TheoryPrep **(Due: 6/7/20)**

Assignment #1: Quantifiers, Logic, Sets, Proofs

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 hours on the problem set and are feeling stuck, feel free to turn that in. If you're still excited, 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!

Problem 1: Quantify it

Learning goal: Building familiarity with quantifiers and how they are used to precisely so they can be understood and utilized when describing mathematical statements and propositions. It's like learning the vocabulary in a foreign language.

(a) Express using quantifiers the statement: every element in the set T of integers has an additive inverse (an additive inverse is a number you can add to get 0 – for example, the additive inverse of 2 is -2).

Solution:
$\forall z \in T \exists z' \in \mathbb{Z} : z + z' = 0$.

(b) Write in English what the following set is (note $|$ means divides)

$$\{z \in \mathbb{Z} | \exists n \in \mathbb{N} \text{ and } n^2 = z \text{ and } \forall m > 1 \in \mathbb{N}, m|n \Rightarrow m = n\} \tag{0.1}$$

Solution:
This is the set of integers that are the square of a a prime number.

(c) For the following three statements, evaluate if they are true or false in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$.

1. $\forall x \exists y . 2x - y = 0$
2. $\forall x \exists y . 2y - x = 0$
3. $\forall x \exists y . (y > x \text{ and } \exists z . y + z = 100)$

Solution:
For $\mathbb{N}$ only the first is true. For $\mathbb{Z}$ statements 1 and 3 are true. For $\mathbb{Q}$ they are all true.

(d) Give give an example of a statement that is ambiguous, meaning the if you were to write it using quantifiers, the order of the quantifiers would influence the meaning (ie if you flip the order of the quantifiers the statement goes from true to false or vice versa). Then, write both possibilities using quantifiers. If it's easier, you can use non-mathematical sets like "Let A be the set of all types of animals."

Solution:
$\forall z \in \mathbb{Z} \exists z' \in \mathbb{Z} : z' + z = 0$ (all integers have an additive inverse). However, it is not true that $\exists z' \forall z \in \mathbb{Z} : z + z' = 0$ (there is not one number that is the additive inverse for all integers). An more intuitive example might be that for all animals, there exists some natural number n which is the number of legs they have, but there does not exist some

natural number n which is the number of legs any animal has.

Problem 2: Types of Proofs

Learning goal: Clarifying and compartmentalizing the different types of proofs can make it easier later on properly determine which candidate proof strategies to employ when trying to construct a proof.

(a) Describe the key difference between a universal and existential proof?

Solution:
A universal statement means something is true in a broad set of classes, and an existential statement means it's true at least sometime. Thus, for a universal proof, we have to prove that no matter what element we choose (as long as it meets the hypothesis), the statement is true. For an existential proof, it's enough to give just one example.

(b) How does the negation symbol (ie "not") relate the universal and existential quantifiers (think about the second video)?

Solution:
Given a quantifier statement, you can generate an equivalent statement by taking the negation, replacing all $\forall$ with $\exists$, replacing all $\exists$ with $\forall$, and negating the predicate. For exanple, for the equation below (where P is a predicate – a statement with truth value dependent on the variable x)

$$\forall x_1 \in S_1 \exists x_2 \in S_2 \exists x_3 \in S_3 ... \forall x_n \in S_n P(x_1, ..., x_n) \tag{0.2}$$

We can rewrite it as

$$\exists x_1 \in S_1 \forall x_2 \in S_2 \forall x_3 \in S_3 ... \exists x_n \in S_n \neg P(x_1, ..., x_n) \tag{0.3}$$

This is most commonly useful for disproving universal or existential statements. If you are trying to prove $\neq \forall x \in S : P(x)$ just prove $\exists x \in S : \neg P(x)$ (in other words, give a counterexample). If you're trying to prove $\neg \exists x \in S : P(x)$ prove $\forall x \in S :\neq P(x)$ (this is easier since we really don't have any other method for disproving existential statements).

