Assignment 2

Hao Dong
h45dong@uwaterloo.ca 20757585

Question 1

a. How many execution paths does Prog1 have? List the paths.

i 1, 2, 3, 4, 8, 9, 10, 11, 12, 13, 17

ii 1, 2, 3, 4, 8, 9, 10, 11, 14, 15, 16, 17

iii 1, 2, 5, 6, 7, 8, 9, 10, 11, 12, 13, 17

iv 1, 2, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16, 17

b. Symbolically execute each path and provide the resulting path condition. Show the table.

Edge	Symbolic State(PV)	Path Condition (PC)
$1 \to 2$	$x \mapsto X_0, y \mapsto Y_0$	true
$2 \to 3$	$x \mapsto X_0, y \mapsto Y_0$	$X_0 + Y_0 > 10$
$3 \to 4$	$x \mapsto X_0 + 1, y \mapsto Y_0$	$X_0 + Y_0 > 10$
$4 \to 8$	$x \mapsto X_0 + 1, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10$
$8 \to 9$	$x \mapsto X_0 + 1, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10$
$9 \to 10$	$x \mapsto X_0 + 3, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10$
$10 \to 11$	$x \mapsto X_0 + 3, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10$
$11 \to 12$	$x \mapsto X_0 + 3, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10 \wedge 2(X_0 + Y_0) - 2 > 27$
$12 \to 13$	$x \mapsto 3(X_0 + 3), y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10 \wedge 2(X_0 + Y_0) - 2 > 27$
$13 \to 17$	$x \mapsto 3(X_0 + 3), y \mapsto 2(Y_0 - 2)$	$X_0 + Y_0 > 10 \wedge 2(X_0 + Y_0) - 2 > 27$

Table 1: symbolic execution table for i

Edge	Symbolic State(PV)	Path Condition (PC)
$1 \to 2$	$x \mapsto X_0, y \mapsto Y_0$	true
$2 \to 3$	$x \mapsto X_0, y \mapsto Y_0$	$X_0 + Y_0 > 10$
$3 \to 4$	$x \mapsto X_0 + 1, y \mapsto Y_0$	$X_0 + Y_0 > 10$
$4 \to 8$	$x \mapsto X_0 + 1, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10$
$8 \to 9$	$x \mapsto X_0 + 1, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10$
$9 \to 10$	$x \mapsto X_0 + 3, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10$
$10 \to 11$	$x \mapsto X_0 + 3, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10$
$11 \to 14$	$x \mapsto X_0 + 3, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10 \wedge 2(X_0 + Y_0) - 2 \leq 27$
$14 \to 15$	$x \mapsto X_0 + 3, y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10 \wedge 2(X_0 + Y_0) - 2 \leq 27$
$15 \to 16$	$x \mapsto 4(X_0 + 3), y \mapsto Y_0 - 2$	$X_0 + Y_0 > 10 \wedge 2(X_0 + Y_0) - 2 \leq 27$
$16 \to 17$	$x \mapsto 4(X_0 + 3), y \mapsto 3Y_0 + 4X_0 + 6$	$X_0 + Y_0 > 10 \wedge 2(X_0 + Y_0) - 2 \leq 27$

Table 2: symbolic execution table for ii

Edge	Symbolic State(PV)	Path Condition (PC)
$1 \to 2$	$x \mapsto X_0, y \mapsto Y_0$	true
$2 \to 5$	$x \mapsto X_0, y \mapsto Y_0$	$X_0 + Y_0 \leq 10$
$5 \to 6$	$x \mapsto X_0, y \mapsto Y_0$	$X_0 + Y_0 \leq 10$
$6 \to 7$	$x \mapsto X_0, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$7 \to 8$	$x \mapsto X_0 - 3, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$8 \to 9$	$x \mapsto X_0 - 3, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$9 \to 10$	$x \mapsto X_0 - 1, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$10 \to 11$	$x \mapsto X_0 - 1, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$11 \to 12$	$x \mapsto X_0 - 1, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10 \wedge 2 * (X_0 + Y_0) + 12 > 27$
$12 \to 13$	$x \mapsto 3(X_0 - 1), y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10 \wedge 2 * (X_0 + Y_0) + 12 > 27$
$13 \to 17$	$x \mapsto 3(X_0 - 1), y \mapsto 2(Y_0 + 7)$	$X_0 + Y_0 \leq 10 \wedge 2 * (X_0 + Y_0) + 12 > 27$

