CS1231/CS1231S: Discrete Structures

Tutorial #1: Propositional Logic and Proofs

Answers

Tutorials are meant to reinforce topics taught in lectures. Please try these questions on your own before coming to tutorial. In doing so, you may discover gaps in your understanding. Usually, a tutorial has a mix of easy, moderate and slightly challenging questions. It is perfectly fine if you cannot do some of the questions, but attempt them nonetheless, to at least get some partial solution.

You will be asked to present your answers. Your tutor's job is to guide you, not to provide the answers for you. Also, please keep in mind that the goal of tutorials is not to answer every question here, but to clarify doubts and reinforce concepts. Solutions to all tutorial questions will be given in the following week, but please treat them as a guide, for there are usually alternative ways of solving a problem.

You are also encouraged to raise your doubts or questions on the LumiNUS "Tutorials" forum.

Tutorials are important so attendance is taken and it contributes 5% of your final grade. If you miss a tutorial with valid reason (eg: due to illness), please submit your document (eg: medical certificate) to your respective tutor (softcopy or hardcopy) in advance or within three days after your absence and you will not be penalized for your absence. You are to stick with your officially assigned tutorial group (we give exception for first week of tutorial), or your attendance will not be taken. If you need to join a different group for just once for valid reason, please email Aaron (tantc@comp.nus.edu.sg) in advance citing your reason.

Discussion Questions

To encourage discussion on LumiNUS forum, the questions in this section will not be discussed in tutorial. You may discuss them or post your answer on LumiNUS forum.

D1. We discussed in class that English is an ambiguous language. Often, it also carries notions of perception, past experiences, cause and effect, etc. For example, in saying "today is rainy but hot", we use "but" because we often associate a rainy day as a cool day. In logic, we write "today is rainy" $\wedge$ "today is hot".

Restate the following symbolically. You may introduce your own statement variables.

(a) $P(B) \leq P(A)$ whenever $B \subseteq A$.

(b) If $A - B$ is countable, then A is countable or B is uncountable.

(c) An undirected graph (V, E) that is connected and acyclic must have $|E| = |V| - 1$.

D2. Use the laws given in **Theorem 2.1.1 (Epp)** and the **implication law** to prove that the following are tautologies.

(a) $(p \wedge q) \rightarrow p$

(b) $\big((p \vee q) \wedge \sim p\big) \rightarrow q$

(c) $\big((p \rightarrow q) \wedge p\big) \rightarrow q$

(d) $\big(\sim p \rightarrow (q \wedge \sim q)\big) \rightarrow p$

Mathematical arguments are often constructed by using one implication (conditional statement) after another. Logically speaking, such an argument is constructed by using implications that are tautologies, like the ones above. For example, (c) is *modus ponens* and (d) is proof by contradiction. Part (b) is used in problems like Knights and Knaves in Q8 below.

D3. The island of Wantuutrewan is inhabited by two types of people: **knights** who always tell the truth and **knaves** who always lie. Wala comes to a fork in a road on the island. One branch leads to the ancient ruins Wala wants to visit, and the other branch leads deep into the deadly jungle. At the fork stand two natives, one is a knight and the other a knave, who know each other well. However, Wala has no idea who is the knight and who is the knave.

Wala wants to ask for direction to the ruins, but he is allowed to ask only one question to one of the two natives, and the natives, who understand English but cannot speak it, can only point with their fingers. What single question should Wala ask so that he is sure to take the branch leading to the ruins and not the jungle?

(There is more than one possible answer.)

D4. Let p stand for the proposition "I went to Universal Studios Singapore" and q stand for "I rode the Battlestar Galactica". Express the following as natural English sentences. For part (f), express it in English before and after simplifying the given proposition.

(a) $\sim p$

(b) $p \vee q$

(c) $p \wedge \sim q$

(d) $p \rightarrow q$

(e) $\sim p \rightarrow \sim q$

(f) $\sim p \vee (p \wedge q)$

D5. Mala has hidden her treasure somewhere on her property. She left a note in which she listed five statements (a-e below) and challenged the reader to use them to figure out the location of the treasure.

