

311 The specification

new $x: \text{nat}$ $x := -1$

introduces a local variable and then assigns it a value that is out of bounds. Is this specification implementable? (Proof required.)

After trying the question, scroll down to the solution.

§ Let the nonlocal variables be σ .

new $x: \text{nat}$ $x := -1$

$= \exists x, x': \text{nat} \ x' = -1 \wedge \sigma' = \sigma$

$= \perp$

so it is unimplementable.

local axiom $x': \text{nat}$ conflicts with $x' = -1$