# CS3234 - Tutorial 8, Solutions

## 1.

Applying the model checking algorithm to check properties of safety, liveness and non-strict sequencing for the first mutual exclusion model:

**(a)** $\phi_1 = \mathrm{AG}\ \neg(c_1 \wedge c_2)$

- $\mathrm{SAT}(\mathrm{AG}\ \neg(c_1 \wedge c_2))\ =$
  $=\ \mathrm{SAT}(\neg\ \mathrm{EF}\ \neg\ \neg(c_1 \wedge c_2))\ =$
  $=\ \mathrm{SAT}(\neg\ \mathrm{EF}\ (c_1 \wedge c_2))\ =$
  $=\ S\ -\ \mathrm{SAT}(\mathrm{EF}\ (c_1 \wedge c_2))\ =$
  $=\ S\ -\ \mathrm{SAT}(\mathrm{E}[\top\ \mathrm{U}\ (c_1 \wedge c_2)])$ relation (1)
- $\mathrm{SAT}(\mathrm{E}[\top\ \mathrm{U}\ (c_1 \wedge c_2)])\ =$
  $\mathrm{W} = \mathrm{SAT}(\top) = \mathrm{S}$
  $\mathrm{X} = \mathrm{S}$
  $\mathrm{Y} = \mathrm{SAT}(c_1 \wedge c_2) = \mathrm{SAT}(c_1) \cap \mathrm{SAT}(c_2) = \{s_2, s_4\} \cap \{s_7, s_6\} = \emptyset$
  step1 $\mathrm{X} = \mathrm{Y} = \emptyset$
  $\mathrm{Y} = \mathrm{Y} \cup (\mathrm{W} \cap \{s/\text{exists } s' \text{ such that } s \to s' \text{ and } s' \in \mathrm{Y}\})$
  $= \emptyset \cup (\mathrm{S} \cap \emptyset) = \emptyset$
  step2 STOP because $\mathrm{X} = \mathrm{Y} = \emptyset$
  So, $\mathrm{SAT}(\mathrm{E}[\top\ \mathrm{U}\ (c_1 \wedge c_2)])\ = \emptyset$
- coming back to relation (1), we get:
  $\mathrm{SAT}(\mathrm{AG}\ \neg(c_1 \wedge c_2))\ = \mathrm{S} \setminus \emptyset = \mathrm{S}.$

**(b)** $\phi_2 = \mathrm{AG}\ (t_1 \to \mathrm{AF}\ c_1)$

- $\mathrm{SAT}(\mathrm{AG}\ (t_1 \to \mathrm{AF}\ c_1))\ =$
  $=\ \mathrm{SAT}(\neg\mathrm{EF}\neg(t_1 \to \mathrm{AF}\ c_1))\ =$
  $=\ \mathrm{S}\ -\ \mathrm{SAT}(\mathrm{EF}\ \neg(t_1 \to \mathrm{AF}\ c_1))\ =$
  $=\ \mathrm{S}\ -\ \mathrm{SAT}(\mathrm{E}[\top\ \mathrm{U}\ (\neg(t_1 \to \mathrm{AF}\ c_1))])\ =$
  $=\ \mathrm{S}\ -\ \mathrm{SAT}_{\mathrm{EU}}(\top, \neg(t_1 \to \mathrm{AF}\ c_1))$ relation (1)
- $\mathrm{SAT}_{\mathrm{EU}}(\top, \neg(t_1 \to \mathrm{AF}\ c_1))\ =$
  $\mathrm{W} = \mathrm{SAT}(\top) = \mathrm{S}$
  $\mathrm{X} = \mathrm{S}$
  $\mathrm{Y} = \mathrm{SAT}(\neg(t_1 \to \mathrm{AF}\ c_1))\ =$
  $=\ \mathrm{S}\ -\ \mathrm{SAT}(t_1 \to \mathrm{AF}\ c_1)\ =$
  $=\ \mathrm{S}\ -\ \mathrm{SAT}(\neg t_1 \vee \mathrm{AF}\ c_1)\ =$
  $=\ \mathrm{S}\ -\ (\mathrm{SAT}(\neg t_1) \cup \mathrm{SAT}(\mathrm{AF}\ c_1))\ =$
  $=\ \mathrm{S}\ -\ ((\mathrm{S}\ -\ \mathrm{SAT}(t_1)) \cup \mathrm{SAT}_{\mathrm{AF}}(c_1))\ =$
  $=\ \mathrm{S}\ -\ ((\mathrm{S}\ -\ \{s_1, s_3, s_7\}) \cup \mathrm{SAT}_{\mathrm{AF}}(c_1))\ =$
  $=\ \mathrm{S}\ -\ (\{s_0, s_2, s_4, s_5, s_6\} \cup \mathrm{SAT}_{\mathrm{AF}}(c_1))\ =$
  relation (2)

- $\mathrm{SAT}_{\mathrm{AF}}(c_1)\ =$
  $\mathrm{X} = \mathrm{S}$
  $\mathrm{Y} = \mathrm{SAT}(c_1) = \{s_2, s_4\}$
  step1 $\mathrm{X} = \mathrm{Y} = \{s_2, s_4\}$
  $\quad\quad \mathrm{Y} = \mathrm{Y} \cup \{s/\text{for all } s' \text{ with } s \rightarrow s' \text{ we have } s' \in \mathrm{Y}\}\ =$
  $\quad\quad =\ \{s_2, s_4\} \cup \emptyset\ = \{s_2, s_4\}$
  step2 STOP because $\mathrm{X} = \mathrm{Y} = \{s_2, s_4\}$
  So, $\mathrm{SAT}_{\mathrm{AF}}(c_1) = \{s_2, s_4\}$

