1.) Consider the following problem:

**EXACT HITTING SET (EHS)**

**INSTANCE:** A collection \( C \) of sets of elements.

**QUESTION:** Does there exist a set \( S \) of elements, such that for each \( C \in C \), \(|S \cap C| = 1\), i.e. each set in \( C \) contains exactly one element from \( S \)?

Example: Consider \( C = \{\{a, b, d\}, \{b, c\}, \{c, d\}\} \). \( S = \{a, c\} \) witnesses that \( C \) is a positive instance of **EHS**. On the other hand, \( C' = \{\{a, b, d\}, \{a, b, c\}, \{c, d\}\} \) is a negative instance.

By providing a suitable reduction from the **1-IN-3-SAT** problem, prove that **EXACT-HITTING-SET** is an NP-hard problem. Argue formally that your reduction is correct.

Recall that **1-IN-3-SAT** is defined as follows:

**1-IN-3-SAT**

**INSTANCE:** Boolean formula \( \varphi \) in 3-CNF.

**QUESTION:** Does there exists a satisfying truth assignment \( T \) on \( \varphi \), such that in each clause of \( \varphi \), exactly one literal is true in \( T \)?

**Hint:** For each variable \( v \) in \( \varphi \), use two elements \( v \) and \( \neg v \) in your definition of \( C \). (15 points)

2.) (a) Show that \( b[j] \doteq f \rightarrow b(j \circ f) \doteq b \) is \( T_A^{\sim} \)-valid.

Besides the equality axioms, you have the following ones for the arrays.

i. \( \forall a, i, j \ (i \doteq j \rightarrow a[i] \doteq a[j]) \) (array congruence)

ii. \( \forall a, v, i, j \ (i \doteq j \rightarrow a(i \circ v)[j] \doteq v) \) (read-over-write 1)

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

iv. \( \forall a, b \ (\forall j \ (a[j] \doteq b[j]) \leftrightarrow a \doteq b) \) (extensionality) (12 points)

(b) Consider the clauses \( C_1, \ldots, C_6 \) in **dimacs** format (in this order, shown in the box; recall that 0 indicates the end of a clause) which are given as input to a SAT solver.

- Apply CDCL using the convention that if a variable is assigned as a decision, then it is assigned \( \text{‘true’} \). Select variables as decisions in **increasing** order of their respective integer IDs in the **dimacs** format, starting with variable 1.

- When the first conflict occurs, draw the complete implication graph, mark the first UIP, give the derivation of the learned asserting clause that corresponds to the first UIP, and stop CDCL. You do not have to solve the formula! (3 points)
3.) Show that the following correctness assertion is true with respect to total correctness. Describe the function computed by the program if we consider \( k \) as its input and \( m \) as its output.

Hints: Use the formula \( m^2 \leq k < n^2 \land 0 \leq m < n \leq k + 1 \) as loop invariant. Depending on how you choose the variant, use one of the following annotation rules:

\[
\text{while } e \text{ do} \cdots \text{ od} \mapsto \{ \text{Inv} \}\{ \text{Inv} \land e \land t = t_0 \} \cdots \{ \text{Inv} \land 0 \leq t < t_0 \}\text{ od}\{ \text{Inv} \land \neg e \}
\]

\[
\{ F: k \geq 0 \}
\]
\( m := 0; \)
\( n := k + 1; \)
\( \text{while } m + 1 \neq n \text{ do} \)
\( \quad l := (m + n)/2; \)
\( \quad \text{if } l^2 \leq k \text{ then} \)
\( \quad \quad m := l \)
\( \quad \text{else} \)
\( \quad \quad n := l \)
\( \quad \text{fi} \)
\( \text{od} \)
\( \{ G: m^2 \leq k < (m + 1)^2 \} \)

(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 $M_1$:  
Kripke structure $M_2$:

(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>$F(a \land b)$</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>$AX(b \land c)$</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$EF(c)$</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>$E[(a \land b) ; U ; (b)]$</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td></td>
</tr>
</tbody>
</table>

(5 points)

(c) **LTL tautologies**

Prove or disprove the following LTL formulas:

i. $(\neg Gq) \rightarrow (p \; U \; \neg q)$

ii. $(GFp) \rightarrow (FGp)$

iii. $FXp \rightarrow XFp$

(6 points)