

Rowan Lochrin
MATH3066
Homework 1 Peer Review
11/5/17

Question 1:

1. Clear and correct truth table and explanation. However, what you proved was the *sequent*: $\models (ii) \Rightarrow (i)$ not the *theorem*: $(ii) \models (i)$. The subtle distinction between them is that \models is not a truth functional connective like \Rightarrow , it is a property of the meta-logic so it should not appear in the truth table. Instead you should show that in every configuration (ii) is true (i) must also be true in your explanation. This is probably easiest to do in the contrapositive, e.g. the only configuration where (i) is false (ii) must also be false. The same goes for $(i) \not\models (ii)$ the argument there being by counter example (there exists some configuration in which (i) is true but (ii) is false).
2. Largely the same as above. What makes this answer far better, however, is that you explicitly state, $(ii) \Rightarrow (i)$ is a theorem and $(i) \Rightarrow (ii)$ is not. My only two remaining nit picks are 1) it would great to make it a little bit clearer how you get from the sequent to the theorem, and 2) (in my eyes at least) proving the theorem to prove the sequent is a little indirect. It would probably be better to just prove the sequent directly.
3. Clear, concise and correct.

Question 2a:

1. Valid and elegant proof.
2. It looks like you have the right idea in trying to get $P \wedge Q$ for modus ponens on $(P \wedge Q) \Rightarrow R$ However in line 3 you assume $P \wedge Q$. meaning that line 6 (where you discharge the assumption) would actually be $(P \wedge Q) \Rightarrow R$. This is not what you are trying to prove. Instead the assumption you want is just P and you should be able to build $P \wedge Q$ from that and your initial assumption.
3. (Out of order) The only mistakes here are that you say you got Q and $(P \wedge Q) \Rightarrow R$ by assumption (and I suspect that you meant $\wedge - E$ because you wrote that they both depend on line 1), and you forget to remove P from your assumptions on line 7.

Question 2b:

1. Great proof. My only note is that you could save a step by not discharging the assumption $(P \wedge R)$ until after the $\vee - E$ step (making Q your conclusion for $\vee - E$).
2. You appear to be on the right track logically, however your proof seems to be working under the premise that $B, A \Rightarrow B \models A$ when this is not the case. Modus ponens is the idea that $A, A \wedge B \models B$. You seem to have made a similar mistake for a conditional proof as well. If you began by assuming $P \wedge R$ and worked your way to Q instead of the other way around this proof would be totally correct.
3. Valid and elegant proof.
4. Valid and elegant proof. You deserve a gold star for organizing your $\vee - E$ argument in cases.

Question 2c:

1. Valid and elegant proof.
2. It appears you may be confused with the statement of the problem, you are trying to prove $P \vee (Q \wedge R)$ from $P \vee Q$ and also prove it from $P \vee (Q \wedge R)$. When what $P \vee Q, P \vee R \models P \vee (Q \wedge R)$ really means is $P \vee (Q \wedge R)$ is provable from *both* $P \vee Q$ and $P \vee R$. What you have attempted to prove here is $P \vee Q \models P \vee (Q \wedge R)$ and $P \vee R \models P \vee (Q \wedge R)$ which are both impossible proofs as it is only from the combination of the two assumptions that you can infer the conclusion (It looks like in your argument you're mistaking $\wedge - I$ for $\vee - I$ in your attempt to do so). It's often useful to try and reason your way through the sequent before trying to prove it formally.
3. Valid and elegant proof. Looks largely the same as 1, except with a different order of steps. Might have been nice to put the assumption of P nearer the top to highlight the nested $\vee - E$ structure of the proof but this is a minor stylistic detail.

Question 2d:

1. Correct proof and relatively short. However reductio ad absurdum is not necessary for this proof, a far more direct approach would be to use Modus Tolens from $\sim Q$ to get $\sim P$ in one step. This saves three lines that were spent constructing the contradiction and results in a more succinct proof.

2. Good proof, the only minor mistake is that the label on line 6 should be modus tollens. Modus ponens is the idea that $A, A \Rightarrow B \models B$ when what you actually did was $\sim B, A \Rightarrow B \models \sim A$ (modus tollens).

