Specification of the Nouga DSL

Simon Cockx

October 18, 2021

The goal of this work is two-fold. On the one hand it aims to eliminate flaws from the Rosetta language by formalizing its grammar and typing system. On the other hand it seeks to give solid ground for developers of code generators, giving a single source of truth about the intended semantics of generated code. Note that these goals also constitute two different audiences; one the developers of Rosetta, the other parties interested in translating Rosetta to a new language.

Throughout this document, T and S represent basic types and C represents a cardinality.

1 Syntax

Metavariables: D and E range over entity names, F ranges over function names, a and b range over attribute and parameter names, i and j range over signed integers, k and l range over positive integers, r ranges over signed decimals. Whitespace is ignored.

$\langle \mathrm{DD} \rangle ::=$ *entity declarations:*
  `type` D (`extends` E)? `:`
    $\langle \mathrm{AT} \rangle^*$

$\langle \mathrm{FD} \rangle ::=$ *function declarations:*
  `func` F `:`
    `inputs :` $\langle \mathrm{AT} \rangle^*$
    `output :` $\langle \mathrm{AT} \rangle$
    `assign-output :` $\langle \mathrm{E} \rangle$

$\langle \mathrm{AT} \rangle ::=$ *attribute declarations:*
  $a \, \langle \mathrm{T} \rangle \, \langle \mathrm{CD} \rangle$

$\langle \mathrm{CD} \rangle ::=$ *cardinalities:*
  | `(` l `..` k `)` *bounded*
  | `(` l `.. * )` *unbounded*

$\langle \mathrm{E} \rangle ::=$ *expressions:*
  | $\langle \mathrm{E} \rangle$ `or` $\langle \mathrm{E} \rangle$
  | $\langle \mathrm{E} \rangle$ `and` $\langle \mathrm{E} \rangle$
  | `not` $\langle \mathrm{E} \rangle$
  | $\langle \mathrm{E} \rangle$ (`single` | `multiple`)? `exists`
  | $\langle \mathrm{E} \rangle$ `is absent`
  | $\langle \mathrm{E} \rangle$ `contains` $\langle \mathrm{E} \rangle$
  | $\langle \mathrm{E} \rangle$ `disjoint` $\langle \mathrm{E} \rangle$
  | $\langle \mathrm{E} \rangle$ (`all` | `any`)? (`=` | `<>`) $\langle \mathrm{E} \rangle$
  | $\langle \mathrm{E} \rangle$ (`+` | `-`) $\langle \mathrm{E} \rangle$
  | $\langle \mathrm{E} \rangle$ (`*` | `/`) $\langle \mathrm{E} \rangle$
  | $\langle \mathrm{E} \rangle$ `count`
  | $\langle \mathrm{E} \rangle$ `->` a
  | `if` $\langle \mathrm{E} \rangle$ `then` $\langle \mathrm{E} \rangle$ (`else` $\langle \mathrm{E} \rangle$)?
  | F `(` ($\langle \mathrm{E} \rangle$ (`,` $\langle \mathrm{E} \rangle$)*)? `)`
  | a
  | $\langle \mathrm{LIT} \rangle$
  | `(` $\langle \mathrm{E} \rangle$ `)`
  | $\langle \mathrm{E} \rangle$ `->` a `only exists`
  | $\langle \mathrm{E} \rangle$ `only-element`
  | D `{` (a `=` $\langle \mathrm{E} \rangle$ (`,` b `=` $\langle \mathrm{E} \rangle$)*)? `}`

$\langle \mathrm{LIT} \rangle ::=$ *literals:*
  | `True` | `False` *booleans*
  | i *signed integers*
  | r *signed decimals*
  | `empty` *empty literal*
  | `[` ($\langle \mathrm{E} \rangle$ (`,` $\langle \mathrm{E} \rangle$)*)? `]` *list literals*

$\langle \mathrm{T} \rangle ::=$ *basic types:*
  | D | `boolean` | `int` | `number`

Operator precedence (note: this differs from Rosetta. The precedence of operators common with the C language are based on https://en.cppreference.com/w/c/language/operator_precedence.)

1. `->` (projection), `->` a `only exists`
2. `only-element`
3. `exists`, `is absent`, `count`
4. `not`
5. `*` (multiplication), `/` (division)
6. `+` (addition), `-` (substraction)
7. `=` (equality), `<>` (inequality)
8. `contains`, `disjoint`
9. `and`
10. `or`

Syntactic sugar

$$\texttt{if}\; e_1 \;\texttt{then}\; e_2 \equiv \texttt{if}\; e_1 \;\texttt{then}\; e_2 \;\texttt{else}\;\texttt{empty}$$
$$\texttt{empty} \equiv []$$
$$e \;\texttt{is absent} \equiv \texttt{not}\,(e\;\texttt{exists})$$

Note: Nouga has a couple of differences compared to Rosetta.

1. Nouga replaces the multiple `assign-output` statements with a single statement that fully defines the output of a function. Instead of defining one attribute of the output per `assign-output` statement, you can use a record-like syntax to explicitely create an instance. (see the last option of expressions ⟨E⟩)
2. Empty list literals are allowed.
3. In Nouga you can write `not` expressions.
4. The `only-element` keyword can be written behind any expression.
5. The `only exists` is restricted to expressions that end with a projection `->` a. This simplifies the runtime model (i.e. code generators) as attributes in Nouga do not need to keep track of their parent.