- coming back to relation (2), we have:
  $\mathrm{X} = \mathrm{S}$
  $\mathrm{Y} = \mathrm{S}\ - (\{s_0, s_2, s_4, s_5, s_6\}\ \cup\ \{s_2, s_4\}) = \mathrm{S}\ -\ \{s_0, s_2, s_4, s_5, s_6\} =$
  $= \{s_1, s_3, s_7\}$
  step1 $\mathrm{X} = \mathrm{Y} = \{s_1, s_3, s_7\}$
  $\quad\quad \mathrm{Y} =$
  $\quad\quad = \{s_1, s_3, s_7\}\ \cup\ (\mathrm{S} \cap \{s/ \text{ exists } s' \text{ such that } s \rightarrow s' \text{ and } s' \in \mathrm{Y}\} =$
  $\quad\quad = \{s_1, s_3, s_7\}\ \cup\ (\mathrm{S} \cap \{s_0, s_1, s_3, s_5, s_6, s_7\}) = \{s_0, s_1, s_3, s_5, s_6, s_7\}$
  step2 $\mathrm{X} = \mathrm{Y} = \{s_0, s_1, s_3, s_5, s_6, s_7\}$
  $\quad\quad \mathrm{Y} =$
  $\quad\quad = \{s_0, s_1, s_3, s_5, s_6, s_7\} \cup (\mathrm{S} \cap \{s/\text{exists } s' \text{ s.t. } s \rightarrow s' \text{ and } s' \in \mathrm{Y}\} =$
  $\quad\quad = \{s_0, s_1, s_3, s_5, s_6, s_7\}\ \cup\ (\mathrm{S} \cap \{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7\}) = \mathrm{S}$
  step3 $\mathrm{X} = \mathrm{Y} = \mathrm{S}$
  $\quad\quad \mathrm{Y} = \mathrm{S} \cup\ (\mathrm{S} \cap \{s/ \text{ exists } s' \text{ such that } s \rightarrow s' \text{ and } s' \in \mathrm{Y}\} = \mathrm{S}$
  step4 STOP because $\mathrm{X} = \mathrm{Y} = \mathrm{S}$
  So, $\mathrm{SAT}_{\mathrm{EU}}(\top, \neg(t_1 \rightarrow \mathrm{AF}\ c_1)) = \mathrm{S}$

- coming back to relation (1) we have:
  $\mathrm{SAT}\ \phi_2 = S\ -\ \mathrm{SAT}_{\mathrm{EU}}(\top, \neg(t_1 \rightarrow \mathrm{AF}\ c_1)) = \mathrm{S}\ -\ \mathrm{S} = \emptyset$
  $\mathrm{SAT}\ \phi_2 = \emptyset$

**(3)** $\phi_3 = \mathrm{AG}\ (n_1 \rightarrow \mathrm{EX}\ t_1)$

- $\mathrm{SAT}(\mathrm{AG}\ (n_1 \rightarrow \mathrm{EX}\ t_1))\ =$
  $=\ \mathrm{SAT}(\neg\mathrm{EF}\neg(n_1 \rightarrow \mathrm{EX}\ t_1))\ =$
  $=\ \mathrm{S}\ -\ \mathrm{SAT}(\mathrm{EF}\ \neg(n_1 \rightarrow \mathrm{EX}\ t_1))\ =$
  $=\ \mathrm{S}\ -\ \mathrm{SAT}(\mathrm{E}[\top\ \mathrm{U}\ (\neg(n_1 \rightarrow \mathrm{EX}\ t_1))])\ =$
  $=\ \mathrm{S}\ -\ \mathrm{SAT}_{\mathrm{EU}}(\top, \neg(n_1 \rightarrow \mathrm{EX}\ t_1))$ relation (1)

- $\mathrm{SAT}_{\mathrm{EU}}(\top, \neg(n_1 \rightarrow \mathrm{EX}\ t_1))\ =$
  $\mathrm{W} = \mathrm{SAT}(\top) = \mathrm{S}$
  $\mathrm{X} = \mathrm{S}$
  $\mathrm{Y} = \mathrm{SAT}(\neg(n_1 \rightarrow \mathrm{EX}\ t_1))\ =$
  $\quad =\ \mathrm{S}\ -\ \mathrm{SAT}(n_1 \rightarrow \mathrm{EX}\ t_1)\ =$
  $\quad =\ \mathrm{S}\ -\ \mathrm{SAT}(\neg n_1 \vee \mathrm{EX}\ t_1)\ =$
  $\quad =\ \mathrm{S}\ -\ (\mathrm{SAT}(\neg n_1) \cup \mathrm{SAT}(\mathrm{EX}\ t_1))\ =$
  $\quad =\ \mathrm{S}\ -\ ((\mathrm{S}\ -\ \mathrm{SAT}(n_1)) \cup \mathrm{SAT}_{\mathrm{EX}}(t_1))\ =$

$= \text{S} - ((\text{S} - \{s_0, s_5, s_6\}) \cup \text{SAT}_{\text{EX}}(t_1)) =$
$= \text{S} - (\{s_1, s_2, s_3, s_4, s_7\} \cup \text{SAT}_{\text{EX}}(t_1))$ relation (2)

- $\text{SAT}_{\text{EX}}(t_1) =$
  $\text{X} = \text{SAT}(t_1) = \{s_1, s_3, s_7\}$
  $\text{Y} = \{s \in \text{S}/\ s \to s'$ for some $s' \in \text{X}\} =$
  $= \{s_0, s_1, s_3, s_5, s_6, s_7\}$
  So, $\text{SAT}_{\text{EX}}(t_1) = \{s_0, s_1, s_3, s_5, s_6, s_7\}$

- coming back to relation (2), we have:
  $\text{X} = \text{S}$
  $\text{Y} = \text{S} - (\{s_0, s_2, s_4, s_5, s_6\} \cup \{s_0, s_1, s_3, s_5, s_6, s_7\})$
  $= \text{S} - \{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7\} = \emptyset$
  step1 $\text{X} = \text{Y} = \emptyset$
  $\text{Y} =$
  $= \emptyset \cup (\text{S} \cap \{s/$ exists $s'$ such that $s \to s'$ and $s' \in \text{Y}\} =$
  $= \emptyset \cup (\text{S} \cap \emptyset) = \emptyset$
  step2 STOP because $\text{X} = \text{Y} = \emptyset$
  So, $\text{SAT}_{\text{EU}}(\top, \neg(n_1 \to \text{EX}\ t_1)) = \emptyset$

- coming back to relation (1) we have:
  $\text{SAT}\ \phi_3 = S - \text{SAT}_{\text{EU}}(\top, \neg(n_1 \to \text{EX}\ t_1)) = \text{S} - \emptyset = \text{S}$
  $\text{SAT}\ \phi_3 = \text{S}$

**(4)** $\phi_4 = \text{EF}\ (c_1 \wedge \text{E}[c_1\ \text{U}\ (\neg c_1 \wedge \text{E}[\neg c_2\ \text{U}\ c_1])]) = \text{EF}\ \psi$

- $\text{SAT}\phi_4 =$
  $= \text{SAT}(\text{E}[\top\ \text{U}\ \psi]) =$
  $= \text{SAT}_{\text{EU}}(\top, \psi)$
  $\text{W} = \text{SAT}(\top) = \text{S}$
  $\text{X} = \text{S}$
  $\text{Y} = \text{SAT}(c_1 \wedge \text{E}[c_1\ \text{U}\ (\neg c_1 \wedge \text{E}[\neg c_2\ \text{U}\ c_1])]) =$
  $= \text{SAT}(c_1) \cap \text{SAT}(\text{E}[c_1\ \text{U}\ (\neg c_1 \wedge \text{E}[\neg c_2\ \text{U}\ c_1])]) =$
  $= \{s_2, s_4\} \cap \text{SAT}(\text{E}[c_1\ \text{U}\ (\neg c_1 \wedge \text{E}[\neg c_2\ \text{U}\ c_1])]) =$
  $= \{s_2, s_4\} \cap \text{SAT}_{\text{EU}}(c_1, (\neg c_1 \wedge \text{E}[\neg c_2\ \text{U}\ c_1]))$ relation (1)

