

1 Grammar

\mathbb{S}	<i>System</i>
\mathbb{S}	<i>Subsystem Name</i>
\mathbb{E}	<i>Explanation</i>
\mathbb{C}	<i>Component Name</i>
\mathbb{q}	<i>Query</i>
\mathbb{c}	<i>Command</i>
\mathbb{i}	<i>Constraint</i>
<hr/>	
$\mathbb{S} \leftarrow \mathbb{E}$	<i>Subsystem Explanation</i>
$\mathbb{S} \leftarrow \mathbb{S}$	<i>Subsystem Containment</i>
$\mathbb{C} \leftarrow \mathbb{E}$	<i>Intro Explanation</i>
$\mathbb{C} \leftarrow \mathbb{S}$	<i>Intro Containment</i>
<hr/>	
$\mathbb{C} \leftarrow \mathbb{q}$	<i>Query Introduction</i>
$\mathbb{C} \leftarrow \mathbb{c}$	<i>Command Introduction</i>
$\mathbb{C} \leftarrow \mathbb{i}$	<i>Constraint Introduction</i>

2 Type System

2.1 Type Grammar

τ	$::=$	$\hat{\tau} \mid \check{\tau}$	<i>Type</i>
$\hat{\tau}$	$::=$	$\mathcal{B} \mid \mathcal{Z} \mid \mathcal{N} \mid \textit{System} \mid \textit{Subsystem} \mid \textit{Component}$	<i>Primitive Type (TODO: More!)</i>
$\check{\tau}$	$::=$	$\check{\tau}_1, \check{\tau}_2, \dots$	<i>Derived Type</i>

2.2 Type Environment

In order to define the type system, we must first introduce a few auxilliary structures:

\mathbb{CI}	$::=$	$\{\mathbb{C} \mapsto \mathbb{C}\}$	<i>Component Inheritance Map</i>
\mathbb{CT}	$::=$	$\{\mathbb{C} \mapsto \check{\tau}\}$	<i>Component Type Map</i>
\mathbb{CD}	$::=$	$\{\check{\tau} \mapsto \langle \mathbb{S}, \mathbb{E}, \{\mathbb{f}\} \rangle\}$	<i>Component Data Map</i>
\mathbb{f}	$::=$	$\mathbb{q} \mid \mathbb{c} \mid \mathbb{i}$	<i>Feature</i>
<hr/>			
\mathbb{ST}	$::=$	$\{\mathbb{S} \mapsto \check{\tau}\}$	<i>Subsystem Type Map</i>
\mathbb{SD}	$::=$	$\{\check{\tau} \mapsto \langle \mathbb{SP}, \mathbb{E}, \{\mathbb{S}\}, \{\mathbb{C}\} \rangle\}$	<i>Subsystem Data Map</i>
\mathbb{SP}	$::=$	$\mathbb{S} \mid \mathbb{S}$	<i>Parent of Subsystem</i>
<hr/>			
Γ	$::=$	$\langle \mathbb{CI}, \mathbb{CT}, \mathbb{CD}, \mathbb{T}, \mathbb{ST}, \mathbb{SD} \rangle$	<i>Type Environment</i>

We will need more than this in the type environment. This is to get started!

The type environment consists of a number of distinct elements required by our type system definition. For simplifying the rules, we define a shorthand notation for each of them.

$$\begin{aligned}
\mathbb{CI}^\Gamma &\doteq \mathbb{CI} && \text{where } \Gamma = \langle \mathbb{CI}, \mathbb{CT}, \mathbb{CD}, \mathbb{T}, \mathbb{ST}, \mathbb{SD} \rangle \\
\mathbb{CT}^\Gamma &\doteq \mathbb{CT} && \text{where } \Gamma = \langle \mathbb{CI}, \mathbb{CT}, \mathbb{CD}, \mathbb{T}, \mathbb{ST}, \mathbb{SD} \rangle \\
\mathbb{CD}^\Gamma &\doteq \mathbb{CD} && \text{where } \Gamma = \langle \mathbb{CI}, \mathbb{CT}, \mathbb{CD}, \mathbb{T}, \mathbb{ST}, \mathbb{SD} \rangle \\
\mathbb{T}^\Gamma &\doteq \mathbb{T} && \text{where } \Gamma = \langle \mathbb{CI}, \mathbb{CT}, \mathbb{CD}, \mathbb{T}, \mathbb{ST}, \mathbb{SD} \rangle \\
\mathbb{ST}^\Gamma &\doteq \mathbb{ST} && \text{where } \Gamma = \langle \mathbb{CI}, \mathbb{CT}, \mathbb{CD}, \mathbb{T}, \mathbb{ST}, \mathbb{SD} \rangle \\
\mathbb{SD}^\Gamma &\doteq \mathbb{SD} && \text{where } \Gamma = \langle \mathbb{CI}, \mathbb{CT}, \mathbb{CD}, \mathbb{T}, \mathbb{ST}, \mathbb{SD} \rangle
\end{aligned}$$

2.3 Rules

Currently all rules have the form: $e : \check{\tau}$. This is not strictly necessary; for example many rules can be relations that does not necessarily involve types at all (e.g. Intro explanation). All we have to ensure is that the set of rules are inductive in the right way. But since I haven't worked out all the rules, I am keeping the rules consistent and always including a type for the time being. That can be fixed later.