2 Auxiliary definitions

Data table $\mathrm{DT}(D)$ is a mapping from data type names to data declarations. Function table $\mathrm{FT}(F)$ is a mapping from function names to function declarations.

Attribute lookup

$$\frac{\mathrm{DT}(D) = \texttt{type}\, D : a_1\ T_1\ C_1 \ldots a_n\ T_n\ C_n}{\mathrm{attrs}(D) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n}$$

$$\frac{\mathrm{DT}(D) = \texttt{type}\, D\, \texttt{extends}\, C : a_1\ T_1\ C_1 \ldots a_n\ T_n\ C_n}{\mathrm{attrs}(D) = \mathrm{attrs}(C), a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n}$$

Supertypes

$$\frac{\mathrm{DT}(D) = \texttt{type}\, D\, \texttt{extends}\, E : \ldots}{E \in \mathrm{supertypes}(D)}$$

$$\frac{A \in \mathrm{supertypes}(D) \qquad \mathrm{DT}(A) = \texttt{type}\, A\, \texttt{extends}\, B : \ldots}{B \in \mathrm{supertypes}(D)}$$

Function lookups

$$\frac{\mathrm{FT}(F) = \texttt{func}\, F : \texttt{inputs} : a_1\ T_1\ C_1 \ldots a_n\ T_n\ C_n\, \texttt{output} : \ldots}{\mathrm{inputs}(F) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n}$$

$$\frac{\mathrm{FT}(F) = \texttt{func}\, F : \texttt{inputs} : \ldots \texttt{output} : a\ T\ C \ldots}{\mathrm{output}(F) = a\ T\ C}$$

$$\frac{\mathrm{FT}(F) = \texttt{func}\, F : \ldots \texttt{assign-output} : e}{\mathrm{op}(F) = e}$$

Supertypes

3 Semantics

Semantic domain: $\mathbb{D}$.

Single value: $\mathbb{D}_1$

3.1 Semantics of Types

Semantics of basic types $[\![T]\!]$.

$$
\begin{aligned}
[\![\texttt{boolean}]\!] &= \mathbb{B} = \{\, true, false \,\} \\
[\![\texttt{int}]\!] &= \mathbb{Z} \\
[\![\texttt{number}]\!] &= \mathbb{R} \\
[\![D]\!] &= \{a_k = [\![T_k\ C_k]\!] \mid k \in 1..n\} \\
&\quad \text{where } \mathrm{attrs}(D) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n
\end{aligned}
$$

Semantics of types $[\![T\ C]\!]$.

$$[\![T\ \ (i\,.\,.\,j)]\!] = [\![T]\!]^{[\![i]\!]:[\![j]\!]}$$

Semantics of cardinality limits $[\![c]\!] \in \mathbb{N} \cup \{\, \infty \,\}$.

$$
\begin{aligned}
[\![i]\!] &= i \\
[\![*]\!] &= \infty
\end{aligned}
$$

3.2 Semantical Algebra

Semantic algebra.

$$
\begin{aligned}
A^0 &= Unit = \{\, () \,\} \\
A^n &= A \times A^{n-1} \\
A^{m:n} &= \bigcup_{k \in m..n} A^k \\
A^* &= A^{0:\infty}
\end{aligned}
$$

Note: from the above definition, A^1 formally equals $A \times Unit$, so elements of this set are of the form $(a, ())$ where $a \in A$. I might sometimes write a instead of $(a, ())$ if it is clear from the context what is meant. (similar for A^n, where I will leave out the last element of the cartesian product)

$$
\begin{aligned}
\_\, or \,\_ &: \mathbb{B}^1 \times \mathbb{B}^1 \to \mathbb{B}^1 : (a, ())\, or\, (b, ()) = (a \vee b, ()) \\
\_\, and \,\_ &: \mathbb{B}^1 \times \mathbb{B}^1 \to \mathbb{B}^1 : (a, ())\, and\, (b, ()) = (a \wedge b, ()) \\
not\,(\_) &: \mathbb{B}^1 \to \mathbb{B}^1 : not\,((a, ())) = (\neg a, ()) \\
(\_) \to \_\,[]\,\_ &: \mathbb{B}^1 \times \mathbb{D} \times \mathbb{D} \to \mathbb{D} : ((a, ())) \to b\,[]\,c = \begin{cases} b, & a = true \\ c, & a = false \end{cases} \\
count\,(\_) &: \mathbb{D} \to \mathbb{Z}^1 : count\,((a_1, \ldots, a_n, ())) = (n, ()) \\
flatten_{A,n}\,(\_) &: (A^*)^n \to A^* : \\
&\quad flatten_{A,n}\,((a_{11}, \ldots, a_{1m_1}, ()), \ldots, (a_{n1}, \ldots, a_{nm_n}, ()))
\end{aligned}
$$

$$= (a_{11}, \ldots, a_{1m_1}, \ldots, a_{nm_n}, ())$$

$$contains\,(\_,\_) : \mathbb{D} \times \mathbb{D} \to \mathbb{B}^1 : contains\,((a_1, \ldots, a_n, ()), (b_1, \ldots, b_m, ()))$$

$$= \begin{cases} (true, ()), & \forall i \in 1..n : \exists j \in 1..m : a_i = b_j \\ (false, ()), & \text{otherwise} \end{cases}$$

$$disjoint\,(\_,\_) : \mathbb{D} \times \mathbb{D} \to \mathbb{B}^1 : disjoint\,((a_1, \ldots, a_n, ()), (b_1, \ldots, b_m, ()))$$

