1.) Consider the following problem:

**FIND-INPUT**

**INSTANCE:** A pair \((\Pi, I)\), where (i) \(I\) is a string, and (ii) \(\Pi\) is a program that takes one string as input and returns a string. It is guaranteed that \(\Pi\) terminates on any input.

**QUESTION:** Does there exist a string \(I'\) such that the program \(\Pi\) on input \(I'\) returns \(I\), i.e. \(\Pi(I') = I\)?

Prove that the problem **FIND-INPUT** is semi-decidable. For this, describe a procedure that shows the semi-decidability of the problem (i.e. a semi-decision procedure for **FIND-INPUT**) and argue that it is correct.

Note: we consider only strings that are built from symbols 0 and 1. (15 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! (Hint: Substitution axioms) (9 points)

(b) Let \(\varphi\) be any propositional formula in negation normal form (NNF). Recall that a literal \(\ell\) is pure in a formula \(\varphi\), if the complement of \(\ell\), \(\ell^c\), does not occur in \(\varphi\), where \(\ell^c\) is \(\neg\) if \(\ell\) is \(\neg\) and \(\neg\) if \(\ell\) is \(\neg\).

Prove by induction: If \(\varphi\) contains only pure literals, then \(\varphi\) is satisfiable. (6 points)

3.) Consider the following modified while-rule:

\[
\begin{array}{c}
\{ \text{Inv} \} \ p \ \{ \text{Inv} \} \\
\{ \text{Inv} \} \text{ while } e \text{ do } p \ \text{ od } \{ \text{Inv} \land \neg e \} \\
\end{array}
\]

(a) Show that this rule is admissible regarding partial correctness. (5 points)

(b) Show that the Hoare calculus for partial correctness is no longer complete, if we replace the regular while-rule by the modified one. (10 points)
4.) Model Checking

(a) Provide a non-empty simulation relation $H$ that witnesses $M_1 \leq M_2$, where $M_1$ and $M_2$ are shown below ($M_1$ on the left, $M_2$ on the right), the initial state of $M_1$ is $s_0$, the initial state of $M_2$ is $t_0$:

**Kripke structure $M_1$:**

```
<table>
<thead>
<tr>
<th>State</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>s0</td>
<td>{c}</td>
</tr>
<tr>
<td>s1</td>
<td>{a}</td>
</tr>
<tr>
<td>s2</td>
<td>{a}</td>
</tr>
<tr>
<td>s3</td>
<td>{b}</td>
</tr>
<tr>
<td>s4</td>
<td>{b}</td>
</tr>
<tr>
<td>s5</td>
<td>{b}</td>
</tr>
</tbody>
</table>
```

**Kripke structure $M_2$:**

```
<table>
<thead>
<tr>
<th>State</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>t0</td>
<td>{c}</td>
</tr>
<tr>
<td>t1</td>
<td>{c}</td>
</tr>
<tr>
<td>t2</td>
<td>{b}</td>
</tr>
<tr>
<td>t3</td>
<td>{a}</td>
</tr>
<tr>
<td>t4</td>
<td>{a}</td>
</tr>
</tbody>
</table>
```

(b) Consider the following Kripke structure:

```
<table>
<thead>
<tr>
<th>State</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>s0</td>
<td>a</td>
</tr>
<tr>
<td>s1</td>
<td>c</td>
</tr>
<tr>
<td>s2</td>
<td>a, b, c</td>
</tr>
<tr>
<td>s3</td>
<td>a</td>
</tr>
<tr>
<td>s4</td>
<td>b, c</td>
</tr>
</tbody>
</table>
```

For each of the following formulae
i. determine if the formula is in CTL, LTL, and/or CTL*, and
ii. state on which states $s_i$ the formula holds

- $\text{EG}(a)$
- $\text{EX}(b)$
- $\text{X}(c)$
- $\text{F}(a)$

(c)
Let $M = (S, I, R, L)$ be a Kripke structure over a set of propositional symbols $AP$.

We define a Kripke structure $\hat{M} = (\hat{S}, \hat{I}, \hat{R}, \hat{L})$ as follows:

- $\hat{S} = 2^{AP}$, i.e., a state $\hat{s} \in \hat{S}$ is a subset of $AP$,
- $\hat{I} = \{\hat{s} \in \hat{S} \mid \exists s \in I. L(s) = \hat{s}\}$, i.e., a state $\hat{s} \in \hat{S}$ is an initial state of $\hat{M}$ if there is an initial state $s \in I$ such that $s$ is labeled with $\hat{s}$,
- $\hat{R} = \{((\hat{s}, \hat{t}) \in \hat{S} \times \hat{S} \mid \exists s,t \in S. \hat{s} = L(s) \land \hat{t} = L(t) \land (s,t) \in R\}$, i.e., for each transition $(\hat{s}, \hat{t}) \in \hat{R}$ there are states $s,t \in S$ such that there is a transition from $s$ to $t$ and $s$ is labeled with $\hat{s}$ and $t$ is labeled with $\hat{t}$,
- $\hat{L}(\hat{s}) = \hat{s}$ for all $\hat{s} \in \hat{S}$, i.e., each state $\hat{s} \in \hat{S}$ is labeled with the atomic propositions it contains.

Prove that for any ACTL formula $\varphi$ over propositions from $AP$ the following holds:

If $\hat{M} \models \varphi$, then $M \models \varphi$

Hint: You can use the following theorem from the lecture:

Let $M_1$ and $M_2$ be Kripke structures such that $M_1 \preceq M_2$. Let $\varphi$ be an ACTL* formula.
If $M_2 \models \varphi$, then $M_1 \models \varphi$.

(7 points)