# ASS0 - Dan Nguyen (z5206032)

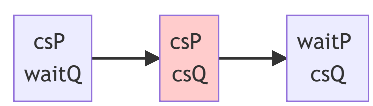
## Part 1

Let:

- $\mathrm{csP}$ be the event where $P$ enters its critical section.
- $\mathrm{csQ}$ be the event where $Q$ enters its critical section.
- $\mathrm{waitP}$ be the event where $P$ is waiting.
- $\mathrm{waitQ}$ be the event where $Q$ is waiting.
- $\mathrm{intentP}$ be $P$'s intent to enter its critical section.
- $\mathrm{intentQ}$ be $Q$'s intent to enter its critical section.

### Mutual Exclusion

Consider the timeline where there is no mutual exclusion:




Mutual exclusion is modelled as:

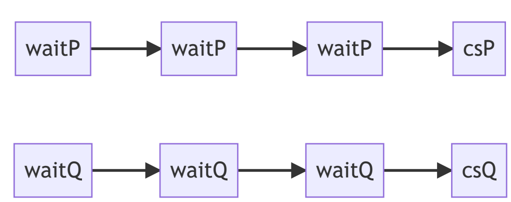
$$\mathrm{mutexPQ} \models \Box\neg(\mathrm{csP} \wedge \mathrm{csQ})$$

The `spin` command to verify this model is:

```
spin -search -ltl mutexPQ algY.pml
```

### Eventual Entry

Consider the timelines where there is an eventual entry:




Eventual entry is modelled as:

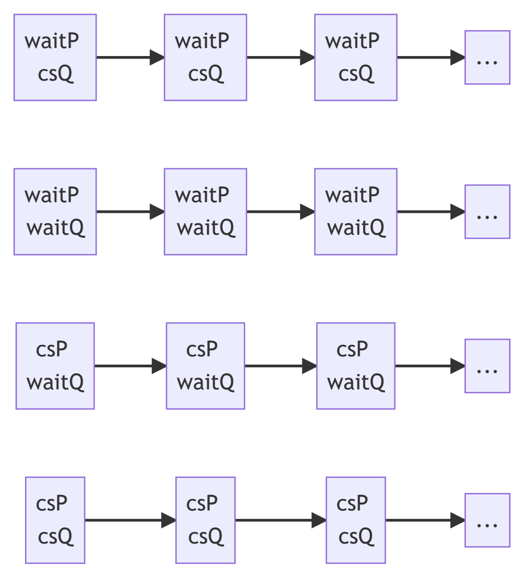
$$\text{entryP} \models \Box(\text{waitP} \implies \Diamond\text{csP})$$
$$\text{entryQ} \models \Box(\text{waitQ} \implies \Diamond\text{csQ})$$

The `spin` commands to verify these models are:

```
spin -search -a -ltl entryP algY.pml
spin -search -a -ltl entryQ algY.pml
```

### Absence of Deadlock

Consider the timelines where there is a deadlock:




Absence of deadlock is modelled as:

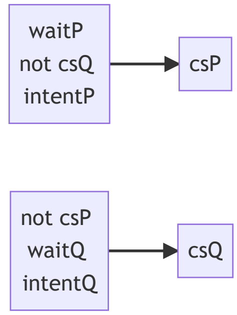
$$\text{deadlock1} \models \Diamond\Box\neg(\text{waitP} \land \text{csQ})$$
$$\text{deadlock2} \models \Diamond\Box\neg(\text{waitP} \land \text{waitQ})$$
$$\text{deadlock3} \models \Diamond\Box\neg(\text{csP} \land \text{waitQ})$$
$$\text{deadlock4} \models \Diamond\Box\neg(\text{csP} \land \text{csQ})$$

The `spin` commands to verify these models are:

```
spin -search -ltl deadlock1 algY.pml
spin -search -ltl deadlock2 algY.pml
spin -search -ltl deadlock3 algY.pml
spin -search -ltl deadlock4 algY.pml
```

### Absence of Unncessary Delay

Consider the timelines where there are no unncessary delays:




Absence of unncessary delay is modelled as:

$$
\begin{aligned}
\text{delayP} &\models \Box((\text{waitP} \land \Box\neg\text{csQ} \land \text{intentP}) \implies \Diamond\text{csP}) \\
\text{delayQ} &\models \Box((\Box\neg\text{csP} \land \text{waitQ} \land \text{intentQ}) \implies \Diamond\text{csQ})
\end{aligned}
$$

The `spin` command to verify this model is:

```
spin -search -a -ltl delayP algY.pml
spin -search -a -ltl delayQ algY.pml
```

### Conclusion

Algorithm Y is a solution to the critical section problem since no failed assertions were raised.