(c) Give an example of a mathematical statement that would require a **universal** proof, using quantifiers. *It could be a very simple and obvious mathematical statement.* You do not need to prove it.

Solution:
Every integer can be expressed as the sum of two distinct integers.

(d) Suppose you were asked to prove the below equivalence. Write out the two directions you would need to prove.

Show that for any two integers $n, m \in \mathbb{Z}$ we have $|n| = |m|$ (recall $|x|$ is the absolute value of x) if and only if $n|m$ and $m|n$.

Solution:
We need to prove both directions.

Forwards (often denoted $\Rightarrow$): For any integers $n, m \in \mathbb{Z}$ if $|n| = |m|$ then $n|m$ and $m|n$.

Backwards (often denoted $\Leftarrow$): For any integers $n, m \in \mathbb{Z}$ if $m|n$ and $n|m$ then $|n| = |m|$.

Problem 3: Practice with Proofs

Learning Goal: We want you to practice the proof techniques you learned this week.

(a) Prove that for every integer $x \in \mathbb{Z}$ there is a unique integer $y \in \mathbb{Z}$ such that the following equation holds[1]

$$(x+1)^3 - x^3 = 3y + 1 \tag{0.4}$$

Solution:
Fix arbitrary $x \in \mathbb{Z}$. First we prove there exists a y that makes the equation hold. Define $y = x^2 + x$. We see that

$$\begin{aligned} 3y + 1 &= 3(x^2 + x) + 1 \\ &= 3x^2 + 3x + 1 \\ &= x^3 + 3x^2 + 3x + 1 - x^3 \\ &= (x+1)^3 - x^3 \end{aligned} \tag{0.5}$$

Thus, y, satisfies the desired relation. Now we want to prove this y is unique. Fix an arbitrary y' such that the desired relation holds, so

$$(x+1)^3 - x^3 = 3y' + 1 \Rightarrow 3x^2 + 3x + 1 = 3y' + 1 \Rightarrow y' = x^2 + x \tag{0.6}$$

Thus, we see $y' = y$, and since we fixed y' arbitrarily as satisfying the desired relationship, anything satisfying the relationship is y–in other words, y is the unique integer that makes the relationship hold.

(b) One of the cool things about math is that we can define any operation we like (just like how someone defined addition and multiplication). Suppose we define the operation $\oslash$ by $x \oslash y = 2(x + y)$. One property we care about with operators is associative, which is to say that it doesn't matter how we parenthesize a statement (it's convenient to have this property since then we can reparenthesize equations however we want without changing their value!). Mathematically, we say some operator $\circ$ is associative if for any a, b, c

$$a \circ (b \circ c) = (a \circ b) \circ c \tag{0.7}$$

Addition and multiplication are associative, but subtraction is not associative (try some examples to see why). Prove that $\oslash$ is not associative. [2]

Solution:
In order to prove this is not associative, we must find and $a, b, c \in \mathbb{Z}$ such that

$$a \oslash (b \oslash c) = (a \oslash b) \oslash c \tag{0.8}$$

Let $a = 3, b = 1, c = -3$. Then

$$a \oslash (b \oslash c) = 3 \oslash -4 = -2 \tag{0.9}$$

However

$$(a \oslash b) \oslash c = 8 \oslash -3 = 10 \tag{0.10}$$

(c) For this problem, the fundamental theorem of arithmetic may be helpful. It says for any integer greater than 1, say n, we can write n as the product of primes, and this representation is unique up to reordering the primes. In particular, we can write

$$n = p_1 p_2 ... p_m \tag{0.11}$$

[1] In order to prove that there exists a unique quantity, first prove that it exists. Then suppose you have another arbitrary quantity y' that satisfies the problem and prove that it must be the same.

[2] Hint: Proving a universal statement false can be done by giving a counterexample

Where the p_i are prime, and any other combination of primes that multiply to n are just a reordering of $p_1, ..., p_m$. To make this conrete, consider 12. We can write

$$12 = 3 \cdot 2 \cdot 2 \tag{0.12}$$

And this is the only way to write it as a product of primes (up to reordering them). The fundamental theorem of arithmetic allows us to rewrite integers as the product of primes, which can often be helpful since primes have many nice properties!