Table 3: symbolic execution table for iii

Edge	Symbolic State(PV)	Path Condition (PC)
$1 \to 2$	$x \mapsto X_0, y \mapsto Y_0$	true
$2 \to 5$	$x \mapsto X_0, y \mapsto Y_0$	$X_0 + Y_0 \leq 10$
$5 \to 6$	$x \mapsto X_0, y \mapsto Y_0$	$X_0 + Y_0 \leq 10$
$6 \to 7$	$x \mapsto X_0, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$7 \to 8$	$x \mapsto X_0 - 3, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$8 \to 9$	$x \mapsto X_0 - 3, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$9 \to 10$	$x \mapsto X_0 - 1, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$10 \to 11$	$x \mapsto X_0 - 1, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10$
$11 \to 14$	$x \mapsto X_0 - 1, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10 \wedge 2 * (X_0 + Y_0) + 12 \leq 27$
$14 \to 15$	$x \mapsto X_0 - 1, y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10 \wedge 2 * (X_0 + Y_0) + 12 \leq 27$
$15 \to 16$	$x \mapsto 4(X_0 - 1), y \mapsto Y_0 + 7$	$X_0 + Y_0 \leq 10 \wedge 2 * (X_0 + Y_0) + 12 \leq 27$
$16 \to 17$	$x \mapsto 4(X_0 - 1), y \mapsto 3Y_0 + 4X_0 + 17$	$X_0 + Y_0 \leq 10 \wedge 2 * (X_0 + Y_0) + 12 \leq 27$

Table 4: symbolic execution table for iv

c. For each path in part (b), indicate whether it is feasible or not. For each feasible path, give values for X_0 and Y_0 that satisfy the path condition.

i Path (i) is feasible. $X_0 = 7, Y_0 = 8$

ii Path(ii) is feasible. $X_0 = 5, Y_0 = 6$

iii Path(iii) is feasible.$X_0 = 5, Y_0 = 4$

iv Path(iv) is feasible. $X_0 = 5, Y_0 = 1$

Question 2

a. Encode the constraint $at - most - one(a_1, a_2, a_3, a_4)$ into an equivalent set of clauses.

$at - most - one(a_1, a_2, a_3, a_4)$ is satisfied if at most one of a_1, a_2, a_3, a_4 is true. Thus, the following must be satisfied:

$$\neg((a_1 \wedge a_2) \vee (a_1 \wedge a_3) \vee (a_1 \wedge a_4) \vee (a_2 \wedge a_3) \vee (a_3 \wedge a_4))$$

which is equivalent to:

$$(\neg a_1 \vee \neg a_2) \wedge (\neg a_1 \vee \neg a_3) \wedge (\neg a_1 \vee \neg a_4) \wedge (\neg a_2 \vee \neg a_3) \wedge (\neg a_2 \vee \neg a_4) \wedge (\neg a_3 \vee \neg a_4)$$

b. Reduce Graph Reachability to Propositional Satisfiability. Specifically, develop a set of clauses in CNF such that $Reachable(G, V, v_{init}, v_{end})$ are satisfiable if and only if there is a path from v_{init} to v_{end} in G.

Each vertex $v \in V$ needs a propositional variable a_v. The constrains needed to be satisfied at the same time (CNF) are as following:

1. The path starts at v_{init} and ends at v_{end}.

$$a_{init} \wedge a_{end}$$

2. For each vertex $v \in V$
   v_{end}, any path that starts from v, that is, any $(v, u) \in E$, proceeds to at least one successor u of v. That is:

$$\neg(a_v \wedge \neg a_{u_1} \wedge \neg a_{u_2} ... \wedge \neg a_{u_k})$$

   which is equivalent to:

$$\neg a_v \vee_{u|(v,u) \in E} a_u$$

Validation:
For the graph in the left part of Figure 1, the constraints are:

$$\neg a_{init} \vee a_1 \vee a_2$$
$$\neg a_1 \vee a_{end}$$
$$\neg a_2 \vee a_{end}$$
$$a_{init} \wedge a_{end}$$