(a) If this house is next to a lake, then the treasure is not in the kitchen.

(b) If the tree in the front yard is an elm, then the treasure is in the kitchen.

(c) If the tree in the back yard is an oak, then the treasure is in the garage.

(d) The tree in the front yard us an elm or the treasure is buried under the flagpole.

(e) The house is next to a lake.

Where has Mala hidden her treasure?

Tutorial Questions

1. Are the following statements true or false?

   a. Assuming that a is a real number, the negation of "$1 < a < 5$" is "$1 \geq a \geq 5$".

   b. In propositional logic, "he's welcome to come along only if he behaves himself" means "if he behaves himself then he's welcome to come along."

   Answers:

   a. The statement of the form "$1 < a < 5$" is short-form for "$(1 < a)$ and $(a < 5)$". By De Morgan's law, its negation is "$(1 \geq a)$ or $(a \geq 5)$". Whereas "$1 \geq a \geq 5$" means "$(1 \geq a)$ and $(a \geq 5)$". Therefore, (a) is false.

   b. Let p be "he's welcome to come along" and q be "he behaves himself". "p only if q" means that "p can hold only in the situations where q holds". In other words, if q does not hold, then p does not hold, which is equivalent to "$\sim q \rightarrow \sim p$", which is in turn logically equivalent to its contrapositive "$p \rightarrow q$".

      Hence, the statement "he's welcome to come along only if he behaves himself" is equivalent to "if he's welcome to come along, then he behaves himself". Therefore, (b) is false.

      Recap: "p only if q" is logically equivalent to "if p then q" (or "$p \rightarrow q$").

2. Simplify the propositions below using the laws given in **Theorem 2.1.1 (Epp)** and the **implication law** (if necessary) with only negation ($\sim$), conjunction ($\wedge$) and disjunction ($\vee$) in your final answers. Supply a justification for every step.

   For the first half of the module, we want students to cite justification <u>for every step</u>. This is to ensure that you do not arrive at the answer by coincidence. Only after you have gained sufficient experience then would we relax this and allow you to skip obvious steps, or combine multiple steps in a line.

   a. $\sim a \wedge (\sim a \rightarrow (a \wedge b))$

      Raflee worked out his answer as shown below. However, he skipped some steps and hence his answer will not be awarded full credit. Can you point out the omissions? (Note: To show that two logical statements are equivalent, we use $\equiv$, not $=$.)

      $\sim a \wedge (\sim a \rightarrow (a \wedge b))$
      $\equiv \sim a \wedge (a \vee (a \wedge b))$ by the implication law (step 1)
      $\equiv \sim a \wedge a$ by the absorption law (step 2)
      $\equiv$ **false** by the negation law (step 3)

   b. $(p \vee \sim q) \rightarrow q$

   c. $\sim(p \vee \sim q) \vee (\sim p \wedge \sim q)$

   d. $(p \rightarrow q) \rightarrow r$

Answers

a. $\sim a \wedge (\sim a \rightarrow (a \wedge b))$

$\equiv \sim a \wedge (\sim(\sim a) \vee (a \wedge b))$ by the implication law

$\equiv \sim a \wedge (a \vee (a \wedge b))$ by the ~~implication law~~ double neg law (step 1)

$\equiv \sim a \wedge a$ by the absorption law (step 2)

$\equiv a \wedge \sim a$ by the commutative law

$\equiv \mathbf{false}$ by the negation law (step 3)

b. $(p \vee \sim q) \rightarrow q$

$\equiv \sim(p \vee \sim q) \vee q$ by the implication law (step 1)

$\equiv (\sim p \wedge \sim(\sim q)) \vee q$ by De Morgan's law (step 2)

$\equiv (\sim p \wedge q) \vee q$ by the double negative law (step 3)

$\equiv q \vee (\sim p \wedge q)$ by the commutative law (step 4)

$\equiv q \vee (q \wedge \sim p)$ by the commutative law (step 5)

$\equiv q$ by the absorption law (step 6)

Check:

- Did you jump from step 1 straight to step 3 by citing only De Morgan's law but omitting double negative law?
- Did you jump from step 3 straight to step 6 by skipping the two steps involving commutative law?

