Modeling Conventions

J-R. Abrial

September 2004
Structure of a Model

- List of **Sets** (identifiers)

- List of **Constants** (identifiers)

- List of **Properties** (predicates built on sets and constants)

- List of **Variables** (identifiers)

- List of **Invariants** (predicates built on sets, constants, and variables)

- List of **Events** (next slide)
\[ <name> \equiv \begin{array}{l}
\text{when} \\
<\text{guard}> \\
\ldots \\
\text{then} \\
<\text{assignment}> \\
\ldots \\
\text{end}
\end{array} \]
Assignments

Deterministic \(< variable > := < expression >\)

Non-deterministic

\[
\text{any } < variable > \text{ where } < condition > \\
\ldots \\
\text{then} \\
\text{then } < variable > := < expression > \\
\ldots \\
\text{end}
\]
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\in$</td>
<td>set membership operator</td>
</tr>
<tr>
<td>$\mathbb{N}$</td>
<td>set of Natural Numbers: ${0, 1, 2, 3, \ldots}$</td>
</tr>
<tr>
<td>$a .. b$</td>
<td>interval from $a$ to $b$: ${a, a + 1, \ldots, b}$</td>
</tr>
<tr>
<td>$S \rightarrow T$</td>
<td>set of total functions from $S$ to $T$</td>
</tr>
<tr>
<td>$S \leftrightarrow T$</td>
<td>set of partial functions from $S$ to $T$</td>
</tr>
<tr>
<td>→</td>
<td>pair constructing operator</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------</td>
</tr>
<tr>
<td>{...}</td>
<td>set defined in extension</td>
</tr>
<tr>
<td>∅</td>
<td>empty set</td>
</tr>
<tr>
<td>$\mathbb{F}_1(S)$</td>
<td>Non-empty set of finite subsets of $S$</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>$\mathbb{F}(S)$</td>
<td>Set of finite subsets of $S$</td>
</tr>
<tr>
<td>$\mathbb{P}_1(S)$</td>
<td>Non-empty set of subsets of $S$</td>
</tr>
<tr>
<td>$\mathbb{P}(S)$</td>
<td>Set of subsets of $S$</td>
</tr>
<tr>
<td>$\text{max}(S)$</td>
<td>Maximum of a non-empty finite set of numbers</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>$S \rightarrow T$</td>
<td>set of bijections from $S$ to $T$</td>
</tr>
<tr>
<td>$S \times T$</td>
<td>Cartesian product of $S$ and $T$</td>
</tr>
<tr>
<td>$f \leftarrow g$</td>
<td>overwriting operator for functions</td>
</tr>
<tr>
<td>dom</td>
<td>domain of a function</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------</td>
</tr>
<tr>
<td>ran</td>
<td>range of a function</td>
</tr>
<tr>
<td>△</td>
<td>domain restriction operator</td>
</tr>
<tr>
<td>▲</td>
<td>domain subtraction operator</td>
</tr>
<tr>
<td>id(S)</td>
<td>identity function built on the set S</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>$S \cup T$</td>
<td>set-theoretic union operator</td>
</tr>
<tr>
<td>$S \cap T$</td>
<td>set-theoretic intersection operator</td>
</tr>
<tr>
<td>$S \setminus T$</td>
<td>set-theoretic difference operator</td>
</tr>
<tr>
<td>$f^{-1}$</td>
<td>converse of a function</td>
</tr>
<tr>
<td>$f[S]$</td>
<td>image of a set under a function</td>
</tr>
</tbody>
</table>
A Small Theory of Parities

Constant: \( pty \)

\[
pty \in \mathbb{N} \rightarrow \{0, 1\}
\]

\[
pty(0) = 0
\]

\[
\forall n \cdot (n \in \mathbb{N} \Rightarrow pty(n + 1) = 1 - pty(n))
\]

\[
\forall x, y \cdot \left( \begin{array}{l}
x \in \mathbb{N} \\
y \in \mathbb{N} \\
x \in y \ldots y + 1 \\
pty(x) = pty(y) \\
\Rightarrow \\
x = y
\end{array} \right)
\]
Set: $N$  

Constants: $nxt, itv$

\[
\begin{align*}
nxt &\in N \rightarrow N \\
itude &\in N \times N \rightarrow \mathcal{P}(N) \\
\forall x \cdot (x \in N \Rightarrow \itude(x, x) = \{ x \}) \\
\forall x, y \cdot (x \neq \text{nxt}(y) \Rightarrow \itude(x, \text{nxt}(y)) = \itude(x, y) \cup \{ \text{nxt}(y) \}) \\
\forall x \cdot (x \in N \Rightarrow \itude(\text{nxt}(x), x) = N)
\end{align*}
\]
Set: $N$  

Constants: $r, f$

\[
\begin{align*}
  r &\in N \\
  f &\in N \setminus \{r\} \to N \\
  \forall S \cdot 
  \begin{cases} 
    S \subseteq N \\
    r \in S \\
    f^{-1}[S] \subseteq S \\
    N \subseteq S 
  \end{cases}
\]