- $\text{SAT}_{\text{EU}}(c_1, (\neg c_1 \wedge \text{E}[\neg c_2\ \text{U}\ c_1])) =$
  $\text{W} = \text{SAT}(c_1) = \{s_2, s_4\}$
  $\text{X} = \text{S}$
  $\text{Y} = \text{SAT}(\neg c_1 \wedge \text{E}[\neg c_2\ \text{U}\ c_1]) =$
  $= \text{SAT}(\neg c_1) \cap \text{SAT}(\text{E}[\neg c_2\ \text{U}\ c_1]) =$
  $= (\text{S} - \text{SAT}(c_1)) \cap \text{SAT}(\text{E}[\neg c_2\ \text{U}\ c_1]) =$
  $= \{s_0, s_1, s_3, s_5, s_6, s_7\} \cap \text{SAT}(\text{E}[\neg c_2\ \text{U}\ c_1]) =$
  $= \{s_0, s_1, s_3, s_5, s_6, s_7\} \cap \text{SAT}_{\text{EU}}(\neg c_2, c_1)$ relation (2)

- $\text{SAT}_{\text{EU}}(\neg c_2, c_1) =$
  $\text{W} = \text{SAT}(\neg c_2) = \text{S} - \text{SAT}(c_2) = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
  $\text{X} = \text{S}$

$\mathrm{Y} = \mathrm{SAT}(c_1) = \{s_2, s_4\}$
step1 $\mathrm{X} = \mathrm{Y} = \{s_2, s_4\}$
$\quad\mathrm{Y} = \mathrm{Y} \cup (\{s_0, s_1, s_2, s_3, s_4, s_5\} \cap \{s_1, s_2, s_3\})$
$\quad= \{s_2, s_4\} \cup \{s_1, s_2, s_3\} = \{s_1, s_2, s_3, s_4\}$
step2 $\mathrm{X} = \mathrm{Y} = \{s_1, s_2, s_3, s_4\}$
$\quad\mathrm{Y} = \mathrm{Y} \cup (\{s_0, s_1, s_2, s_3, s_4, s_5\} \cap \{s_0, s_1, s_2, s_3, s_5, s_7\}) =$
$\quad= \{s_1, s_2, s_3, s_4\} \cup \{s_0, s_1, s_2, s_3, s_5\} =$
$\quad= \{s_0, s_1, s_2, s_3, s_4, s_5\}$
step3 $\mathrm{X} = \mathrm{Y} = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
$\quad\mathrm{Y} = \{s_0, s_1, s_2, s_3, s_4, s_5\} \cup \{s_0, s_1, s_2, s_3, s_4, s_5\} =$
$\quad= \{s_0, s_1, s_2, s_3, s_4, s_5\}$
step4 STOP because $\mathrm{X} = \mathrm{Y} = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
So, $\mathrm{SAT}_{\mathrm{EU}}(\neg c_2, c_1) = \{s_0, s_1, s_2, s_3, s_4, s_5\}$

- coming back to relation (2), we have:
  $\mathrm{W} = \{s_2, s_4\}$
  $\mathrm{X} = \mathrm{S}$
  $\mathrm{Y} = \{s_0, s_1, s_3, s_5, s_6, s_7\} \cap \{s_0, s_1, s_2, s_3, s_4, s_5\} =$
  $\quad= \{s_0, s_1, s_3, s_5\}$
  step1 $\mathrm{X} = \mathrm{Y} = \{s_0, s_1, s_3, s_5\}$
  $\quad\mathrm{Y} = \{s_0, s_1, s_3, s_5\} \cup (\{s_2, s_4\} \cap \{s_0, s_1, s_2, s_4, s_5, s_6, s_7\}) =$
  $\quad= \{s_0, s_1, s_3, s_5\} \cup \{s_2, s_4\} =$
  $\quad= \{s_0, s_1, s_2, s_3, s_4, s_5\}$
  step2 $\mathrm{X} = \mathrm{Y} = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
  $\quad\mathrm{Y} = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
  step3 STOP because $\mathrm{X} = \mathrm{Y} = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
  So, $\mathrm{SAT}_{\mathrm{EU}}(c_1, (\neg c_1 \land \mathrm{E}[\neg c_2 \mathrm{\ U\ } c_1])) = \{s_0, s_1, s_2, s_3, s_4, s_5\}$

- coming back at relation (1). we get:
  $\mathrm{SAT}\phi_4 =$
  $\mathrm{W} = \mathrm{SAT}(\top) = \mathrm{S}$
  $\mathrm{X} = \mathrm{S}$
  $\mathrm{Y} = \{s_2, s_4\} \cap \mathrm{SAT}_{\mathrm{EU}}(c_1, (\neg c_1 \land \mathrm{E}[\neg c_2 \mathrm{\ U\ } c_1])) =$
  $\quad= \{s_2, s_4\} \cap \{s_0, s_1, s_2, s_3, s_4, s_5\}$
  $\quad= \{s_2, s_4\}$
  step1 $\mathrm{X} = \mathrm{Y} = \{s_2, s_4\}$
  $\quad\mathrm{Y} = \mathrm{Y} \cup (\mathrm{S} \cap \{s_1, s_2, s_3\}) =$
  $\quad= \{s_2, s_4\} \cup \{s_1, s_2, s_3\} =$
  $\quad= \{s_1, s_2, s_3, s_4\}$
  step2 $\mathrm{X} = \mathrm{Y} = \{s_1, s_2, s_3, s_4\}$
  $\quad\mathrm{Y} = \{s_1, s_2, s_3, s_4\} \cup (S \cap \{s_0, s_1, s_2, s_3, s_5, s_7\}) =$
  $\quad= \{s_1, s_2, s_3, s_4\} \cup \{s_0, s_1, s_2, s_3, s_5, s_7\} =$
  $\quad= \{s_0, s_1, s_2, s_3, s_4, s_5, s_7\}$
  step3 $\mathrm{X} = \mathrm{Y} = \{s_0, s_1, s_2, s_3, s_4, s_5, s_7\}$
  $\quad\mathrm{Y} = \{s_0, s_1, s_2, s_3, s_4, s_5, s_7\} \cup (S \cap \{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7\} =$

$= \{s_0, s_1, s_2, s_3, s_4, s_5, s_7\} \cup S =$
$= \text{S}$
step4 $\text{X} = \text{Y} = \text{S}$
$\text{Y} = \text{S} \cup (\text{S} \cap \text{S}) = \text{S}$
step5 STOP because $\text{X} = \text{Y} = \text{S}$
So, $\text{SAT}\phi_4 = \text{S}$

**2.** and **3.**

Similar reasoning to the first exercise.