Question 3a:

1. Good method of investigating which, of the two WWF's was a theorem without having to go into a truth table.

Question 3b:

1. Stealer proof, cleaver use of the "anything for a contradiction sequent" in your first $\vee - E$ step and proving the conclusion from P and from $\sim P$ was a fantastic way to structure it. I give it 5 stars and 2 thumbs up!
2. There are a few flaws in your proof. Firstly if you assume a direct contradiction like $Q \wedge \sim Q$ everything you infer from it will always in some way be predicated on that contradiction making it useless (because anything follows from a contradiction). Secondly from lines 11 and 12 it looks like you are misunderstanding conditional proof. Conditional proof is the idea that $P \models Q$ implies $\models P \Rightarrow Q$. This is also where you lose track of the assumption of $Q \wedge \sim Q$. Lastly your proof should always end with everything on the right side of the \models , with your only assumptions being things on the left side of the \models .
3. This is a valid proof, and organizationally you appear to be on the right track. I like that you started with $P \vee \sim P$ in order to frame the final $\vee - E$ step. However this poof is way longer then it needs to be because you're using conditional proof throughout the proof. Conditional proof really only needs to be used twice at the end to discharge your assumptions of Q and $P \Rightarrow (\sim Q \vee R)$. As a rule of thumb when you get a theorem of the form $\models (A \Rightarrow (B \Rightarrow C))$ usually the best strategy is prove $A, B \models C$ and then discharge A, B through conditional proof. It also may be useful to remember that $\vee - E$ can have asymmetric assumptions, that is to say as long as you pool the assumptions that lead you to your conclusion from both branches of the or statement it doesn't matter if they're the same.

Question 4:Question 4:

1. Good careful proof by induction. I liked how you combined all the binary operators into one symbol to avoid having to write out every

case. The only line I found confusing is $3c(U) + v(U) + 3 = 3(c(W) - 1) + v(W) + 3$ for the unary operators, might have been nice to explain why or at least explicitly state that $v(W) = v(U)$ but $c(W) = c(U) - 1$.

2. You seem to have the right idea but there are a few things wrong with this proof. P is the only base case you need (although it would be best to state explicitly that P is any WFF consisting of only a single sentence). $(P \wedge Q)$ is covered by your inductive step so including it in your base case is unnecessary and confusing to the reader. Also it looks like your inductive step only covers the binary operator \wedge , you could easily modify this proof to include all the other binary connectives however you'll need another inductive step to cover the unary operator (namely \sim). Lastly the algebra for your inductive step isn't very clear (although it looks like you're on the right track). In particular I don't understand what ℓ is supposed to mean here. If you use symbols not in the statement of the problem make sure to define them first.
3. The only base case you need is where your WFF consists of only a single sentence letter, $(\sim P)$ and $(P \Rightarrow Q)$ are covered by your inductive step. You set up your inductive step for the negation operator well, you made the correct assumptions and $v(K_2) = v(K)$, $c(K_2) = c(K) + 1$ are the key observations for the step. However what you're trying to prove is $\#K_2 = 3c(K_2) + v(K_2)$ From your inductive hypothesis and the observations you made. e.g.

$$\#K_2 = \#(K) = \#K + 3 = 3c(K) + v(K) + 3 = \dots = 3c(K_2) + v(K_2)$$

It looks like you're trying to do the inductive step for the binary operators in words, and you make a pretty coherent argument, but it's generally best to try and express your ideas in symbols as words can create ambiguity. This feels more like an explanation than a proof. Think about what assumptions you need to make for your inductive hypothesis, and what your conclusion needs to be. Once you have these two things formulated in symbols it's just a matter of doing the algebra (and showing your work!) to get between the two.

Question 5a:

1. Concise and correct, good idea to include $\sim P$ in the truth table.
2. Looks good to me!

Question 5b:

1. A truth table does function as a proof here. However I believe the question was asking for some type of deduction e.g. if $V(X) = T$ How could you simplify $W_{X,Y,Z}$ with part a and the truth table for \Rightarrow , What if you knew $V(X) = T$? From these two simplifications you can build the piece-wise function in the question.
2. Very good, if I had to make one small critique it would be cite the truth table for \Rightarrow when you do steps like $V(F \Rightarrow \sim Y) = T$.

Question 5c:

1. You have the right idea. However to fully answer this question you need to describe $\mathcal{T}_{W_{P_1,Y,Z}}$ as a combination of \mathcal{T}_Z and \mathcal{T}_Y , not just state the truth table where P_1 is true and where P_1 is false.
2. The first part of your explanation is perfect. However in the second part you're treating the symbols \mathcal{T}_Y and \mathcal{T}_Z as WFF's instead of as truth tables. You should instead be plugging in the WFF's Y and Z into $W_{P_1,Y,Z}$ and describing it's truth table in terms of \mathcal{T}_Y and \mathcal{T}_Z .

Question 5d:

1. Your base cases don't make sense to me, I'm unsure of what your truth tables represent. In this step what you want to show is that any truth table with one sentence letter can be achieved by a WFF consisting of only one sentence letter and the logical connectives \Rightarrow and \sim e.g. The truth table that is always true regardless of the value of P comes from the WFF $P \Rightarrow P$. What other possible truth tables are there containing only a single sentence letter? What WFFs can you construct (with only \Rightarrow and \sim) that have these truth tables? Your inductive step appears to be headed in the right direction. However you still have a little ways to go; my feedback on the next response applies here.
2. It's good that you built every truth table for a WFF containing only a single sentence letter; this is a valid base case. However your inductive hypothesis is a little unclear. I believe this is because you're confusing the truth tables for the WFF's they represent (a mistake I made myself). This question concerns any hypothetical truth table with n sentence letters. The thing to note here is that every truth table with n sentence letters can be built from two truth tables with $n - 1$ sentence letters each. This is where question 3 comes in.