Also, remember to add appropriate parenthesis to avoid ambiguous statements. For example, from $\sim(p \vee \sim q) \vee q$ (step 1) to $(\sim p \wedge \sim(\sim q)) \vee q$ (step 2), if step 2 were written as $\sim p \wedge \sim(\sim q) \vee q$, it would become an ambiguous statement since $\wedge$ and $\vee$ are coequal in precedence.

c. $\sim(p \vee \sim q) \vee (\sim p \wedge \sim q)$

$\equiv (\sim p \wedge \sim(\sim q)) \vee (\sim p \wedge \sim q)$ by De Morgan's law

$\equiv (\sim p \wedge q) \vee (\sim p \wedge \sim q)$ by the double negative law

$\equiv \sim p \wedge (q \vee \sim q)$ by the distributive law

$\equiv \sim p \wedge \mathbf{true}$ by the negation law

$\equiv \sim p$ by the identity law

d. $(p \rightarrow q) \rightarrow r$

$\equiv (\sim p \vee q) \rightarrow r$ by the implication law

$\equiv (\sim(\sim p \vee q)) \vee r$ by the implication law

$\equiv (\sim(\sim p) \wedge \sim q) \vee r$ by De Morgan's law

$\equiv (p \wedge \sim q) \vee r$ by the double negative law

3. Prove, or disprove, that $(p \rightarrow q) \rightarrow r$ is logically equivalent to $p \rightarrow (q \rightarrow r)$.

Answers

$(p \rightarrow q) \rightarrow r$ is not logically equivalent to $p \rightarrow (q \rightarrow r)$.

Counterexample: Let p, q and r be false. Then $(p \rightarrow q) \rightarrow r$ is false but $p \rightarrow (q \rightarrow r)$ is true.

For such questions, sometimes you do not know whether the given statement is true or false. In this case, you would probably have to do some trial-and-errors, or to fill in the truth table:

p	q	r	$p \rightarrow q$	$(p \rightarrow q) \rightarrow r$	$q \rightarrow r$	$p \rightarrow (q \rightarrow r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	T	T	T
T	F	F	F	T	T	T
F	T	T	T	T	T	T
F	T	F	T	F	F	T
F	F	T	T	T	T	T
F	F	F	T	F	T	T

You can see that there are two counterexamples, the sixth and eighth rows.

Certainly, filling out the whole truth table is tedious and should be avoided.

4. The SAFRA-DBS NS50 Lucky Draw 2017 is a lucky draw to win 100,000 AirAsia Miles.[1]

The rule says that to qualify for the draw, SAFRA-DBS credit card holders must "charge a minimum of S$50 nett to their card during the Qualifying Period", which is 1 July to 30 September 2017.

Let *C* = "Charge a minimum of S$50 nett", *P* = "Charge during the Qualifying Period", and *W* = "Win 100,000 AirAsia Miles".

a. Write a **conditional statement** using *C*, *P* and *W* that describes the rule above.

b. Write the **converse**, **inverse**, **contrapositive** and **negation** forms of the statement in part (a).

Answers

a. The qualifying conditions are necessary but not sufficient conditions. They are needed to participate in the draw, but do not guarantee winning the prizes. Thus, *C* and *P* are necessary conditions for *W*, which translates to:

if W then $(C \wedge P)$ or $W \rightarrow (C \wedge P)$

b.
Statement: $W \rightarrow (C \wedge P)$
Converse: $(C \wedge P) \rightarrow W$
Inverse: $\sim W \rightarrow \sim(C \wedge P)$
Contrapositive: $\sim(C \wedge P) \rightarrow \sim W$
Negation: $\sim\big(W \rightarrow (C \wedge P)\big)$

[1] https://www.dbs.com.sg/iwov-resources/pdf/cards/promotions/safra-cards-taipei-tnc.pdf

5. The conditional statement $p \rightarrow q$ is an important logical statement. Recall that it is defined by the following truth table:

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Oftentimes, students are perplexed by this definition. The first two rows look reasonable, but the last two rows seem strange. However, this way of defining $p \rightarrow q$ actually gives us the nice intuitive property of the following statement:

$$\big((p \rightarrow q) \wedge (q \rightarrow r)\big) \rightarrow (p \rightarrow r)$$

which is the **transitive rule of inference** we studied in lecture (Lecture #2, slide 67):

$$p \rightarrow q$$
$$q \rightarrow r$$
$$\therefore p \rightarrow r$$

For example, given premises "if x is a square then x is a rectangle" and "if x is a rectangle than x is a quadrilateral", the conclusion is "if x is a square then x is a quadrilateral". We use such intuitive reasoning very often in our life.

Show that if we define the conditional statement alternatively as follows, then the transitive rule of inference would no longer hold.

Alternative 1: $\rightarrow_a$

p	q	$p \rightarrow_a q$
T	T	T
T	F	F
F	T	F
F	F	F

Alternative 2: $\rightarrow_b$

p	q	$p \rightarrow_b q$
T	T	T
T	F	F
F	T	T
F	F	F

Alternative 3: $\rightarrow_c$

p	q	$p \rightarrow_c q$
T	T	T
T	F	F
F	T	F
F	F	T

Answers

Alternative 1: $\rightarrow_a$

p	q	r	$p \rightarrow_a q$	$q \rightarrow_a r$	$p \rightarrow_a r$	$(p \rightarrow_a q) \wedge (q \rightarrow_a r)$	$\big((p \rightarrow_a q) \wedge (q \rightarrow_a r)\big) \rightarrow_a (p \rightarrow_a r)$
T	T	F	T	F	F	F	F

Therefore, $\big((p \rightarrow_a q) \wedge (q \rightarrow_a r)\big) \rightarrow_a (p \rightarrow_a r)$ is not a tautology.

Alternative 2: $\rightarrow_b$

p	q	r	$p \rightarrow_b q$	$q \rightarrow_b r$	$p \rightarrow_b r$	$(p \rightarrow_b q) \wedge (q \rightarrow_b r)$	$\big((p \rightarrow_b q) \wedge (q \rightarrow_b r)\big) \rightarrow_b (p \rightarrow_b r)$
T	T	F	T	F	F	F	F

Therefore, $\big((p \rightarrow_b q) \wedge (q \rightarrow_b r)\big) \rightarrow_b (p \rightarrow_b r)$ is not a tautology.

Alternative 3: $\rightarrow_c$

p	q	r	$p \rightarrow_c q$	$q \rightarrow_c r$	$p \rightarrow_c r$	$(p \rightarrow_c q) \wedge (q \rightarrow_c r)$	$\big((p \rightarrow_c q) \wedge (q \rightarrow_c r)\big) \rightarrow_c (p \rightarrow_c r)$
F	T	F	F	F	T	F	F

Therefore, $\big((p \rightarrow_c q) \wedge (q \rightarrow_c r)\big) \rightarrow_c (p \rightarrow_c r)$ is not a tautology.

6. Some of the arguments below are valid, whereas others exhibit the converse or inverse error. Use symbols to write the logical form of each argument. If the argument is valid, identify the rule of inference that guarantees its validity. Otherwise, state whether the converse or the inverse error is made.

   a. Sandra knows Java and Sandra knows C++.

      ∴ Sandra knows C++.

   b. If at least one of these two numbers is divisible by 6, then the product of these two numbers is divisible by 6.

      Neither of these two numbers is divisible by 6.

      ∴ The product of these two numbers is not divisible by 6.

   c. If there are as many rational numbers as there are irrational numbers, then the set of all irrational numbers is infinite.

      The set of all irrational numbers is infinite.

      ∴ There are as many rational numbers as there are irrational numbers.

   d. If I get a Christmas bonus, I'll buy a stereo.

      If I sell my motorcycle, I'll buy a stereo.

      ∴ If I get a Christmas bonus or I sell my motorcycle, I'll buy a stereo.