**4.**

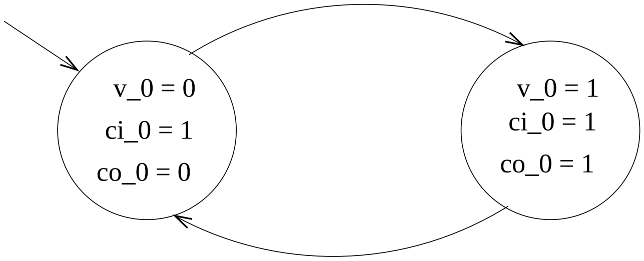
```
MODULE main
VAR
   p : boolean;
   q : boolean;
   state : {s0, s1, s2, s3, s4};
ASSIGN
   p := case
        (state = s0) : 0;
        (state = s1) : 1;
        (state = s2) : 0;
        (state = s3) : 1;
        (state = s4) : 0;
        1 : {0, 1};
        esac;
   q : = case
        (state = s0) : 1;
        (state = s1) : 1;
        (state = s2) : 0;
        (state = s3) : 0;
        (state = s4) : 1;
        1 : {0, 1};
        esac;
   init(state) := s0;
   next(state) := case
                  (state = s0) : {s1, s4};
                  (state = s1) : {s2, s3};
                  (state = s2) : {s1, s4};
                  (state = s3) : {s0, s1, s2, s4};
                  (state = s4) : s4;
                  1 : {s0, s1, s2, s3, s4};
  esac;

SPEC
```

```
AG (p -> A [p U (!p & A [!p U q])])
```

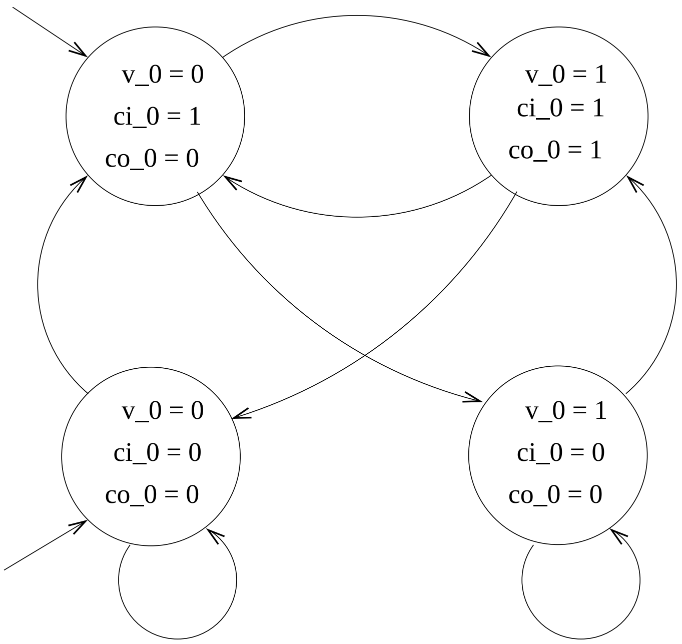
You may change the initial state to be one of s1, s2, s3, s4 to establish its truth value for the given model and chosen initial state.

## 5.

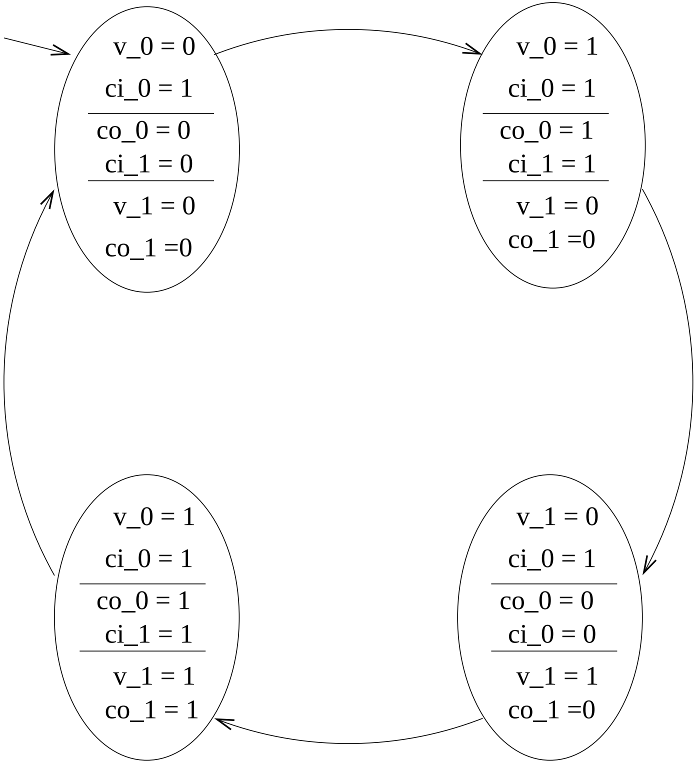
- If we analyze the SMV program, we notice that there are two instances of the same process, `counter_cell`, expressing the behavior of `bit0` and `bit1`. Thus, we would have two models (automaton), each for one bit (`bit0`, `bit1`).When building the models, we need to extract information about the states, transitions and the labeling function (values of variables in each state). Noting that:
  - for both models corresponding to `bit0` and `bit1`, there are three variables (`value, carry_in, carry_out`).
  - the `carry_in` value for the `bit0` model is always 1, thus the model has only two states (depending if `value` is 0 or 1). (`carry_out` is calculated from values of `value` and `carry_in`).
  - the model for `bit1` has 4 states, since in this case `carry_in` is not anymore a constant.
  - with `v_0, ci_0, co_0` we denote `value, carry_in, carry_out` for `bit0` and with `v_1, ci_1, co_1` we denote `value, carry_in, carry_out` for `bit1`.
- For `bit0` we have the model:



- For `bit1` we have the model:



- Combining both models, synchronously, we get:



## 6.

We have to prove:

$$\mathrm{AF}\,\phi \;=\; \mu Z.\phi \vee \mathrm{AX}\,Z$$

where:

$Y \;=\; \{\; p/\; p \in \mathrm{T},\; p \models \phi \;\}$

$\mathcal{G}(Z) \;=\; \{\; p/\; p \in \mathrm{T},\; (\text{for all } s,\; p \to s,\; s \in Z) \;\}$

Let us denote $\mathcal{F} \;:\; 2^{\mathrm{T}} \;\longrightarrow\; 2^{\mathrm{T}}$ such that:

$$\mathcal{F}(Z) \;=\; Y \;\cup\; \mathcal{G}(Z)$$

We have to prove that:

**(1)** $\mathcal{F}$ is monotonic

**(2)** $\mathcal{F}$ is continuous

**(3)** the least fixed point of $\mathcal{F}$ is the set of positions in the tree T where the formula AF $\phi$ is true.

