Sets and Types in B

Michael Butler, University of Southampton

Types

Let T be some set and x some constant or variable.
$x \in T$ says that x is of type T.
All variables and expressions in B must have a type.

$$
\begin{array}{lcl}
x & \in & \mathbb{N} \\
y & \in & \mathbb{Z} \\
unix & \in & OperatingSystem \\
7 & \in & \mathbb{N} \\
(3+5) & \in & \mathbb{N}
\end{array}
$$

What are the types of the following expressions?

$$(a+b) \times (3!)$$
$$windows$$

Types in B

- Basic Types:
  - $\mathbb{Z}$ Integers
  - $\mathbb{N}$ Natural numbers (including 0)
  - $\mathbb{B}$ Booleans (TRUE, FALSE)

- Deferred Types:
  - SETS $Word$; $Name$

  We defer a decision about how these types are formed.

- Enumerated Types:
  - SETS $Direction = \{ north, south, east, west \}$

  We enumerate all the possible values of these types.

Sets have types too

$\{3, 4, 5\}$ is a set of natural numbers.

More Precisely: $\{3, 4, 5\} \in \mathbb{P}(\mathbb{N})$.

IMPORTANT $S \in \mathbb{P}(T)$ is the same as $S \subseteq T$

Example

$$\mathbb{P}(\ \{a, b, c\}\ ) = \{\ \{\},\ \{a\},\ \{b\},\ \{c\},\ \{a, b\},\ \{a, c\},\ \{b, c\},\ \{a, b, c\}\ \}$$

$$\{a, b\} \in \mathbb{P}(\ \{a, b, c\}\ )$$
$$\{a, b\} \subseteq \{a, b, c\}$$

Assume S and T have type $\mathbb{P}(M)$. What are the types of:

$$S \cup T$$
$$S \cap T$$

Type of $\{\ 3.4,\ 5.78,\ \pi\ \}$?

Type of $\{\ \{3,4\},\ \{4,6\},\ \{7\}\ \}$?

Expressions which are incorrectly typed are meaningless:

$$\{4, 6, unix\}$$
$$\{windows, mac\} \cup \{bwm, rover, ford\}$$

Classification of Types

Simple Types:

- $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{B}$
- Deferred types ($Word$, $Name$)
- Enumerated types ($Direction = \{\ north,\ south,\ east,\ west\ \}$)

Constructed Types:

- $\mathbb{P}(T)$

$\mathbb{P}(T)$ is a type constructed from T.
We will see more constructed types later.

Why Types?

- Help to structure specifications by differentiating objects.
- Help to prevent errors by not allowing us to write meaningless things.
- Types can be checked by computer.

Example System Requirements

- Specify a system that monitors users entering and leaving a building.
- A person can only enter the building if they are recognised by the monitor.
- The system should be aware of whether a recognised user is currently inside or outside the building.

Is there anything missing from this set of requirements?

MACHINE $Monitor$

SETS $User$; $Status = \{ is\_in, is\_out \}$

VARIABLES $register, in, out$

INVARIANT

$$
\begin{array}{l}
register \in \mathbb{P}(User) \ \wedge \\
in \in \mathbb{P}(User) \ \wedge \\
out \in \mathbb{P}(User) \ \wedge \\
\\
in \subseteq register \ \wedge \\
out \subseteq register \ \wedge \\
in \cap out = \{\} \ \wedge \\
register \subseteq in \cup out
\end{array}
$$

INITIALISATION $in,\ out,\ register\ :=\ \{\},\ \{\},\ \{\}$

$Enter(s)\ \widehat{=}$ PRE
$s \in out$
THEN
$in := in \cup \{s\} \quad \| \quad out := out \setminus \{s\}$
END

$Leave(s)\ \widehat{=}$ PRE
$s \in in$
THEN
$in := in \setminus \{s\} \quad \| \quad out := out \cup \{s\}$
END

$res \longleftarrow GetStatus(s) \;\; \widehat{=}$

PRE

$s \in register$

THEN

IF $s \in in$

THEN $res := is\_in$

ELSE $res := is\_out$ END

END

$NewUser(s) \;\; \widehat{=}$

PRE

$s \in (User \setminus register)$

THEN

$register := register \cup \{s\}$

END

$res \longleftarrow GetStatus(s) \;\widehat{=}$

PRE

$s \in register$

THEN

IF $s \in in$

THEN $res := is\_in$

ELSE $res := is\_out$ END

END

$NewUser(s) \;\widehat{=}$

PRE

$s \in (User \setminus register)$

THEN

$register := register \cup \{s\} \quad \| \quad out := out \cup \{s\}$

END