1 Modeling

We present the specification of a mutual exclusion protocol.

1.1 Rigid data types

Example 1 (Labels)**.**

```
 spec! LABEL
 sort Label .
 ops re wt cs : -> Label [ctor].
 op _~_ : Label Label -> Bool [comm].
 var  L : Label .
 eq (re ~ wt) = false .
 eq (re ~ cs) = false .
 eq (wt ~ cs) = false .
---
 ceq true = false if re = wt .
 ceq true = false if re = cs .
 ceq true = false if wt = cs .
```

Example 2 (Process identifiers)**.**

```
 spec* PID
 inc BOOL .
 sort Pid .
 op _~_ : Pid Pid -> Bool [comm].
 vars I J : Pid .
 eq I ~ I = true .
 ceq I = J if I ~ J [nonexec].
```

Example 3 (lists of process identifiers)**.**

```
 spec! SEQUENCE{X :: PID}
 sort Sequence .
 subsorts X$Pid < Sequence .
--- constructors
 op empty : -> Sequence [ctor] .
 op _,_ : Sequence Sequence -> Sequence [ctor id: empty assoc].
 vars Q Q' : Sequence . var I : X$Pid .
---
 op top : Sequence -> X$Pid .
 eq top(empty) = empty .
 eq top(I,Q) = I .
---
 op get : Sequence -> Sequence .
 eq get(empty) = empty .
 eq get(I,Q) = Q .
---
 ceq true = false if Q,I,Q' := empty .
 ceq [lemma-top]: top(Q,I) = top(Q) if top(Q) :: X$Pid .
```

1.2 Nominals

Example 4 (Agents)**.**

```
 spec* AGENT
 sort Agent
```

Example 5 (Nominals).

```
spec! NOMINAL{Y :: AGENT}
sorts Sys.
--- actions
op init : -> Sys [ctor].
ops want try exit : Sys Y$Agent -> Sys [ctor].
```

1.3 Flexible data types

Example 6 (Mutual exclusion protocol).

spec* QLOCK{X :: PID, Y :: AGENT}

pr SEQUENCE{X} . pr NOMINAL{Y} . pr LABEL .

--- observers

op pid $:\rightarrow$ X\$Pid --- extract pid from agents

op sq $:\rightarrow$ Sequence --- gives the waiting queue for each state

op pc $:\rightarrow$ Label --- indicates the label of each agent at a given state

--- variables

vars S S_1 S_2 : Sys

vars I J K : X\$Pid

vars A B C : Y\$Agent

var Q : Sequence

--- restrictions ---

(1) $\forall \mathtt{A}, \mathtt{S}_1, \mathtt{S}_2 \cdot @_{\mathtt{S}_1} @_{\mathtt{A}} \mathtt{pid} = @_{\mathtt{S}_2} @_{\mathtt{A}} \mathtt{pid}$ --- pid depends only of the agent

(2) $\forall \mathtt{A}, \mathtt{B}, \mathtt{S} \cdot @_{\mathtt{S}} @_{\mathtt{A}} \mathtt{sq} = @_{\mathtt{S}} @_{\mathtt{B}} \mathtt{sq}$ --- sq depends only of the current state

--- init ---

(3) $\forall \mathtt{A} \cdot @_{\mathtt{init}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{re}$

(4) $@_{\mathtt{init}} \mathtt{sq} = \mathtt{empty}$

--- want ---

(5) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{want(S,A)}} @_{\mathtt{B}} \mathtt{pc} = \mathtt{wt}$ if $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{re} \ \bigwedge \ \mathtt{A} = \mathtt{B}$

(6) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{want(S,A)}} @_{\mathtt{B}} \mathtt{pc} = @_{\mathtt{S}} @_{\mathtt{B}} \mathtt{pc}$ if $\mathtt{A} \sim \mathtt{B} = \mathtt{false}$

(7) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{want(S,A)}} @_{\mathtt{B}} \mathtt{pc} = @_{\mathtt{S}} @_{\mathtt{B}} \mathtt{pc}$ if $@_{\mathtt{A}} @_{\mathtt{S}} \mathtt{pc} \sim \mathtt{re} = \mathtt{false}$

(8) $\forall \mathtt{S}, \mathtt{A} \cdot @_{\mathtt{want(S,A)}} \mathtt{sq} = (@_{\mathtt{S}} \mathtt{sq}), (@_{\mathtt{A}} \mathtt{pid})$ if $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{re}$

(9) $\forall \mathtt{S}, \mathtt{A} \cdot @_{\mathtt{want(S,A)}} \mathtt{sq} = @_{\mathtt{S}} \mathtt{sq}$ if $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} \sim \mathtt{re} = \mathtt{false}$

