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 : $\to$ X$Pid --- extract pid from agents

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

op pc : $\to$ 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) $\forall A, S_1, S_2 \cdot @_{S_1}\, @_A\, pid = @_{S_2}\, @_A\, pid$ --- pid depends only of the agent

(2) $\forall A, B, S \cdot @_S\, @_A\, sq = @_S\, @_B\, sq$ --- sq depends only of the current state

--- init ---

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

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

--- want ---

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

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

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

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

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

--- try ---

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

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

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

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

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

--- exit ---

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

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

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

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

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

2 Formal verification

We are interested in proving formally $\mathtt{QLOCK} \vdash \forall \mathtt{S},\mathtt{A}\cdot \mathtt{top}(@_{\mathtt{S}}\,\mathtt{sq}) = @_{\mathtt{A}}\,\mathtt{pid}$ if $@_{\mathtt{S}}\,@_{\mathtt{A}}\,\mathtt{pc} = \mathtt{cs}$.

==========

spec $\mathtt{QLOCK}_I$

pr QLOCK .

op s : -> Sys .

(20) $\forall \mathtt{A}\cdot \mathtt{top}(@_{\mathtt{s}}\,\mathtt{sq}) = @_{\mathtt{A}}\,\mathtt{pid}\ \mathtt{if}\ @_{\mathtt{s}}\,@_{\mathtt{A}}\,\mathtt{pc} = \mathtt{cs}$ [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 $\texttt{QLOCK} \vdash \texttt{true} = \texttt{false}$ if $\texttt{wt} = \texttt{cs}$

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

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

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

3 discharged — by the induction hypothesis

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

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

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

3 discharged — by the induction hypothesis

[try]

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

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

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

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

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

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

4 discharged — by reflexivity

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

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

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

3 discharged — by the induction hypothesis

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

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

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

3 discharged — by the induction hypothesis

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

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

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

3 discharged — by the induction hypothesis

[exit]

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

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

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

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

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

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

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

⋮

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

⋮