1.) Recall the HAILING problem which takes a program and a string as input, and consider the following variant thereof:

**HALTING-ODD**

INSTANCE: A program $\Pi$ that takes a string as input, a string $I$.

QUESTION: Does $\Pi$ terminate on $I$ in an even number of computation steps.

(a) The following function $f$ provides a polynomial-time many-one reduction from HAILING to HALTING-ODD: for a program $\Pi$ and a string $I$ let $f(\Pi, I) = (\Pi', I')$ with $I' = I$ and $\Pi'$ given as follows:

$$
\Pi'(\text{string } S)\
\quad \text{call } \Pi(S); \\
\quad \text{call } \Pi(S); \\
\quad S := S; \quad \text{//dummy operation ... 1 computation step} \\
\quad \text{return;}
$$

(Remark: We assume that calls and return-statements do not count as computation steps).

Show that $(\Pi, I)$ is a yes-instance of HAILING $\iff (\Pi', I')$ is a yes-instance of HALTING-ODD.

(9 points)

(b) Please answer the following questions and explain your answers

- Is HALTING-ODD undecidable?
- Is HALTING-ODD semi-decidable?

(6 points)
2.) (a) Consider the following clause set \( \hat{\delta}(\varphi) \) which has been derived from an (unknown) formula \( \varphi \) by an improved version of Tseitin’s translation (atoms have not been labeled and \( \overline{z} \) means \( \neg z \)).

\[
\begin{align*}
C_1 & : \ell_1 \lor x_1 \lor x_2 \\
C_2 & : \ell_1 \lor \overline{x_1} \lor \overline{x_2} \\
C_3 & : \ell_1 \lor x_1 \lor x_2 \\
C_4 & : \ell_1 \lor x_1 \lor \overline{x_2} \\
C_5 & : \ell_2 \lor x_2 \lor x_3 \\
C_6 & : \ell_2 \lor \overline{x_2} \lor \overline{x_3} \\
C_7 & : \ell_2 \lor \overline{x_2} \lor \overline{x_3} \\
C_8 & : \ell_2 \lor x_2 \lor \overline{x_3} \\
C_9 & : \ell_3 \lor \ell_1 \\
C_{10} & : \ell_3 \lor \ell_2 \\
C_{11} & : \ell_3 \lor \overline{\ell_1} \lor \overline{\ell_2} \\
C_{12} & : \ell_4 \lor \ell_1 \\
C_{13} & : \ell_4 \lor \ell_2 \\
C_{14} & : \ell_4 \lor \overline{\ell_1} \lor \overline{\ell_2} \\
C_{15} & : \ell_5 \lor \ell_4 \lor x_2 \\
C_{16} & : \ell_5 \lor \ell_4 \\
C_{17} & : \ell_5 \lor \overline{\ell_3} \\
C_{18} & : \ell_6 \lor \ell_3 \lor \ell_5 \\
C_{19} & : \ell_6 \lor \ell_3 \\
C_{20} & : \ell_6 \lor \overline{\ell_5}
\end{align*}
\]

(i) Reconstruct \( \varphi \) from \( \hat{\delta}(\varphi) \).

(ii) Prove the validity of \( \varphi \) by resolution (no additional translation to normal form is allowed!). You are allowed to add a single unit clause (i.e., a clause containing exactly one literal). Please explain your approach!

(7 points)

(b) Let \( \mathcal{T}^E_f \) be the theory containing all equality axioms (from \( \mathcal{T}^E \)) and the following two additional axioms.

- \( \forall x \forall y (f(x) \overset{\approx}{=} f(y) \rightarrow x \overset{\equiv}{=} y) \) (f-injectivity)
- \( \forall x f(x) \overset{\approx}{=} f(f(x)) \) (f-idempotency)

Clarify the logical status of each of the following formulas. If one is \( \mathcal{T}^E_f \)-valid or \( \mathcal{T}^E_f \)-unsatisfiable, then prove it using the semantic argument method. If one is \( \mathcal{T}^E_f \)-satisfiable but not \( \mathcal{T}^E_f \)-valid, then present a satisfying and a falsifying interpretation. Argue formally that the formula evaluates to true resp. false under the constructed interpretations.

\[
\begin{align*}
\varphi & : f(f(f(a))) \overset{\approx}{=} f(b) \rightarrow a \overset{\equiv}{=} b \\
\psi & : f(f(f(a))) \not\overset{\approx}{=} f(b) \land a \overset{\equiv}{=} b
\end{align*}
\]

(8 points)
3. (a) Let \( p \) be the following IMP program loop, containing the integer-valued program variables \( i, x, y \):

\[
\text{while } i < 10 \text{ do } \\
y := y + 2 \times i; \\
i := i + 1; \\
x := x - 2 \times i; \\
\text{od}
\]

Give a loop invariant for the \textbf{while} loop in \( p \) and prove the validity of the total correctness triple \([i = 0 \land x = 100 \land y = 0] \ p \ [x + y = 80] \).

(10 points)

(b) Let \( p \) be the IMP program:

\[
\text{if } 2 \times x \leq y \text{ then } x := x + 2 \text{ else } y := y - 2
\]

What is the \( \text{wlp}(p, x = 2 \land y = 4) \)?

(3 points)

(c) Let \( p \) be an IMP program such that \([2 \times x \leq y] \ p \ [x \neq y] \) is valid.

Is \([x = -3 \land y = -1] \ p \ [3 \times y - 3 \times x \neq 0] \) valid? If so, give a formal proof. Otherwise, give a counterexample.

(2 points)
4.) (a) Consider the Kripke structures $M_1$ and $M_2$. The initial state of $M_1$ is $s_0$, the initial state of $M_2$ is $t_0$.

**Kripke structure $M_1$:**

- Initial state: $s_0: \{x\}$
- State $s_2: \{y\}$
- State $s_3: \{z\}$
- State $s_4: \{y\}$
- State $s_1: \{x\}$

**Kripke structure $M_2$:**

- Initial state: $t_0: \{x\}$
- State $t_2: \{y\}$
- State $t_1: \{z\}$
- State $t_4: \{y\}$
- State $t_5: \{z\}$
- State $t_3: \{y\}$

i. Briefly explain why $M_2$ does not simulate $M_1$.

ii. Add a minimal set of edges to $M_2$ such that the extended Kripke structure $M'_2$ simulates $M_1$. Provide the additional edges and a non-empty simulation relation $H$ that witnesses $M_1 \preceq M'_2$.

(4 points)
(b) Consider the following Kripke structure $M$:

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>$AF(y \land z)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$X(x)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$G(z)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$EF(z)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$E[(y) U (z)]$</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. $(GFx) \land (GFy) \Rightarrow G(x \Rightarrow Fy)$

ii. $G(x \Rightarrow Fy) \Rightarrow (GFx) \land (GFy)$

(6 points)