1.) Consider the following decision problem:

**REACHING LINE in LESS STEPS (RLLS)**

**INSTANCE:** A tuple \((\Pi_1, \Pi_2, I, n_1, n_2)\), where \(\Pi_1, \Pi_2\) are programs that take a string as input, \(I\) a string, and \(n_1, n_2\) integers.

**QUESTION:** Does \(\Pi_1\) when applied to \(I\) reach line \(n_1\) (of the source code of \(\Pi_1\)) in strictly less computation steps than \(\Pi_2\) when applied to \(I\) reaches line \(n_2\) (of the source code of \(\Pi_2\))? 

Remark: If neither \(\Pi_1\) reaches line \(n_1\) nor \(\Pi_2\) reaches line \(n_2\), we have a negative instance of RLLS.

(1) By providing a suitable many-one reduction from the **HALTING** problem, prove that **REACHING LINE in LESS STEPS** is undecidable.

(2) Is **REACHING LINE in LESS STEPS** semi-decidable? Explain your answer.

(15 points)
(a) Consider $\varphi: a[i] = e \rightarrow a(i \triangleleft e) = a$. If $\varphi$ is $T_{\text{A}}^n$-valid then provide a proof using the semantic argument method from the lecture. If $\varphi$ is not $T_{\text{A}}^n$-valid then provide a counter-example. Besides the equality axioms, you have the following ones for arrays.

i. $\forall a, i, j \ (i \neq j \rightarrow a[i] \equiv a[j])$ (array congruence)

ii. $\forall a, v, i, j \ (i \neq j \rightarrow a(i \triangleleft v)[j] \equiv v)$ (read-over-write 1)

iii. $\forall a, v, i, j \ (i \neq j \rightarrow a(i \triangleleft v)[j] \equiv a[j])$ (read-over-write 2)

iv. $\forall a, b \ ((\forall j \ a[j] \equiv b[j]) \leftrightarrow a \equiv b)$ (extensionality)

Please be precise. In a proof indicate exactly why proof lines follow from some other(s). If you use derived rules you have to prove them. Recall that a counter-example has to satisfy all axioms and falsifies $\varphi$.

(11 points)

(b) First define the concept of a theory and of a $T$-interpretation. Then use them to define:

i. the $T$-satisfiability of a formula;

ii. the $T$-validity of a formula.

Additionally define the completeness of a theory $T$.

(4 points)
3.) Note that all programs within this exercise are programs over the integers, that is, every program variable can only take integer values.

(a) Show that the Hoare triple \([y \geq 0] \ p \ [x = 5 \ast y + 2]\) is valid with respect to total correctness, where \(p\) is the following program:

\[
\begin{align*}
c &:= y; \\
x &:= 2; \\
\textbf{while} \ c > 0 \ \textbf{do} \\
\quad x &:= x + 5; \\
\quad c &:= c - 1 \\
\textbf{od}
\end{align*}
\]

(b) Let \(q\) be the program

\[
\begin{align*}
r &:= 0; \ a := x; \ b := y; \\
\textbf{while} \ (a \geq 0 \lor b \geq 0) \ \textbf{do} \\
\quad \textbf{if} \ a \geq b \\
\quad \quad \textbf{then} \ r := r + 1; \ a := a - 1 \\
\quad \quad \textbf{else} \ r := r + 1; \ b := b - 1 \\
\quad \textbf{od}
\end{align*}
\]

Prove that the Hoare triple \(\{true\} \ c \ {r = x + y}\) is invalid.

**Hint:** Provide a counterexample, i.e., a state that does not satisfy the correctness assertion.

(2 points)

(c) Let \(q\) be the program from exercise 3b. State the weakest precondition \(P\) such that the triple \(\{P\} \ q \ {r = x + y}\) is valid.

You are *not* required to prove that \(P\) is the weakest precondition.

(2 points)
4.) (a) Provide a 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 $M_1$:**

- $s_0$: \{b\}
- $s_1$: \{a\}
- $s_2$: \{c\}
- $s_4$: \{b\}

**Kripke structure $M_2$:**

- $t_0$: \{b\}
- $t_2$: \{a\}
- $t_4$: \{c\}
- $t_3$: \{b\}
- $t_1$: \{c\}
- $t_5$: \{b\}

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

\[
\begin{array}{c}
\text{s0: \{a\}} \\
\text{s1: \{b\}} \\
\text{s2: \{a\}} \\
\text{s3: \{a, c\}} \\
\text{s4: \{a\}}
\end{array}
\]

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>$G(a)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$((a \land c) \mathbf{U} (a))$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$AF(a \land c)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$AX(b)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$E[(c) \mathbf{U} (b)]$</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. 
$$F(Fp \land Gq) \Rightarrow Fp \land FGq$$

ii. 
$$F(Fp \land Gq) \Leftarrow Fp \land FGq$$

(5 points)