$$= \begin{cases} (true, ()), & \forall i \in 1..n : \forall j \in 1..m : a_i \neq b_j \\ (false, ()), & \text{otherwise} \end{cases}$$

$$onlyexists_{\{\, a_k = A_k | k \in 1..n \,\}, a_i}\,(\_) : \{\, a_k = A_k \mid k \in 1..n \,\}^1 \to \mathbb{B}^1 :$$

$$onlyexists_{\{\, a_k = A_k | k \in 1..n \,\}, a_i}\,((\{\, a_k = v_k \mid k \in 1..n \,\}, ()))$$

$$= \begin{cases} (true, ()), & v_i \neq () \wedge \forall j \in 1..n : j \neq i \Rightarrow v_j = () \\ (false, ()), & \text{otherwise} \end{cases}$$

$$project_{\left\{\, a_k = A_k^{l_k : u_k} | k \in 1..n \,\right\}, a_i}\,(\_) : \left\{\, a_k = A_k^{l_k : u_k} \mid k \in 1..n \,\right\}^* \to A_i^* :$$

$$project_{\left\{\, a_k = A_k^{l_k : u_k} | k \in 1..n \,\right\}, a_i}\,((\{\, a_k = v_{k1} \mid k \in 1..n \,\}, \ldots, \{\, a_k = v_{km} \mid k \in 1..n \,\}, ()))$$

$$= flatten_{A_i, m}\,(v_{i1}, \ldots, v_{im})$$

$$\_\,eq\,\_ : \mathbb{D} \times \mathbb{D} \to \mathbb{B}^1 : (a_1, \ldots, a_n, ())\, eq\, (b_1, \ldots, b_m, ())$$

$$= \begin{cases} (true, ()), & n = m \wedge \forall i \in 1..n : a_i = b_i \\ (false, ()), & \text{otherwise} \end{cases}$$

$$\_\,neq\,\_ : \mathbb{D} \times \mathbb{D} \to \mathbb{B}^1 : (a_1, \ldots, a_n, ())\, neq\, (b_1, \ldots, b_m, ())$$

$$= \begin{cases} (true, ()), & n \neq m \vee \forall i \in 1..n : a_i \neq b_i \\ (false, ()), & \text{otherwise} \end{cases}$$

$$\_\,alleq\,\_ : \mathbb{D} \times \mathbb{D}_1^1 \to \mathbb{B}^1 : (a_1, \ldots, a_n, ())\, alleq\, (b, ())$$

$$= \begin{cases} (true, ()), & \forall i \in 1..n : a_i = b \\ (false, ()), & \text{otherwise} \end{cases}$$

$$\_\,allneq\,\_ : \mathbb{D} \times \mathbb{D}_1^1 \to \mathbb{B}^1 : (a_1, \ldots, a_n, ())\, allneq\, (b, ())$$

$$= \begin{cases} (true, ()), & \forall i \in 1..n : a_i \neq b \\ (false, ()), & \text{otherwise} \end{cases}$$

$$\_\,anyeq\,\_ : \mathbb{D} \times \mathbb{D}_1^1 \to \mathbb{B}^1 : (a_1, \ldots, a_n, ())\, anyeq\, (b, ())$$

$$= \begin{cases} (true, ()), & \exists i \in 1..n : a_i = b \\ (false, ()), & \text{otherwise} \end{cases}$$

$$\_\,anyneq\,\_ : \mathbb{D} \times \mathbb{D}_1^1 \to \mathbb{B}^1 : (a_1, \dots, a_n, ())\, anyneq\, (b, ())$$

$$= \begin{cases} (true, ()), & \exists i \in 1..n : a_i \neq b \\ (false, ()), & \text{otherwise} \end{cases}$$

$$\_\,plus_A\,\_ : A^1 \times A^1 \to A^1 : (a, ())\, plus_A\, (b, ()) = (a + b, ())$$

$$\_\,substract_A\,\_ : A^1 \times A^1 \to A^1 : (a, ())\, substract_A\, (b, ()) = (a - b, ())$$

$$\_\,mult_A\,\_ : A^1 \times A^1 \to A^1 : (a, ())\, mult_A\, (b, ()) = (a * b, ())$$

$$\_\,div\,\_ : \mathbb{R}^1 \times \mathbb{R}^1 \to \mathbb{R}^1 : (a, ())\, div\, (b, ()) = (a/b, ())$$

$$onlyelement\,(\_) : \mathbb{D} \to \mathbb{D} : onlyelement\,((a_1, \dots, a_n, ()))$$

$$= \begin{cases} (a_1, ()), & n = 1 \\ (), & \text{otherwise} \end{cases}$$

Note: equality is checked deeply, i.e. recursively on attributes of records.
Given $f : A_1 \times \cdots \times A_n \to B$ where $A_1, \dots, A_n \subset \mathbb{D}$ and $B \subset \mathbb{D}$, let

$$\hat{f} : \mathbb{D}_\perp^n \to \mathbb{D}_\perp : \hat{f}(a_1, \dots, a_n) = \begin{cases} f(a_1, \dots, a_n), & (a_1, \dots, a_n) \in \mathrm{Dom}\, f \\ \perp, & \text{otherwise.} \end{cases}$$