Answers

a. Let p = "Sandra knows Java".
   Let q = "Sandra knows C++".
   $p \wedge q$ (premise)
   $\therefore q$ (valid by specialization)

b. Let p = "the first number is divisible by 6.".
   Let q = "the second number is divisible by 6".
   Let r = "the product of these two numbers is divisible by 6".
   $p \vee q \rightarrow r$ (premise)
   $\sim p \wedge \sim q$ (premise)
   $\therefore \sim r$ (invalid: inverse error; explicit counter-example: 2 and 3)
   Note that such a deduction is invalid even if there are no counter-examples.

c. Let p = "there are as many rational numbers as there are irrational numbers".
   Let q = "the set of all irrational numbers is infinite".
   $p \rightarrow q$ (premise)
   q (premise)
   $\therefore p$ (invalid: converse error; in fact, p is false, but both premises are true)

d. Let p = "I get a Christmas bonus".
Let q = "I sell my motorcycle".
Let r = "I'll buy a stereo".

$p \rightarrow r$	(premise)
$q \rightarrow r$	(premise)
$(p \rightarrow r) \wedge (q \rightarrow r)$	(conjunction rule of inference)
$(\sim p \vee r) \wedge (\sim q \vee r)$	(implication law)
$(\sim p \wedge \sim q) \vee r$	(distributive law)
$\sim(p \vee q) \vee r$	(De Morgan's law)
$\therefore (p \vee q) \rightarrow r$	(implication law)

7. Prove that there exist $x, y, z \in \mathbb{Z}_{>10}$ such that $x^2 + y^2 = z^2$. What is your proof called? What are these values called?

   (We want students to cultivate the habit of writing number lines for proofs. See question 8 below for an example. This is to help you organize your thoughts better, and sometimes allows for easier references.)

   Answers

   1. Let $x = 11, y = 60, z = 61$.
   2. Then $x, y, z \in \mathbb{Z}_{>10}$ and $x^2 + y^2 = 11^2 + 60^2 = 121 + 3600 = 3721 = 61^2$.
   3. Thus $\exists x, y, z \in \mathbb{Z}_{>10}$ such that $x^2 + y^2 = z^2$.

   This is proof by construction. The values are called Pythagorean triples.

8. The island of Wantuutrewan is inhabited by two types of people: **knights** who always tell the truth and **knaves** who always lie. You visit the island and have the following encounters with the natives.

a. Two natives *A* and *B* speak to you:

A says: Both of us are knights.
B says: *A* is a knave.

What are *A* and *B*?

b. Two natives *C* and *D* speak to you:

C says: *D* is a knave.
D says: *C* is a knave.

How many knights and knaves are there?

Part (a) has been solved for you (see below). Study the solution, and use the same format in answering part (b).

Answer for part (a):

Proof (by contradiction).

1. If *A* is a knight, then:
   - 1.1 What *A* says is true. (by definition of knight)
   - 1.2 ∴ *B* is a knight too. (that's what *A* says)
   - 1.3 ∴ What *B* says is true. (by definition of knight)
   - 1.4 ∴ *A* is a knave. (that's what *B* says)
   - 1.5 ∴ *A* is not a knight. (since *A* is either a knight or a knave, but not both)
   - 1.6 ∴ Contradiction to 1.
2. ∴ *A* is not a knight.
3. ∴ *A* is a knave. (since *A* is either a knight or a knave, but not both)
4. ∴ What *B* says is true.
5. ∴ *B* cannot be a knave. (as *B* has said something true)
6. ∴ *B* is a knight. (as there are only knights and knaves)
7. Conclusion: *A* is a knave and *B* is a knight.

Notes:

- It is tempting to say "Contradiction" right after line 1.4. However, this is not valid because contradiction requires $p \wedge \sim p$, but 'knave' is not the negation of 'knight'. Hence line 1.5 is required before we arrive at the contradiction in 1.6.

Answer

b. Proof (by division into cases)

1. If *C* is a knight:
   - 1.1 What *C* says is true. (by definition of knight)
   - 1.2 ∴ *D* is a knave. (that's what *C* says)
2. If *C* is not a knight:
   - 2.1 Then *C* is a knave. (one is either a knight or a knave)
   - 2.2 ∴ what *C* says is false. (by definition of knave)
   - 2.3 ∴ *D* is not a knave. (*C* says *D* is a knave, but what *C* says is false)
   - 2.4 ∴ *D* is a knight. (one is either a knight or a knave)
3. In both cases, there is one knight and one knave.

