CSC165H1: Problem Set 2

Due February 15, 2017 before 10pm

General instructions

Please read the following instructions carefully before starting the problem set. They contain important information about general problem set expectations, problem set submission instructions, and reminders of course policies.

- Your problem sets are graded on both correctness and clarity of communication. Solutions which are technically correct but poorly written will not receive full marks. Please read over your solutions carefully before submitting them.
- Each problem set may be completed in groups of up to three. If you are working in a group for this problem set, please consult `https://github.com/MarkUsProject/Markus/wiki/Student_Groups` for a brief explanation of how to create a group on MarkUs.

  Exception: Problem Set 0 must be completed individually.
- Solutions must be typeset electronically, and submitted as a PDF with the correct filename. **Hand-written submissions will receive a grade of ZERO.**

  The required filename for this problem set is **problem_set2.pdf**.
- Problem sets must be submitted online through MarkUs. If you haven't used MarkUs before, give yourself plenty of time to figure it out, and ask for help if you need it! If you are working with a partner, you must form a group on MarkUs, and make one submission per group. "I didn't know how to use MarkUs" is not a valid excuse for submitting late work.
- Your submitted file should not be larger than 9MB. This may happen if you are using a word processing software like Microsoft Word; if it does, you should look into PDF compression tools to make your PDF smaller, although please make sure that your PDF is still legible before submitting!
- Submissions must be made *before* the due date on MarkUs. You may use *grace tokens* to extend the deadline; please see the Problem Set page for details on using grace tokens.
- The work you submit must be that of your group; you may not refer to or copy from the work of other groups, or external sources like websites or textbooks. You may, however, refer to any text from the Course Notes (or posted lecture notes), except when explicitly asked not to.

Additional instructions

- For each proof you write, make sure to first write in predicate logic the precise statement, fully simplified, that you're going to prove. For a disproof, clearly write the fully simplified negation. Unlike Problem Set 1, you do *not* need to show your work for computing negations of statements.
- For proofs involving divisibility, primes, and the floor function, you **may not use any external facts other than those mentioned in the questions**. You should not (and will not need to) prove any external facts to complete this problem set.
- For any *concrete numbers*, you may state whether one divides another, or whether a number is prime, without proof. For example, you can write statements "$3 \mid 12$" and "15 is not prime" without justification.

- We'll post some more guidelines for how you should structure and write your proofs for this assignment in a day or two, so please remember to check this before your final submission!

1. **[7 marks] AND vs. IMPLIES.** Students often confuse the meanings of the two propositional operators $\Rightarrow$ and $\land$. In this question, you'll examine each of these in a series of statements by writing formal proofs/disproofs of each one.

   Reminder: read the "Extra Instructions" for this problem set carefully. In particular, we do not mention any external facts about divisibility in this question, and you should not use any in your proofs here.

   (a) Prove or disprove: $\forall x, y, z \in \mathbb{Z},\ (x \mid y \land y \mid z) \Rightarrow x \mid z$.

   (b) Prove or disprove: $\forall x, y, z \in \mathbb{Z},\ (x \mid y \land y \mid z) \land x \mid z$.

2. **[10 marks] Alternating quantifiers and the floor function.** Here is a question that really gets at the meaning of alternating quantifiers. Recall the definition of the *floor* function $\lfloor x \rfloor$, which is equal to the greatest integer that is less than or equal to x. Here are some properties of the floor function that you can use in this question:[1]

$$\forall x \in \mathbb{R},\ \exists \epsilon \in \mathbb{R},\ 0 \leq \epsilon < 1 \land x = \lfloor x \rfloor + \epsilon \tag{1}$$
$$\forall x \in \mathbb{Z},\ \forall y \in \mathbb{R},\ \ \lfloor x + y \rfloor = x + \lfloor y \rfloor \tag{2}$$
$$\forall x \in \mathbb{Z},\ \ \lfloor x \rfloor = x \tag{3}$$

   Prove or disprove each of the following statements. Whenever you use one of the above properties in your proof, **clearly state which property you are using**.

   (a) $\forall n \in \mathbb{N},\ \exists k \in \mathbb{N},\ \forall x \in \mathbb{R},\ \ \lfloor nx \rfloor - n \lfloor x \rfloor \leq k$.

   (b) $\exists k \in \mathbb{N},\ \forall n \in \mathbb{N},\ \forall x \in \mathbb{R},\ \ \lfloor nx \rfloor - n \lfloor x \rfloor \leq k$.

3. **[8 marks] More with primes.** Recall the definition of the prime predicate (defined over the natural numbers):

$$Prime(n) : n > 1 \land \big(\forall d \in \mathbb{N}, d \mid n \Rightarrow d = 1 \lor d = n\big)$$

   Now consider the following related definition.

   Definition 1 (composite)**.** Let n be a natural number. We say that n is **composite** if and only if it is greater than 1 and not prime.

   (a) Show how to express the composite predicate $Composite(n)$: "n is composite" in predicate logic, *without* using the $Prime$ predicate. (But of course you can use the definition of the $Prime$ predicate for ideas.)

   You may use the following fact about divisibility to help simplify your predicate:

$$\forall n \in \mathbb{N}, n > 0 \Rightarrow \big(\forall d \in \mathbb{N}, d \mid n \Rightarrow 1 \leq d \land d \leq n\big)$$

   (b) Prove that for all natural numbers x, $x^2 + 5x + 4$ is composite. **Hint**: factor.

   (c) Prove or disprove: for all natural numbers x and y, if $x > y$ then $x^2 - y^2$ is composite.

[1] The first says that the difference $x - \lfloor x \rfloor$ is always between 0 and 1, and the second and third say that you can "take integers out of the floor function."

4. **[7 marks] Function growth.** Now let's leave numbers and talk about functions. Consider the following definition:[2]

Definition 2. Let $f, g : \mathbb{N} \to \mathbb{R}^{\geq 0}$. We say that g **is eventually dominated by** f if and only if there exists $n_0 \in \mathbb{R}^{\geq 0}$ such that every natural number n greater than or equal to n_0 satisfies $g(n) \leq f(n)$.

We can express this definition in a predicate $Edom(f, g)$: "g is eventually dominated by f", where $f, g : \mathbb{N} \to \mathbb{R}^{\geq 0}$, in the following way:

$$EDom(f, g) : \exists n_0 \in \mathbb{R}^{\geq 0},\ \forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow g(n) \leq f(n)$$

(a) Let $f(n) = n^2$ and $g(n) = n + 165$. Prove that g is eventually dominated by f. Do **NOT** use part (b) to prove this part; we want to see you construct a proof with concrete numbers rather than the variables you'll use in part (b).

Hint: pay attention to the order of the quantifiers. The first line of your proof should introduce the variable n_0, and give it a concrete value.

(b) Prove the following statement, which is a generalization of the previous part:

$$\forall a, b \in \mathbb{R}^{\geq 0},\ g(n) = an + b \text{ is eventually dominated by } f(n) = n^2.$$

Hint: you don't need to pick the "best" n_0 here, just pick one that works and makes the proof's calculations easy for you to work with! Which variables can n_0 depend on?

[2] The symbol $\mathbb{R}^{\geq 0}$ denotes the set of all nonnegative real numbers, i.e., $\mathbb{R}^{\geq 0} = \{x \mid x \in \mathbb{R} \wedge x \geq 0\}$.