--- try ---

(10) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{try(S,A)}} @_{\mathtt{B}} \mathtt{pc} = \mathtt{cs}$ if $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{wt} \ \bigwedge \ (@_{\mathtt{A}} \mathtt{pid}), \mathtt{Q} := @_{\mathtt{S}} \mathtt{sq} \ \bigwedge \ \mathtt{A} = \mathtt{B}$

(11) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{try(S,A)}} @_{\mathtt{B}} \mathtt{pc} = @_{\mathtt{S}} @_{\mathtt{B}} \mathtt{pc}$ if $\mathtt{A} \sim \mathtt{B} = \mathtt{false}$

(12) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{try(S,A)}} @_{\mathtt{B}} \mathtt{pc} = @_{\mathtt{S}} @_{\mathtt{B}} \mathtt{pc}$ `if` $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} \sim \mathtt{wt} = \mathtt{false}$

(13) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{B}} @_{\mathtt{try(S,A)}} \mathtt{pc} = @_{\mathtt{B}} @_{\mathtt{S}} \mathtt{pc}$ `if` $\mathtt{top}(@_{\mathtt{S}} \mathtt{sq}) \sim @_{\mathtt{A}} \mathtt{pid} = \mathtt{false}$

(14) $\forall \mathtt{S}, \mathtt{A} \cdot @_{\mathtt{try(S,A)}} \mathtt{sq} = @_{\mathtt{S}} \mathtt{sq}$

`--- exit ---`

(15) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{exit(S,A)}} @_{\mathtt{B}} \mathtt{pc} = \mathtt{re}$ `if` $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{cs} \ \bigwedge \ \mathtt{A} = \mathtt{B}$

(16) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{exit(S,A)}} @_{\mathtt{B}} \mathtt{pc} = @_{\mathtt{A}} @_{\mathtt{B}} \mathtt{pc}$ `if` $\mathtt{A} \sim \mathtt{B} = \mathtt{false}$

(17) $\forall \mathtt{S}, \mathtt{A}, \mathtt{B} \cdot @_{\mathtt{exit(S,A)}} @_{\mathtt{B}} \mathtt{pc} = @_{\mathtt{A}} @_{\mathtt{B}} \mathtt{pc}$ `if` $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} \sim \mathtt{cs} = \mathtt{false}$

(18) $\forall \mathtt{S}, \mathtt{A} \cdot @_{\mathtt{exit(S,A)}} \mathtt{sq} = \mathtt{get}(@_{\mathtt{S}} \mathtt{sq})$ `if` $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{cs}$

(19) $\forall \mathtt{S}, \mathtt{A} \cdot @_{\mathtt{exit(S,A)}} \mathtt{sq} = @_{\mathtt{S}} \mathtt{sq}$ `if` $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} \sim \mathtt{cs} = \mathtt{false}$

2 Formal verification

We are interested in proving both invariant and liveness properties.

2.1 Invariant property

We will prove prove formally that $\mathtt{QLOCK} \vdash \forall \mathtt{S}, \mathtt{A} \cdot \mathtt{top}(@_{\mathtt{S}} \mathtt{sq}) = @_{\mathtt{A}} \mathtt{pid}$ if $@_{\mathtt{S}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{cs}$.

==

spec $\mathtt{QLOCK}_I$

pr QLOCK .

op s : -> Sys .

(20) $\forall \mathtt{A} \cdot \mathtt{top}(@_{\mathtt{s}} \mathtt{sq}) = @_{\mathtt{A}} \mathtt{pid}$ `if` $@_{\mathtt{s}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{cs}$ [induction hypothesis].

==

spec $\mathtt{QLOCK}_{TC}$

pr $\mathtt{QLOCK}_I$.

op a b : -> Y$Agent .

==

Apply induction on S:

[init]

1	$\mathtt{QLOCK} \vdash \forall \mathtt{A} \cdot \mathtt{top}(@_{\mathtt{init}} \mathtt{sq}) = @_{\mathtt{A}} \mathtt{pid}$ if $@_{\mathtt{init}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{cs}$	
2	$\mathtt{QLOCK} \vdash \forall \mathtt{A} \cdot \mathtt{top}(@_{\mathtt{init}} \mathtt{sq}) = @_{\mathtt{A}} \mathtt{pid}$ if $\mathtt{re} = \mathtt{cs}$	by sentence (3)
3	discharged	since $\mathtt{QLOCK} \vdash \mathtt{true} = \mathtt{false}$ if $\mathtt{re} = \mathtt{cs}$

