Exercise 1

$$\varphi_1 = \mathbf{G}(\mathbf{F}p \to q) \quad \varphi_2 = \mathbf{G}(q \,\mathcal{U}\, p) \quad \varphi_3 = \mathbf{G}(\mathbf{F}p \vee \neg q \,\mathcal{U}\, \neg p)$$

(a) Consider the word $w_a = \{q\}^\omega$. We have:

- $w_a \models \mathbf{F}p \to q$, because $w_a \not\models \mathbf{F}p$).
- $w_a \models \mathbf{G}(\mathbf{F}p \to q) = \varphi_1$. We have to show $w_a^i \models \mathbf{F}p \to q$ for every $i \geq 0$. This follows from $w_a \models \mathbf{F}p \to q$ and $w_a^i = w_a$ for every $i \geq 0$.

(b) Consider the word $w_b = \{p\}^\omega$.

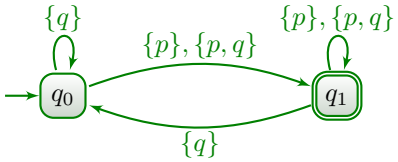
- Since $w_b \models q \,\mathcal{U}\, p$ and $w_b^i = w_b$ for every $i \geq 0$, we have therefore $w_b^i \models q \,\mathcal{U}\, p$ for every $i \geq 0$, and so $w_b \models \mathbf{G}(q \,\mathcal{U}\, p)$.
- Since $w_b \not\models q$ (as the first letter of w_b does not contain the atomic proposition q), and $w_b \models \mathbf{F}p$, we get $w_b \not\models (\mathbf{F}p \to q)$, and so $w_b \not\models \mathbf{G}(\mathbf{F}p \to q)$.

(c) Consider the word $w_c = \{p, q\}^\omega$.

Since $w_c = w_c^i$ for every $i \geq 0$, it sufficies to show that w_c satisfies the formulas below the $\mathbf{G}$ operator.

- Since $w_c \models q$, we have $w_c \models \mathbf{F}p \to q$, and so $w_c \models \varphi_1$.
- Since p holds at the first position of w_c, we have $w_c \models q \,\mathcal{U}\, p$, and so $w_c \models \varphi_2$.
- Since $w_c \models \mathbf{F}p$, we have $w_c \models \mathbf{F}p \vee (\neg q \,\mathcal{U}\, \neg p)$, and so $w_c \models \varphi_3$.

(d) The following two-state Bc̈hi automaton recognizes $L(\varphi_2)$:



It is also possible to use the construction given in the lecture, which yields an automaton with 16 states (φ_2 is already in NNF and has 4 subformulas including itself). 8 of these states are unreachable (all those not containing φ_2), and another 5 do not admit outgoing transitions (those not containing $q \,\mathcal{U}\, p$ and $\{\varphi_2, q \,\mathcal{U}\, p, \neg p, \neg q\}$. Out of the remaining 3 states, two are final ($\{\varphi_2, q \,\mathcal{U}\, p, p, \neg q\}$ and $\{\varphi_2, q \,\mathcal{U}\, p, p, q\}$) and the third is not ($\{\varphi_2, q \,\mathcal{U}\, p, \neg p, q\}$).

Exercise 2

1. Yes. Processes `x` and `y` communicate synchronously through the channel `c`. The value of g is initially `0`. The only possible execution sequence is the following:

   - At line 5, `x` sends `1` through the channel `c`.
   - Now, the following two steps are repeated for ever:

- At line 13, `y` receives `1`, increases `g` by one (`g` is now 1), and sends `0` through `c`.
- At line 7, `x` receives `0`, decreases `g` by one (`g` is now 0), and sends `1` through `c` at `label1`.

The value of `g` always alternates between `0` and `1`. Therefore, the formula holds.

2. We can take:

```
active proctype z() {  c!2;  }
```

3. No. If process `z` is executed first, then the value of `g` will alternate only between `1` and `2`.

Exercise 3

$$\phi = [(p \,\mathcal{U}\, q) \rightarrow (r \,\mathcal{R}\, q)] \,\mathcal{U}\, (\mathbf{X}(p \wedge q \wedge r))$$

(a)

$$\begin{array}{rcl} \neg\phi & = & \neg\,([(p \,\mathcal{U}\, q) \rightarrow (r \,\mathcal{R}\, q)] \,\mathcal{U}\, (\mathbf{X}(p \wedge q \wedge r))) \\ & = & \neg\,[(p \,\mathcal{U}\, q) \rightarrow (r \,\mathcal{R}\, q)] \;\mathcal{R}\; \neg\,(\mathbf{X}(p \wedge q \wedge r)) \\ & = & \neg\,[\neg(p \,\mathcal{U}\, q) \vee (r \,\mathcal{R}\, q)] \;\mathcal{R}\; \mathbf{X}\neg(p \wedge q \wedge r) \\ \psi & = & ((p \,\mathcal{U}\, q) \wedge (\neg r \,\mathcal{U}\, \neg q)) \;\mathcal{R}\; \mathbf{X}(\neg p \vee \neg q \vee \neg r) \end{array}$$