9. Prove Tutorial #1 Lemma #1:

The product of any two odd integers is an odd integer.

Answer

Proof (direct proof).

1. Take any two odd integers n, m.
2. Then $n = 2k + 1$ and $m = 2p + 1$ for $k, p \in \mathbb{Z}$ (by definition of odd numbers).
3. Hence $nm = (2k + 1)(2p + 1) = \big(2k(2p + 1)\big) + (2p + 1)$
   $= (4kp + 2k) + (2p + 1) = 2(2kp + k + p) + 1$ (by basic algebra)
4. Let $q = 2kp + k + p$ which is an integer by closure under $+$ and $\times$.
5. Then $nm = 2q + 1$ which is odd (by definition of odd numbers).
6. Therefore, the product of any two odd integers is an odd integer.

10. Your classmate Smart came across this question:

    If a, b, c are integers such that $a^2 + b^2 = c^2$, then a, b cannot both be odd.

a. Smart attempts to prove the above as follows:

   Proof.

   1. Suppose a, b are both odd.
   2. Then $\exists k, m \in \mathbb{Z}$ s.t. $a = 2k + 1$ and $b = 2m + 1$.
   3. Then $a^2 + b^2 = (2k + 1)^2 + (2m + 1)^2$
      $= 4k^2 + 4k + 4m^2 + 4m + 2 = c^2$
   4. Then $c = \sqrt{4k^2 + 4k + 4m^2 + 4m + 2}$.
   5. But the right-hand side is not an integer.
   6. This contradicts the fact that c is an integer.
   7. Hence, a, b cannot both be odd.

   Comment on Smart's proof.

b. Write your own proof using **contraposition**. You may start your proof with the same line 1 as above. You may also make use of Lemma 1 in the previous question.

Answers

a. In Line 5, Smart is claiming that $\sqrt{4k^2 + 4k + 4m^2 + 4m + 2}$ is not an integer, but did not provide a proof nor cite any theorem to support his claim. Thus, Smart's proof is incomplete, which means we cannot be sure if it is correct.

b.

Proof by contraposition: if a, b are both odd, then $a^2 + b^2 \neq c^2$.

1. Suppose a, b are both odd.
2. Then $\exists k, m \in \mathbb{Z}$ s.t. $a = 2k + 1$ and $b = 2m + 1$ (by definition of odd numbers).
3. Thus $a^2 + b^2 = (2k + 1)^2 + (2m + 1)^2 = 4k^2 + 4k + 4m^2 + 4m + 2$ (by basic algebra)
4. or, $a^2 + b^2 = 2(2z + 1)$, where $z = k^2 + k + m^2 + m$.
5. Now, z is an integer by closure of integers under multiplication and addition. Likewise, $(2z + 1)$ is an integer also by the closure property.
6. Hence $a^2 + b^2$ is even (by definition of even numbers).
7. Moreover, since $2(2z + 1) = 4z + 2$, it follows that $a^2 + b^2$ has remainder 2 when divided by 4.
8. Now, c is either odd or even.
   - 8.1 Case 1: c is odd
     - 8.1.1 Then c^2 is odd (by Lemma 1 in previous question).
     - 8.1.2 Then $c^2 \neq a^2 + b^2$ since the RHS is even (line 6).
   - 8.2 Case 2: c is even
     - 8.2.1 Then $\exists p \in \mathbb{Z}$ s.t. $c = 2p$ (by definition of even numbers)
     - 8.2.2 Then $c^2 = 4p^2$, which means that c^2 has remainder 0 when divided by 4.
     - 8.2.3 Hence $c^2 \neq a^2 + b^2$ since RHS has remainder 2 when divided by 4 (line 7).
9. In all cases, $c^2 \neq a^2 + b^2$.
10. Therefore, by contraposition, the original statement is true.