1.) We provide next a reduction from Vertex Cover to Set Cover.

**Vertex Cover:**
Instance: An undirected graph $G = (V,E)$ and integer $k$.
Question: Does there exist a vertex cover $N$ of size $\leq k$? i.e., $N \subseteq V$, s.t. for all $[i,j] \in E$, either $i \in N$ or $j \in N$?

**Set Cover:**
Instance: A finite set $X$ of elements, a collection of $n$ subsets $S_i \subseteq X$, such that every element of $X$ belongs to at least one subset $S_i$, and an integer $m$.
Question: Does there exist a collection $C$ of at most $m$ of these subsets, such that the members of $C$ cover all elements of $X$? i.e., $\bigcup_{S \in C} S = X$.

**Example:** The following Set Cover instance: $X = \{1,2,3,4,5\}, S_1 = \{1,2,3\}, S_2 = \{3,4\}, S_3 = \{1,2,5\}, S_4 = \{4,5\}$ and $m = 2$, is a yes instance, because there exists a collection $C$ with two subsets that cover all elements of $X$: $C = \{S_1, S_3\}$.

**Reduction:** Given an instance of Vertex Cover (i.e. a graph $G = (V, E)$ and an integer $k$), we will construct an instance of the Set Cover problem. Let $X = E$. We will define $n$ subsets of $X$ as follows: label the vertices of $G$ from 1 to $n$, and let $S_i$ be the set of edges that are incident to vertex $i$ (i.e., the edges which have vertex $i$ as an end-point). Note that $S_i \subseteq X$ for all $i$. Furthermore, let $m = k$.

**Example:** Suppose that we are given an instance of Vertex Cover with $G = (V,E), V = \{1,2,3,4,5\}, E = \{e_{12}, e_{13}, e_{14}, e_{15}, e_{34}, e_{45}\}$ ($e_{ij}$ represents an edge connecting vertices $i$ and $j$) and $k = 2$. By the above reduction we get the following Set Cover instance: $X = \{e_{12}, e_{13}, e_{14}, e_{15}, e_{34}, e_{45}\}, m = 2, S_1 = \{e_{12}, e_{13}, e_{14}, e_{15}\}, S_2 = \{e_{12}\}, S_3 = \{e_{13}, e_{34}\}, S_4 = \{e_{14}, e_{34}, e_{45}\}, S_5 = \{e_{15}, e_{45}\}$.

**Task:** Prove the “$\Rightarrow$” direction in the proof of correctness of the reduction, i.e. prove the following statement: if a Vertex Cover instance is a yes instance then the created Set Cover instance is also a yes instance.

**Note:** For any property that you use in your proof, make it perfectly clear why this property holds (e.g., “by the problem reduction”, “by the assumption $X$”, “by the definition $X$”, etc.)

(15 points)

2.) (a) Use Ackermann’s reduction and translate

$$\varphi : \quad F(x_1, b) = F(a, x_2) \rightarrow a = b$$

... to a validity-equivalent E-formula $\varphi^E$.

(5 points)

(b) For the following clause set,

$$(a \lor \neg b \lor d) \quad (\neg b \lor \neg c) \quad (\neg c \lor f) \quad (c \lor \neg d)$$

i. construct the corresponding implication graph with decisions $a = 0, b = 1$ until you reach a conflict.

ii. find all UIPs in the above implication graph, determine the first UIP.

iii. learn a new conflict clause using the first-UIP schema.

(5 points)

(c) Answer the following questions and explain your answers.
3. (a) Extend the programming language introduced in the course by an if-statement without else-branch. Define its syntax, semantics, and a rule for the Hoare calculus. The semantics and the verification rule should not rely on other program statements. (5 points)

(b) Verify that the following program doubles the value of x. For which inputs does it terminate? Choose appropriate pre- and postconditions and show that the assertion is totally correct.

Hint: Use $y = 2x_0 + x$ as a starting point for the invariant, where $x_0$ denotes the initial value of x. You may have to extend the formula to prove termination.

\[
y \leftarrow 3x;
\]
\[
\text{while } 2x \neq y \text{ do }
\]
\[
x \leftarrow x + 1;
\]
\[
y \leftarrow y + 1;
\]
\[
\text{od}
\]

(10 points)

4. AP-deterministic Kripke Structures and Bisimulation.

Let $M_1 = (S_1, I_1, R_1, L_1)$ and $M_2 = (S_2, I_2, R_2, L_2)$ be two Kripke structures.

Remember, a relation $H' \subseteq S_1 \times S_2$ is a bisimulation relation if for each $(s, s') \in H'$ holds:

- $L_1(s) = L_2(s')$,
- for each $(s, t) \in R_1$ there is a $(s', t') \in R_2$ such that $(t, t') \in H'$, and
- for each $(s', t') \in R_2$ there is a $(s, t) \in R_1$ such that $(t, t') \in H'$.

Further remember, $M_1$ and $M_2$ are bisimilar if there is a bisimulation relation $H' \subseteq S_1 \times S_2$ such that:

- for each initial state $s \in I_1$ there is an initial state $s' \in I_2$ with $(s, s') \in H'$, and
- for each initial state $s' \in I_2$ there is an initial state $s \in I_1$ with $(s, s') \in H'$.

In the following, we say that $H'$ witnesses the bisimilarity of $M_1$ and $M_2$ in case $H'$ is a bisimulation relation between $M_1$ and $M_2$ that satisfies the conditions stated above.

A Kripke structure $M = (S, I, R, L)$ over a set of atomic predicates $AP$ is called AP-deterministic, if

(a) for all $A \subseteq AP$ we have $|I \cap \{s \mid L(s) = A\}| \leq 1$, and

(b) for all $s \in S$ we have that $(s, t_1) \in R$, $(s, t_2) \in R$ and $L(t_1) = L(t_2)$ imply $t_1 = t_2$.

We define a sequence of relations $H_n$, for $n \geq 0$:

- $H_0 = \{(s, s') \mid s \in I_1, s' \in I_2, L_1(s) = L_2(s')\}$
- $H_{n+1} = H_n \cup \{(t, t') \mid \exists (s, s') \in H_n, (s, t) \in R_1, (s', t') \in R_2, L_1(t) = L_2(t')\}$

Finally, we define the relation $H$ as follows:

$$H = \bigcup_{n \geq 0} H_n$$
(a) Assume that $M_1$ and $M_2$ are bisimilar and AP-deterministic Kripke structures. Prove that $H$ is a bisimulation relation. Further prove that $H$ is the smallest bisimulation relation that witnesses the bisimilarity of $M_1$ and $M_2$.

*Hint:* Let $H'$ be a bisimulation relation that witnesses the bisimilarity of $M_1$ and $M_2$. Show that, for all $n \geq 0$, $H_n \subseteq H'$ holds and use this fact to show that $H$ satisfies the conditions of a bisimulation relation. \hfill (10 points)

(b) Assume that $M_1$ and $M_2$ are bisimilar. Prove that, in general, $H$ is not a bisimulation relation. \hfill (5 points)