[want]

1	$\mathtt{QLOCK}_I \vdash \forall \mathtt{A}, \mathtt{B} \cdot \mathtt{top}(@_{\mathtt{want(s,B)}} \mathtt{sq}) = @_{\mathtt{A}} \mathtt{pid}$ if $@_{\mathtt{want(s,B)}} @_{\mathtt{A}} \mathtt{pc} = \mathtt{cs}$
2	$\mathtt{QLOCK}_{TC} \vdash \mathtt{top}(@_{\mathtt{want(s,b)}} \mathtt{sq}) = @_{\mathtt{a}} \mathtt{pid}$ if $@_{\mathtt{want(s,b)}} @_{\mathtt{a}} \mathtt{pc} = \mathtt{cs}$

[$\mathtt{b} = \mathtt{a}$, $@_{\mathtt{s}} @_{\mathtt{b}} \mathtt{pc} = \mathtt{re}$]

1 $\mathtt{QLOCK}_{TC} + \{\mathtt{b} = \mathtt{a}, @_{\mathtt{s}}\, @_{\mathtt{b}}\, \mathtt{pc} = \mathtt{re}\} \vdash$
$\mathtt{top}(@_{\mathtt{want(s,b)}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{want(s,b)}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by case analysis

2 $\mathtt{QLOCK}_{TC} + \{\mathtt{b} = \mathtt{a}, @_{\mathtt{s}}\, @_{\mathtt{b}}\, \mathtt{pc} = \mathtt{re}\} \vdash$
$\mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}, @_{\mathtt{b}}\, \mathtt{pid}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $\mathtt{wt} = \mathtt{cs}$ — by rew

3 discharged — since $\mathtt{QLOCK} \vdash \mathtt{true} = \mathtt{false}$ if $\mathtt{wt} = \mathtt{cs}$

[$\mathtt{b} \sim \mathtt{a} = \mathtt{false}$]

1 $\mathtt{QLOCK}_{TC} + \{\mathtt{b} \sim \mathtt{a} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{want(s,b)}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{want(s,b)}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by case analysis

2 $\mathtt{QLOCK}_{TC} + \{\mathtt{a} \sim \mathtt{b} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{s}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by rew

3 discharged — by the induction hypothesis

[$@_{\mathtt{s}}\, @_{\mathtt{b}}\, \mathtt{pc} \sim \mathtt{re} = \mathtt{false}$]

1 $\mathtt{QLOCK}_{TC} + \{@_{\mathtt{s}}\, @_{\mathtt{b}}\, \mathtt{pc} \sim \mathtt{re} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{want(s,b)}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{want(s,b)}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by case analysis

2 $\mathtt{QLOCK}_{TC} + \{@_{\mathtt{s}}\, @_{\mathtt{b}}\, \mathtt{pc} \sim \mathtt{re} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{s}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by rew

3 discharged — by the induction hypothesis

[$\mathtt{try}$]

1 $\mathtt{QLOCK}_{I} \vdash \forall \mathtt{A}, \mathtt{B} \cdot \mathtt{top}(@_{\mathtt{try(s,B)}}\, \mathtt{sq}) = @_{\mathtt{A}}\, \mathtt{pid}$ if $@_{\mathtt{try(s,B)}}\, @_{\mathtt{A}}\, \mathtt{pc} = \mathtt{cs}$

2 $\mathtt{QLOCK}_{TC} \vdash \mathtt{top}(@_{\mathtt{try(s,b)}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{try(s,b)}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$

[$\mathtt{b} = \mathtt{a},\ @_{\mathtt{s}}\, @_{\mathtt{b}}\, \mathtt{pc} = \mathtt{wt},\ @_{\mathtt{s}}\, \mathtt{sq} = (@_{\mathtt{b}}\, \mathtt{pid}, \mathtt{q})$]

1 $\mathtt{QLOCK}_{TC} + \{\mathtt{q} :\to \mathtt{Sequence}, \mathtt{b} = \mathtt{a}, @_{\mathtt{s}}\, \mathtt{sq} = (@_{\mathtt{b}}\, \mathtt{pid}, \mathtt{q})\} \vdash$
$\mathtt{top}(@_{\mathtt{try(s,b)}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{try(s,b)}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by case analysis