**(1)** $\mathcal{F}$ is monotonic

Let us take $Z_1,\; Z_2 \;\in\; 2^{\mathrm{T}}$ two sets of positions in T, such that

$$Z_1 \subseteq Z_2$$

**(a)** We prove first that $\mathcal{G}(Z_1) \;\subseteq\; \mathcal{G}(Z_2)$

Let us take $p \;\in\; \mathcal{G}(Z_1)$

**iff** $p \in \mathrm{T},\; (\text{for all } s,\; p \to s,\; s \in Z_1)$

**since** $Z_1 \subseteq Z_2$

**then** $p \in \mathrm{T},\; (\text{for all } s,\; p \to s,\; s \in Z_2)$

**iff** $p \;\in\; \mathcal{G}(Z_2)$

So, if $p \;\in \mathcal{G}(Z_1)$ then $p \;\in \mathcal{G}(Z_2)$.
That is $\mathcal{G}(Z_1) \;\subseteq\; \mathcal{G}(Z_2)$.

Now we have:

$\mathcal{F}(Z_1) \;=\; Y \;\cup\; \mathrm{G}(Z_1) \;\subseteq\; Y \;\cup\; \mathrm{G}(Z_2) \;=\; \mathcal{F}(Z_2)$
(since if $Z_1 \subseteq Z_2$ then $\mathcal{G}(Z_1) \;\subseteq\; \mathcal{G}(Z_2)$, so $Y \cup \mathcal{G}(Z_1) \;\subseteq\; Y \cup \mathcal{G}(Z_2)$)

Hence, $\mathcal{F}(Z_1) \;\subseteq\; \mathcal{F}(Z_2)$, so $\mathcal{F}$ is monotone.

**(2)** $\mathcal{F}$ is continuous.

Let us take an increasing sequence $Z_0 \;\subseteq\; Z_1 \;\subseteq\; \ldots$

We prove first that $\mathcal{G}(\cup_i Z_i) = \cup_i \mathcal{G}(Z_i)$

Let us take $p \in \mathcal{G}(\cup_i Z_i)$

**iff** $p \in \mathrm{T}$ and for all $s,\ p \to s,\ s \in \cup_i Z_i$

**iff** $p \in \mathrm{T}$ and for all $s,\ p \to s$, exists $i_s$ such that $s \in Z_{i_s}$

**let us** take $i_p = \max_{p \to s} i_s$. Since $Z_0 \subseteq Z_1 \subseteq \ldots$, then for all $s,\ p \to s$, we have $s \in Z_{i_s} \subseteq Z_{i_p}$ (because $i_s \leq i_p$, so $Z_{i_s} \subseteq Z_{i_p}$).

**then** $p \in \mathrm{T}$ and for all $s,\ p \to s$, exists $i_p$ such that $s \in Z_{i_p}$

**then** exists $i_p \in \mathbb{N}$ such that $p \in \mathcal{G}(Z_{i_p})$

**iff** $p \in \cup_i \mathcal{G}(Z_i)$

So, we have $\mathcal{G}(\cup_i Z_i) \subseteq \cup_i \mathcal{G}(Z_i)$.

The other inclusion is proved based on the property **(a)** from previous point:

Since for all $i \in \mathbb{N}$ we have $Z_i \subseteq \cup_i Z_i$ then, for all $i \in \mathbb{N}$ we have $\mathcal{G}(Z_i) \subseteq \mathcal{G}(\cup_i Z_i)$.

Hence $\cup_i \mathcal{G}(Z_i) \subseteq \mathcal{G}(\cup_i Z_i)$.

Finally, we can conclude that $\mathcal{G}(\cup_i Z_i) = \cup_i \mathcal{G}(Z_i)$.

Now, the proof for $\mathcal{F}$ continuous is obvious:

$$\cup_i \mathcal{F}(Z_i) = \cup_i (Y \cup \mathcal{G}(Z_i)) = (Y \cup \mathcal{G}(Z_0)) \cup (Y \cup \mathcal{G}(Z_1)) \cup \ldots = Y \cup (\mathcal{G}(Z_0) \cup \mathcal{G}(Z_1) \cup \ldots) = Y \cup (\cup_i \mathcal{G}(Z_i)) = Y \cup \mathcal{G}(\cup_i Z_i) = \mathcal{F}(\cup_i Z_i)$$

Hence. $\mathcal{F}$ is also continuous.

From **(1)** and **(2)** we deduce that $\mathcal{F}$ has a least fixed point.

**(3)** We denote by

$$\mathcal{S}_{\mathrm{AF}\ \phi} = \{p /\ p \in \mathrm{T},\ p \models \mathrm{AF}\ \phi\}$$

(the set of positions in T where AF $\phi$ holds).

**(3.1)** First we show that $\mathcal{S}_{\mathrm{AF}\ \phi}$ is a fixed point of $\mathcal{F}$. That is we have to prove that

$$\mathcal{F}(\mathcal{S}_{\mathrm{AF}\ \phi}) = \mathcal{S}_{\mathrm{AF}\ \phi}$$

”$\subseteq$” Let us take $p \in \mathcal{F}(\mathcal{S}_{\mathrm{AF}\ \phi})$

that is $p \in Y \cup \mathcal{G}(\mathcal{S}_{\mathrm{AF}\ \phi})$.

**if** $p \in Y$ **then** $p \in \mathrm{T}$ and $p \models \phi$, **then** $p \models \mathrm{AF}\ \phi$, **then** $p \in \mathcal{S}_{\mathrm{AF}\ \phi}$

**if** $p \in \mathcal{G}(\mathcal{S}_{\mathrm{AF}\ \phi})$
**then** $p \in \mathrm{T}$, and for all $s,\ p \to s$, we have $s \in \mathcal{S}_{\mathrm{AF}\ \phi}$
**then** $p \in \mathrm{T}$, and for all $s,\ p \to s,\ s \models \mathrm{AF}\ \phi$
**then** $p \in \mathrm{T}$, and for all $s_0^k,\ p \to s_0^k$, and for any path $s_0^k \to s_1^k \to s_2^k \to \ldots$

exists $i(k) \in \mathbb{N}$ such that $s^k_{i(k)} \models \phi$
**then** $p \in$ T, and for all paths $p \to s^k_0 \to s^k_1 \to s^k_2 \to \ldots$ exists $i(k) \in \mathbb{N}$ such that $s^k_{i(k)} \models \phi$
**then** $p \in$ T and $p \models$ AF $\phi$, **so** $p \in \mathcal{S}_{\text{AF } \phi}$.

