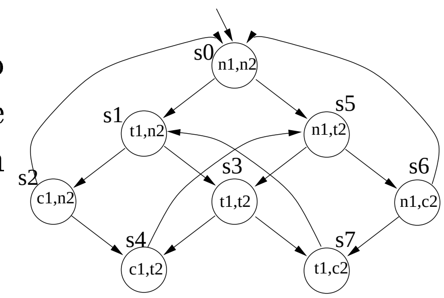
National University of Singapore
School of Computing
CS3234 — Logic and Formal Systems
Semester I, 2004/2005

Tutorial 6

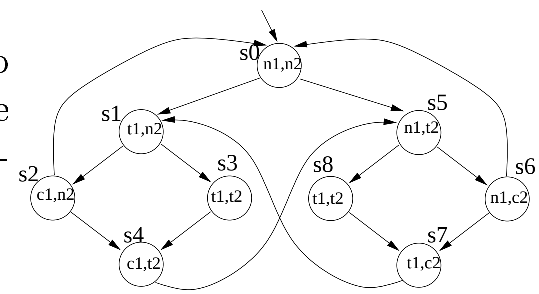
1. **Model checking, 1**:

   Apply the model checking algorithm to check properties ϕ_1, ϕ_2, ϕ_3, and ϕ_4 in the course notes on the first mutual exclusion model.



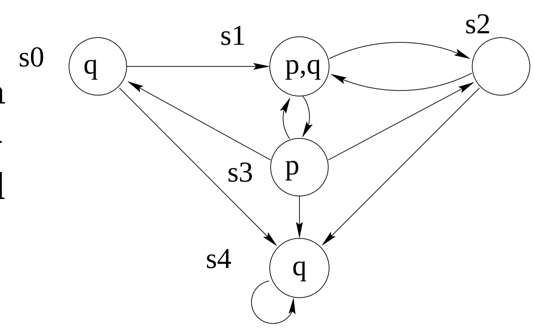
2. **Model checking, 2**:

   Apply the model checking algorithm to check properties ϕ_1, ϕ_2, ϕ_3, and ϕ_4 in the course notes on the second mutual exclusion model.



3. **Model checking, 3**:

   Apply the model checking algorithm to check the formula $\phi = \text{AG}(p \rightarrow \text{A}[p \text{ U } (\neg p \wedge \text{A}[\neg p \text{ U } q])])$ for the model described in the figure.



4. **From graphs to SMV**: Write an SMV program for the question in Exercise 3.

5. **From SMV to graphs**: Draw the state transition diagram associated to the following SMV program and check its CTL formula.

```
MODULE main
VAR
   bit0 :  counter_cell(1);
   bit1 :  counter_cell(bit0.carry_out);
```

```
SPEC
   AG AF bit1.carry_out

MODULE counter_cell(carry_in)
VAR
   value :  boolean;
   carry_out :  boolean;
ASSIGN
   init(value) := 0;
   next(value) := value + carry_in mod 2;
   carry_out := value & carry_in;
```

For questions 6-7: One can define fixed point operators on a (possibly infinite) tree as follows. By Z, Z', etc. we denote subsets of positions in the tree. Let $\mathcal{F}$ be a mapping $Z \mapsto \mathcal{F}(Z)$. $\mathcal{F}$ is *monotone* if $Z \subseteq Z'$ implies $\mathcal{F}(Z) \subseteq \mathcal{F}(Z')$; it is *continous* if $\mathcal{F}(\bigcup_i Z_i) = \bigcup_i \mathcal{F}(Z_i)$, for any increasing sequence $Z_0 \subseteq Z_1 \subseteq \ldots$. For such a monotone and continous $\mathcal{F}$ the increasing sequence

$$\emptyset \subseteq \mathcal{F}(\emptyset) \subseteq \mathcal{F}(\mathcal{F}(\emptyset)) \subseteq \ldots$$

define the *least fixed point* of $\mathcal{F}$

$$\mu Z.\mathcal{F}(Z) =_{def} \emptyset \cup \mathcal{F}(\emptyset) \cup \mathcal{F}(\mathcal{F}(\emptyset)) \cup \ldots$$

Similarly, for a monotone and continous $\mathcal{F}$ the decreasing sequence (T is the set of all positions in the tree)

$$T \supseteq \mathcal{F}(T) \supseteq \mathcal{F}(\mathcal{F}(T)) \supseteq \ldots$$

define the *greatest fixed point* of $\mathcal{F}$

$$\nu Z.\mathcal{F}(Z) =_{def} T \cap \mathcal{F}(T) \cap \mathcal{F}(\mathcal{F}(T)) \cap \ldots$$

6. **Minimal fixed point** ($\text{AF}\ \phi = \mu Z.\phi \vee \text{AX}\ Z$): Let Y be the positions in a tree where ϕ is true and $\mathcal{G}(Z) = \{p\colon p$ is a position in the tree and any next position of p is in $Z\}$. Show that $Z \mapsto Y \cup \mathcal{G}(Z)$ is monotone and continous and its minimal fixed point $\mu Z.Y \cup \mathcal{G}(Z)$ represents the set of positions in the tree where AF ϕ holds.

7. **Maximal fixed point** ($\text{AG}\ \phi = \nu Z.\phi \wedge \text{AX}\ Z$): Let Y and $\mathcal{G}(Z)$ be as before. Show that $Z \mapsto Y \cap \mathcal{G}(Z)$ is monotone and continous and its maximal fixed point $\nu Z.Y \cap \mathcal{G}(Z)$ represents the set of positions in the tree where AG ϕ holds.