1.) 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 \( u \in S \).

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

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

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

Prove the \( \Leftarrow \) 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) 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! (5 points)

(b) Show the following:

\( \varphi^{EUF} \) is satisfiable iff \( FC^E \land flat^E \) is satisfiable.

\( FC^E \) and \( flat^E \) are obtained from \( \varphi^{EUF} \) by Ackermann’s reduction.

(Hint: \( FC^E \) is the same for \( \varphi^{EUF} \) and \( \neg \varphi^{EUF} \).) (10 points)
(a) Let $p$ be the following program:

$$
\begin{align*}
  x &:= 3; \\
  y &:= 1; \\
  \textbf{while } y \geq N \textbf{ do} \\
  &\quad x := x - 4 \ast y + 2; \\
  &\quad y := y - 1 \\
  \textbf{od}
\end{align*}
$$

Give a loop invariant for the \textbf{while} loop in $p$ and prove the validity of the partial correctness triple \{ $N < 0$ \} $p$ \{ $x = 2 \ast N \ast N - 4 \ast N + 3$ \}.

(10 points)
(b) We add for loops with the following syntax to the IMP language.

\[\text{for } v := e_1 \text{ until } e_2 \text{ do } c \text{ od},\]

where \(v\) is a variable, \(e_1\) and \(e_2\) are arithmetic expressions and \(c\) is a program. The informal semantics of the for loop is as follows.

- \(v\) is initialized to \(e_1\);
- in every loop iteration, \(c\) is executed and then \(v\) is incremented, i.e., \(v := v + 1\);
- the loop terminates when \(v > e_2\).

Stated differently, the above for loop is equivalent to

\[v := e_1; \text{while } v \leq e_2 \text{ do } c; v := v + 1 \text{ od.}\]

Prove the soundness of or provide a counterexample to the following proof rule.

\[
\begin{align*}
\{P\} & v := e_1 \{I\} \quad \{I \land v \leq e_2\} \quad c; v := v + 1 \{I\} \\
\{P\} & \text{for } v := e_1 \text{ until } e_2 \text{ do } c \text{ od } \{I \land v > e_2\}
\end{align*}
\]

(5 points)
4.) (a) Provide a simulation relation $H$ that witnesses $M_1 \preceq M_2$, where $M_1$ and $M_2$ are shown below. The initial state of $M_1$ is $s_0$, the initial state of $M_2$ is $t_0$:

**Kripke structure $M_1$:**

![Diagram of Kripke structure $M_1$]

**Kripke structure $M_2$:**

![Diagram of Kripke structure $M_2$]

(5 points)
(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, LTL, and/or CTL*, and

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

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

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

Prove that the following formulas are tautologies, i.e., they hold for every Kripke structure $M$ and every path $\pi$ in $M$, or find a Kripke structure $M$ and path $\pi$ in $M$, for which the formula does not hold and justify your answer.

i. 

$$p \Rightarrow \top \land U (\bot \land U p)$$

ii. 

$$q \land FGp \Rightarrow q \land U (Gp)$$

(5 points)