Hence $\mathcal{F}(\mathcal{S}_{\text{AF } \phi}) \subseteq \mathcal{S}_{\text{AF } \phi}$

"$\supseteq$" Let us take $p \in \mathcal{S}_{\text{AF } \phi}$

that is $p \in$ T and for any path $p \to s_0 \to s_1 \to \ldots$ exists $i \in \mathbb{N}$ such that $s_i \models \phi$, or $p \models \phi$.

**if** $p \models \phi$ **then** $p \in Y$

**else** for all $s_0,\ p \to s_0$, and for all paths $s_0 \to s_1 \to \ldots$ exists $i \in \mathbb{N}$, such that $s_i \models \phi$
**then** for all $s_0,\ p \to s_0$, $s_0 \models$ AF $\phi$
**that is** for all $s_0,\ p \to s_0$, $s_0 \in \mathcal{S}_{\text{AF } \phi}$
**then** $p \in \mathcal{G}(\mathcal{S}_{\text{AF } \phi})$.

Hence $\mathcal{S}_{\text{AF } \phi} \subseteq \mathcal{F}(\mathcal{S}_{\text{AF } \phi})$

In conclusion, $\mathcal{S}_{\text{AF } \phi} = \mathcal{F}(\mathcal{S}_{\text{AF } \phi})$, so $\mathcal{S}_{\text{AF } \phi}$ is a fixed point for $\mathcal{F}$

**(3.2)** We prove that $\mathcal{S}_{\text{AF } \phi} \subseteq \mu Z.\ \mathcal{F}(Z)$.

Let us analyze first $\mu Z.\ \mathcal{F}(Z)$:

$\mu Z.\ \mathcal{F}(Z) = \mu Z.\, Y \cup \mathcal{G}(Z) = \emptyset \cup (Y \cup \mathcal{G}(\emptyset)) \cup (Y \cup \mathcal{G}(Y \cup \mathcal{G}(\emptyset))) \cup \ldots = Y \cup \mathcal{G}(\emptyset) \cup \mathcal{G}(Y \cup \mathcal{G}(\emptyset)) \cup \ldots$

where:
$Y = \{p/\ p \in \text{T},\ p \models \phi\}$
$\mathcal{G}(\emptyset) = \{p/\ p \in \text{T and for all } s,\ p \to s,\ s \in \emptyset\} = \emptyset$
( because $s \in \emptyset$ is false, so the entire conjunction inside curly brackets is false, hence $\mathcal{G}(\emptyset)$ has no element )

Hence $\mathcal{F}(\emptyset) = Y \cup \mathcal{G}(\emptyset) = Y = \{p/\ p \in \text{T},\ p \models \phi\}$

$\mathcal{G}(Y \cup \mathcal{G}(\emptyset)) = \{p/\ p \in \text{T, for all } s,\ p \to s,\ s \in Y \cup \mathcal{G}(\emptyset)\} =$
$\{p/\ p \in \text{T, for all } s,\ p \to s,\ s \in Y\ \} = \{p/\ p \in \text{T, for all } s,\ p \to s,\ s \models \phi\ \}$

Hence $\mathcal{F}^2(\emptyset) = Y \cup \mathcal{G}(Y \cup \mathcal{G}(\emptyset)) =$
$\{p/\ p \in \text{T},\ p \models \phi\} \cup \{p/\ p \in \text{T, for all } s,\ p \to s,\ s \models \phi\ \} =$
$\{p/\ p \in \text{T, for all } s,\ p \to s,\ (p \models \phi \text{ or } s \models \phi)\ \}$

$\mathcal{G}(Y \cup \mathcal{G}(Y \cup \mathcal{G}(\emptyset))) =$
$\{p/\ p \in \text{T, for all } s_0,\ p \to s_0,\ s_0 \in Y \cup \mathcal{G}(Y \cup \mathcal{G}(\emptyset))\} =$
$\{p/\ p \in \text{T, for all } s_0,\ p \to s_0,\ (s_0 \in Y \text{ or } s_0 \in \mathcal{G}(Y \cup \mathcal{G}(\emptyset)))\} =$
$\{p/\ p \in \text{T, for all } s_0,\ p \to s_0,\ (s_0 \models \phi \text{ or for all } s_1,\ s_0 \to s_1,\ s_1 \in Y)\} =$

$\{p/\ p \in \mathrm{T},\ \text{for all } s_0,\ p \rightarrow s_0,\ (s_0 \models \phi \text{ or for all } s_1,\ s_0 \rightarrow s_1,\ s_1 \models \phi)\} =$
$\{p/\ p \in \mathrm{T},\ \text{for all } s_0,\ s_1,\ p \rightarrow s_0 \rightarrow s_1,\ (s_0 \models \phi \text{ or } s_1 \models \phi)\}$

Hence $\mathcal{F}^3(\emptyset) = Y \cup \mathcal{G}(Y \cup \mathcal{G}(Y \cup \mathcal{G}(\emptyset))) = \{p/\ p \in \mathrm{T},\ p \models \phi\} \cup$
$\cup \{p/\ p \in \mathrm{T},\ \text{for all } s_0,\ s_1,\ p \rightarrow s_0 \rightarrow s_1,\ (s_0 \models \phi \text{ or } s_1 \models \phi)\} =$
$\{p/\ p \in \mathrm{T},\ \text{for all } s_0,\ s_1,\ p \rightarrow s_0 \rightarrow s_1,\ (p \models \phi \text{ or } s_0 \models \phi \text{ or } s_1 \models \phi)\}$

. . .

