1.) Consider the following variant of the dominating set problem \textbf{DOM}:

**DOMINATING SET VARIATION (DOM)**

**INSTANCE:** A directed graph \( G = (V, E) \) and an integer \( k \).

**QUESTION:** Does there exist a set \( S \subseteq V \) of cardinality \(|S| \leq k\) such that for each \( v \in V \) either \( v \in S \) or there is an \( u \in S \) with \((u,v) \in E\).

(a) The following function \( f \) provides a polynomial-time many-one reduction from \textbf{3SAT} to \textbf{DOM}: for a 3-CNF formula \( \varphi = \bigwedge_{j=1}^{m} (l_{j1} \lor l_{j2} \lor l_{j3}) \) over atoms \( A = \{a_1, \ldots, a_n\} \) let \( f(\varphi) = (G, k) \), where \( G = (V, E) \) with

\[
V = \{v_1, v'_1, \ldots, v_n, v'_n, c_1, \ldots, c_m\};
\]

\[
E = \{(v_i, v'_i), (v'_i, v_i) \mid 1 \leq i \leq n\} \cup
\{(v_i, c_j) \mid a_i \in \{l_{j1}, l_{j2}, l_{j3}\}, 1 \leq i \leq n, 1 \leq j \leq m\} \cup
\{(v'_i, c_j) \mid \neg a_i \in \{l_{j1}, l_{j2}, l_{j3}\}, 1 \leq i \leq n, 1 \leq j \leq m\}; \text{ and}
\]

\( k = n \)

It holds that \( \varphi \) is a yes-instance of \textbf{3SAT} \iff \( f(\varphi) \) is a yes-instance of \textbf{DOM}.

Show the \( \implies \) direction of the statement.

(b) In what follows assume the reduction from \textbf{3SAT} to \textbf{DOM} is correct, and further assume we have shown that \textbf{DOM} is in NP. Also recall that \textbf{3SAT} is NP-complete.

Tick the correct statements (for ticking a correct statement a certain number of points is given; ticking an incorrect statement results in a subtraction of the same amount; you cannot go below 0 points):

- DOM is NP-complete
- DOM is NP-hard
- there exists a polynomial-time many-one reduction from DOM to SAT
- DOM is decidable
- a polynomial-time many-one reduction from DOM to SAT shows P=NP
- DOM is in P

(6 points)
(a) Consider the implementation of the function `pow4` in C, which is supposed to compute \( x^4 \) for a signed 32 bit integer \( x \).

```c
uint32_t pow4(int32_t x){
    uint32_t y;
    y = x * x * x * x;
    return y;
}
```

Suppose the function is called with a parameter of correct type. Does this function return the mathematically correct value \( x^4 \)? If your answer is yes, then prove the correctness of the function. Otherwise describe exactly and in detail what is going on.

Would you answer differently, if \( y \) is of type `uint64_t`? Explain.

(4 points)

(b) Consider the following clause set \( \hat{\delta}(\phi) \) which has been derived from an (unknown) formula \( \phi \) by Tseitin’s translation (atoms have not been labeled).

\[ C_1: \ell_1 \lor \neg x \lor \neg y \]
\[ C_4: \neg \ell_2 \lor \neg y \lor z \]
\[ C_7: \neg \ell_3 \lor \neg \ell_1 \lor z \]
\[ C_{10}: \neg \ell_4 \lor \neg x \lor \ell_2 \]
\[ C_{13}: \neg \ell_5 \lor \neg \ell_3 \lor \ell_4 \]
\[ C_2: \neg \ell_1 \lor x \]
\[ C_5: \ell_2 \lor y \]
\[ C_8: \ell_3 \lor \ell_1 \]
\[ C_{11}: \ell_4 \lor x \]
\[ C_{12}: \ell_4 \lor \neg \ell_2 \]
\[ C_{14}: \ell_5 \lor \ell_3 \]
\[ C_{15}: \ell_5 \lor \neg \ell_4 \]

(i) Reconstruct \( \phi \) from \( \hat{\delta}(\phi) \) using the smallest number of connectives.
(ii) Start from \( \hat{\delta}(\phi) \) and extend it by a single nonempty clause \( C \) in such a way that \( \phi \) is valid iff \( \hat{\delta}(\phi) \land C \) is unsatisfiable.
(iii) Use resolution to prove the validity of \( \phi \) (no additional translation is allowed!).

(5 points)

(c) Let \( R \) be \( \forall x \ p(x, x) \), and let \( \varphi \) be \( \exists x \exists y \forall z [p(x, y) \land p(y, z)] \), where \( p \) is a binary predicate symbol. Check whether \( R \models \varphi \) holds. If yes, then give a proof; otherwise give a counter-example and prove that the entailment does not hold.

(6 points)
3.) (a) Let $p$ be the following IMP program:

\[
\begin{align*}
    &x := 0; y := 0; z := 1; \\
    &\textbf{while} \ z < n \ \textbf{do} \\
    &\quad x := x + 2; \\
    &\quad y := y + 6 \cdot x; \\
    &\quad z := z + 1 \\
    &\textbf{od}
\end{align*}
\]

Give a loop invariant for the while loop in $p$ and prove the validity of the partial correctness triple $\{ n > 1 \} \ p \ { y = 3 \cdot x \cdot n \}$. 

Hint: Make sure that your invariant expresses equalities among $y, z, x$, as well as equalities among $z, x$. 

(9 points)

(b) Let $p$ be an IMP program such that $\{ \text{true} \} \ p \ { x = -2 \land y = 2 \}$ is valid. Is $\{ x = -2 \} \ p \ { x \leq 0 \}$ valid? If so, give a formal proof. Otherwise, give a counterexample. 

(3 points)

(c) Let $p$ be the IMP program

\[
\textbf{while} \ x > 0 \ \textbf{do} \ x := x - 2
\]

Give a pre-condition $A$ such that $[A] \ p \ [x = 0]$ is valid. Your precondition $A$ should not be $x = 0$ and it should not be equivalent to $\text{true}$ nor to $\text{false}$. 

(3 points)
4.) (a) Provide a non-empty simulation relation $H$ that witnesses $M_1 \leq M_2$, 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 $M_2$]
(b) Consider the following Kripke structure $M$:

![Kripke structure diagram]

For each of the following formulae $\varphi$,

i. indicate whether 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 $M, s_i \models \varphi$?

(If $\varphi$ is a path formula, list the states $s_i$ such that $M, s_i \models A\varphi$.)

<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>$\text{AG}(b)$</td>
<td>⊘</td>
<td>⊘</td>
<td>⊘</td>
<td></td>
</tr>
<tr>
<td>$\text{G}(c)$</td>
<td>⊘</td>
<td>⊘</td>
<td>⊘</td>
<td></td>
</tr>
<tr>
<td>$\text{X}(a \land c)$</td>
<td>⊘</td>
<td>⊘</td>
<td>⊘</td>
<td></td>
</tr>
<tr>
<td>$\text{E}[(a \land c) \text{ U } c]$</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. $(G(\neg a \land \neg b) \land F(a \land Xb)) \Rightarrow F(a \ U \neg a)$

ii. $(G((a \Rightarrow Xb) \land (b \Rightarrow Xa))) \Rightarrow (a \ U \ b)$

(6 points)