1.) (a) Consider the following decision problem:

**AT-LEAST-ONE-HALTS (ALOH)**

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 \(\Pi_1(I)\) halt, \(\Pi_2(I)\) halt, or do both halt?

By providing a suitable reduction from the **HALTING** problem, prove that **AT-LEAST-ONE-HALTS** is undecidable.

(10 points)
(b) Is **AT-LEAST-ONE-HALTS** semi-decidable? Explain your answer. (5 points)
2. (a) Show that $a[i] \models e \rightarrow a\langle i\#e \rangle \models a$ is $\mathcal{T}_A^+\text{-valid}$ using the semantic argument method from the lecture. Besides the equality axioms, you have the following ones for the arrays.

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

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

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

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

Besides the axioms, you are allowed to use *modus ponens* and *modus tollens*.

(12 points)
(b) Let \( f(x_1, x_2) = x_1 \oplus x_2 \) and \( f(x_1, \ldots, x_{n+1}) = f(x_1, \ldots, x_n) \oplus x_{n+1} \) for \( n > 2 \).

(i) What is the number of clauses in a satisfiability-equivalent CNF version of \( f(x_1, \ldots, x_n) \).

(ii) What is the number of clauses in a logically equivalent CNF version of \( f(x_1, \ldots, x_n) \).

Explain and justify your answers in detail. (3 points)
3.) (a) Consider the program $p$:

\begin{verbatim}
r := 0;
i := 0;
s := 1;
while i < n do
    r := r + s;
    s := s + 2;
    i := i + 1
end
\end{verbatim}

Let $p' = \text{while } i < n \text{ do } \ldots \text{ od}$ be the while loop of the program $p$. Give an inductive invariant for $p'$, such that the Hoare triple $\{\text{true}\} \ p' \ \{\text{true}\}$ is valid with respect to partial correctness. (2 points)
(b) Let $p$ be the program from exercise 3a. Show that the Hoare triple \( \{ n \geq 0 \} \ p \ \{ r = n \cdot n \} \) is valid with respect to partial correctness. The program $p$ is given again for your convenience:

\[
\begin{align*}
& r := 0; \\
& i := 0; \\
& s := 1; \\
& \textbf{while } i < n \textbf{ do} \\
& \quad r := r + s; \\
& \quad s := s + 2; \\
& \quad i := i + 1 \\
& \textbf{od}
\end{align*}
\]
(c) Is the following Hoare triple valid with respect to total correctness? If yes, prove its validity using the Hoare calculus. Otherwise, provide a counterexample, that is, a state that does not satisfy the correctness assertion.

\[ [n \geq 0] \text{ if } n = 0 \text{ then abort else } m := n \text{ [m = n]} \]

(3 points)
4.) (a) Show that the simulation relation for Kripke structures is transitive, i.e., if $A \leq B$ and $B \leq C$ for some Kripke structures $A, B, C$, then $A \leq C$.

(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, and

ii. list the states $s_i$ on which the formula $\varphi$ holds; i.e. for which states $s_i$ do we have $M, s_i \models \varphi$?

Recall that for an LTL formula $\varphi$ it holds that $M, s \models \varphi \iff M, s \models A\varphi$.

<table>
<thead>
<tr>
<th>$\varphi$</th>
<th>CTL</th>
<th>States $s_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X(a)$</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$(b) \ U (a)$</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$AF(b \land c)$</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$A[(a) \ U (b)]$</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$EF(c)$</td>
<td>☐</td>
<td></td>
</tr>
</tbody>
</table>

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

Prove or disprove that the following formulas are tautologies, i.e., they hold for every Kripke structure $M$ and every path $\pi$:

i. $$(\mathrm{GF}p) \land (\mathrm{GF}q) \Rightarrow \mathrm{G}(p \mathbin{U} q)$$

ii. $$((\mathrm{G}\neg p) \mathbin{U} p) \land \neg p \Rightarrow (\mathrm{G}q) \lor (\neg q \mathbin{U} r)$$

(5 points)