Tutorial Letter 201/0/2020

Formal Program Verification

COS4892

Year module

School of Computing

This tutorial letter contains the solutions to Assignment 1.

Define tomorrow.

UNISA university of south africa

Dear Student

Hope you are doing well in these challenging times. This tutorial letter contains the solutions to the first Assignment. Mark allocation is as follows:

The following questions have been marked for a total of 50 marks.

Q1:	6 marks
Q2:	15 marks (3 * 5)
Q4:	19 marks (a-e: 3 * 5 + f-g: 2 * 24)
Q6a:	5 marks
Q7c:	5 marks
Total:	50 marks

Best wishes for your COS4892 studies.

Question 1 6 marks

Define and discuss the difference between formal, syntactic and semantic proofs. Include an example in each discussion.

This question posed no challenges. See prescribed book p23 – 27.

2 marks for each definition and example.

Question 2 15 marks

Consider the well-known puzzles of the island of knights and knaves. The assumptions are that on this island knights always tell the truth and knaves always lie. As a visitor, you will be told some statements, and you must decide whether the islanders you are speaking to are knights or knaves. You meet two islanders A and B. You have to decide what A and B are in each of the following cases. Make use of truth tables and show your workings.

Mark allocation: 5 marks per question.

Expression – 1 mark
Truth table/ calculations – 2 marks
Conclusion – 2 marks

We use the following notation:

$A \equiv$ A is a knight; $B \equiv$ B is a knight;

$\neg A \equiv$ A is a knave; $\neg B \equiv$ B is a knave;

a. A says: I am a knave, but he is not.

- The implications of A's statements:

  $A \equiv \neg A$ [A said: I am a knave]

  $A \equiv B$ [A said: But he is not, therefor B is a knight]

  Combine these two statements together:

  $$A \equiv (\neg A \land B)$$

- Truth table:

A	B	¬A	¬A ∧ B	A ≡ (¬A ∧ B)	
1	1	0	0	0	A is a knight and B is a knight
1	0	0	0	0	A is a knight and B is a knave
0	1	1	1	0	A is a knave and B is a knight
0	0	1	0	1	A is a knave and B is a knave

Therefore, A is a knave and B is a knave

b. A says: If I am a knight then so is he.

- The implications of A's statements:

  $A \equiv (A \Longrightarrow B)$ [A said: If I am a knight, then so is he]

  $A \equiv A \Rightarrow B$

  $=$ { Implication (7.19) }

  Definition of "only-if"
  $p \Rightarrow q \equiv p \equiv p \land q$

  $A \equiv A \equiv A \land B$

  $=$ { Reflexivity of $\equiv$: true $\equiv B \equiv B$ }

  true $\equiv A \land B$

  $=$

  $A \land B$

  Therefore, A and B are both knights

- Truth table:

A	B	A ⇒ B	A ≡ A ⇒ B	A ∧ B	
1	1	1	1	1	A is a knight and B is a knight
1	0	0	0	0	A is a knight and B is a knave
0	1	1	0	0	A is a knave and B is a knight
0	0	1	0	0	A is a knave and B is a knave

Therefore, A and B are both knights

c. A says: We are both knaves.

- The implications of A's statements:

  $A \equiv \neg A$ [A said: We are both knaves]

  $A \equiv \neg B$

  Combine these two statements together:

  $$A \equiv \neg A \land \neg B$$

- Truth table:

A	B	$\neg A$	$\neg B$	$\neg A \land \neg B$	$A \equiv \neg A \land \neg B$	
1	1	0	0	0	0	A is a knight and B is a knight
1	0	0	1	0	0	A is a knight and B is a knave
0	1	1	0	0	1	A is a knave and B is a knight
0	0	1	1	1	0	A is a knave and B is a knave

Therefore, A is a knave and B is a and B are both knaves

‘

Question 3

While walking through the island of knights and knaves, you encounter three inhabitants guarding a bridge. Each is either a knight, who always tells the truth, or a knave, who always lies. Each guard makes a single statement. The guards will not let you pass until you correctly identify each as either a knight or a knave in each of the following cases.

a. Guard 1: I am a knight.
   Guard 2: I am a knight.
   Guard 3: At least two of us are knaves.

b. Guard 1: I am a knight.
   Guard 2: I am a knave .
   Guard 3: At most one of us is a knight.

Exercises 7.36 and 7.37 are like these questions. You will not be expected to attempt questions of this length in summative assessment.

Question 4 19 marks

a. Discuss and define the floor function.

