1.) (a) Consider the following decision problem:

**INDEPENDENT DOMINATING SET (IDS)**

**INSTANCE:** A directed graph $G = (V, E)$.

**QUESTION:** Does there exist a set $S \subseteq V$ of vertices, such that

1. For each $(u,v) \in E$, $\{u,v\} \not\subseteq S$;
2. For each $v \in V$, either $v \in S$ or there exists an $(u,v) \in E$, such that $u \in S$.

The following function $f$ provides a polynomial-time many-one reduction from IDS to SAT: for a directed graph $G = (V, E)$, let

$$f(G) = \bigwedge_{(u,v) \in E} (\neg x_u \lor \neg x_v) \land \bigwedge_{v \in V} (x_v \lor \bigvee_{(u,v) \in E} x_u) .$$

It holds that $G$ is a yes-instance of IDS $\iff f(G)$ is a yes-instance of SAT.

Prove the $\Rightarrow$ direction of the claim.

(10 points)
(b) Given that SAT is NP-complete, what can be said about the complexity of IDS from the above reduction? NP-hardness of IDS, NP-membership of IDS, neither of them, or both (NP-completeness of IDS)

(5 points)
2.) (a) The topic of this exercise is translation validation (discussed in the fifth lecture of the second block). Given a statement in a source program of the form

\[ z = (y_1 * x) + (y_2 * x) \]  \hspace{1cm} (S)

and the result of the compiler optimization of the form

\[ u_1 = y_1 + y_2, \quad u_2 = u_1 * x, \]  \hspace{1cm} (O)

the goal is to check the correctness of the translation.

i. Formulate the verification condition.

\[ (VC) \]

ii. Formulate the abstract verification condition (using uninterpreted functions).

\[ (AVC) \]

iii. Prove the correctness of the translation process (using the semantic proof method from the third lecture (on First-order Logic and Theories), or present a counterexample for (AVC). The symbols \( u_1, u_2, x, y_1, y_2, z \) are all free variables!

Hint: Do not use Ackermann!

(6 points)
(b) Let \( \varphi \) be the first-order formula

\[
\forall x \forall y \left[ (r(x, y) \rightarrow (p(x) \rightarrow p(y))) \land (r(x, y) \rightarrow (p(y) \rightarrow p(x))) \right].
\]

i. Is \( \varphi \) valid? If yes, present a proof. If no, give a counter-example and prove that it falsifies \( \varphi \).

ii. Replace \( r \) in \( \varphi \) by \( = \) (equality) resulting in \( \psi \). Is \( \psi \) \( E \)-valid? Argue formally!

(9 points)
3. (a) Show that the assertion

\[ F : y > 0 \]

\[ x := 0; \]

\[ i := y; \]

\[ \textbf{while} \ i > 0 \ \textbf{do} \]

\[ x := x + 2; \]

\[ i := i - 1 \]

\[ \textbf{od} \]

\[ G : x = 2 \ast y \]

is correct with respect to partial correctness. (12 points)
(b) Consider the program $q$ below.

\[
y := 1;
\]
\[
\textbf{while } x > 0 \textbf{ do}
\]
\[
\text{if } y > 0 \text{ then}
\]
\[
x := x - 1;
y := y - 1
\]
\[
\text{else}
\]
\[
y := y + 5
\]
\[
\textbf{od}
\]

Find a loop variant $t$ that is positive at the start of each loop iteration, and strictly decreases with each loop iteration.

(3 points)
4.) (a) The Kripke structure $M_1 = (S, S_0, R, AP, L)$ is depicted below, with $S_0 = \{t_1, t_2\}$ and $AP = \{\otimes, \triangledown, \triangle, \star\}$.

i. Find a Kripke structure $M_2$ with the smallest number of states and transitions, for which $M_1 \leq M_2$, and write down a witnessing simulation relation.

ii. Show that there exists no Kripke structure $M_3$ with fewer states than $M_2$, for which $M_1 \leq M_3$.

iii. Does $M_2 \leq M_1$ hold?
(b) Consider the following Kripke structure $M$:

For each of the following formulae $\varphi$,

i. check the respective box if the formula is in CTL, and

ii. list the states $s_i$ on which the formula $\varphi$ holds; i.e. for which states $s_i$ do we have $M, s_i \models \varphi$?

Recall that for an LTL formula $\varphi$ it holds that $M, s \models \varphi \iff M, s \models A \varphi$.

<table>
<thead>
<tr>
<th>$\varphi$</th>
<th>CTL</th>
<th>States $s_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X(a)$</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>$AG(b \land c)$</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>$AX(a \land c)$</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>$A[(b) \ U (c)]$</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>$E[(b \land c) \ U (a)]$</td>
<td>□</td>
<td></td>
</tr>
</tbody>
</table>

(5 points)
(c) **LTL tautologies**

Prove or disprove that the following formulas are tautologies, i.e., they hold for every Kripke structure $M$ and every path $\pi$:

i. 
$$XFp \iff XFXp$$

ii. 
$$\left(G\neg p\right) \cup p \iff p$$

(5 points)