2 $\mathtt{QLOCK}_{TC} + \{\mathtt{q} :\to \mathtt{Sequence}, \mathtt{b} = \mathtt{a}, @_{\mathtt{s}}\, \mathtt{sq} = (@_{\mathtt{b}}\, \mathtt{pid}, \mathtt{q})\} \vdash$
$@_{\mathtt{a}}\, \mathtt{pid} = @_{\mathtt{a}}\, \mathtt{pid}$ if $\mathtt{cs} = \mathtt{cs}$ — by rew, $\mathtt{top}(@_{\mathtt{try(s,b)}}\, \mathtt{sq}) = \mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}) = \mathtt{top}(@_{\mathtt{b}}\, \mathtt{pid}, \mathtt{q}) = @_{\mathtt{b}}\, \mathtt{pid} = @_{\mathtt{a}}\, \mathtt{pid}$ and $@_{\mathtt{try(s,b)}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$

3 $\mathtt{QLOCK}_{TC} + \{\mathtt{q} :\to \mathtt{Sequence}, \mathtt{b} = \mathtt{a}, @_{\mathtt{s}}\, \mathtt{sq} = (@_{\mathtt{b}}\, \mathtt{pid}, \mathtt{q})\} \vdash$
$@_{\mathtt{a}}\, \mathtt{pid} = @_{\mathtt{a}}\, \mathtt{pid}$ — by implication

4 discharged — by reflexivity

[$\mathtt{b} \sim \mathtt{a} = \mathtt{false}$]

1 $\mathtt{QLOCK}_{TC} + \{\mathtt{b} \sim \mathtt{a} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{try(s,b)}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{try(s,b)}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by case analysis

2 $\mathtt{QLOCK}_{TC} + \{\mathtt{a} \sim \mathtt{b} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{s}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by rew

3 discharged — by the induction hypothesis

[$@_{\mathtt{s}}\, @_{\mathtt{b}}\, \mathtt{pc} \sim \mathtt{wt} = \mathtt{false}$]

1 $\mathtt{QLOCK}_{TC} + \{@_{\mathtt{s}}\, @_{\mathtt{b}}\, \mathtt{pc} \sim \mathtt{wt} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{try(s,b)}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{try(s,b)}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by case analysis

2 $\mathtt{QLOCK}_{TC} + \{@_{\mathtt{s}}\, @_{\mathtt{b}}\, \mathtt{pc} \sim \mathtt{wt} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{s}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by rew

3 discharged — by the induction hypothesis

[$\mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}) \sim @_{\mathtt{b}}\, \mathtt{pid} = \mathtt{false}$]

1 $\mathtt{QLOCK}_{TC} + \{\mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}) \sim @_{\mathtt{b}}\, \mathtt{pid} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{try(s,b)}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{try(s,b)}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by case analysis

2 $\mathtt{QLOCK}_{TC} + \{\mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}) \sim @_{\mathtt{b}}\, \mathtt{pid} = \mathtt{false}\} \vdash$
$\mathtt{top}(@_{\mathtt{s}}\, \mathtt{sq}) = @_{\mathtt{a}}\, \mathtt{pid}$ if $@_{\mathtt{s}}\, @_{\mathtt{a}}\, \mathtt{pc} = \mathtt{cs}$ — by rew

3 discharged — by the induction hypothesis

[exit]

1 $\mathtt{QLOCK}_I \vdash \forall \mathtt{A},\mathtt{B} \cdot \mathtt{top}(@_{\mathtt{exit(s,B)}}\,\mathtt{sq}) = @_{\mathtt{A}}\,\mathtt{pid}$ if $@_{\mathtt{exit(s,B)}}\,@_{\mathtt{A}}\,\mathtt{pc} = \mathtt{cs}$

2 $\mathtt{QLOCK}_{TC} \vdash \mathtt{top}(@_{\mathtt{exit(s,b)}}\,\mathtt{sq}) = @_{\mathtt{a}}\,\mathtt{pid}$ if $@_{\mathtt{exit(s,b)}}\,@_{\mathtt{a}}\,\mathtt{pc} = \mathtt{cs}$

[$\mathtt{b} = \mathtt{a},\ @_{\mathtt{s}}\,@_{\mathtt{b}}\,\mathtt{pc} = \mathtt{cs}$]

1 $\mathtt{QLOCK}_{TC} + \{\mathtt{b} = \mathtt{a}, @_{\mathtt{s}}\,@_{\mathtt{b}}\,\mathtt{pc} = \mathtt{cs}\} \vdash$ $\mathtt{top}(@_{\mathtt{exit(s,b)}}\,\mathtt{sq}) = @_{\mathtt{a}}\,\mathtt{pid}$ if $@_{\mathtt{exit(s,b)}}\,@_{\mathtt{a}}\,\mathtt{pc} = \mathtt{cs}$ — by case analysis