The floor function is discussed on p71 and p72 in the textbook. Ensure that your discussion include and discuss definition 6.1 on p 72.

b. Evaluate the floor function of 6.5 and -6.5 and explain your answer.

The floor of a real number is the last integer number greater than or equal to the given number. In the case of 6.5, the integer greater than 6.5 are 6, 7,8,… The smallest of all is 6.

Therefore $\lfloor 6.5 \rfloor = 6$.

In the case of and $\lfloor -6.5 \rfloor$, the integers that are greater than -6.5 are -7, -6, -5… The smallest of them is -7. Therefore, $\lfloor -6.5 \rfloor = -7$

c. Find all the values of x that satisfy $\lfloor 0.5 + \lfloor x \rfloor \rfloor = 20$. Hint: Let $\lfloor x \rfloor = y$.

$\lfloor 0.5 + y \rfloor = 20$

$\equiv$ $20 - \lfloor 0.5 + y \rfloor$ Symmetry

$\equiv$ $20 \leq 0.5 + y < 20 + 1$

$\equiv$ $19.5 \leq y < 20.5$

Since y is an integer and y = 20 is the only integer in the interval, this becomes

$y = 20 = \lfloor x \rfloor$

$20 \leq x < 21$

Any value less than 21 and greater or equal than 20 will satisfy this equation.

Therefore, all the real numbers such that $20 \leq x < 21$.

d. Find all the values of x that satisfy $\lfloor 5 - \lfloor x \rfloor \rfloor = 15$. Hint: Let $\lfloor x \rfloor = y$.

$15 \leq 5 - y < 16$

$\equiv$ $10 \leq - y < 11$

$\equiv$ $-11 < y \leq -10$

Therefore $\lfloor x \rfloor = -10$.

$-10 = \lfloor x \rfloor$

$-10 \leq x < -9$

Any value greater than -10 and greater or equal than -9 will satisfy this equation.

Therefore, all the real numbers such that $-10 \leq x < -9$.

e. Give a counter example to disprove the following:

$$\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$$

Counter example: $x = 0.5$ and $y = 0.5$

$\lceil x + y \rceil \quad = \lceil 0.5 + 0.5 \rceil \;\; = 1$

$\lceil x \rceil + \lceil y \rceil \quad = \lceil 0.5 \rceil + \lceil 0.5 \rceil$

$= \;\; 1 \;\; + \;\; 1$

$= \qquad 2$

And $1 \neq 2$

f. Prove the following property of the floor function:

$\lfloor x + n \rfloor = \lfloor x \rfloor + n$, where n is any integer.

Suppose $\lfloor x \rfloor = m$ where m is an integer.

$\lfloor x \rfloor = m$

$\equiv \quad m \leq x \leq m + 1$

$\equiv \quad m + n \leq x + n \leq m + n + 1$

$\equiv \quad \lfloor x + n \rfloor = m + n$

$\equiv \quad \lfloor x \rfloor \; + n$

g. Use the floor function to compute the following:

- 3850 div 17

  $= \lfloor \frac{3850}{17} \rfloor$

  $= \lfloor 226.4705 \rfloor$

  $= 226$

- 3850 mod 17

  $= 3850 - 17. \lfloor \frac{3850}{17} \rfloor$

  $= 3850 - 17.226$

  $= 3850 - 3842$

  $= 8$

Question 5

Using A, B and/or C to represent arbitrary expressions, prove the symmetry, associativity and transitivity of boolean equality by using truth tables.

Answer:

Symmetry: (A = B) = (B = A)

A	B	A = B	B = A
		1	2
1	1	1	1
1	0	0	0
0	1	0	0
0	0	1	1

As the values in columns marked 1 and 2 is the same, therefore the Boolean equality is symmetric.

Associativity: ((A = B) = C) = (A = (B = C)

A	B	C	A = B	(A = B) = C	B = C	A = (B = C)
				1		2
1	1	1	1	1	1	1
1	1	0	1	0	0	0
1	0	1	0	0	0	0
1	0	0	0	1	1	1
0	1	1	0	0	1	0
0	1	0	0	1	0	1
0	0	1	1	1	0	1
0	0	0	1	0	1	0

As the values in columns marked 1 and 2 is the same, therefore the Boolean equality is associative.

Transitivity: **A = B and B = C, then A = C**

A	B	C	A = B	B = C	A = C	A = C
1	2	3	4	5	1 = 3 6	4 = 5 7
1	1	1	1	1	1	1
1	1	0	1	0	0	0
1	0	1	0	0	1	1
1	0	0	0	1	0	0
0	1	1	0	1	0	0
0	1	0	0	0	1	1
0	0	1	1	0	0	0
0	0	0	1	1	1	1

As the values in columns marked 6 and 7 is the same, therefore the Boolean equality is transitive.

