TheoryPrep **(Due: 6/14/20)**

Assignment #2: Induction and Casework

Name: Student name(s)

We don't want these problem sets to become a source of stress for you. We did our best to design them to be doable during the problem sessions, but it's early in the course so we may not have hit the nail on the head. If you've spent more than 6 or 7 hours on the problem set and are feeling stuck, feel free to turn that in. If you're still excited to keep working on it though, we'll never tell you to stop doing math!

Throughout the problem set, there are footnotes that give hints for problems. Please try to solve the problem on your own first, and if you're stuck see if the hint gives you inspiration!

We've taken some problems from the course texts and Book of Proofs (Hammack, 2013).

Problem 1: Induction

Learning goal: The problems in this section will help you practice your proofs by induction. You may need to use the various techniques you've learned like strong induction or strengthening the hypothesis!

(a) Prove the well-ordering principle that every non-empty set of positive integers has a least element. While this might seem obvious, consider the subset of the positive reals $S = \{r \in \mathbb{R}^+ | 1 < r\}$ which has no least element (you don't have to prove anything with respect to this second sentence–it's purely to help motivate the problem)!

Solution:
Suppose towards contradiction that there exists a non-empty set of positive integers S that has no least element. We will derive a contradiction by proving that it is empty (using induction). Specifically, we will prove by induction that for any $n \in \mathbb{Z}^+$, S contains no elements $\leq n$.

First the base case $n = 1$. We know $1 \notin S$ since it would be the least element because S only contains positive integers. Now for the inductive step. Assume that S has no elements $\leq n$. Clearly $n+1 \notin S$ because if it was, it would be the least element of S (by the inductive hypothesis there are no elements $\leq n$). This completes the inductive step.

This implies that $\forall n \in \mathbb{Z}^+ . n \notin S$, so S is empty. This is a contradiction since we assumed S is nonempty. Thus, we see that such an S cannot exist.

Students may try to prove this inducting on the number of elements in some non-empty set of positive integers S. You should discuss why this fails since induction is not a valid proof techniques for infinite sized sets. This would only prove the result for all finite sized sets.

(b) Alice and Bob have a pile of n coins and play the following game. They take turns taking either 1 or 2 coins from the pile, and the winner is the player to take the last coin. Say Alice is playing is first. Assuming that Alice plays optimally, for which initial values of n does Bob have a winning strategy? Prove this inductively (and prove that in the other cases, Alice will win).[1]

Solution:

[1] Try out some simple examples to build a better understanding of the problem. When you have an idea about the strategy Bob should use, try to phrase it as a statement "The inactive player has a winning strategy if and only if the current number of coins is...". Then use strong induction!

Students should try out small examples (1-3 coins to get a sense for the game). They will likely conclude something along the lines of "Bob wins if and only if $3|n$" because after Alice takes her move, Bob takes exactly enough such that together they have taken 3. Eventually it will be Alice's turn with 3 coins left, and regardless of what she takes, Bob takes the remainder.

We prove the statement $P(n) =$ "The inactive player has a winning strategy if and only if the current number of coins n is divisible by 3" (if students are having trouble coming up with the iff, maybe remind them that they need to prove a result about both when Bob will win and when he will lose). We induct on the current number of coins. Base case. $P(1), P(2)$ hold since the inactive player has no winning strategy since the active player just takes all the coins. $P(3)$ holds since the inactive player guarantees the win by taking the remaining coins after the active player goes.

Now for the inductive step. We use strong induction here (I would also have a discussion with students about how strong induction and normal induction are really the same thing–this is briefly discussed in their reading). Suppose $P(m)$ holds for all $m \leq n$. We want to prove $P(m+1)$. Remember we're proving a bidirectoinal statement, so we need to prove both statements.

