COS4892 Assignment 1 - 816353

Christopher Deon Steenkamp - 36398934

Question 1

There are three broad techniques of providing proofs, namely Formal, Informal and Calculational.

Formal Proofs

Formal proofs are those which use purely mathematical notation as a means of proving a sone conjectured theory. They provide the sequence of steps to move from the premises to the conclusion, where each step relies either on something that was proved in a previous step, or something which is known to be a well established fact. These types of proofs are typically constructed in such a way that make them easy to verify that the steps are correct but they do not make it clear why a particular approach was taken and so it is not easy to apply the proof to another problem of a similar form.

As an example:
Suppose x and y are even integers. We must show that $x + y$ is even. By definition of even, we have that $x = 2k$ and $y = 2m$, with $k, m \in \mathbb{Z}$. Then

$$\begin{aligned} x + y &= 2k + 2m && \text{(substitution)} \\ &= 2(k + m) && \text{(factoring out 2)} \\ &= 2n && \text{(let } n = k + m\text{)} \end{aligned}$$

$\therefore x + y$ is even.

Semantic Proofs

Semantic proofs are an informal method of proof. They are a very common proof technique as they make use of a combination of natural language for the outline of the proof and mathematical calculations where more detailed explanations are required. Semantic proofs require the reader to have a good understanding of the problem domain and the the language and mathematical notation used. They are known as semantic proofs because they require the reader to understand the meaning of the words and phrases used to explain the proof. Because of their reliance on meaning, semantic proofs are difficult to check for validity.

As an example, the same proof as given earlier, written informally would look like the following:
Consider two even integers x and y. Since they are even, they can be written as $x = 2k$ and $y = 2m$, respectively, for integers k and m. Then the sum $x + y = 2a + 2b = 2(a + b)$. Therefore $x + y$ has 2 as a factor and, by definition, is even. Hence, the sum of any two even integers is even.

Syntactic Proofs

Syntactic proofs use calculational methods to show that certain unknown properties are true given a particular problem statement. I.e. we use syntactic proofs to show that certain relationships hold between the elements given in the problem statement. These types of proof are great at discovering unknown / unconsidered properties.

As an example:

$$
\begin{array}{rr}
 & x+y \text{ is even } \equiv x \text{ is even } \equiv y \text{ is even} \\
= & \{\text{equivalence is associative}\} \\
 & (x+y \text{ is even } \equiv x \text{ is even}) \equiv y \text{ is even} \\
= & \{\text{equivalence is associative}\} \\
 & x+y \text{ is even } \equiv (x \text{ is even } \equiv y \text{ is even})
\end{array}
$$

Which, in addition to showing that the sum of two even numbers is even, also shows that the addition of two odd numbers is even as well. This method of proof also highlights that the addition of x to y does not change the parity of x when y is even.

Question 2

2 (a)

Equivalence to prove: $A \equiv \neg A \wedge B$

A	B	$\neg A$	$\neg A \wedge B$	$A \equiv \neg A \wedge B$
T	T	F	F	F
T	F	F	F	F
F	T	T	T	F
F	F	T	F	T

The last row of the truth table is the only one where the equivalence is *true* and this is where both A and B are $false$.

From this we know that A and B are both knaves.

2 (b)

Equivalence to prove: $A \equiv A \Rightarrow B$

A	B	$A \Rightarrow B$	$A \equiv A \Rightarrow B$
T	T	T	T
T	F	F	F
F	T	T	F
F	F	T	F

The first row of the truth table is the only one where the equivalence is *true* and this is where both A and B are *true*.

From this we know that A and B are both knights.

2 (c)

Equivalence to prove: $A \equiv \neg A \wedge \neg B$

A	B	$\neg A$	$\neg B$	$\neg A \wedge \neg B$	$A \equiv \neg A \wedge \neg B$
T	T	F	F	F	F
T	F	F	T	F	F
F	T	T	F	F	T
F	F	T	T	T	F

The second last row of the truth table is the only one where the equivalence is $true$ and this is where A is $false$ and B is $true$.

From this we know that A is a knave and B is a knight.

Question 3

3 (a)

Let A be that Guard1 is a knight, B be that Guard2 is a knight and C be that Guard3 is a knight. Also, let a be that the statement made by Guard1 is $true$, b be that the statement made by Guard2 is $true$ and c be that the statement made by Guard3 is $true$.

Let the statements made by the guards be the following:

1. $a \equiv A$
2. $b \equiv B$
3. $c \equiv (\neg A \wedge \neg B) \vee (\neg A \wedge \neg C) \vee (\neg B \wedge \neg C)$

3 (b)

Let A be that Guard1 is a knight, B be that Guard2 is a knight and C be that Guard3 is a knight. Also, let a be that the statement made by Guard1 is $true$, b be that the statement made by Guard2 is $true$ and c be that the statement made by Guard3 is $true$.

Then we have:

1. $a \equiv A$
2. $b \equiv \neg B$
3. $c \equiv \neg\big((A \wedge B) \vee (A \wedge C) \vee (B \wedge C)\big)$

Question 4

4(a)

The floor function is a function which maps a real value to an integer in a very specific way. It does this conversion by rounding in a leftwards direction on the number line (i.e. round down towards 0 for postive real inputs and away from 0 for negative real inputs).