3.3 Semantics of Expressions

Some denotations depend on the type derivation of an expression. For this reason, I will evaluate typing derivations instead of expressions. However, because I only need this in a few cases, I will often omit the derivation, i.e. I will write $[\![e]\!]$ instead of $[\![\mathcal{D} :: \emptyset \vdash e : T\ C]\!]$ if the type $T\ C$ and the derivation $\mathcal{D}$ are unimportant.
Values $[\![v]\!]$.

$$[\![True]\!] = (true, ()) \qquad \text{E-TRUE}$$

$$[\![False]\!] = (false, ()) \qquad \text{E-FALSE}$$

$$[\![i]\!] = (i, ()) \qquad \text{E-INT}$$

$$[\![r]\!] = (r, ()) \qquad \text{E-NUMBER}$$

Expressions $[\![e]\!]$.

$$[\![\mathcal{D} :: \emptyset \vdash [e_1, \dots, e_n] : T\ C]\!] = flatten_{[\![T]\!],n}\,([\![e_1]\!], \dots, [\![e_n]\!]) \qquad \text{E-LIST}$$

$$[\![e_1\, \texttt{or}\, e_2]\!] = [\![e_1]\!]\ \widehat{or}\ [\![e_2]\!] \qquad \text{E-OR}$$

$$[\![e_1\, \texttt{and}\, e_2]\!] = [\![e_1]\!]\ \widehat{and}\ [\![e_2]\!] \qquad \text{E-AND}$$

$$[\![\texttt{not}\, e]\!] = \widehat{not}\,([\![e]\!]) \qquad \text{E-NOT}$$

$$[\![e\, \texttt{exists}]\!] = \begin{cases} false, & [\![e]\!] = () \\ true, & \text{otherwise} \end{cases} \qquad \text{E-EXISTS}$$

$$[\![e\ \texttt{single exists}]\!] = \begin{cases} true, & \widehat{count}\left([\![e]\!]\right) = (1, ()) \\ false, & \text{otherwise} \end{cases} \qquad \text{E-SingleExists}$$

$$[\![e\ \texttt{multiple exists}]\!] = \begin{cases} true, & \widehat{count}\left([\![e]\!]\right) = (k, ()) \wedge k \geq 2 \\ false, & \text{otherwise} \end{cases} \qquad \text{E-MultipleExists}$$

$$[\![e_1\ \texttt{contains}\ e_2]\!] = \widehat{contains}\left([\![e_1]\!], [\![e_2]\!]\right) \qquad \text{E-Contains}$$

$$[\![e_1\ \texttt{disjoint}\ e_2]\!] = \widehat{disjoint}\left([\![e_1]\!], [\![e_2]\!]\right) \qquad \text{E-Disjoint}$$

$$[\![e_1 \texttt{=} e_2]\!] = [\![e_1]\!]\ \widehat{eq}\ [\![e_2]\!] \qquad \text{E-Equals}$$

$$[\![e_1 \texttt{<>} e_2]\!] = [\![e_1]\!]\ \widehat{neq}\ [\![e_2]\!] \qquad \text{E-NotEquals}$$

$$[\![e_1\ \texttt{all =}\ e_2]\!] = [\![e_1]\!]\ \widehat{alleq}\ [\![e_2]\!] \qquad \text{E-AllEquals}$$

$$[\![e_1\ \texttt{all <>}\ e_2]\!] = [\![e_1]\!]\ \widehat{allneq}\ [\![e_2]\!] \qquad \text{E-AllNotEquals}$$

$$[\![e_1\ \texttt{any =}\ e_2]\!] = [\![e_1]\!]\ \widehat{anyeq}\ [\![e_2]\!] \qquad \text{E-AnyEquals}$$

$$[\![e_1\ \texttt{any <>}\ e_2]\!] = [\![e_1]\!]\ \widehat{anyneq}\ [\![e_2]\!] \qquad \text{E-AnyNotEquals}$$

$$\left[\!\!\left[\frac{\mathcal{D}_1 :: \emptyset \vdash e_1 : T\ (1..1) \qquad \mathcal{D}_2 :: \emptyset \vdash e_2 : T\ (1..1)}{\emptyset \vdash e_1 \texttt{+} e_2 : T\ (1..1)} \right]\!\!\right] = [\![e_1]\!]\ \widehat{plus}_{[\![T]\!]}\ [\![e_2]\!] \qquad \text{E-Plus}$$

$$\left[\!\!\left[\frac{\mathcal{D}_1 :: \emptyset \vdash e_1 : T\ (1..1) \qquad \mathcal{D}_2 :: \emptyset \vdash e_2 : T\ (1..1)}{\emptyset \vdash e_1 \texttt{-} e_2 : T\ (1..1)} \right]\!\!\right] = [\![e_1]\!]\ \widehat{substract}_{[\![T]\!]}\ [\![e_2]\!] \qquad \text{E-Subs}$$

$$\left[\!\!\left[\frac{\mathcal{D}_1 :: \emptyset \vdash e_1 : T\ (1..1) \qquad \mathcal{D}_2 :: \emptyset \vdash e_2 : T\ (1..1)}{\emptyset \vdash e_1 \texttt{*} e_2 : T\ (1..1)} \right]\!\!\right] = [\![e_1]\!]\ \widehat{mult}_{[\![T]\!]}\ [\![e_2]\!] \qquad \text{E-Mult}$$

$$[\![e_1 \texttt{/} e_2]\!] = [\![e_1]\!]\ \widehat{div}\ [\![e_2]\!] \qquad \text{E-Div}$$

$$[\![e\ \texttt{count}]\!] = \widehat{count}\left([\![e]\!]\right) \qquad \text{E-Count}$$