- $3|m+1$. We want to show that the inactive player has a winning strategy. After the active player goes, the inactive player takes coins such that they have in total taken 3, so there are now $m-2$ coins. $3|m-2$, and we know $P(m-2)$, so the inactive player has a winning strategy from here.
- $3 \nmid m+1$. We want to show the inactive player (call them Sarah) has no winning strategy against the active player (call them George). Let the active player take exactly enough coins such that the remainder is divisible by 3 (students don't need to prove but should understand why this is always possible; if $3 \nmid m+1$ then $m+1$ must be either 1 or 2 greater than a quantity divisible by 3–you can discuss mod if you want but we won't cover it in class so might just confuse students). Now George is the active player and the number of coins is both $\leq n$ and divisible by 3, so by the inductive hypothesis, we know Sarah has a winning strategy that she will employ (a "winning strategy" is a strategy that wins regardless of opponent moves, so the existence of one player's winning strategy necessarily precludes a winning strategy for the other player–this may be worth discussing if students are confused). Thus, George has no winning strategy. This proves that the initial inactive player, George, has no winning strategy.

This completes our inductive proof. Thus, we know that Bob wins exactly if $3|n$, because n is the initial allotment of coins and Bob is the initial inactive player.

(c) Prove for any positive integer $z \in \mathbb{Z}^+$ the following relationship holds[2]

$$\frac{1}{2}\frac{3}{4}\cdots\frac{2n-1}{2n} < \frac{1}{\sqrt{3n}} \tag{0.1}$$

Solution:
We need to strengthen the hypothesis. Students should try to prove this directly first, and they'll realize it's pretty difficult because they will need to prove something along the lines of

$$\frac{2n+1}{2n+2} < \frac{\sqrt{3n}}{\sqrt{3n+3}} \tag{0.2}$$

This is false–try plugging in 6. What is the issue here? We need more "wiggle room" so we might try a tighter bound. Why not add a bit to the denominator then?

[2] Try strengthening the hypothesis

Instead, prove $\forall z \in \mathbb{Z}^+$ (this implies the theorem since $\frac{1}{\sqrt{3n+1}} < \frac{1}{\sqrt{3n}}$)

$$\frac{1}{2}\frac{3}{4}\cdots\frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}} \tag{0.3}$$

First base case, $n = 1$, so we see

$$\frac{1}{2} \leq \frac{1}{2} = \frac{1}{\sqrt{3+1}} \tag{0.4}$$

Now for the inductive step, we assume the statement for n and prove it for $n+1$. Wiritng the statement for n, we get

$$\frac{1}{2}\frac{3}{4}\cdots\frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}} \tag{0.5}$$

Multiplying both sides by $\frac{2n+1}{2(n+1)}$ gives us

$$\frac{1}{2}\frac{3}{4}\cdots\frac{2n-1}{2n}\frac{2n+1}{2(n+1)} \leq \frac{2n+1}{2(n+1)}\frac{1}{\sqrt{3n+1}} \tag{0.6}$$

Thus, if we can prove $\frac{2n+1}{2(n+1)}\frac{1}{\sqrt{3n+1}} \leq \frac{1}{\sqrt{3(n+1)+1}}$, this completes the proof. We prove this below

$$\begin{gathered} n > 0 \\ \Downarrow \\ 12n^3 + 38n^2 + 20n + 4 > 12n^3 + 38n^2 + 19n + 4 \\ \Downarrow \\ (2n+2)^2(3n+1) > (2n+1)^2(3n+4) \\ \Downarrow \\ \frac{(2(n+1))^2}{(2n+1)^2} < \frac{3n+1}{3(n+1)+1} \\ \Downarrow \\ \frac{2(n+1)}{2n+1} < \frac{\sqrt{3n+1}}{\sqrt{3(n+1)+1}} \end{gathered} \tag{0.7}$$

As a pedagogical note, it's easier to start with $\frac{2n+1}{2(n+1)}\frac{1}{\sqrt{3n+1}} \leq \frac{1}{\sqrt{3(n+1)+1}}$ and then work out how you would prove it is true. The "proof" will then be running those steps in reverse, since you need to start with something true. This is an important facet of proofs that you may want to discuss with students (that you may need to do scratch work before you do a proof, and to prove an algebraic statement true you need to derive it from a true statement not simplify it to one–an instructive example is if the latter was true you could "prove" almost anything by mutliplying both sides by 0).