(b) We have

$$\begin{array}{rcl} Sub(\psi) & = & \{\psi, (p \,\mathcal{U}\, q) \wedge (\neg r \,\mathcal{U}\, \neg q)\ ,\ \mathbf{X}(\neg p \vee \neg q \vee \neg r)\ ,\ (p \,\mathcal{U}\, q), \\ & & (\neg r \,\mathcal{U}\, \neg q)\ ,\ (\neg p \vee \neg q \vee \neg r)\ ,\ \neg p\ ,\ \neg q \vee \neg r\ ,\ \neg q\ , \neg r, p, q, r\} \\ & & \bigcup \text{ (let us not forget the negated formulas)} \\ & & \{\neg\psi, \neg((p \,\mathcal{U}\, q) \wedge (\neg r \,\mathcal{U}\, \neg q)), \neg\mathbf{X}(\neg p \vee \neg q \vee \neg r), \neg(p \,\mathcal{U}\, q), \\ & & \neg(\neg r \,\mathcal{U}\, \neg q), \neg(\neg p \vee \neg q \vee \neg r), \neg(\neg q \vee \neg r)\} \end{array}$$

A smallest consistent state containing $\psi, \mathbf{X}(\neg p \vee \neg q \vee \neg r), p, q, \neg r$

- also contains $(\neg p \vee \neg q \vee \neg r), \neg q \vee \neg r$, and $p \,\mathcal{U}\, q$; and
- also contains the formulas $\neg((p \,\mathcal{U}\, q) \wedge (\neg r \,\mathcal{U}\, \neg q)), \neg(\neg r \,\mathcal{U}\, \neg q), \neg r$

Observe: You can choose to take $p \,\mathcal{U}\, q$ or its negation, and the same for $\neg r \,\mathcal{U}\, \neg q$, and $(p \,\mathcal{U}\, q) \wedge (\neg r \,\mathcal{U}\, \neg q)$, but your choice must be consistent. Further: $p \,\mathcal{U}\, q$ must belong to the state if you want it to have outgoing transitions, as needed for (c).

(c) Let M be the state of (b). We construct a successor M'. The transition is labeled by $\{p, q\}$, the atomic propositions holding in M.

- Since $\psi \in M$, $(p \,\mathcal{U}\, q) \wedge (\neg r \,\mathcal{U}\, \neg q) \notin M$, and $\mathbf{X}(\neg p \vee \neg q \vee \neg r) \in M$, we must have $\psi \in M'$.
- Since $p \,\mathcal{U}\, q \in M$ and $q \in M$, we can have any of $p \,\mathcal{U}\, q$ or $\neg(p \,\mathcal{U}\, q)$ in M'

- Since $\neg r \,\mathcal{U}\, \neg q \notin M$, $\neg r \in M$, and $\neg q \notin M$, we must have $\neg r \,\mathcal{U}\, \neg q \notin M'$.
- Since $X(\neg p \vee \neg q \vee \neg r) \in M$, we must have $(\neg p \vee \neg q \vee \neg r) \in M'$

It follows that we can take $M' = M$.

Exercise 4

(a) a and c are dependent, because $a, c \in en(s_5)$ where $s_5 \xrightarrow{a} s_7$ and $s_5 \xrightarrow{c} s_8$, but there is no v s.t. $c \in en(s_7)$, $a \in en(s_8)$, $s_7 \xrightarrow{c} v$ and $s_5 \xrightarrow{a} v$.

(b)
- $red(s_7) = \emptyset$ violates C_0 because $en(s_7) \neq \emptyset$.
- $red(s_1) = \{c\}$ satisfies the conditions C_0–C_3:
  - (C_0) $red(s_1) \neq \emptyset$;
  - (C_1) for all paths starting at s_1, the action a, which is the only action that depends on c, does not occur;
  - (C_2) c is invisible; and
  - (C_3) there are no cycles in $\mathcal{K}$.
- $red(s_0) = \{c\}$ violates C_1 because the action a, which depends on c, can occur before c via $s_0 \xrightarrow{a} s_1$.

Exercise 5

(a) All states satisfy ψ_1, exactly a_3, a_4, b_3 satisfy ψ_2.

Observe that b_4 does *not* satisfy $A\mathbf{F}E\mathbf{G}p$, because the path b_4^ω does not satisfy $E\mathbf{G}p$.