## Part 2

### Programs

Programs $p$ and $q$ shares a bit array, $b$, which is initialised as:

```
bit b[2] = {0, 0}
```

The program $p$ is:

```
    loop forever
p1:     non-critical section
p2:     b[0] = 1
p3:     while b[1] == 1
p4:         b[0] = 1
p5:         await (b[0] == 1)
p6:         b[0] = 1
p7:     critical section
p8:     b[0] = 0
```

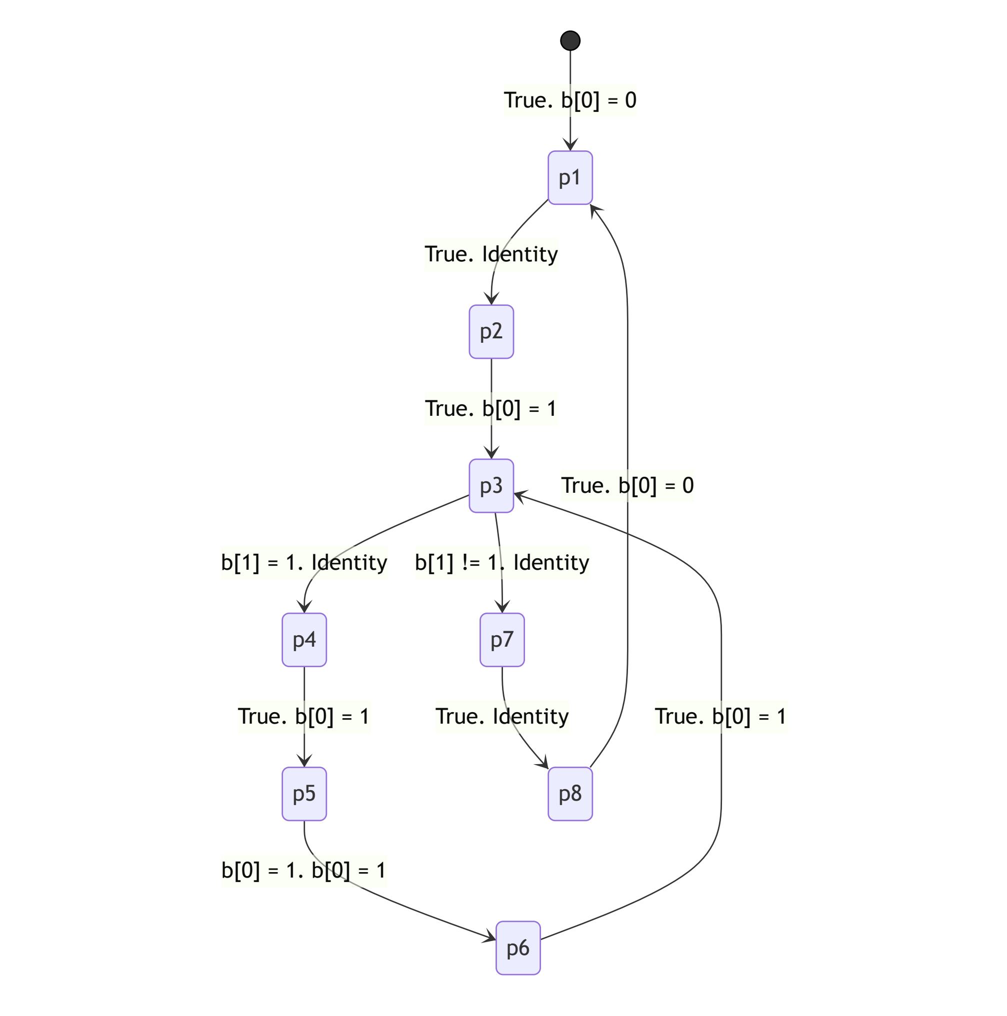
The program $q$ is:

```
    loop forever
q1:     non-critical section
q2:     b[1] = 1
```