(d) Now a bogus proof. Find the erroneous step in the below proof and explain why it is flawed.

Suppose that an architect would like to tile a $2^n \times 2^n$ region with a tile of the shape in Figure 1. However, there is also a statue that takes up one tile of the courtyard that must be placed at a pre-specified location. The architect claims that this is possible for any $2^n \times 2^n$ region and statue location.

They proceed by induction. For $n = 0$, there is only one space, so the statue must go in that space, filling the entire courtyard. Now for the inductive step. We can divide the $2^{n+1} \times 2^{n+1}$ courtyard up into four $2^n \times 2^n$ quadrants. Applying the inductive hypothesis, we know we can tile those courtyards leaving exactly one space wherever we want. We choose to leave the spaces exactly as in Figure 1 (with B marking the pre-specified statue location). Thus, we can tile the $2^{n+1} \times 2^{n+1}$ courtyard. By the inductive principle, we can tile any courtyard.

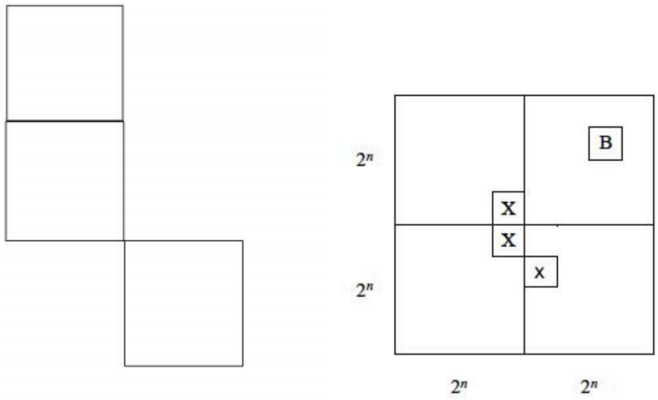

Figure 1: The architect's tile and the spaces left empty in the inductive step.

> **Solution:**
> The error in this proof happens when going from $n = 0$ to $n = 1$, similar to the flawess Horse proof that students saw in the reading. In a 2×2 grid, the tiling strategy in Figure 1 does not work since it implicitly assumes that each of the quarters is at least 2×2. As with last week's bogus proofs, have students walk through the various steps of the proof and test what logic is sold (kind of like debugging!).

Problem 2: Generalizing Induction

Learning goal: We presented induction as a technique to prove a predicate over all natural numbers, but we can also use it to prove statements over the integers. It will actually work over any inductively defined set–inductively defined means the set is constructed from a bunch of rules that specify an element is part of the set based on other members. For example, $\mathbb{N}$ can be defined as by the rule $0 \in \mathbb{N}$ and $n \in \mathbb{N} \Rightarrow n + 1 \in \mathbb{N}$ (do you see the similarity to induction?). It's important to understand the relationship between which implications we prove and what sets they guarantee our result for (like proving $P(n) \Rightarrow P(n + 2)$ and $P(0)$ implies it for all even natural numbers).

(a) Explain how the technique of induction could be generalized to prove a predicate $P(z)$ for all integers $z \in \mathbb{Z}$. Looking at the "rules" required for induction on page 132, replace the two bullet points in the hypothesis of the Induction Principle. Explain why this would be a valid proof technique.

> **Solution:**
> I think there will be two main answers that students provide. Both (and any other constructions) are valid–just probably want to stay away from really complex ones. Make sure quantifiers are included where necessary.
>
> - $P(0)$
> - $\forall n \in \mathbb{N}. P(n) \Rightarrow P(n + 1)$
> - $\forall n \in \mathbb{Z}_{\leq}. P(n) \Rightarrow P(n - 1)$
>
> Or they may do something like
>
> - $P(0)$
> - $\forall n \in \mathbb{N}. P(n) \Rightarrow P(n + 1)$
> - $\forall n \in \mathbb{N}. P(n) \Rightarrow P(-n)$

