

An Event-B Specification of Typing Tests

I assume that typing can be made arbitrarily smart, however I do not yet know the limits of how much typing Rodin can do.

For sure both evbt and Rodin does explicit typing based on statements like: ‘ $x \in \mathbb{N}$ ’ ‘ $\text{alfa} \in \mathbb{N} \rightarrow \text{BOOL}$ ’ or ‘ $p \in \text{STAFF}$ ’

But Rodin also does implicit typing based on operations. For example:

“ ‘ $\text{@inv1 } \text{alfa} \in \mathbb{N} \rightarrow \text{BOOL}$ ‘ $\text{@inv2 } \text{beta} \cap \text{ran}(\text{alfa}) = \emptyset$ “

The disjunction forces the type of beta to be the same as the type of $\text{ran}(\text{alfa})$ ie \mathbb{N} .

“ ‘ $\text{@inv3 } x \in \mathbb{N}$ ‘ $\text{@inv4 } x + y = 7$ “

The addition forces Rodin the type of y to be \mathbb{Z} (not \mathbb{N} !!)

This projects tests the extent of implicit typing implemented so far in evbt.

1	MACHINE MoreTyping	2
1.1	<i>alfa beta x y</i>	2
1.2	<i>gamma(b)</i>	2

VARIABLES

1.1

alfa
beta
x
y

INVARIANTS

inv1: $alfa \in \mathbb{N} \leftrightarrow \text{BOOL}$
inv2: $beta \cap \text{ran}(alfa) = \emptyset$

The type of $\text{ran}(alfa)$ will propagate to $beta$.

inv3: $x \in \mathbb{N}$

inv4: $x + y = 7$

The type of y is deduced to \mathbb{Z} .

EVENT INITIALISATION

THEN

init1: $alfa := \emptyset$
init2: $beta := \emptyset$
init3: $x := 14$
init4: $y := 7$

END

EVENT gamma

1.2

ANY

b

WHERE

grd11: $b \in beta$

THEN

act11: $beta := beta \setminus \{b\}$

END

alfa, 2

beta, 2

gamma, 2

INITIALISATION, 2

MoreTyping, 2

x, 2

y, 2