Prove that for any $p \in \mathbb{N}$ prime, there does not exist a natural number $n \in \mathbb{N}$ not divisible by p such that n^2 is divisible by p. [3]

Solution:
Fix aribtrary $p \in \mathbb{N}$ prime. Suppose towards a contradiction that there exists a natural number n such that $p \nmid n$ but $p \mid n^2$. By the fundamental theorem of arithmetic, we can write

$$n = p_1 p_2 ... p_m \tag{0.13}$$

We know that $\forall i p_i \neq p$ since this would imply that $p \mid n$. Thus, by substitution we can write

$$n^2 = p_1 p_1 p_2 p_2 ... p_m p_m \tag{0.14}$$

This gives an equation for n^2 as the product of primes. We will give another prime factorization of n^2 which contradicts the fundamental theorem of arithmetic (which says all prime factorizations are the same up to reordering). Since $p \mid n^2$, we can write $n^2 = pc$ for some $c \in \mathbb{Z}$, and by the fundamental theorem of arithmetic $c = p'_1 p'_2 ... p'_j$, so we can write

$$n^2 = p p'_1 p'_2 ... p'_j \tag{0.15}$$

These are all primes, so this is another prime factorization of n^2. However we know that the prime factorizations given in Equations 0.14 and 0.15 cannot be the same since the former contains no copies of p, but the latter contains at least one copy of p. This contradicts the fundamental theorem of arithmetic that says that all prime factorizations are the same up to reordering. Thus a contradiction, so there does not exist a $n \in \mathbb{N}$ such that $p \nmid n$ and $p \mid n^2$. This completes the proof since this is what we wanted to prove.

Problem 4: Bogus Proofs

Learning goal: Building intuition is important for mathematical proofs, because erroneous logic can happen if one does not have a solid intuitive grasp on certain principles. Identifying faulty logic can help prevent one from making similar mistakes when constructing proofs. In other words, in math you can do certain operations but not others. It is very important to have a strong understanding of *why* you can do certain things and not others. Understanding what the manipulation of mathematical symbols means intuitively (and therefore being able to identify faulty manipulations) is thus important.

(a) Explain why the below result cannot be true. Then identify the faulty logic in the proof.

I will prove that $\forall a, b \in \mathbb{Z}$ if $a = b$ then $a = 0$. We give the following proof. Fix arbitrary equal integers a, b.

$$\begin{aligned} a &= b \\ a^2 &= ab \\ a^2 - b^2 &= ab - b^2 \\ (a-b)(a+b) &= (a-b)b \\ a + b &= b \\ a &= 0 \end{aligned} \tag{0.16}$$

[3] Hint: Contradiction. If n is not divisible by p, we can write it as $ap + b$ for $b < p$ and $a, b \in \mathbb{N}$, which is to say we can write it as a product of p and a "remainder"

Solution:
The faulty step in this proof is that we divide by $(a - b)$ to get from line 4 to line 5. You can't do that if $a = b$ (because you are dividing by zero). Ask students what "you can't do that" means. The series of equalities in 0.16 is a chain of implications. We start with something we know, $a = b$, and each step says that because the equality before it holds, the next equality holds as well. For example, the first line says $a = b \Rightarrow a^2 = ab$ (some may find it helpful to say that mulitplying by a on both sides "preserves the truth value").

Thus, the error is that dividing by 0 does not "preserve the truth value", ie the rule $(a - b)(a + b) = (a - b)b \Rightarrow a + b = b$ is not true. Consider, for example that $a = b = 3$. Then clearly $(a - b)(a + b) = 0 \cdot 6 = 0 \cdot 3 = (a - b)b$, but $a + b = 6 \neq 3 = b$, so the implication does not hold.

Students may know intuitively "you can't divide by zero," but it's important that they also understand *why* this is wrong, as explained above.

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)?