(b) First we compute $[\![E\mathbf{G}p]\!]$ as the greatest fixpoint of the equation: $X = \mu(p) \cap pre(X)$

$$
\begin{aligned}
X_0 &= \{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4\} \\
X_1 &= \mu(p) \cap pre(\{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4\}) \\
&= \{a_1, a_2, a_3, a_4\} \cap \{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4\} \\
&= \{a_1, a_2, a_3, a_4\} \\
X_2 &= \mu(p) \cap pre(\{a_1, a_2, a_3, a_4\}) \\
&= \{a_1, a_2, a_3, a_4\} \cap \{b_1, b_2, a_3, b_3, a_4, b_4\} \\
&= \{a_3, a_4\} \\
X_3 &= \{a_1, a_2, a_3, a_4\} \cap pre(\{a_3, a_4\}) \\
&= \{a_1, a_2, a_3, a_4\} \cap \{a_3, b_3, a_4, b_4\} \\
&= \{a_3, a_4\}
\end{aligned}
$$

Then we compute $[\![E\mathbf{X}(E\mathbf{G}p)]\!] = pre(\{a_3, a_4\}) = \{a_3, b_3, a_4, b_4\}$.

Finally we compute $[\![A\mathbf{F}(E\mathbf{X}(E\mathbf{G}p))]\!] = [\![\neg E\mathbf{G}\neg(E\mathbf{X}(E\mathbf{G}p))]\!]$. So we compute $E\mathbf{G}$ over the complement of $\{a_3, b_3, a_4, b_4\}$ and then take its complement.

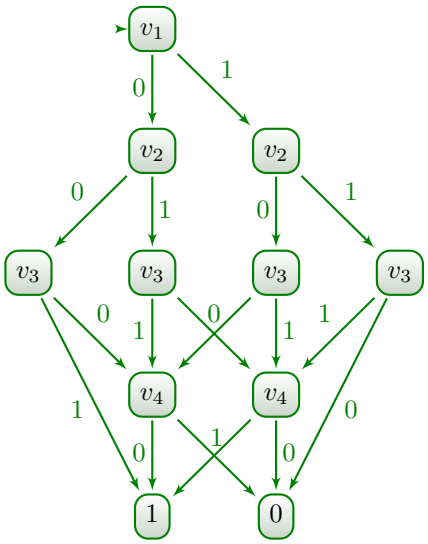
Applying the fixpoint equation, we compute $[\![E\mathbf{G}\neg(E\mathbf{X}(E\mathbf{G}p))]\!]$ as the greatest fixpoint of the equation $Y = \mu(\varphi) \cap pre(Y)$ with $[\![\varphi]\!] = \{a_1, a_2, b_1, b_2\}$.

$$
\begin{aligned}
Y_0 &= \{a_1, a_2, b_1, b_2, a_3, a_4, b_3, b_4\} \\
Y_1 &= \{a_1, a_2, b_1, b_2\} \cap pre(\{a_1, a_2, b_1, b_2, a_3, a_4, b_3, b_4\}) \\
&= \{a_1, a_2, b_1, b_2\} \cap \{a_1, a_2, b_1, b_2, a_3, a_4, b_3, b_4\} \\
&= \{a_1, a_2, b_1, b_2\} \\
Y_2 &= \{a_1, a_2, b_1, b_2\} \cap pre(Y_1) \\
&= \{a_1, a_2, b_1, b_2\} \cap \{a_1, a_2, b_1, b_2\} \\
&= \{a_1, a_2, b_1, b_2\}
\end{aligned}
$$

Thus $[\![A\mathbf{F}(E\mathbf{X}(E\mathbf{G}p))]\!]$ is the complement of $\{a_1, a_2, b_1, b_2\}$, that is $\{a_3, b_3, a_4, b_4\}$.

Exercise 6

(a)



(b) Any BDD of a boolean function with four variables has at most 5 levels. The last level contains at most two states 0 and 1.

The first level contains exactly 1 state.

The second level contains at most 2 states (as the first state has two outgoing transitions).

The third level contains at most 4 states: if the second level has 2 states, then the first level does not have any transitions going directly to the third level, and each of the two states on the second level has two outgoing transitions, so no more than 4 states on the third level. If the second level has one state or fewer, at most two transitions can come from the second level, and at most two can come from the first level.

The fourth level contains at most 2 states: any state on the fourth level has transitions to a lower level, i.e. level 5 in this case, and they can not lead both to the same state, otherwise that (4-th level) state should have been omitted. So any state on the fourth level needs to have a transition towards each of the states 0 and 1. There are only two possibilities: (go to 0 with 1 and to 1 with 0), or (go to 0 with 0 and to 1 with 1). If two

states do the same thing, they should have been merged. Therefore there can be at most be two states on level four.

Summing up these bounds yield the desired upper bound of 11 states.