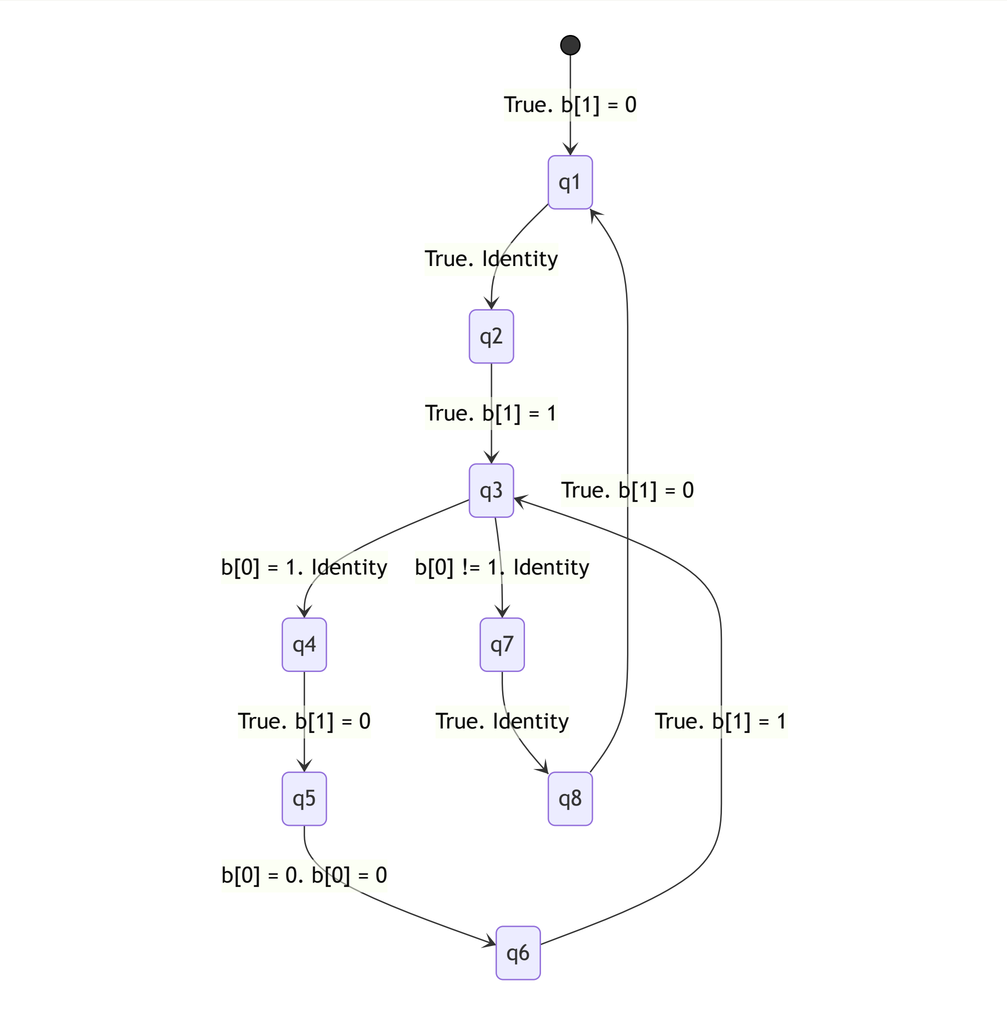
```
q3:     while b[0] == 1
q4:         b[1] = 0
q5:         await (b[0] == 0)
q6:         b[1] = 1
q7:     critical section
q8:     b[1] = 0
```

### Transition Diagrams

$p$'s transition diagram is:




$q$'s transition diagram is:




### Assertion Networks

$p$'s assertion network is:

$$\begin{aligned}
\mathcal{P}(p_1) &\Rightarrow b[0] = 0 \\
\mathcal{P}(p_2) &\Rightarrow b[0] = 0 \\
\mathcal{P}(p_3) &\Rightarrow b[0] = 1 \\
\mathcal{P}(p_4) &\Rightarrow b[0] = 1 \land b[1] = 1 \\
\mathcal{P}(p_5) &\Rightarrow b[0] = 1 \\
\mathcal{P}(p_6) &\Rightarrow b[0] = 1 \\
\mathcal{P}(p_7) &\Rightarrow b[0] = 1 \land b[1] = 0 \\
\mathcal{P}(p_8) &\Rightarrow b[0] = 1
\end{aligned}$$

$q$'s assertion network is:

$$\begin{aligned}
\mathcal{Q}(q_1) &\Rightarrow b[1] = 0 \\
\mathcal{Q}(q_2) &\Rightarrow b[1] = 0 \\
\mathcal{Q}(q_3) &\Rightarrow b[1] = 1 \\
\mathcal{Q}(q_4) &\Rightarrow b[0] = 1 \land b[1] = 1 \\
\mathcal{Q}(q_5) &\Rightarrow b[1] = 0 \\
\mathcal{Q}(q_6) &\Rightarrow b[0] = 0 \land b[1] = 0 \\
\mathcal{Q}(q_7) &\Rightarrow b[0] = 0 \land b[1] = 1 \\
\mathcal{Q}(q_8) &\Rightarrow b[1] = 1
\end{aligned}$$