$$\left[\!\!\left[\frac{\mathcal{D} :: \emptyset \vdash e : D\ C}{\emptyset \vdash e \texttt{->} a : T\ C_a} \right]\!\!\right] = \widehat{project}_{[\![D]\!], a}\left([\![e]\!]\right) \qquad \text{E-Project}$$

$$[\![\texttt{if}\ e_1\ \texttt{then}\ e_2\ \texttt{else}\ e_3]\!] = \left([\![e_1]\!]\right) \widehat{\rightarrow} [\![e_2]\!]\ []\ [\![e_3]\!] \qquad \text{E-If}$$

$$\frac{\text{inputs}(F) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n}{[\![F(e_1, \ldots, e_n)]\!] = [\![\ [\ a_1 \mapsto e_1, \ldots, a_n \mapsto e_n\ ]\ \text{op}(F)]\!]} \qquad \text{E-Func}$$

$$\frac{\text{attrs}(D) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n}{[\![D \{\ a_1 : e_1, \ldots, a_n : e_n\ \}]\!] = \{\ a_1 = [\![e_1]\!], \ldots, a_n = [\![e_n]\!]\ \}} \qquad \text{E-Construct}$$

$$\left[\!\!\left[\frac{\emptyset \vdash e : D\ (1..1)}{\emptyset \vdash e \texttt{->} a\ \texttt{only exists} : \texttt{boolean}\ (1..1)} \right]\!\!\right] = \widehat{onlyexists}_{[\![D]\!], a}\left([\![e]\!]\right) \qquad \text{E-OnlyExists}$$

$$[\![e\ \texttt{only-element}]\!] = \widehat{onlyelement}\left([\![e]\!]\right) \qquad \text{E-OnlyElement}$$

Note: equality between two empty lists (i.e. true) is different than the usual equality with null (i.e. always false) in other programming languages (and the official Rosetta documentation).

4 Typing

4.1 Declarative Typing

Basic subtyping $S <: T$.

$$T <: T \qquad \text{S-Refl}$$

$$\frac{S <: U \qquad U <: T}{S <: T} \qquad \text{S-Trans}$$

$$\texttt{int} <: \texttt{number} \qquad \text{S-Num}$$

$$\frac{\mathrm{DT}(D) = \texttt{type}\, D\, \texttt{extends}\, E : \ldots}{D <: E} \qquad \text{S-Extends}$$

Subtyping $S\ C_1 <: T\ C_2$.

$$\frac{S <: T \qquad l_S \geq l_T \qquad u_S \leq u_T}{S\ (l_S..u_S) <: T\ (l_T..u_T)} \qquad \text{S-Card}$$

Typing rules $\Gamma \vdash e : T\ C$.

$$\frac{\Gamma \vdash e_1 : \texttt{boolean}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{boolean}\ (1..1)}{\Gamma \vdash e_1\, \texttt{or}\, e_2 : \texttt{boolean}\ (1..1)} \qquad \text{T-Or}$$

$$\frac{\Gamma \vdash e_1 : \texttt{boolean}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{boolean}\ (1..1)}{\Gamma \vdash e_1\, \texttt{and}\, e_2 : \texttt{boolean}\ (1..1)} \qquad \text{T-And}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\, \texttt{exists} : \texttt{boolean}\ (1..1)} \qquad \text{T-Exists}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\, \texttt{single}\, \texttt{exists} : \texttt{boolean}\ (1..1)} \qquad \text{T-SingleExists}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\, \texttt{multiple}\, \texttt{exists} : \texttt{boolean}\ (1..1)} \qquad \text{T-MultipleExists}$$

$$\frac{\Gamma \vdash e_1 : T\ C_1 \qquad \Gamma \vdash e_2 : T\ C_2}{\Gamma \vdash e_1\, \texttt{contains}\, e_2 : \texttt{boolean}\ (1..1)} \qquad \text{T-Contains}$$

$$\frac{\Gamma \vdash e_1 : T\ C_1 \qquad \Gamma \vdash e_2 : T\ C_2}{\Gamma \vdash e_1\, \texttt{disjoint}\, e_2 : \texttt{boolean}\ (1..1)} \qquad \text{T-Disjoint}$$

$$\frac{\Gamma \vdash e_1 : T\ C \qquad \Gamma \vdash e_2 : T\ C}{\Gamma \vdash e_1\, \texttt{=}\, e_2 : \texttt{boolean}\ (1..1)} \qquad \text{T-Equals}$$

$$\frac{\Gamma \vdash e_1 : T\ C \qquad \Gamma \vdash e_2 : T\ C}{\Gamma \vdash e_1\, \texttt{<>}\, e_2 : \texttt{boolean}\ (1..1)} \qquad \text{T-NotEquals}$$

$$\frac{\Gamma \vdash e_1 : T\ C \qquad \Gamma \vdash e_2 : T\ (1..1)}{\Gamma \vdash e_1\,\texttt{all}\,\texttt{=}\,e_2 : \texttt{boolean}\ (1..1)}\ \textsc{T-AllEquals}$$

$$\frac{\Gamma \vdash e_1 : T\ C \qquad \Gamma \vdash e_2 : T\ (1..1)}{\Gamma \vdash e_1\,\texttt{all}\,\texttt{<>}\,e_2 : \texttt{boolean}\ (1..1)}\ \textsc{T-AllNotEquals}$$

