1.) Consider the following decision problem:

**EXACTLY-ONE-HALTS (EOH)**

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

QUESTION: Does either \(\Pi_1\) halt on \(I\) or \(\Pi_2\) halt on \(I\) (but not both halt on \(I\))? 

(a) By providing a suitable many-one reduction from the **HALTING** problem, prove that **EXACTLY-ONE-HALTS** is undecidable.

(10 points)
(b) Is EXACTLY-ONE-HALTS semi-decidable? Explain your answer.

(5 points)
2.) (a) Consider $\mathcal{T}_{PA}^+$, which is Peano arithmetic with the axioms

\[
\forall x \ (x + 0 = 0) \quad \text{(zero)}
\]
\[
\forall x \forall y \ (x + 1 = y + 1 \rightarrow x = y) \quad \text{(successor)}
\]
\[
F[0] \land (\forall x \ (F[x] \rightarrow F[x + 1])) \rightarrow \forall x \ F[x] \quad \text{(induction)}
\]
\[
\forall x \ (x + 0 = x) \quad \text{(plus zero)}
\]
\[
\forall x \forall y \ (x + (y + 1) = (x + y) + 1) \quad \text{(plus successor)}
\]
\[
\forall x \ (x \cdot 0 = 0) \quad \text{(times zero)}
\]
\[
\forall x \forall y \ (x \cdot (y + 1) = (x \cdot y) + x) \quad \text{(times successor)}
\]

Together with the following additional axioms:

\[
\forall x \ (x^0 = 1) \quad \text{(exp zero)}
\]
\[
\forall x \forall y \ (x^{y+1} = x^y \cdot x) \quad \text{(exp succ)}
\]
\[
\forall x \forall z \ (\exp_3(x, 0, z) = z) \quad \text{(exp}_3 \text{ zero)}
\]
\[
\forall x \forall y \forall z \ (\exp_3(x, y+1, z) = \exp_3(x, y, x \cdot z)) \quad \text{(exp}_3 \text{ succ)}
\]

Show by induction that $\forall x \forall y \ (\exp_3(x, y, 1) = x^y \cdot 1)$ is $\mathcal{T}_{PA}^+$-valid. Use the semantic argument method from the lecture to formally prove the formula in the base case and in the step case. In order to simplify the proof, you may use the formulas $(L): \forall x \ (1 \cdot x = x)$ and $(A): \forall x \forall y \forall z \ (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$ as additional lemmas.

Please be precise and indicate exactly why proof lines follow from some other(s). Moreover, recall that equality handling is performed using equality axioms.

Hint: You need to prove a stronger formula from which $\varphi$ follows.

(12 points)
(b) Apply the Ackermann reduction to the formula

$$\varphi^{EUF}: F(F(x_1)) \models G(x_2, G(x_1, x_3, x_4), F(x_2)) \rightarrow p(x_1, y)$$

and obtain the validity-equivalent formula $$\varphi^E$$.  

(3 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 \( \{ a \geq 0 \land b \geq 0 \} \ p \ \{ a - b + c - d = 0 \} \) is valid with respect to partial correctness where \( p \) is the following program:

\[
\begin{align*}
c &:= 0; \\
d &:= a; \\
\textbf{while} \ b \leq d \ \textbf{do} \\
\quad d &:= d - b; \\
\quad c &:= c + 1; \\
\textbf{od}
\end{align*}
\]

(8 points)
(b) Is the Hoare triple from Exercise 3a totally correct? If yes, provide a variant, otherwise provide a counterexample. In both cases, justify your answer! (2 points)

(c) Let $p$ be a program and let $A, B \in \text{Assn}$. Is the following Hoare rule sound/admissible? If yes, provide a proof. Otherwise, provide a counterexample and argue why it is a counterexample.

\[
\begin{array}{c}
\{A\} \text{ skip; } p \{B\} \\
\{A\} p \{B\}
\end{array}
\]

(5 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 $M_1$:**

**Kripke structure $M_2$:**

(4 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>$((b \land c) U (c))$</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>$AX(a \land b)$</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>$EG(c)$</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>$E[(a \land b \land c) U (a)]$</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td></td>
</tr>
</tbody>
</table>

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

Provide a Kripke structure, which satisfies all of the following CTL* formulas:

\[-q\]

\[\text{AG}p \Rightarrow q\]

\[\text{EF}p\]

\[\text{EFG} \neg p\]

(6 points)