} &= \text{any} \quad \text{if } \text{empty} < \mathcal{R} < \text{every} \\
! - \mathcal{R} &= \text{empty} \quad \text{if } ! \leq \mathcal{R} \\
! - \text{any} &= \text{any} \\
\text{any} - \mathcal{R} &= \text{any} \quad \text{if } \text{empty} < \mathcal{R} < \text{every}
\end{aligned}$$

Note that we write  $(Q \ T) \oplus \mathcal{R}$  to mean  $(Q \oplus \mathcal{R}) \ T$  and similarly  $(Q \ T) \ominus \mathcal{R}$  to mean  $(Q \ominus \mathcal{R}) \ T$ .

**Definition 4.** We can consider a type environment  $\Gamma$  as a function  $\text{IDENTIFIERS} \rightarrow \text{TYPES} \cup \{\perp\}$  as follows:

$$\Gamma(x) = \begin{cases} \tau & \text{if } x : \tau \in \Gamma \\ \perp & \text{otherwise} \end{cases}$$

We write  $\text{dom}(\Gamma)$  to mean  $\{x \in \text{IDENTIFIERS} \mid \Gamma(x) \neq \perp\}$ , and  $\Gamma|_X$  to mean the environment  $\{x : \tau \in \Gamma \mid x \in X\}$  (restricting the domain of  $\Gamma$ ).

**Definition 5.** Let  $Q$  and  $\mathcal{R}$  be type quantities,  $T_Q$  and  $T_{\mathcal{R}}$  base types, and  $\Gamma$  and  $\Delta$  type environments. Define the following orderings, which make types and type environments into join-semilattices. For type quantities, define the partial order  $\sqsubseteq$  as the reflexive closure of the strict partial order  $\sqsubset$  given by

$$Q \sqsubset \mathcal{R} \Leftrightarrow (Q \neq \text{any} \text{ and } \mathcal{R} = \text{any}) \text{ or } (Q \in \{!, \text{every}\} \text{ and } \mathcal{R} = \text{nonempty})$$

For types, define the partial order  $\leq$  by

$$\mathcal{Q} \ T_Q \leq \mathcal{R} \ T_R \Leftrightarrow T_Q = T_R \text{ and } \mathcal{Q} \sqsubseteq \mathcal{R}$$

For type environments, define the partial order  $\leq$  by

$$\Gamma \leq \Delta \Leftrightarrow \forall x. \Gamma(x) \leq \Delta(x)$$

Denote the join of  $\Gamma$  and  $\Delta$  by  $\Gamma \sqcup \Delta$ .

$$\boxed{\text{elemtype}(T) = \tau}$$

$$\text{elemtype}(T) = \begin{cases} \text{elemtype}(T') & \text{if } T = \text{type } t \text{ is } \overline{M} \ T' \\ \tau & \text{if } T = \mathcal{C} \ \tau \\ ! \ T & \text{otherwise} \end{cases}$$

$$\boxed{\text{modifiers}(T) = \overline{M}} \text{ Type Modifiers}$$

$$\text{modifiers}(T) = \begin{cases} \overline{M} & \text{if } T = \text{type } t \text{ is } \overline{M} \ T \\ \emptyset & \text{otherwise} \end{cases}$$

$$\boxed{\text{demote}(\tau) = \sigma} \quad \boxed{\text{demote}_*(T_1) = T_2}$$

**Type Demotion**  $\text{demote}$  and  $\text{demote}_*$  take a type and “strip” all the asset modifiers from it, as well as unfolding named type definitions. This process is useful, because it allows selecting asset types without actually having a value of the desired asset type. Note that demoting a transformer type changes nothing. This is because a transformer is **never** an asset, regardless of the types that it operators on, because it has no storage.

$$\text{demote}(\mathcal{Q} \ T) = \mathcal{Q} \ \text{demote}_*(T)$$

$$\text{demote}_*(\text{bool}) = \text{bool}$$

$$\text{demote}_*(\text{nat}) = \text{nat}$$

$$\text{demote}_*({\overline{\{x : \tau\}}}) = {\overline{\{x : \text{demote}(\tau)\}}}$$

$$\text{demote}_*(\text{type } t \text{ is } \overline{M} \ T) = \text{demote}_*(T)$$

$$\boxed{\text{fields}(T) = \overline{x : \tau}} \text{ Fields}$$

$$\text{fields}(T) = \begin{cases} \overline{x : \tau} & \text{if } T = {\overline{\{x : \tau\}}} \\ \text{fields}(T) & \text{if } T = \text{type } t \text{ is } \overline{M} \ T \\ \emptyset & \text{otherwise} \end{cases}$$

$$\boxed{\text{update}(\Gamma, x, \tau)} \text{ Type environment modification}$$

$$\text{update}(\Gamma, x, \tau) = \begin{cases} \Delta, x : \tau & \text{if } \Gamma = \Delta, x : \sigma \\ \Gamma & \text{otherwise} \end{cases}$$

$$\boxed{\text{compat}(n, m, \mathcal{Q})}$$

The relation  $\text{compat}(n, m, \mathcal{Q})$  holds when the number of values sent,  $n$ , is compatible with the original number of values  $m$ , and the type quantity used,  $\mathcal{Q}$ .

$\text{compat}(n, m, Q) \Leftrightarrow (Q = \text{nonempty} \text{ and } n \geq 1) \text{ or}$   
 $(Q = ! \text{ and } n = 1) \text{ or}$   
 $(Q = \text{empty} \text{ and } n = 0) \text{ or}$   
 $(Q = \text{every} \text{ and } n = m) \text{ or}$   
 $Q = \text{any}$

$\text{values}(T) = \mathcal{V}$  The function **values** gives a list of all of the values of a given base type.

$\text{values}(\text{bool}) = [\text{true}, \text{false}]$   
 $\text{values}(\text{nat}) = [0, 1, 2, \dots]$   
 $\text{values}(\text{list } T) = [L \mid L \subseteq \text{values}(T), |L| < \infty]$   
 $\text{values}(\text{type } t \text{ is } \overline{M} T) = \text{values}(T)$   
 $\text{values}(\{\overline{x : Q} \overline{T}\}) = [\{\overline{x : \tau} \mapsto v\} \mid v \in \text{values}(T)]$