Question 6a:

1. Good very complete answer. I liked how you solved for both x and y before consulting the multiplication table and finding the value of x .
2. I can't really follow your train of thought here, but it appears you're trying to derive an equation for y in terms of x from a system of two equations. This is only possible when both equations describe the same line. It's also not usually a good idea to think of these equations describing lines on a plane, as this is an analogy better suited to \mathbb{R} . What you really want to be doing here is finding two elements of \mathbb{Z}_{11} that satisfy both equations when you plug them in. This process is exactly like the one you learned for solving systems of two equations in \mathbb{R} . The only difference is how we define addition and multiplication in \mathbb{Z}_{11} . If you have a equation like $3x = 4$ to solve for x , you need to consult the multiplication table and figure out what multiplied by 3 gives you 4. The same goes for addition.

Question 6b:

1. Good answer. My one small critique is that writing out the whole 0 row of the multiplication table is unnecessary.
2. See my response to your part a.

Question 7:

1. You made a few mistakes in the first half of your proof. All elements in \mathbb{Z}_3 are greater then 0 so no need to assume this, $\{5b^2 : b \in \mathbb{Z}_3\} = \{0, 2\}$ not $\{0\}$ and $x^2 + 5y^2 = 0 \pmod 3 \Rightarrow x^2 = y^2 \pmod 3$ not $x^2 = -y^2 = 0 \pmod 3$. There's really not enough information to deduce $x = y = 0 \pmod 3$. Instead try starting with mod 5. The next part is correct from the assumption that $x = 3c, y = 3d$ to the conclusion that $z = 0 \pmod 3$ and you're correct in thinking that x, y, z sharing a common divisor leads to a contradiction. However your method of getting to the contradiction seems a little off. Think about what must also be a solution. If x, y, z have a common divisor, can your argument be applied to this new solution as well? How might you get a contradiction from this?
2. Good valid proof. I liked how you used a table to show that $3z^2 - x^2 = 0 \pmod 5$ implies $z = x = 0 \pmod 5$. The only change I would make to this proof is that I would start with the idea that the existence of a

non-zero solution implies there exists a solution, (x, y, z) , such that $\gcd(x, y, z) = 1$. This would save you the infinite descent step and allow you to get a contradiction straight from $x = y = z = 0 \pmod{5}$.

3. You're on the right track in that there always exists a solution, (x, y, z) , such that $\gcd(x, y, z) = 1$ for an equation of this type but there's no guarantee that every pair of x, y, z will be co-prime. Consider the equation $x^2 + y^2 = 8z^2$. $(x, y, z) = (2, 2, 1)$ is a solution and there's no way to reduce this solution to a pairwise co-prime solution. Basically what this means for your proof is that you have to go the extra step from $\gcd(x, z) > 1$ to $\gcd(x, y, z) > 1$ (hint: look at the proof the $\sqrt{2}$ is irrational). It is also probably necessary to explain why you know there exists a solution, (x, y, z) , such that $\gcd(x, y, z) = 1$. A good strategy here is to start by assuming that there exists a solution such that $\gcd(x, y, z) > 1$ and show that this implies there exists solutions such that $\gcd(x, y, z) = 1$.
4. This is my proof, and reading it back now I'm mostly satisfied with it. However there are a few places that I feel I could have improved the clarity of it. On the last step of the first row of equations I dropped the squares. Also I think saying there exists a solution (x', y', z') such that $\gcd(x', y', z') = 1$ would have better related the conclusion to the argument. I chose to go through $\pmod{4}$ instead of $\pmod{5}$ as module 4 has a smaller residue set with respect to taking the square, so even though none of the terms dropped out it's still possible to establish a greatest common denominator from the modulo equation, and this greatest common denominator applies to x, y and z without needing to plug back in. This leads to a cleaner proof.
5. Expressing (x, y, z) as $(a + b, a + c, a)$ is an interesting idea but I don't think it's really applicable in this problem. Your algebra looks good throughout but you can't assume that $10c^2 + 10bc - 2b^2$ is not a perfect square just because you can't factor it there may be some values of b and c such that $10c^2 + 10bc - 2b^2$ is a perfect square. It may be the case that there are no such integers but you would have to make an argument as to why. There may still be a valid proof in this line of thinking but I can't find it, and usually in these types of questions it's useful to think about the solutions to these equations in certain modulus. In this way you can break up the problem into smaller chunks to prove properties of a solution and try to get to a contradiction from there.