$$\frac{\Gamma \vdash e_1 : T\ C \qquad \Gamma \vdash e_2 : T\ (1..1)}{\Gamma \vdash e_1\,\texttt{any}\,\texttt{=}\,e_2 : \texttt{boolean}\ (1..1)}\ \textsc{T-AnyEquals}$$

$$\frac{\Gamma \vdash e_1 : T\ C \qquad \Gamma \vdash e_2 : T\ (1..1)}{\Gamma \vdash e_1\,\texttt{any}\,\texttt{<>}\,e_2 : \texttt{boolean}\ (1..1)}\ \textsc{T-AnyNotEquals}$$

$$\frac{\Gamma \vdash e_1 : \texttt{int}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{int}\ (1..1)}{\Gamma \vdash e_1 \texttt{+} e_2 : \texttt{int}\ (1..1)}\ \textsc{T-PlusInt}$$

$$\frac{\Gamma \vdash e_1 : \texttt{number}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{number}\ (1..1)}{\Gamma \vdash e_1 \texttt{+} e_2 : \texttt{number}\ (1..1)}\ \textsc{T-PlusNumber}$$

$$\frac{\Gamma \vdash e_1 : \texttt{int}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{int}\ (1..1)}{\Gamma \vdash e_1 \texttt{*} e_2 : \texttt{int}\ (1..1)}\ \textsc{T-MultInt}$$

$$\frac{\Gamma \vdash e_1 : \texttt{number}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{number}\ (1..1)}{\Gamma \vdash e_1 \texttt{*} e_2 : \texttt{number}\ (1..1)}\ \textsc{T-MultNumber}$$

$$\frac{\Gamma \vdash e_1 : \texttt{int}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{int}\ (1..1)}{\Gamma \vdash e_1 \texttt{-} e_2 : \texttt{int}\ (1..1)}\ \textsc{T-SubsInt}$$

$$\frac{\Gamma \vdash e_1 : \texttt{number}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{number}\ (1..1)}{\Gamma \vdash e_1 \texttt{-} e_2 : \texttt{number}\ (1..1)}\ \textsc{T-SubsNumber}$$

$$\frac{\Gamma \vdash e_1 : \texttt{number}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{number}\ (1..1)}{\Gamma \vdash e_1 \texttt{/} e_2 : \texttt{number}\ (1..1)}\ \textsc{T-Division}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\,\texttt{count} : \texttt{int}\ (1..1)}\ \textsc{T-Count}$$

$$\frac{\Gamma \vdash e : D\ (l..u) \qquad \mathrm{attrs}(D) = a_1\ T_1\ (l_1..u_1), \ldots, a_n\ T_n\ (l_n..u_n)}{\Gamma \vdash e\,\texttt{->}\,a_k : T_k\ (l * l_k..u * u_k)}\ \textsc{T-Project}$$

$$\frac{\Gamma \vdash e_1 : \texttt{boolean}\ (1..1) \qquad \Gamma \vdash e_2 : T\ C \qquad \Gamma \vdash e_3 : T\ C}{\Gamma \vdash \texttt{if}\,e_1\,\texttt{then}\,e_2\,\texttt{else}\,e_3 : T\ C}\ \textsc{T-If}$$

$$\frac{\begin{array}{c}\forall i \in 1..n : \Gamma \vdash e_i : T_i\ C_i \\ \mathrm{inputs}(F) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n \qquad \mathrm{output}(F) = a\ T\ C\end{array}}{\Gamma \vdash F(e_1, \ldots, e_n) : T\ C}\ \textsc{T-Func}$$

$$\frac{\forall i \in 1..n : \Gamma \vdash e_i : T_i\ C_i \qquad \mathrm{attrs}(D) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n}{\Gamma \vdash D\,\{\,a_1 = e_1, \ldots, a_n = e_n\,\} : D\ (1..1)}\ \textsc{T-Construct}$$

$$\frac{x : T\ C \in \Gamma}{\Gamma \vdash x : T\ C} \quad \textsc{T-Var}$$

$$\Gamma \vdash \texttt{True} : \texttt{boolean}\ \ (1..1) \quad \textsc{T-True}$$

$$\Gamma \vdash \texttt{False} : \texttt{boolean}\ \ (1..1) \quad \textsc{T-False}$$

$$\Gamma \vdash i : \texttt{int}\ \ (1..1) \quad \textsc{T-Int}$$

$$\Gamma \vdash r : \texttt{number}\ \ (1..1) \quad \textsc{T-Number}$$

$$\frac{\forall i \in 1..n : \Gamma \vdash e_i : T\ (l_i..u_i)}{\Gamma \vdash [e_1, \ldots, e_n] : T\ (\sum_{i \in 1..n} l_i\ ..\sum_{i \in 1..n} u_i)} \quad \textsc{T-List}$$

$$\frac{\Gamma \vdash e : D\ (1..1) \qquad \mathrm{attrs}(D) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n}{\Gamma \vdash e\,\texttt{->}\,a_k\,\texttt{only}\,\texttt{exists} : \texttt{boolean}\ \ (1..1)} \quad \textsc{T-OnlyExists}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\,\texttt{only-element} : T\ (0..1)} \quad \textsc{T-OnlyElement}$$

$$\frac{\Gamma \vdash e : S \qquad S <: T}{\Gamma \vdash e : T} \quad \textsc{T-Sub}$$

Typing function declarations F OK.

$$\frac{\begin{array}{c}\mathrm{inputs}(F) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n \\ \mathrm{output}(F) = a\ T\ C \qquad a_1 : T_1\ C_1, \ldots, a_n : T_n\ C_n \vdash \mathrm{op}(F) : T\ C\end{array}}{F\ \mathrm{OK}}$$

Note: for equality, there are two sensible choices as premises. Either $\Gamma \vdash e_1 : T\ C_1$ and $\Gamma \vdash e_2 : T\ C_2$ or $\Gamma \vdash e_1 : T\ C$ and $\Gamma \vdash e_2 : T\ C$. The second possibility eliminates equality checks that are always false because the operands can never have the same length.