2 $\mathtt{QLOCK}_{TC} + \{\mathtt{b} = \mathtt{a}, @_{\mathtt{s}}\,@_{\mathtt{b}}\,\mathtt{pc} = \mathtt{cs}\} \vdash$ $\mathtt{top}(\mathtt{get}(@_{\mathtt{s}}\,\mathtt{sq})) = @_{\mathtt{a}}\,\mathtt{pid}$ if $\mathtt{re} = \mathtt{cs}$ — by rew

3 discharged — since $\mathtt{QLOCK} \vdash \mathtt{true} = \mathtt{false}$ if $\mathtt{re} = \mathtt{cs}$

[$\mathtt{b} \sim \mathtt{a} = \mathtt{false}$]

⋮

[$@_{\mathtt{s}}\,@_{\mathtt{b}}\,\mathtt{pc} \sim \mathtt{cs} = \mathtt{false}$]

⋮

2.2 Liveness property

In this section, we will prove formally that $\mathtt{QLOCK} \vdash \forall \mathtt{S},\mathtt{A} \cdot \exists \mathtt{S}' \cdot @_{\mathtt{S}'}\,@_{\mathtt{A}}\,\mathtt{pc} = \mathtt{cs}$. There are several choices for the definition of witnesses. The first definition of θ is as follows:

$$\theta(\mathtt{S},\mathtt{A}) = \begin{cases} \theta(\mathtt{want}(\mathtt{S},\mathtt{A}),\mathtt{A}) & \text{if } @_{\mathtt{S}}\,@_{\mathtt{A}}\,\mathtt{pc} = \mathtt{re} \\ \theta(\mathtt{try}(\mathtt{exit}(\mathtt{S},\mathtt{B}),\mathtt{C}),\mathtt{A}) & \text{if } @_{\mathtt{S}}\,@_{\mathtt{A}}\,\mathtt{pc} = \mathtt{wt} \bigwedge \mathtt{C} := \mathtt{top}(@_{\mathtt{exit(S,B)}}\,\mathtt{sq}) \bigwedge \mathtt{B} := \mathtt{top}(@_{\mathtt{S}}\,\mathtt{sq}) \\ \mathtt{S} & \text{if } @_{\mathtt{S}}\,@_{\mathtt{A}}\,\mathtt{pc} = \mathtt{cs} \end{cases}$$

The second definition of θ is by induction on $\mathtt{S}$.

[init] $\forall \mathtt{A} \cdot \theta(\mathtt{init},\mathtt{A}) = \mathtt{try}(\mathtt{want}(\mathtt{init},\mathtt{A}),\mathtt{A})$

[want]

$\forall \mathtt{S},\mathtt{A},\mathtt{B} \cdot \theta(\mathtt{want}(\mathtt{S},\mathtt{A}),\mathtt{B}) = \theta(\mathtt{try}(\mathtt{exit}(\mathtt{want}(\mathtt{S},\mathtt{A}),\mathtt{C}),\mathtt{D}))$

if $\mathtt{A} = \mathtt{B} \bigwedge @_{\mathtt{S}}\,@_{\mathtt{A}}\,\mathtt{pc} = \mathtt{re} \bigwedge \mathtt{D} := \mathtt{top}(@_{\mathtt{exit(want(S,A),C)}}\,\mathtt{sq}) \bigwedge @_{\mathtt{C}}\,\mathtt{pid},\mathtt{Q} := @_{\mathtt{S}}\,\mathtt{sq}$

$\forall \mathtt{S},\mathtt{A},\mathtt{B} \cdot \theta(\mathtt{want}(\mathtt{S},\mathtt{A}),\mathtt{B}) = \theta(\mathtt{S},\mathtt{B})$ if $(\mathtt{A} \sim \mathtt{B}) = \mathtt{false}$

$\forall \mathtt{S},\mathtt{A},\mathtt{B} \cdot \theta(\mathtt{want}(\mathtt{S},\mathtt{A}),\mathtt{B}) = \theta(\mathtt{S},\mathtt{B})$ if $@_{\mathtt{S}}\,@_{\mathtt{A}}\,\mathtt{pc} \sim \mathtt{re} = \mathtt{false}$

[try]

[exit]

It suffices to prove that $\mathtt{QLOCK} \vdash \forall \mathtt{S},\mathtt{A} \cdot \mathtt{top}(@_{\theta(\mathtt{S},\mathtt{A})}\,\mathtt{sq}) = @_{\mathtt{A}}\,\mathtt{pid}$. We apply induction on $\mathtt{S}$.

[init]

[want]

[try]

[exit]