$Boolean ::= True \mid False$

Data

$dia: \mathbb{N}_1$
$mes: \mathbb{N}_1$
$ano: \mathbb{N}_1$

anteriorOuIgual

$this?: Data$
$d?: Data$
$result!: Boolean$

[*CARRO*]

Sistema

$roubados: CARRO \pfun Data$
$encontrados: CARRO \pfun Data$

$\dom encontrados \subseteq \dom roubados$

carroRoubado

$\Delta Sistema$
$c?: CARRO$
$d?: Data$

$c? \notin \dom roubados$
$roubados' = roubados \cup \{(c? \mapsto d?)\}$

removerCarroRoubado

$\Delta Sistema$
$c?: CARRO$

$c? \in \dom roubados$
$roubados' = roubados \setminus \{(c? \mapsto roubados\ c?)\}$

Sistema1

$roubados1: \seq (CARRO \times Data)$
$encontrados1: \seq (CARRO \times Data)$

$\dom (\ran encontrados1) \subseteq \dom (\ran roubados1)$

carroRoubado1

$\Delta Sistema1$
$c?: CARRO$

d?: Data

$c? \notin \text{dom}\ (\text{ran}\ roubados1)$
$roubados1' = roubados1 \frown \langle (c?, d?) \rangle$

Retrieve

Sistema
Sistema1

---

ran *roubados1* = *roubados*
ran *encontrados1* = *encontrados*

---

theorem *CarroRoubado1Aplicabilidade*
pre *carroRoubado* $\wedge$ *Retrieve* $\Rightarrow$ pre *carroRoubado1*

incomplete proof of *CarroRoubado1Aplicabilidade*
invoke *Retrieve*
prove by reduce

theorem *CarroRoubado1Corretude*
pre *carroRoubado* $\wedge$ *Retrieve* $\wedge$ *carroRoubado1* $\wedge$ *Retrieve'* $\Rightarrow$ *carroRoubado*

proof of *CarroRoubado1Corretude*
invoke *carroRoubado*
invoke *Retrieve*
prove by reduce

Sistema2

roubados21: seq *CARRO*
roubados22: seq *Data*
encontrados21: seq *CARRO*
encontrados22: seq *Data*

---

ran *encontrados21* $\subseteq$ ran *roubados21*

---

carroRoubado2

Δ*Sistema2*
c?: CARRO
d?: Data

$c? \notin$ ran *roubados21*
$roubados21' = roubados21 \frown \langle c? \rangle$
$roubados22' = roubados22 \frown \langle d? \rangle$

Retrieve2

Sistema1
Sistema2

---

ran *roubados21* = dom (ran *roubados1*)
ran *roubados22* = ran (ran *roubados1*)
ran *encontrados21* = dom (ran *encontrados1*)
ran *encontrados22* = ran (ran *encontrados1*)

theorem *CarroRoubado2Aplicabilidade*
pre *carroRoubado1* ∧ *Retrieve* ⇒ pre *carroRoubado2*

theorem *CarroRoubado2Corretude*
pre *carroRoubado1* ∧ *Retrieve* ∧ *carroRoubado2* ∧ *Retrieve'* ⇒ *carroRoubado1*

incomplete proof of *CarroRoubado2Corretude*
invoke *carroRoubado1*
invoke *Retrieve*
prove by reduce

CadEnc

encontrados31: seq *CARRO*
encontrados32: seq *Data*

CadRoubos

roubados31: seq *CARRO*
roubados32: seq *Data*

Sistema3

cadRoubos: CadRoubos
cadEnc: CadEnc

---

ran *cadEnc* . *encontrados31* ⊆ ran *cadRoubos* . *roubados31*

carroRoubado3

Δ*Sistema3*
c?: CARRO
d?: Data

---

c? ∉ ran *cadRoubos* . *roubados31*
cadRoubos' . *roubados31* = *cadRoubos* . *roubados31* ⌢ ⟨*c?*⟩
cadRoubos' . *roubados32* = *cadRoubos* . *roubados32* ⌢ ⟨*d?*⟩

incomplete proof of *carroRoubado3$domainCheck*
apply *inDom to predicate* (*cadRoubos* . *roubados32*, ⟨*d?*⟩) ∈ dom (_⌢_)
apply *inDom to predicate* (*cadRoubos* . *roubados31*, ⟨*c?*⟩) ∈ dom (_⌢_)
prove by reduce

Retrieve3

Sistema2

Sistema3

---

ran *cadRoubos* . *roubados31* = ran *roubados21*
ran *cadRoubos* . *roubados32* = ran *roubados22*
ran *cadEnc* . *encontrados31* = ran *encontrados21*
ran *cadEnc* . *encontrados32* = ran *encontrados22*

---

theorem *CarroRoubado3Aplicabilidade*
pre *carroRoubado2* ∧ *Retrieve* ⟹ pre *carroRoubado3*

theorem *CarroRoubado3Corretude*
pre *carroRoubado2* ∧ *Retrieve* ∧ *carroRoubado3* ∧ *Retrieve'* ⟹ *carroRoubado2*