4.2 Algorithmic Typing

These typing rules should be consistent with the declarative version, but they are defined in a way that is more straightforward to implement, because every rule is syntax-directed.

Basic subtyping $S <:: T$.

$$\texttt{int} <:: \texttt{number} \quad \textsc{SA-Num}$$

$$\frac{E \in \mathrm{supertypes}(D)}{D <:: E} \quad \textsc{SA-Super!}$$

Define $\mathrm{comparable}(D, E) = D <:: E \vee E <:: D$

Subtyping $S\ C_1 <:: T\ C_2$.

$$\frac{S <:: T \qquad l_S \geq l_T \qquad u_S \leq u_T}{S\ (l_S..u_S) <:: T\ (l_T..u_T)} \quad \textsc{SA-Card}$$

Typing rules $\Gamma \vdash e : T\ C$.

$$\frac{\Gamma \vdash e_1 : \texttt{boolean}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{boolean}\ (1..1)}{\Gamma \vdash e_1\,\texttt{or}\,e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{Or}$$

$$\frac{\Gamma \vdash e_1 : \texttt{boolean}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{boolean}\ (1..1)}{\Gamma \vdash e_1\,\texttt{and}\,e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{And}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\,\texttt{exists} : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{Exists}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\,\texttt{single}\,\texttt{exists} : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{SingleExists}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\,\texttt{multiple}\,\texttt{exists} : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{MultipleExists}$$

$$\frac{\Gamma \vdash e_1 : T_1\ C_1 \qquad \Gamma \vdash e_2 : T_2\ C_2 \qquad \text{comparable}(T_1, T_2)}{\Gamma \vdash e_1\,\texttt{contains}\,e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{Contains}!$$

$$\frac{\Gamma \vdash e_1 : T_1\ C_1 \qquad \Gamma \vdash e_2 : T_2\ C_2 \qquad \text{comparable}(T_1, T_2)}{\Gamma \vdash e_1\,\texttt{disjoint}\,e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{Disjoint}!$$

$$\frac{\Gamma \vdash e_1 : T_1\ C_1 \qquad \Gamma \vdash e_2 : T_2\ C_2 \qquad \text{comparable}(T_1, T_2)}{\Gamma \vdash e_1 \,\texttt{=}\, e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{Equals}!$$

$$\frac{\Gamma \vdash e_1 : T_1\ C \qquad \Gamma \vdash e_2 : T_2\ C \qquad \text{comparable}(T_1, T_2)}{\Gamma \vdash e_1 \,\texttt{<>}\, e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{NotEquals}!$$

$$\frac{\Gamma \vdash e_1 : T_1\ C \qquad \Gamma \vdash e_2 : T_2\ (1..1) \qquad \text{comparable}(T_1, T_2)}{\Gamma \vdash e_1\,\texttt{all}\,\texttt{=}\,e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{AllEquals}!$$

$$\frac{\Gamma \vdash e_1 : T_1\ C \qquad \Gamma \vdash e_2 : T_2\ (1..1) \qquad \text{comparable}(T_1, T_2)}{\Gamma \vdash e_1\,\texttt{all}\,\texttt{<>}\,e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{AllNotEquals}!$$

$$\frac{\Gamma \vdash e_1 : T_1\ C \qquad \Gamma \vdash e_2 : T_2\ (1..1) \qquad \text{comparable}(T_1, T_2)}{\Gamma \vdash e_1\,\texttt{any}\,\texttt{=}\,e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{AnyEquals}!$$

$$\frac{\Gamma \vdash e_1 : T_1\ C \qquad \Gamma \vdash e_2 : T_2\ (1..1) \qquad \text{comparable}(T_1, T_2)}{\Gamma \vdash e_1\,\texttt{any}\,\texttt{<>}\,e_2 : \texttt{boolean}\ (1..1)} \quad \text{TA-}\textsc{AnyNotEquals}!$$

$$\frac{\Gamma \vdash e_1 : \texttt{int}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{int}\ (1..1)}{\Gamma \vdash e_1 \,\texttt{+}\, e_2 : \texttt{int}\ (1..1)} \quad \text{TA-}\textsc{PlusInt}$$

$$\frac{\begin{array}{c}\Gamma \vdash e_1 : T_1\ (1..1) \qquad \Gamma \vdash e_2 : T_2\ (1..1) \\ T_1 <:: \texttt{number} \qquad T_2 <:: \texttt{number} \qquad T_1 \neq \texttt{int} \vee T_2 \neq \texttt{int}\end{array}}{\Gamma \vdash e_1 \,\texttt{+}\, e_2 : \texttt{number}\ (1..1)} \quad \text{TA-}\textsc{PlusNumber}!$$

$$\frac{\Gamma \vdash e_1 : \texttt{int}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{int}\ (1..1)}{\Gamma \vdash e_1 \,\texttt{*}\, e_2 : \texttt{int}\ (1..1)} \quad \text{TA-}\textsc{MultInt}$$