This is a valid proof technique, because to prove $\forall z \in \mathbb{Z}.P(z)$ means if we fix an arbitrary $z \in \mathbb{Z}$, we should be able to prove $P(z)$. If we prove either of the above sets of results, we can prove $P(z)$ using something like (assume the complicated case where $z < 0$)

$$P(0) \Rightarrow P(-1) \Rightarrow ... \Rightarrow P(z) \tag{0.8}$$

Or using the second set of propositions

$$P(0) \Rightarrow P(1) \Rightarrow ... \Rightarrow P(|z|) \Rightarrow P(z) \tag{0.9}$$

(b) Use the principle you explained in Part A to prove (here | means divide)

$$\forall z \in \mathbb{Z}.3|z^3 + 2z \tag{0.10}$$

Solution:
We prove the results from A (we prove it for the first set of rules)

- $P(0)$ holds since $3|0$.
- Suppose $P(n)$ holds for some $n \in \mathbb{N}$, so $3|n^3 + 2n$

$$\begin{aligned}(n+1)^3 + 2(n+1) &= n^3 + 3n + 3n^2 + 1 + 2n + 2 \\ &= \underbrace{n^3 + 2n}_{\text{divisible by inductive hypothesis}} + 3(n^2 + n + 1)\end{aligned} \tag{0.11}$$

  Thus, we see that $3|(n+1)^3 + 2(n+1)$.
- Suppose that $P(n)$ holds for some $n \in \mathbb{Z}_{\leq}$, so $3|n^3 + 2n$

$$\begin{aligned}(n-1)^3 + 2(n-1) &= n^3 - 3n^2 + 3n - 3 + 2n \\ &= \underbrace{n^3 + 2n}_{\text{divisible by inductive hypothesis}} + 3(-n^2 + n - 1)\end{aligned} \tag{0.12}$$

  Thus, we see that $3|(n-1)^3 + 2(n-1)$.

We can also prove it under the other set of rules. Assume $P(n)$ for some $n \in \mathbb{N}$, so $3|n^3 + 2n$. We see that

$$(-n)^3 + 2(-n) = -(n^3 + 2n) \tag{0.13}$$

Since $3|n^3 + 2n$, $3| - (n^3 + 2n)$. You might discuss how different sets of rules (ie different inductive constructions of the integers) made the proof easier or harder.

(c) Explain how you would generalize the technique of induction to the rational numbers (similarly to part **2.a**). Write out the Induction Principle with the hypotheses replaced (there are multiple ways to do this–depending on the proof you may want to do it different ways–but since we're doing this in the abstract, any construction will suffice). Explain why this would be a valid proof technique.

Solution:
Similarly to A there are many ways to do this. Here's one

- $P(0)$
- $\forall p, q \in \mathbb{Z}.P\left(\frac{p}{q}\right) = P\left(\frac{p+1}{q}\right)$
- $\forall p, q \in \mathbb{Z}.P\left(\frac{p}{q}\right) = P\left(\frac{p}{q+1}\right)$
- $\forall q \in \mathbb{Q}.P(q) = P(-q)$

(d) Let $P(n)$ be a predicate for natural number $n \in \mathbb{N}$ (so whenever you see n in a quantifier statement in this problem assume it is a natural number). Suppose Alice has proven $\forall n P(n) \Rightarrow P(n+3)$ and $P(5)$. Which of the following statements must be true.

1. $\forall n \geq 5, P(n)$
2. $\forall n \geq 5, P(3n)$
3. $P(n)$ holds for $8, 11, 14, \ldots$
4. $\forall n < 5. \neg P(n)$ (meaning that $P(n)$ is false).
5. $\forall n. P(3n+5)$
6. $\forall n > 2. P(3n-1)$
7. $P(0) \Rightarrow \forall n. P(3n+2)$
8. $P(0) \Rightarrow \forall n. P(3n)$

Suppose Alice wants to prove $\forall n \geq 5. P(n)$. Which of the following would be sufficient. Assume for this part that unless specified in the answer, Alice has not proven $P(5)$

1. $P(5), P(6)$
2. $P(0), P(1), P(2)$
3. $P(2), P(4), P(5)$
4. $P(3), P(5), P(7)$

Solution:
For the first set of problems (student's don't have to justify, and hopefully since they're not getting a grade they're not just going to copy other people's answers).

