An Event-B Specification of

TypingTests

Event-B performs type checking of formulas and variables. Within evbt these types are called checked types. Such checked types can be used for implementing a variable but they have neither limits on integers nor restrictions on the sets. Thus the generated code is not very efficient.

Therefore evbt will try to deduce suitable implementation types to be able use an efficient map for a partial function or a vector for a full function with a domain 1..100.

If no implementation type can be found, then evbt will fall back to using the checked type for implementation.

MACHINE Typing 3 a \boxed{1}

VARIABLES \boxed{1.1}

settings

INVARIANTS

inv_1: $settings \in \mathbb{N} ⇸ \mathbb{N}$

The core type is $\mathbb{P}(\mathbb{Z}\times\mathbb{Z})$ ie it looks like a generic relation with unbounded integers. However it could be implemented using a map with bigints since it is a partial function. So the implementation type is $\mathbb{N}⇸\mathbb{N}$.

EVENT INITIALISATION

THEN

init_1: $settings :\in \mathbb{N} ⇸ \mathbb{N}$

END

EVENT setKeyValue \boxed{1.2}

ANY

k
v

WHERE

grd_1: $k \in \mathrm{dom}(settings)$

grd_2: $v \in \mathrm{ran}(settings)$

THEN

act_1: $settings(k) := v$

END

REFINEMENT Typing_R1_NarrowIntoAVector 4 a $\boxed{2}$

REFINES Typing

VARIABLES $\boxed{2.1}$
INVARIANTS

inv1_1: $\mathit{settings} \in 1..20 \rightarrow 0..255$

We narrow the partial function into a full function and limit the bounds of the domain and the range. The checked type is still $\mathbb{P}(\mathbb{Z}\times\mathbb{Z})$ but the implementation type is $1..20{\rightarrow}0..255$ which can be implemented using a fixed size vector.

EVENT INITIALISATION
THEN

init1_1: $\mathit{settings} :\in 1..20 \rightarrow 0..255$

END