Question 6

A tautology is a propositional expression that is always true. Two methods available to determine whether a propositional expression is a tautology are 1) truth tables and 2) logical equivalences. Use the theory introduced in Chapter 5 as well as the equivalences in the Appendix of RB to determine whether the propositional expressions below are a tautology or not, first by employing truth tables and second by using logical equivalences.

a. $(((A \wedge B) \Rightarrow C) \wedge (A \Rightarrow B)) \Rightarrow (A \Rightarrow C)$

Truth table

A	*B*	*C*	*A ⋀ B*	*⇒ C*	*A ⇒ B*	*1 ∧ 2*	*A ⇒ C*	*3 ⇒ 4*
				1	*2*	*3*	*4*	
1	1	1	1	1	1	1	1	1
1	1	0	1	0	1	0	0	1
1	0	1	0	1	0	0	1	1
1	0	0	0	1	0	0	0	1
0	1	1	0	1	1	1	1	1
0	1	0	0	1	1	1	1	1
0	0	1	0	1	1	1	1	1
0	0	0	0	1	1	1	1	1

Conclusion, $(((A \wedge B) \Rightarrow C) \wedge (A \Rightarrow B)) \Rightarrow (A \Rightarrow C)$ is a tautology (all true)

Proof

$(((A \land B) \Rightarrow C) \land (A \Rightarrow B)) \Rightarrow (A \Rightarrow C)$

$p \Rightarrow q = \neg(p \land q) = \neg p \lor q$

It can help if one start with the innermost expressions:

$(A \land B) \Rightarrow C) \equiv (\neg(A \land B) \lor C$ Implication (7.19)

$\equiv (\neg A \lor \neg B \lor C)$

$(A \Rightarrow B) \equiv (\neg A \lor B)$

$(A \Rightarrow C) \equiv (\neg A \lor C)$

$\neg\neg p \equiv p$

$(((A \land B) \Rightarrow C) \land (A \Rightarrow B)) \Rightarrow (A \Rightarrow C)$

$\equiv \neg\, [((\neg A \lor \neg B) \lor C)) \land (\neg A \lor B)] \lor (\neg A \lor C)$

$\equiv (A \lor B \lor \neg C) \lor \neg(\neg A \lor B)) \lor (\neg A \lor C)$ Double negation

$\equiv (A \lor B \lor \neg C) \lor (A \lor \neg B) \lor (\neg A \lor C)$ Double negation

$\equiv (A \lor (B \lor \neg B \lor \neg C)) \lor (\neg A \lor C)$ Distributivity

$\equiv (A \lor (B \lor \neg B) \lor \neg C) \lor (\neg A \lor C)$ Associativity

$\equiv (A \lor \neg A) \lor (\neg C \lor C)$

$\equiv$ true $\lor$ true

$\equiv$ true

Conclusion, $(((A \land B) \Rightarrow C) \land (A \Rightarrow B)) \Rightarrow (A \Rightarrow C)$ is a tautology

b. $(\neg A \Rightarrow B) \land (\neg (\neg A \Rightarrow (B \lor C))) \Rightarrow (\neg B \Rightarrow C)$

Truth table

A	*B*	*C*	*¬A*	*¬C*	*¬A ⇒ B*	*B ∨ C*	*(¬A ⇒ 2)*	*¬3*	*¬B ⇒ C*	*4 ⇒ 5*
					1	*2*	*3*	*4*	*5*	
1	1	1	0	0	1	1	1	0	1	1
1	1	0	0	1	1	1	1	0	1	1
1	0	1	0	0	1	1	1	0	1	1
1	0	0	0	1	1	0	1	0	0	1
0	1	1	1	0	1	1	1	0	1	1
0	1	0	1	1	1	1	1	0	1	1
0	0	1	1	0	0	1	1	0	1	1
0	0	0	1	1	0	0	0	1	0	1

Conclusion, $(\neg A \Rightarrow B) \land (\neg (\neg A \Rightarrow (B \lor C))) \Rightarrow (\neg B \Rightarrow C)$ is a tautology (all true)

Proof

(¬ A ⇒ B) ∧ (¬ (¬A ⇒ (B ∨ C)) ⇒ (¬B ⇒ C)

Start by addressing each component of the expression individually.

