1.) Consider the following decision problem:

<table>
<thead>
<tr>
<th><strong>HALTING AFTER LINE-REMOVAL (HALR)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INSTANCE:</strong> A tuple ((\Pi, I)), where (\Pi) is a program that takes a string as input; (I) a string.</td>
</tr>
<tr>
<td><strong>QUESTION:</strong> Does there exist a line of code in (\Pi), such that when the line is removed from (\Pi), the resulting program (a) is syntactically correct and (b) halts on (I)?</td>
</tr>
</tbody>
</table>

(1) By providing a suitable many-one reduction from the `HALTING` problem, prove that `HALR` is undecidable.

(2) Is `HALR` semi-decidable? Explain your answer.

(15 points)
2.) We consider a slightly restricted and simplified form $M$ of the Ackermann-Péter function, which we discussed in the exercise part.

**Algorithm 1:** The function $M$

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong></td>
<td>$x, y$, two positive integers</td>
</tr>
<tr>
<td><strong>Output:</strong></td>
<td>The computed positive integer value for $x, y$</td>
</tr>
<tr>
<td>1</td>
<td>if $x == 1$ then</td>
</tr>
<tr>
<td>2</td>
<td>return $2y$;</td>
</tr>
<tr>
<td>3</td>
<td>else if $y == 1$ then</td>
</tr>
<tr>
<td>4</td>
<td>return $x$;</td>
</tr>
<tr>
<td>5</td>
<td>else return $M(x - 1, M(x, y - 1))$;</td>
</tr>
</tbody>
</table>

(a) Let $\mathbb{N}$ denote the natural numbers without $0$. Use well-founded induction to show

\[
\forall x \forall y \left((x \in \mathbb{N} \land y \in \mathbb{N}) \rightarrow M(x, y) \geq 2^y\right).
\]

(11 points)

(b) Suppose $\mathcal{M}_C$ is an implementation of $M$ in the C programming language with $x$ and $y$ of type unsigned integers of size 32 bit (i.e., of type `uint32_t`). Is

$M(x', y') = \mathcal{M}_C(x', y')$

true for all integers $x', y'$ satisfying $1 \leq x', y' \leq \text{UINT32}_\text{MAX}$, where $\text{UINT32}_\text{MAX}$ is the largest value for a variable of type `uint32_t`?

If so, then prove this fact. Otherwise provide a counterexample with an exact explanation of what is computed and what is happening.

(4 points)

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

```imp
while $y < 10$ do
  $x := x + z + 1$;
  $z := z + 2$;
  $y := y + 1$
end
```

where $x, y, z$ are program variables. For each Hoare triple below, prove/disprove its total correctness. If the Hoare triple is correct, prove its total correctness by providing a formal proof. If the Hoare triple is not correct, provide a counterexample.

(3a) Hoare triple: $[x = 0 \land y = 0 \land z = 0] \ p [x = 100].$

(3b) Hoare triple: $[x = 0 \land y = 20 \land z = 0] \ p [x = 100].$

(15 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 $M_1$:**

- $s_0: \{a\}$
- $s_1: \{b\}$
- $s_2: \{a\}$
- $s_3: \{c\}$
- $s_4: \{b\}$

**Kripke structure $M_2$:**

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

(5 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>$\text{X}(a \land b)$</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$\text{AX}(b)$</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$\text{EG}(a)$</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$\text{EX}(a \land b)$</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$\text{E}[ (a \land b \land c) \text{ U } (c) ]$</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. $(p U (Xq)) U r \iff p U ((Xq) U r)$

ii. $((Fp) \Rightarrow q) \Rightarrow (p \Rightarrow Fq)$

(5 points)