1. F
2. F
3. T
4. F (induction says nothing about where the proposition is false, unless you induct $\neg P(n)$)
5. T
6. T
7. F ($P(2)$ not true)
8. T

For the second set of problems. The core takeaway for students from doing this problem should be realizing the different ways to prove $P(n)$ for the numbers they need to cover.

1. Not Sufficient
2. Sufficient
3. Not Sufficient
4. Sufficient

Problem 3: Casework

Learning Goal: This section gives some problems to help you practice casework. We purposefully present problems where the cases may not be immediately apparent (and remember to at least verify to yourself that they are exhaustive).

(a) Let $a, b, c, d \in \mathbb{Z}_{\geq}$ be nonnegative integers such that

$$a^2 + b^2 + c^2 = d^2 \tag{0.14}$$

Prove that d is even if and only if all three of a, b, c are even.[3]

Solution:
We split into cases

1. a, b, c are even. We can then write by definition $a = 2a', b = 2b', c = 2c'$, so we have
$$d^2 = 4a'^2 + 4b'^2 + 4c'^2 = 2(2a'^2 + 2b'^2 + 2c'^2) \tag{0.15}$$
Thus, d^2 is even, and we proved earlier that this implies d is even.

2. None of a, b, c are even, and the sum of the squares of 3 odd number is odd (sum of three odd numbers is odd and we proved x odd $\Rightarrow x^2$ odd). We know that if d^2 is odd, then d cannot be even. A short proof is by contradiction, suppose that d^2 is odd and d is even so $d = 2d'$. Then $d^2 = 4d'^2 = 2(2d'^2)$, which is even hence a contradiction.

3. Exactly two of a, b, c are even. Then d^2 is the sum of two even and an odd number, so it is odd. Thus d cannot be even.

4. Exactly one of a, b, c is even. We will show that this case cannot happen since a, b, c, d must be integers. In other words, we will show that in this case, d is not an integer. Without loss of generality, assume that a, b are odd, so we write $a = 2a' + 1, b = 2b' + 1, c = 2c'$, so we have
$$\begin{aligned} d^2 &= (2a' + 1)^2 + (2b' + 1)^2 + (2c')^2 \\ &= 2(2(a'^2 + a' + b'^2 + b' + c') + 1) \end{aligned} \tag{0.16}$$
We can tell now that d cannot be an integer because there is only one factor of 2 on the righthand side. Let's prove this rigorously. Suppose that d is an integer, so we can write it as $d = p_1 p_2 ... p_m$. We can also write as the product of primes $2(a'^2 + a' + b'^2 + b' + c') + 1 = p'_1 p'_2 ... p'_k$. Thus,
$$p_1^2 p_2^2 ... p_m^2 = 2p'_1 p'_2 ... p'_k \tag{0.17}$$
Without loss of generality $p_1 = 2$, so we have
$$2p_2^2 ... p_m^2 = p'_1 p'_2 ... p'_k \tag{0.18}$$
This implies that $p'_i = 2$ for some i. This implies that $2(a'^2 + a' + b'^2 + b' + c') + 1$ is divisible by 2, which is a contradiction because it is odd. Thus, we see d is not an integer. Thus, we see this case cannot happen because d will not be an integer.

(b) There is a nice exposition about Hippos on page 153 of Math for CS if you would like some motivation, but the tl;dr is that if you make a drawing of unit squares, the resulting shape always has an even number length perimeter (see Figure 2). Prove this (make sure your casework is exhaustive).[4]

[3] Sometimes you may need to prove that a case cannot occur.
[4] Hint: You will likely need both induction and casework.

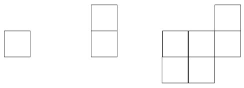

Figure 2: Diagrams of unit squares with perimeter 4, 6, and 12 respectively.