A possible satifying assignment is: $a_{init} \mapsto 1, a_1 \mapsto 1, a_2 \mapsto 1, a_{end} \mapsto 1$.
For the graph in the right part of Figure 1, the constraints are:

$$\neg a_{init} \vee a_1 \vee a_2$$
$$\neg a_1$$
$$\neg a_2$$
$$a_{init} \wedge a_{end}$$

The constraints can not be satisfied.

Question 3

a. Write down quantifier free constraints in First Order Logic to solve the puzzle above for any positive integer n.

$n_{/0}$	constant of the size of square
$Square_{/2}$	value of a square element at a given position eg:$Square(0, 0)$
$Sum_{/n}$	sum of a list of values

$\forall i_1, i_2, j_1, j_2 \cdot 0 \leq i_1 < n \wedge 0 \leq i_2 < n \wedge 0 \leq j_1 < n \wedge 0 \leq j_2 < n \wedge 1 \leq Square(i_1, j_1) \leq n^2 \wedge 1 \leq Square(i_2, j_2) \leq n^2 \wedge (i_1 \neq i_2 \vee j_1 \neq j_2) \Longrightarrow Square(i_1, j_1) \neq Square(i_2, j_2)$

$\forall i \cdot 0 \leq i < n \Longrightarrow Sum(\forall j \cdot 0 \leq j < n \cdot Square(i, j)) = \frac{(1+n^2)n^2}{2n}$
$\forall j \cdot 0 \leq i < n \Longrightarrow Sum(\forall i \cdot 0 \leq j < n \cdot Square(i, j)) = \frac{(1+n^2)n^2}{2n}$
$Sum(\forall i \cdot 0 \leq i < n \cdot Square(i, i)) = \frac{(1+n^2)n^2}{2n}$
$Sum(\forall i \cdot 0 \leq i < n \cdot Square(i, n - i - 1)) = \frac{(1+n^2)n^2}{2n}$

Question 4

(e) Provide a program on which your symbolic execution engine diverges (i.e., takes longer than a few seconds to run).

```
havoc x, y, z;
while (x > 1 and y < 1) or z = 1 do {
    x := x - 1;
    y := y + 1;
    z := z * -1;
    while (x > 10 and y < 1000) or z = 100 do {
        x := x - 1;
        y := y + 1;
        z := z * -1
    }
}
```

Question 5

a. Show whether the following First Order Logic (FOL) sentence is valid or not. Either give a proof of validity, or show a model in which the sentence is false.

$$(\forall \boldsymbol{x} \cdot \exists \boldsymbol{y} \cdot \boldsymbol{P}(\boldsymbol{x}) \vee \boldsymbol{Q}(\boldsymbol{y})) \iff (\forall \boldsymbol{x} \cdot \boldsymbol{P}(\boldsymbol{x})) \vee (\exists \boldsymbol{y} \cdot \boldsymbol{Q}(\boldsymbol{y}))$$

Answer:
Valid. By algebraic manipulation of the formulas:

$$\begin{aligned}
\forall x \cdot \exists y \cdot (P(x) \vee Q(y)) &\equiv \forall x \cdot (\exists y \cdot P(x)) \vee (\exists y \cdot Q(y))) \\
&\equiv \forall x \cdot (P(x) \vee (\exists y \cdot Q(y))) \\
&\equiv (\forall x \cdot P(x)) \vee (\forall x \cdot \exists y \cdot Q(y)) \\
&\equiv (\forall x \cdot P(x)) \vee (\exists y \cdot Q(y))
\end{aligned}$$

b. Question same as above for

$$(\forall \boldsymbol{x} \cdot \exists \boldsymbol{y} \cdot \boldsymbol{P}(\boldsymbol{x}, \boldsymbol{y}) \vee \boldsymbol{Q}(\boldsymbol{x}, \boldsymbol{y})) \implies (\forall \boldsymbol{x} \cdot \exists \boldsymbol{y} \cdot \boldsymbol{P}(\boldsymbol{x}, \boldsymbol{y})) \vee (\forall \boldsymbol{x} \cdot \exists \boldsymbol{y} \cdot \boldsymbol{Q}(\boldsymbol{x}, \boldsymbol{y}))$$