## Inductivity

Now verify our assertion networks with our transitions by induction:

$$l_i \xrightarrow{g;\ f} l_j : \mathcal{A}(l_i) \land g \implies \mathcal{A}(l_j) \circ f$$

For $p$:

$$\begin{aligned}
\bullet \xrightarrow{\top;\ b[0]=0} p_1 : \quad \top &\implies b[0]=0 \circ b[0]=0 \\
\top &\implies b[0]=0 \to b[0]=0 \\
&\implies \top
\end{aligned}$$

$$\begin{aligned}
p_1 \xrightarrow{\top;\ I} p_2 : \quad b[0]=0 \land \top &\implies b[0]=0 \circ I \\
b[0]=0 &\implies b[0]=0 \\
&\implies \top
\end{aligned}$$

$$\begin{aligned}
p_2 \xrightarrow{\top;\ b[0]=1} p_3 : \quad b[0]=1 \land \top &\implies b[0]=1 \circ b[0]=1 \\
b[0]=1 &\implies b[0]=1 \to b[0]=1 \\
&\implies \top
\end{aligned}$$

$$\begin{aligned}
p_3 \xrightarrow{b[1]=1;\ I} p_4 : \quad b[0]=1 \land b[1]=1 &\implies (b[0]=1 \land b[1]=1) \circ I \\
b[0]=1 \land b[1]=1 &\implies b[0]=1 \land b[1]=1 \\
&\implies \top
\end{aligned}$$

$$\begin{aligned}
p_4 \xrightarrow{\top;\ b[0]=1} p_5 : \quad b[0]=1 \land b[1]=1 \land \top &\implies b[0]=1 \circ b[0]=1 \\
b[0]=1 \land b[1]=1 &\implies b[0]=1 \to b[0]=1 \\
&\implies \top
\end{aligned}$$

$$\begin{aligned}
p_5 \xrightarrow{b[0]=1;\ b[0]=1} p_6 : \quad b[0]=1 \land b[0]=1 &\implies b[0]=1 \circ b[0]=1 \\
b[0]=1 &\implies \top
\end{aligned}$$

$$\begin{aligned}
p_6 \xrightarrow{\top;\ b[0]=1} p_3 : \quad b[0]=1 \land \top &\implies b[0]=1 \circ b[0]=1 \\
b[0]=1 &\implies \top
\end{aligned}$$

$$\begin{aligned}
p_3 \xrightarrow{b[1]\neq 1;\ I} p_7 : \quad b[0]=1 \land b[1]\neq 1 &\implies (b[0]=1 \land b[1]=0) \circ I \\
b[0]=1 \land b[1]=0 &\implies b[0]=1 \land b[1]=0 \\
&\implies \top
\end{aligned}$$

$$\begin{aligned}
p_7 \xrightarrow{\top;\ I} p_8 : \quad b[0]=1 \land b[1]=0 \land \top &\implies b[0]=1 \circ I \\
b[0]=1 \land b[1]=0 &\implies b[0]=1 \\
&\implies \top
\end{aligned}$$

$$\begin{aligned}
p_8 \xrightarrow{\top;\ b[0]=0} p_1 : \quad b[0]=1 \land \top &\implies b[0]=0 \circ b[0]=0 \\
b[0]=1 &\implies \top
\end{aligned}$$

Therefore, $p$'s assertion network is inductive.

For $q$:

$$\bullet \xrightarrow{\top;\ b[1]=0} q_1 : \quad \begin{aligned} \top &\implies b[1]=0 \circ b[1]=0 \\ \top &\implies b[1]=0 \rightarrow b[1]=0 \\ &\implies \top \end{aligned}$$

$$q_1 \xrightarrow{\top;\ I} q_2 : \quad \begin{aligned} b[1]=0 \wedge \top &\implies b[1]=0 \circ I \\ b[0]=0 &\implies b[0]=0 \\ &\implies \top \end{aligned}$$

$$q_2 \xrightarrow{\top;\ b[1]=1} q_3 : \quad \begin{aligned} b[1]=0 \wedge \top &\implies b[1]=1 \circ b[1]=1 \\ b[1]=0 &\implies b[1]=1 \rightarrow b[1]=1 \\ &\implies \top \end{aligned}$$