$$\begin{array}{c}
\text{SYSTEM INTRODUCTION} \\
\hline
\mathbb{S} : \text{System}
\end{array}$$

$$\begin{array}{c}
\text{SUBSYSTEM INTRODUCTION} \\
\check{\tau} <: \text{Subsystem} \\
\hline
\mathbb{S} : \check{\tau}
\end{array}$$

$$\begin{array}{c}
\text{SUBSYSTEM EXPLANATION INTRODUCTION} \\
\mathbb{S} \mapsto \check{\tau} \in \mathbb{ST}^\Gamma \quad \check{\tau} \mapsto \langle \mathbb{SP}, \mathbb{E}, \{\mathbb{S}\}, \{\mathbb{C}\} \rangle \in \mathbb{SD}^\Gamma \quad \mathbb{E} = \mathbb{E}' \\
\hline
\mathbb{S} \leftarrow \mathbb{E}' : \check{\tau}
\end{array}$$

$$\begin{array}{c}
\text{SUBSYSTEM CONTAINMENT} \\
\mathbb{S} \mapsto \check{\tau} \in \mathbb{ST}^\Gamma \quad \check{\tau} \mapsto \langle \mathbb{SP}, \mathbb{E}, \{\mathbb{S}\}, \{\mathbb{C}\} \rangle \in \mathbb{SD}^\Gamma \quad \mathbb{SP} = \mathbb{S}' \\
\hline
\mathbb{S} \leftarrow \mathbb{S}' : \check{\tau}
\end{array}$$

$$\begin{array}{c}
\text{COMPONENT INTRODUCTION} \\
\mathbb{C} \mapsto \check{\tau} \in \mathbb{CT}^\Gamma \\
\hline
\Gamma \vdash \mathbb{C} : \check{\tau}
\end{array}$$

COMPONENT SUBTYPING

$$\begin{array}{c}
\mathbb{C} \mapsto \check{\tau} \in \mathbb{CT}^\Gamma \\
\mathbb{C} \mapsto \mathbb{C}' \in \mathbb{CI}^\Gamma \quad \mathbb{C}' \mapsto \check{\tau}' \in \mathbb{CT}^\Gamma \quad \text{NCI}(\mathbb{CI}^\Gamma, \mathbb{C}, \mathbb{C}') \quad \check{\tau} <: \check{\tau}' \in \mathbb{T}^\Gamma \\
\check{\tau} \mapsto \langle _, _, \{\mathbb{f}\} \rangle \in \mathbb{CD}^\Gamma \quad \check{\tau}' \mapsto \langle _, _, \{\mathbb{f}'\} \rangle \in \mathbb{CD}^\Gamma \quad \{\mathbb{f}\} \subset \{\mathbb{f}'\} \\
\hline
\Gamma \vdash \mathbb{C} : \check{\tau}
\end{array}$$

$$\begin{array}{c}
\text{COMPONENT IMPLICIT SUBTYPING} \\
\frac{C \mapsto \check{\tau} \in \mathbb{CT}^\Gamma \quad \nexists C'. C \mapsto C' \in \mathbb{CI}^\Gamma \quad \check{\tau} <: \text{Component} \in \mathbb{T}^\Gamma}{\Gamma \vdash C : \check{\tau}}
\\[10pt]
\text{COMPONENT EXPLANATION INTRODUCTION} \\
\frac{C \mapsto \check{\tau} \in \mathbb{CT}^\Gamma \quad \check{\tau} \mapsto \langle S, E, \{f\} \rangle \in \mathbb{CD}^\Gamma \quad E = E'}{C \leftarrow E' : \check{\tau}}
\\[10pt]
\text{COMPONENT CONTAINMENT} \\
\frac{\begin{array}{l} C \mapsto \check{\tau} \in \mathbb{CT}^\Gamma \quad \check{\tau} \mapsto \langle S, E, \{f\} \rangle \in \mathbb{CD}^\Gamma \quad S = S' \\ S' \mapsto \check{\tau}' \in \mathbb{ST}^\Gamma \quad \check{\tau}' \mapsto \langle SP, E, \{S\}, \{C\} \rangle \in \mathbb{SD}^\Gamma \quad C \in \{C\} \end{array}}{C \leftarrow S' : \check{\tau}}
\\[10pt]
\text{QUERY INTRODUCTION} \\
\frac{C \mapsto \check{\tau} \in \mathbb{CT}^\Gamma \quad \check{\tau} \mapsto \langle S, E, \{f\} \rangle \in \mathbb{CD}^\Gamma \quad q \in \{f\}}{C \leftarrow q : \check{\tau}}
\\[10pt]
\text{COMMAND INTRODUCTION} \\
\frac{C \mapsto \check{\tau} \in \mathbb{CT}^\Gamma \quad \check{\tau} \mapsto \langle S, E, \{f\} \rangle \in \mathbb{CD}^\Gamma \quad c \in \{f\}}{C \leftarrow c : \check{\tau}}
\\[10pt]
\text{CONSTRAINT INTRODUCTION} \\
\frac{C \mapsto \check{\tau} \in \mathbb{CT}^\Gamma \quad \check{\tau} \mapsto \langle S, E, \{f\} \rangle \in \mathbb{CD}^\Gamma \quad i \in \{f\}}{C \leftarrow i : \check{\tau}}
\end{array}$$

2.4 Auxiliary Functions and Relations

Non-circular-Inheritance indicates that a component's inheritance chain does not have a cycle. Note that the particular relation only checks for circles that includes the specific component. However since this relation must be satisfied by every component, any cycle in the chain will be detected at some point. Formally non-circularity is a ternary relation defined inductively as below:

$$\text{NCI}(\mathbb{CI}^\Gamma, C, C') = \begin{cases} \text{undefined iff } C = C' \\ \text{undefined iff } \text{NCI}(\mathbb{CI}^\Gamma, C, C'') \text{ where } C' \mapsto C'' \in \mathbb{CI}^\Gamma \\ \text{defined otherwise} \end{cases}$$