By mathematical induction, we see that for all $n \in \mathbb{N}$ we have:
$\mathcal{F}^{n+2}(\emptyset) =$
$\{p/p \in \mathrm{T}, \text{for all} s_0 \ldots s_n,\ p \rightarrow s_0 \rightarrow \ldots \rightarrow s_n,\ (p \models \phi \text{ or } s_0 \models \phi \text{ or} \ldots s_n \models \phi)\}$

Let us consider $p \in \mathcal{S}_{\mathrm{AF}\ \phi}$

**then** $p \in \mathrm{T}$ and $p \models \mathrm{AF}\ \phi$

**then** $p \in \mathrm{T}$ and for all paths $p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots$ we have ( $p \models \phi$ **or**
exists $i_{(p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots)} \in \mathbb{N}$ such that $s_{i(p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots)} \models \phi$)

let us consider a path $p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots$
**if** $p \models \phi$ **then** $p \in Y$,**so** $p \in \mathcal{F}(\emptyset)$
**else** (i.e. exists $i_{(p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots)} \in \mathbb{N}$ such that $s_{i(p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots)} \models \phi$)
we have $p \in \mathcal{F}^{i(p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots)\ +\ 2}$

**then** $p \in \mathrm{T}$ and for all paths $p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots$ we have ( $p \in \mathcal{F}(\emptyset)$ **or**
exists $i_{(p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots)} \in \mathbb{N}$ such that $p \in \mathcal{F}^{i(p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots)\ +\ 2}$)

**then** $p \in \mathrm{T}$ and for all paths $p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots$ we have $p \in \mu Z.\ \mathcal{F}(Z)$ **or**
(because $\mathcal{F}(\emptyset) \subseteq \mu Z.\ \mathcal{F}(Z)$ and $\mathcal{F}^{i(p \rightarrow s_0 \rightarrow s_1 \rightarrow \ldots)\ +\ 2} \subseteq \mu Z.\ \mathcal{F}(Z)$)

**then** $p \in \mu Z.\ \mathcal{F}(Z)$

So, we proved that $\mathcal{S}_{\mathrm{AF}\ \phi} \subseteq \mu Z.\ \mathcal{F}(Z)$

Since $\mathcal{S}_{\mathrm{AF}\ \phi}$ is a fixed point of $\mathcal{F}$ then we have that $\mu Z.\ \mathcal{F}(Z) \subseteq \mathcal{S}_{\mathrm{AF}\ \phi}$ (least fixed point is a subset of any other fixed point)

From the last two inclusions we conclude that $\mu Z.\ \mathcal{F}(Z) = \mathcal{S}_{\mathrm{AF}\ \phi}$

## 7.

We have to prove:

$$\mathrm{AG}\,\phi \;=\; \nu\, Z.\phi \wedge \mathrm{AX}\, Z$$

where:

$Y \;=\; \{\; p/\; p \in \mathrm{T},\; p \models \phi \;\}$

$\mathcal{G}(Z) \;=\; \{\; p/\; p \in \mathrm{T},\; (\text{for all } s,\; p \rightarrow s,\; s \in Z) \;\}$

Let us denote $\mathcal{F} \;:\; 2^{\mathrm{T}} \;\longrightarrow\; 2^{\mathrm{T}}$ such that:

$$\mathcal{F}(Z) \;=\; Y \;\cap\; \mathcal{G}(Z)$$

We have to prove that:

- **(1)** $\mathcal{F}$ is monotonic
- **(2)** $\mathcal{F}$ is continuous
- **(3)** the least fixed point of $\mathcal{F}$ is the set of positions in the tree T where the formula AG $\phi$ is true.

**(1)** $\mathcal{F}$ is monotonic

Let us take $Z_1,\; Z_2 \;\in\; 2^{\mathrm{T}}$ two sets of positions in T, such that

$$Z_1 \subseteq Z_2$$

We proved at **6.(1).(a)** that $\mathcal{G}(Z_1) \;\subseteq\; \mathcal{G}(Z_2)$

So we have:

$\mathcal{F}(Z_1) \;=\; Y \;\cap\; \mathrm{G}(Z_1) \;\subseteq\; Y \;\cap\; \mathrm{G}(Z_2) \;=\; \mathcal{F}(Z_2)$
(since if $Z_1 \subseteq Z_2$ then $\mathcal{G}(Z_1) \;\subseteq\; \mathcal{G}(Z_2)$, so $Y \cap \mathcal{G}(Z_1) \;\subseteq\; Y \cap \mathcal{G}(Z_2)$)

Hence, $\mathcal{F}(Z_1) \;\subseteq\; \mathcal{F}(Z_2)$, so $\mathcal{F}$ is monotone.

**(2)** $\mathcal{F}$ is continuous.

Let us take an increasing sequence $Z_0 \;\subseteq\; Z_1 \;\subseteq\; \ldots$

We proved at **6.(2)** that $\mathcal{G}(\cup_i\, Z_i) \;=\; \cup_i\; \mathcal{G}(Z_i)$

Now, the proof for $\mathcal{F}$ continuous:

$\cup_i\; \mathcal{F}(Z_i) \;=\; \cup_i\; (Y \cap \mathcal{G}(Z_i)) \;=\; (Y \cap \mathcal{G}(Z_0)) \;\cup\; (Y \cap \mathcal{G}(Z_1)) \;\cup\; \ldots \;=$
$Y \;\cap\; (\mathcal{G}(Z_0) \cup \mathcal{G}(Z_1) \cup \ldots) \;=\; Y \;\cap\; (\cup_i\; \mathcal{G}(Z_i)) \;=\; Y \;\cap\; \mathcal{G}(\cup_i Z_i) \;=\; \mathcal{F}(\cup_i Z_i)$

Hence. $\mathcal{F}$ is also continuous.

From **(1)** and **(2)** we deduce that $\mathcal{F}$ has a greatest fixed point.

**(3)** We denote by

$$\mathcal{S}_{\mathrm{AG}\ \phi} = \{p /\ p \in \mathrm{T},\ p \models \mathrm{AG}\ \phi\}$$

(the set of positions in T where AG $\phi$ holds).

**(3.1)** First we show that $\mathcal{S}_{\mathrm{AG}\ \phi}$ is a fixed point of $\mathcal{F}$. That is we have to prove that

$$\mathcal{F}(\mathcal{S}_{\mathrm{AG}\ \phi}) = \mathcal{S}_{\mathrm{AG}\ \phi}$$

Let us take $p \in \mathcal{F}(\mathcal{S}_{\mathrm{AG}\ \phi})$

that is $p \in Y \cap \mathcal{G}(\mathcal{S}_{\mathrm{AG}\ \phi})$

**iff** $p \in Y$ and $p \in \mathcal{G}(\mathcal{S}_{\mathrm{AG}\ \phi})$

**iff** $p \in \mathrm{T},\ p \models \phi$ and for all $s,\ p \to s,\ s \models \mathrm{AG}\ \phi$

**iff** $p \in \mathrm{T},\ p \models \phi$ and for all $s,\ p \to s$, for all paths $s \to s_1 \to \ldots$ we have $s \models \phi$ and for all $i \in \mathbb{N}^+$, $s_i \models \phi$