(¬ A ⇒ B) (Implication 7.19) ¬(¬ A ∧ B) (double negation) A ⋁ B	∧	¬(¬A ⇒ (B ∨ C)) (Implication 7.19) ¬[¬(¬A) ¬ (B ∨ C)] (Double negation) ¬[A ⋀ (B ∨ C)] (Negation) ¬A ∨ ¬(B ⋀ C) ¬A ∨ ¬B ∨ ¬C	⇒	(¬B ⇒ C) (Implication 7.19) ¬ (¬B ∨ C) (Negation) B ∨ ¬C
A ⋀ ¬A ∨¬B ∨¬B ∨¬C) false ⋁¬B ∨¬C B ∨ ¬C			⇒	B ∨ ¬C
true				

Conclusion, (¬ A ⇒ B) ∧ (¬ (¬A ⇒ (B ∨ C)) ⇒ (¬B ⇒ C) is a tautology

c. (¬A ∨ ¬B) ⇔ (A ⇒ ¬B)

Truth table :

A	*B*	*¬A*	*¬B*	*¬A ⋁ ¬B*	*A ⇒ ¬B*	*1 ≡ 2*
				1	*2*	
1	1	0	0	0	0	1
1	0	0	1	1	1	1
0	1	1	0	1	1	1
0	0	1	1	1	1	1

Conclusion, (¬A ∨ ¬B) ⇔ (A ⇒ ¬B) is a tautology (all true)

p ⇒ q = ¬(p⋀ q) = ¬p ∨ q

Proof:

¬A ∨ ¬B ≡ ¬A ∨ ¬B Implication (7.19)

true

Conclusion, (¬A ∨ ¬B) ⇔ (A ⇒ ¬B) is a tautology

Question 7

Prove that the following propositional expressions hold by using logical equivalences:

a. $(A \wedge C) \vee (B \wedge C) \equiv (A \wedge B) \vee C$

Start with the left-hand side:

$\mathbf{(A \wedge C) \vee (B \wedge C)}$

= { symmetry }

$(C \wedge A) \vee (C \wedge B)$

= { distributivity $(p \wedge q) \vee (p \wedge r) \equiv p \wedge (q \vee r)$ }

$(C \wedge A) \vee C) \wedge (C \wedge A) \vee B)$

= { absorption $p \vee (p \wedge q) \equiv p$
$(p \wedge q) \vee p \equiv p$ (symmetry) }

$C \wedge ((C \wedge A) \vee B)$

= { distributivity $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ }

$C \wedge (C \vee B) \wedge (A \vee B)$

= { absorption $p \wedge (p \vee q) \equiv p$ }

$C \wedge (A \vee B)$

= { symmetry $p \wedge (p \vee q) \equiv p$ }

$\mathbf{(A \vee B) \wedge C}$

As $(A \wedge C) \vee (B \wedge C)$is not equivalent to $(A \wedge B) \vee C)$, the expression does not hold.

b. $\neg(A \vee B) \equiv (A \vee \neg B)$

Start with the right-hand side:

$\mathbf{A \vee \neg B}$

= { Definition of false }

$A \vee (B \equiv \text{false})$

= { Associativity of disjunction }

$(A \vee B) \equiv \text{false}$

= { Unit of disjunction: $p \vee \text{false} = p$ }

$\mathbf{(A \vee B)}$

As $\neg(A \vee B)$ is not equivalent to $(A \vee \neg B)$, the expression dos not hold.

c. $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

Start with the right-hand side:

$$
\begin{array}{lll}
 & \mathbf{(A \vee C) \wedge (B \vee C)} & \\
= & \{ \ \text{distributivity} & (p \vee q) \wedge (p \vee r) \ \equiv \ p \vee (q \wedge r) \quad \} \\
 & ((A \vee B) \wedge A) \vee ((A \vee B) \wedge C) & \\
= & \{ \ \text{absorption} & p \wedge (p \vee q) \equiv \ p \quad \} \\
 & A \ \vee ((A \vee B) \wedge C) & \\
 & \{ \ \text{distributivity} & p \vee (q \wedge r) \equiv \ (p \vee q) \wedge (p \vee r) \quad \} \\
 & (A \vee (C \wedge A) \vee (C \wedge B) & \\
= & \{ \ \text{symmetry} & \quad \} \\
 & (A \vee (A \wedge C)) \vee (B \wedge C) & \\
= & \{ \ \text{absorption} & p \wedge (p \vee q) \equiv \ p \quad \} \\
 & \mathbf{A \vee (B \wedge C)} &
\end{array}
$$

As $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$, the expression holds.