It is defined as:

$$\begin{aligned} &\forall x \in \mathbb{R}, n \in \mathbb{Z} \\ n \leq \lfloor x \rfloor &\equiv n \leq x \end{aligned}$$

4(b)

$\lfloor 6.5 \rfloor = 6$ (Going with the definition of rounding leftwards on the number line we have that 6 is to the left of 6.5)

Formally,

$$\begin{aligned} 6 &\leq \lfloor 6.5 \rfloor \\ &\leq 6 \end{aligned}$$

$$\text{and also } 6 \leq 6.5$$

For the floor of a negative number we have the following:

$\lfloor -6.5 \rfloor = -7$ (Going with the definition of rounding leftwards on the number line we have that -7 is to the left of -6.5)

Formally,

$$
\begin{aligned}
-7 &\leq \lfloor -6.5 \rfloor \\
&\leq -7
\end{aligned}
$$

$$\text{and also } -7 \leq -6.5$$

4(c)

$20 \leq x < 21, x \in \mathbb{R}$

4(d)

$-10 \leq x < -9, x \in \mathbb{R}$

4(e)

Let $x = 1.5$ and $y = 1.3$, then:

$$
\begin{aligned}
\lceil 1.5 + 1.3 \rceil &= \lceil 2.8 \rceil \\
&= 3 \\
\text{But,} & \\
\lceil 1.5 \rceil + \lceil 1.3 \rceil &= 2 + 2 \\
&= 4
\end{aligned}
$$

Thus we have shown that $\lceil x + y \rceil \neq \lceil x \rceil + \lceil y \rceil$

4(f)

$$
\begin{aligned}
&\text{For all } m \in \mathbb{Z} \\
&\quad m \leq \lfloor x + n \rfloor \\
&= && \{\text{definition of floor}\} \\
&\quad m \leq x + n \\
&= && \{\text{arithmetic}\} \\
&\quad m - n \leq x \\
&= && \{\text{definition of floor}\} \\
&\quad m - n \leq \lfloor x \rfloor \\
&= && \{\text{arithmetic}\} \\
&\quad m \leq \lfloor x \rfloor + n
\end{aligned}
$$

We have shown that $m \leq \lfloor x + n \rfloor \equiv m \leq \lfloor x \rfloor + n$.

We can further show that because the above equivalence is of the form $n \leq l \equiv n \leq m$, and by indirect equivalence that $l = m$, that $\lfloor x + n \rfloor = \lfloor x \rfloor + n$.

4(g)

Let $DIV(x, y) = \lfloor x/y \rfloor$

Let $MOD(x, y) = x - (DIV(x, y) \times y)$

Then, with $x = 3850$ and $y = 17$

$$\begin{aligned} DIV &= \lfloor 3850/17 \rfloor \\ &= \lfloor 226.4705882 \rfloor \\ &= 226 \end{aligned}$$

And

$$\begin{aligned} MOD &= 3850 - (DIV(3850, 17) \times 17) \\ &= 3850 - (226 \times 17) \\ &= 3850 - 3842 \\ &= 8 \end{aligned}$$

Question 5

Symmetry

A	B	$A = B$	$B = A$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	T	T

The truth values for $A = B$ and $B = A$ are equivalent and so we have proven that boolean equality is symmetric.

Associativity

A	B	C	$A = B$	$B = C$	$A = (B = C)$	$(A = B) = C$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	T	T	T
F	T	T	F	T	F	F
F	T	F	F	F	T	T
F	F	T	T	F	T	T
F	F	F	T	T	F	F

The truth values for $A = (B = C)$ and $(A = B) = C$ are equivalent and so we have proven that boolean equality is associative.

Transitivity

A	B	C	$A = B$	$B = C$	$(A = B) \wedge (B = C)$	$A = C$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	T
T	F	F	F	T	F	F
F	T	T	F	T	F	F
F	T	F	F	F	F	T

A	B	C	$A = B$	$B = C$	$(A = B) \wedge (B = C)$	$A = C$
F	F	T	T	F	F	F
F	F	F	T	T	T	T

It can be seen from the truth table that whenever both $A = B$ and $B = C$ are true, then $A = C$ is true also. Thus we have proven that equality is transitive.

Question 6

6 (a)

$x = (((A \wedge B) \Rightarrow C) \wedge (A \Rightarrow B)) \Rightarrow (A \Rightarrow C)$

A	B	C	$A \wedge B$	$(A \wedge B) \Rightarrow C$	$A \Rightarrow B$	$A \Rightarrow C$	x
T	T	T	T	T	T	T	T
T	T	F	T	F	T	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	F	T	T	T	T
F	T	F	F	T	T	T	T
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

All values in the final column show that the formula x is a tautology.

6 (b)

$x = (\neg(A \Rightarrow B) \wedge (\neg(\neg A \Rightarrow (B \vee C)))) \Rightarrow (\neg B \Rightarrow C)$

A	B	C	$\neg(A \Rightarrow B)$	$\neg(\neg A \Rightarrow (B \vee C))$	$\neg B \Rightarrow C$	x
T	T	T	F	F	T	T
T	T	F	F	F	F	T
T	F	T	T	F	T	T
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	T	F	F	F	T	T
F	F	T	F	F	T	T
F	F	F	F	T	T	T

All values in the final column show that the formula x is a tautology.

6 (c)

$x = (\neg A \vee \neg B) \Leftrightarrow (A \Rightarrow \neg B)$

A	B	$\neg A \vee \neg B$	$A \Rightarrow \neg B$	$(\neg A \vee \neg B) \Rightarrow (A \Rightarrow \neg B)$	$(A \Rightarrow \neg B) \Rightarrow (\neg A \vee \neg B)$
T	T	F	F	T	T
T	F	T	T	T	T
F	T	T	T	T	T
F	F	T	T	T	T

All values in the last two columns are the same, which indicates equivalence between the two implications and because they are all *true* it shows that both formulas (and by implication, formula x) are all tautologies.

Question 7

7 (a)

7 (b)

7 (c)