$$q_3 \xrightarrow{b[0]=1;\ I} q_4 : \quad \begin{aligned} b[1]=1 \wedge b[0]=1 &\implies (b[0]=1 \wedge b[1]=1) \circ I \\ b[1]=1 \wedge b[0]=1 &\implies b[0]=1 \wedge b[1]=1 \\ &\implies \top \end{aligned}$$

$$q_4 \xrightarrow{\top;\ b[1]=0} q_5 : \quad \begin{aligned} b[0]=1 \wedge b[1]=1 \wedge \top &\implies b[1]=0 \circ b[0]=1 \\ b[0]=1 \wedge b[1]=1 &\implies b[0]=1 \rightarrow b[0]=1 \\ &\implies \top \end{aligned}$$

$$q_5 \xrightarrow{b[0]=0;\ b[0]=0} q_6 : \quad \begin{aligned} b[1]=0 \wedge b[0]=0 &\implies (b[0]=0 \wedge b[1]=0) \circ b[0]=0 \\ b[1]=0 \wedge b[0]=0 &\implies b[0]=0 \wedge b[1]=0 \\ &\implies \top \end{aligned}$$

$$q_6 \xrightarrow{\top;\ b[1]=1} q_3 : \quad \begin{aligned} b[0]=0 \wedge b[1]=0 \wedge \top &\implies b[1]=1 \circ b[1]=1 \\ b[0]=0 \wedge b[1]=0 &\implies b[1]=1 \rightarrow b[1]=1 \\ &\implies \top \end{aligned}$$

$$q_3 \xrightarrow{b[0]\neq 1;\ I} q_7 : \quad \begin{aligned} b[1]=1 \wedge b[0]\neq 1 &\implies (b[0]=0 \wedge b[1]=1) \circ I \\ b[1]=1 \wedge b[0]=0 &\implies b[0]=0 \wedge b[1]=1 \\ &\implies \top \end{aligned}$$

$$q_7 \xrightarrow{\top;\ I} q_8 : \quad \begin{aligned} b[0]=0 \wedge b[1]=1 \wedge \top &\implies b[1]=1 \circ I \\ b[0]=0 \wedge b[1]=1 &\implies b[1]=1 \\ &\implies \top \end{aligned}$$

$$q_8 \xrightarrow{\top;\ b[1]=0} q_1 : \quad \begin{aligned} b[1]=1 \wedge \top &\implies b[1]=0 \circ b[1]=0 \\ b[0]=1 &\implies \top \end{aligned}$$

Therefore, $q$'s assertion network is inductive.

### Interference

Trivially, there is no interference since $p$ does not modify $b[1]$ and $q$ does not modify $b[0]$.

### Mutual Exclusion

> *Might as well prove mutual exclusion.*

$$\begin{aligned} \mathcal{P}(p_7) \land \mathcal{Q}(q_7) &\iff (b[0] = 1 \land b[1] = 0) \land (b[0] = 0 \land b[1] = 1) \\ &\iff (b[0] = 0 \land b[0] = 1) \land (b[1] = 0 \land b[1] = 1) \\ &\iff \bot \land \bot \\ \therefore \mathcal{P}(p_7) \land \mathcal{Q}(q_7) &\iff \bot \end{aligned}$$

$p$ at $p_7$ and $q$ at $q_7$ are thus mutually exclusive.

## Part 3

Consider $p$'s transition diagram. It is clear to see that in the chain: $p_3 \to p_4 \to p_5 \to p_6 \to p_3$, there exists a superfluous transition of $b[0] = 1$ at each step. This chain can be simplified with an identity transition:

$$p_3 \xrightarrow{b[1]=1;\ I} p_4 \to p_5 \to p_6 \to p_3 \equiv p_3 \xrightarrow{b[1]=1;\ I} p_3$$

Furthermore, considering the assertions of the chain $p$:

$$\{\mathcal{P}(p_3), \mathcal{P}(p_4), \mathcal{P}(p_5), \mathcal{P}(p_6)\} \Rightarrow b[0] = 1$$

It is clear to see that the state of $b[0]$ does not change.

Therefore, $p$ is simplified as:

```
    loop forever
p1:     non-critical section
p2:     b[0] = 1
p3:     while b[1] == 1
p4:         skip
p7:     critical section
p8:     b[0] = 0
```

Program $q$ cannot be simplified further.