Answer:
The sentence is not valid. Suppose there is a model $M = (S, Q^M, P^M)$ where:

- the universe $S = a, b$
- $Q^M = (b, b)$
- $P^M = (a, a)$

Because $P(a, a), Q(b, b)$ are true in M,it can be deduced that $M \models (\forall x \cdot \exists y \cdot P(x, y) \vee Q(x, y))$. However, neither $\exists y \cdot P(b, y)$ nor $\exists y \cdot Q(a, y)$ are true in M, $M \not\models (\forall x \cdot \exists y \cdot P(x, y)) \vee (\forall x \cdot \exists y \cdot Q(x, y))$. Therefore, the sentence is invalid.

c. Consider the following FOL formula Φ: $\exists x \exists y \exists z(P(x,y) \wedge P(z,y) \wedge P(x,z) \wedge \neg P(z,x))$ For each of the following FOL models, explain whether they satisfy or violate the formulaΦ

a) $M_1 =< S_1, P_1 >$, where $S_1 = \mathbb{N}$, and $P_1 = (x,y)|x,y \in \mathbb{N} \wedge x < y$. Does $M_1 \models \Phi$

Answer:
Satisfy.
For example, $x = 0, z = 1, y = 2$. It satisfies

$$x < y \wedge z < y \wedge x < z \wedge z \not< x$$

, which means satisfying

$$P(x,y) \wedge P(z,y) \wedge P(x,z) \wedge \neg P(z,x)$$

b) $M_2 =< S_2, P_2 >$, where $S_2 = \mathbb{N}$, and $P_2 = (x, x+1)|x \in \mathbb{N} \wedge x < y$. Does $M_2 \models \Phi$

Answer:
Violate.
For proving by contradiction, we assume that there exist $x, y, z \in \mathbb{N}$ that satisfies

$$P(x,y) \wedge P(z,y) \wedge P(x,z) \wedge \neg P(z,x)$$

. That means,

$$y = x+1 \wedge y = z+1 \wedge z = x+1 \wedge x \neq z+1$$

in which the first three equations can lead to the contradiction:

$$y = x+1 \wedge y = x+2$$

So this FOL model violates the formula Φ.

c) $M_3 =< S_3, P_3 >$, where $S_3 = P(\mathbb{N})$, the powerset of natural numbers, and $P_3 = \{(A,B)|A,B \subseteq \mathbb{N} \wedge A \subseteq B\}$. Does $M_3 \models \Phi$

Answer:
Satisfy. For example, $x = \{0\}, z = \{1\}, y = \{0,1\}$. It satisfies

$$x \subseteq y \wedge z \subseteq y \wedge x \subseteq z \wedge z \not\subseteq x$$

, which means satisfying

$$P(x,y) \wedge P(z,y) \wedge P(x,z) \wedge \neg P(z,x)$$

d. Express in FOL: "Location i is a pivot of an array A such that all elements in locations lower than i are less than any elements in locations higher than i".

Answer:
$isArray(A) \wedge 0 \leq i < len(A) \wedge (\forall j,k \cdot 0 \leq j < i < k < len(A) \implies read(A,j) < read(A,k))$

e. Express in FOL: an array A is a permutation of an array B.

Answer:

$Sort_{/1}$ the sorted array

$isArray(A) \wedge isArray(B) \wedge len(A) = len(B) \wedge (\forall i \cdot 0 \leq i < len(A) \implies read(Sort(A),i) = read(Sort(B),i))$

f. Axiomatize Stack operations in FOL with equality by writing a set of FOL formulas.

Answer:

$$empty(nil) = true$$
$$\forall x, y \cdot empty(push(x, y)) = false$$
$$\forall x, y \cdot push(x, y) \neq nil$$
$$\forall x, y \cdot pop(push(x, y)) = x$$
$$\forall x, y \cdot top(push(x, y)) = y$$