Solution:
We will induct on the number of squares in the diagram. In the base case with one square, it has a perimeter of 4.

Now for the inductive step. Suppose we have an arbitrary diagram with n squares, and we know the perimeter is even, call it m. There are four possibilities (although the analysis is similar)

1. The square we place touches the diagram on 1 edge. In this case, the other three edges aren't touching anything, so they increase the perimeter by 3. However, the shared edge used to be on the perimeter, so it decreases it by 1, for a new perimeter of $m + 2$, which is even.
2. The square we place touches the diagram on 2 edges. In this case, 2 edges are taken away and 2 added, so the new perimeter is m, even.
3. The square we place touches the diagram on 3 edges. The perimeter falls by 3 from shared edges and increases by 1, for a new perimeter of $m - 2$ which is even.
4. The square we place touches the diagram on 4 edges. The perimeter decreases by 4, but $m - 4$ is still even.

Problem 4: Review

Learning goal: It's important to keep skills fresh. This will also give you the opportunity to work on any feedback you got from the previous week (some problems may also require the contrapositive, so it's not all review).

(a) Let $x \in \mathbb{Z}$ an integer. Prove that if $x^2 - 6x + 5$ is even then x is odd.

Solution:
This problem begs the contrapositive because it's difficult to work with the fact that $x^2 - 6x + 5$ is even. It's hard to deduce much about x from the equation $x^2 - 6x + 5 = 2x'$

We prove the contrapositive that if x is even then $x^2 - 6x + 5$ is odd. Since x is even, we write $x = 2x'$. Thus,

$$\begin{aligned} x^2 - 6x + 5 &= 4x'^2 - 12x' + 5 \\ &= 2(2x'^2 - 6x + 2) + 1 \end{aligned} \tag{0.19}$$

Thus, we see that x^2 is odd.

(b) Prove of disprove:

$$\forall x \in \mathbb{Z}.\exists y, z \in \mathbb{Z}.(x = y + z \text{ and } |y| \neq |z|) \tag{0.20}$$

Solution:
As a pedagogical note, a great strategy for this type of problem is to plug in some numbers to get a sense of if it's possible or not, then try to do the formal proof after. The formal proof is a good exercise in making sure students understand how to manipulate negations and quantifier statements.

We'll disprove this. In order to disprove a quantifier statement, flip the quantifiers, negate the predicate, and prove that statment. Thus, we want to prove that

$$\exists x \in \mathbb{Z}, \forall y, z \in \mathbb{Z} \neg (x = y + z \text{ and } |y| \neq |z|) \tag{0.21}$$

First, what does it mean for $\neg(P \text{ and } Q)$. Well if it is not true that both P and Q are true, that's exactly the same as saying at least one of P or Q is wrong. Thus, we are trying to prove $(\neg P)$ or $(\neg Q)$. The more general version of this rule is called "DeMorgan's Law". Thus, we want to prove

$$\exists x \in \mathbb{Z}, \forall y, z \in \mathbb{Z} (x \neq y + z \text{ or } |y| = |z|) \tag{0.22}$$

We are doing an existence proof, so we just need to find an x. We'll choose $x = 0$. Thus, we want to show that

$$\forall y, z \in \mathbb{Z} (0 \neq y + z \text{ or } |y| = |z|) \tag{0.23}$$

Fix arbitrary $y, z \in \mathbb{Z}$. We want to show either $0 \neq y + z$ or $|y| = |z|$. Suppose that $0 = y + z$ (so the first statement is false), then $-y = z \Rightarrow |y| = |z|$. Thus, we see either the first statement is true (in which case we're good), or the first is false but then the second must be true.

Problem 5: Logistics

Purpose: This helps us make sure the course is going at the right speed!

(a) How long did you spend on the videos and readings this week?

(b) How long (including time in problem sessions) did you spend on this problem set?

(c) Do you have any feedback about the course in general (did the videos and readings sufficiently prepare you for the problem set)?