**iff** $p \in \mathrm{T}$ and for all paths $p \to s \to s_1 \to \ldots$ we have $p \models \phi,\ s \models \phi,\ s_1 \models \phi,\ \ldots$

**iff** $p \in \mathrm{T}$ and $p \models \mathrm{AG}\ \phi$

In conclusion, $\mathcal{S}_{\mathrm{AG}\ \phi} = \mathcal{F}(\mathcal{S}_{\mathrm{AG}\ \phi})$, so $\mathcal{S}_{\mathrm{AG}\ \phi}$ is a fixed point for $\mathcal{F}$

**(3.2)** We prove that $\nu\, Z.\ \mathcal{F}(Z) \subseteq \mathcal{S}_{\mathrm{AG}\ \phi}$.

Let us analyze first $\nu\, Z.\ \mathcal{F}(Z)$:

$\nu\, Z.\ \mathcal{F}(Z) = \nu\, Z.\, Y \cap \mathcal{G}(Z) = \mathrm{T} \cap (Y \cap \mathcal{G}(\mathrm{T})) \cap (Y \cap \mathcal{G}(Y \cap \mathcal{G}(\mathrm{T}))) \cap \ldots = Y \cap \mathcal{G}(\mathrm{T}) \cap \mathcal{G}(Y \cap \mathcal{G}(\mathrm{T})) \cap \ldots$

where:
$Y = \{p /\ p \in \mathrm{T},\ p \models \phi\}$
$\mathcal{G}(\mathrm{T}) = \{p /\ p \in \mathrm{T}$ and for all $s,\ p \to s,\ s \in \mathrm{T}\} = \mathrm{T}$
( because $s \in \mathrm{T}$ is always true, so the entire conjunction inside curly brackets is always true for the elements of T, hence $\mathcal{G}(\mathrm{T})$ contains all the elements in T )

Hence $\mathcal{F}(\mathrm{T}) = Y \cap \mathcal{G}(\mathrm{T}) = Y \cap \mathrm{T} = Y = \{p /\ p \in \mathrm{T},\ p \models \phi\}$

$\mathcal{G}(Y \cap \mathcal{G}(\mathrm{T})) = \{p /\ p \in \mathrm{T}$, for all $s,\ p \to s,\ s \in Y \cap \mathcal{G}(\mathrm{T})\} =$
$\{p /\ p \in \mathrm{T}$, for all $s,\ p \to s,\ s \in Y\} = \{p /\ p \in \mathrm{T}$, for all $s,\ p \to s,\ s \models \phi\}$

Hence $\mathcal{F}^2(\mathrm{T}) = Y \cap \mathcal{G}(Y \cup \mathcal{G}(\mathrm{T})) =$
$\{p /\ p \in \mathrm{T},\ p \models \phi\} \cap \{p /\ p \in \mathrm{T}$, for all $s,\ p \to s,\ s \models \phi\} =$
$\{p /\ p \in \mathrm{T}$, for all $s,\ p \to s,\ (p \models \phi$ and $s \models \phi)\}$

$\mathcal{G}(Y \cap \mathcal{G}(Y \cap \mathcal{G}(\mathrm{T}))) =$
$\{p/\ p \in \mathrm{T},\ \text{for all}\ s_0,\ p \to s_0,\ s_0 \in Y \cup \mathcal{G}(Y \cap \mathcal{G}(\mathrm{T}))\} =$
$\{p/\ p \in \mathrm{T},\ \text{for all}\ s_0,\ p \to s_0,\ (s_0 \in Y\ \text{and}\ s_0 \in \mathcal{G}(Y \cap \mathcal{G}(\mathrm{T})))\} =$
$\{p/\ p \in \mathrm{T},\ \text{for all}\ s_0,\ p \to s_0,\ (s_0 \models \phi\ \text{and for all}\ s_1,\ s_0 \to s_1,\ s_1 \in Y)\} =$
$\{p/\ p \in \mathrm{T},\ \text{for all}\ s_0,\ p \to s_0,\ (s_0 \models \phi\ \text{and for all}\ s_1,\ s_0 \to s_1,\ s_1 \models \phi)\} =$
$\{p/\ p \in \mathrm{T},\ \text{for all}\ s_0,\ s_1,\ p \to s_0 \to s_1,\ (s_0 \models \phi\ \text{and}\ s_1 \models \phi)\}$

Hence $\mathcal{F}^3(\mathrm{T}) = Y \cap \mathcal{G}(Y \cap \mathcal{G}(Y \cap \mathcal{G}(\mathrm{T}))) = \{p/\ p \in \mathrm{T},\ p \models \phi\} \cap$
$\cap \{p/\ p \in \mathrm{T},\ \text{for all}\ s_0,\ s_1,\ p \to s_0 \to s_1,\ (s_0 \models \phi\ \text{and}\ s_1 \models \phi)\} =$
$\{p/\ p \in \mathrm{T},\ \text{for all}\ s_0,\ s_1,\ p \to s_0 \to s_1,\ (p \models \phi\ \text{and}\ s_0 \models \phi\ \text{and}\ s_1 \models \phi)\}$

$\ldots$

By mathematical induction, we see that for all $n \in \mathbb{N}$ we have:
$\mathcal{F}^{n+2}(\mathrm{T}) =$
$\{p/p \in \mathrm{T}, \text{for all}\ p \to s_0 \to \ldots \to s_n,\ (p \models \phi\ \text{and}\ s_0 \models \phi\ \text{and} \ldots s_n \models \phi)\}$

Let us consider $p \in \nu Z.\ \mathcal{F}(Z)$

**then** $p \in \mathrm{T}$ and for all paths $p \to s_0 \to s_1 \to$ ... we have
( $p \models \phi$ and $s_0 \models \phi$ and $s_1 \models \phi$ and $\ldots$)
(using the description of $\mathcal{F}^{n+2}(\mathrm{T})$)

**iff** $p \in \mathrm{T}$ and $p \models \mathrm{AG}\ \phi$

**iff** $p \in \mathcal{S}_{\mathrm{AG}\ \phi}$

So, we proved that $\nu Z.\ \mathcal{F}(Z) \subseteq \mathcal{S}_{\mathrm{AG}\ \phi}$

Since $\mathcal{S}_{\mathrm{AG}\ \phi}$ is a fixed point of $\mathcal{F}$ then we have that $\mathcal{S}_{\mathrm{AF}\ \phi} \subseteq \nu Z.\ \mathcal{F}(Z)$ (greatest fixed point is a supra-set of any other fixed point)

From the last two inclusions we conclude that $\nu Z.\ \mathcal{F}(Z) = \mathcal{S}_{\mathrm{AG}\ \phi}$