$$\frac{\Gamma \vdash e_1 : T_1\ (1..1) \qquad \Gamma \vdash e_2 : T_2\ (1..1) \qquad T_1 <:: \texttt{number} \qquad T_2 <:: \texttt{number} \qquad T_1 \neq \texttt{int} \lor T_2 \neq \texttt{int}}{\Gamma \vdash e_1 \,\texttt{*}\, e_2 : \texttt{number}\ (1..1)} \quad \text{TA-MultNumber!}$$

$$\frac{\Gamma \vdash e_1 : \texttt{int}\ (1..1) \qquad \Gamma \vdash e_2 : \texttt{int}\ (1..1)}{\Gamma \vdash e_1 \,\texttt{-}\, e_2 : \texttt{int}\ (1..1)} \quad \text{TA-SubsInt}$$

$$\frac{\Gamma \vdash e_1 : T_1\ (1..1) \qquad \Gamma \vdash e_2 : T_2\ (1..1) \qquad T_1 <:: \texttt{number} \qquad T_2 <:: \texttt{number} \qquad T_1 \neq \texttt{int} \lor T_2 \neq \texttt{int}}{\Gamma \vdash e_1 \,\texttt{-}\, e_2 : \texttt{number}\ (1..1)} \quad \text{TA-SubsNumber!}$$

$$\frac{\Gamma \vdash e_1 : T_1\ (1..1) \qquad \Gamma \vdash e_2 : T_2\ (1..1) \qquad T_1 <:: \texttt{number} \qquad T_2 <:: \texttt{number}}{\Gamma \vdash e_1 \,\texttt{/}\, e_2 : \texttt{number}\ (1..1)} \quad \text{TA-Division!}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\,\texttt{count} : \texttt{int}\ (1..1)} \quad \text{TA-Count}$$

$$\frac{\Gamma \vdash e : D\ (l..u) \qquad \text{attrs}(D) = a_1\ T_1\ (l_1..u_1), \ldots, a_n\ T_n\ (l_n..u_n)}{\Gamma \vdash e \,\texttt{->}\, a_k : T_k\ (l * l_k..u * u_k)} \quad \text{TA-Project}$$

$$\frac{\Gamma \vdash e_1 : \texttt{boolean}\ (1..1) \qquad \Gamma \vdash e_2 : T_1\ C_1 \qquad \Gamma \vdash e_3 : T_2\ C_3 \qquad T\ C = \text{join}(T_1\ C_1, T_2\ C_2)}{\Gamma \vdash \texttt{if}\, e_1\, \texttt{then}\, e_2\, \texttt{else}\, e_3 : T\ C} \quad \text{TA-If!}$$

$$\frac{\text{inputs}(F) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n \qquad \forall i \in 1..n : \Gamma \vdash e_i : T_i'\ C_i' \qquad \forall i \in 1..n : T_i'\ C_i' <:: T_n\ C_n \qquad \text{output}(F) = a\ T\ C}{\Gamma \vdash F(e_1, \ldots, e_n) : T\ C} \quad \text{TA-Func!}$$

$$\frac{\text{attrs}(D) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n \qquad \forall i \in 1..n : \Gamma \vdash e_i : T_i'\ C_i' \qquad \forall i \in 1..n : T_i'\ C_i' <:: T_i\ C_i}{\Gamma \vdash D\,\{\, a_1 = e_1, \ldots, a_n = e_n \,\} : D\ (1..1)} \quad \text{TA-Construct!}$$

$$\frac{x : T\ C \in \Gamma}{\Gamma \vdash x : T\ C} \quad \text{TA-Var}$$

$$\Gamma \vdash \texttt{True} : \texttt{boolean}\ (1..1) \quad \text{TA-True}$$

$$\Gamma \vdash \texttt{False} : \texttt{boolean}\ (1..1) \quad \text{TA-False}$$

$$\Gamma \vdash i : \texttt{int}\ (1..1) \quad \text{TA-Int}$$

$$\Gamma \vdash r : \texttt{number}\ (1..1) \quad \text{TA-Number}$$

$$\frac{\forall i \in 1..n : \Gamma \vdash e_i : T_i\ (l_i..u_i) \qquad T = \text{join}(T_1, \ldots, T_n)}{\Gamma \vdash [e_1, \ldots, e_n] : T\ (\sum_{i \in 1..n} l_i \,..\, \sum_{i \in 1..n} u_i)} \quad \text{TA-List!}$$

$$\frac{\Gamma \vdash e : D\ (1..1) \qquad \text{attrs}(D) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n}{\Gamma \vdash e \,\texttt{->}\, a_k\, \texttt{only exists} : \texttt{boolean}\ (1..1)} \quad \text{TA-OnlyExists}$$

$$\frac{\Gamma \vdash e : T\ C}{\Gamma \vdash e\ \texttt{only-element} : T\ (0..1)} \qquad \textsc{TA-OnlyElement}$$

Typing function declarations $F\,\mathrm{OK}$.

$$\frac{\begin{array}{cc}\mathrm{inputs}(F) = a_1\ T_1\ C_1, \ldots, a_n\ T_n\ C_n & \mathrm{output}(F) = a\ T\ C \\ a_1 : T_1\ C_1, \ldots, a_n : T_n\ C_n \vdash \mathrm{op}(F) : T'\ C' & T'\ C' <:: T\ C\end{array}}{F\,\mathrm{OK}} \qquad !$$