CSE 4111 Computability & COSC 6111 Advanced Design and Analysis of Algorithms
Jeff Edmonds
Assignment 0: Quantifiers
Due: One week after first class.

First Person:
Family Name:
Given Name:
Student #:
Email:

Second Person:
Family Name:
Given Name:
Student #:
Email:

Guidelines:

- You are strongly encouraged to work in groups of two. Do not get solutions from other pairs. Though you are to teach & learn from your partner, you are responsible to do and learn the work yourself. Write it up together. Proof read it.
- Please make your answers clear and succinct.
- Relevant Readings: Slides and steps.
- This page should be the cover of your assignment.

Do questions $\{2, 3, 4\}$.

Problem Name	Max Mark	
1 Church's Thesis	10	
2 Induction with Quantifiers	10	
3 Epsilon Delta Proofs	10	
4 Minimum Value Theorem	10	
Total	40	

CSE 4111 Computability & COSC 6111 Advanced Design and Analysis of Algorithms
Jeff Edmonds
Assignment 0: Quantifiers
Due: One week after first class.

Recall:

1. Prove first order logic statements by playing the game outlined in the slides and steps. For example, prove $\forall x,\ \exists y,\ P(x,y)$ by playing the following game. Express that the adversary provides a worst case x by saying "Let x be arbitrary." Then the prover knowing x must construct y. Then you win by proving that $P(x,y)$ is true.
2. Prove $A \Rightarrow B$ by assuming A and proving B.
3. Suppose you have assumed a first order logic statement to be true. This means that you have a strategy for winning the above game. For example, suppose you know that $\forall x,\ \exists y,\ P(x,y)$ is true. Then this asks like a black box oracle in which you can feed it any value for x and it returns to you a value of y for which $P(x,y)$ is guaranteed to be true.
4. One can proceed mechanically, but it is good practice to *understand* each statement as well.

Questions:

1. For years, I had gave the homework to prove that the following statement is false.

   - $\forall A, \exists P, \forall I, Works(P,A,I)$.

   This states that every algorithm correctly solves some problem. I argued that this was not true because some algorithms do not halt on some input instances and hence these algorithms do not "correctly" solve any computational problem.

   It is all about notation, but I have come to believe that it is more useful to redefine the term "computational problem" so that the above statement is true. Given an algorithm A define the computational problem P_A that it solves as follows. For each input instance I, if $A(I)$ halts, then define $P_A(I)$ to be the output $A(I)$. On the other hand, if $A(I)$ does not halt, then define $P_A(I)$ to be the "value" ∞. This definition will be helpful in answering this question.

   You are to formally prove that the following three statements are equivalent.

   S0: $\{P \mid$ Computational Problem P is computed by a Java Program$\}$
   $\subseteq \{P \mid$ Computational Problem P is computed by a Turing Machine$\}$

   S1: $\forall$ computational problems P
   $[[\exists$ Java Program J_P $\forall$ Inputs I $J_P(I) = P(I)]$
   $\Rightarrow [\exists$ Turing Machine M_P $\forall$ Inputs I $M_P(I) = P(I)]]$

   S2: $\forall$ Java Program J $\exists$ Turing Machine M_J $\forall$ Inputs I $M_J(I) = J(I)$

   The proof proceeds in three steps.

   (a) First argue that statements S0 and S1 say the same thing.
   (b) Assume that S1 is true. Now go through the first order logic game to prove that S2 is true.
   (c) Assume that S2 is true. Now go through the first order logic game to prove that S1 is true.

2. Induction.

   (a) Let $P()$ be a predicate that for each integer n specifies whether $P(n)$ is true or is false. The goal is to prove that it is true for each $n \geq 0$. Induction is a standard axiom.

   $$[P(0) \text{ and } \forall n \geq 0,\ [P(n) \Rightarrow P(n+1)]] \Rightarrow [\forall n \geq 0,\ P(n)]$$

The reason we believe this is as follows. If we assume the left, then we know that $P(0)$ is true. Hence we know that $P(1)$ is true. Hence we know that $P(2)$ is true. And so on. This is obvious for any finite number of steps. The induction axiom takes this further. It says that the nature of integers is that if you count $0, 1, 2, 3, \ldots$ then for each integer n, you eventually hit it and as such prove that $P(n)$ is true.

The contra positive of $A \Rightarrow B$ is that $\neg B \Rightarrow \neg A$. State the contra positive of the induction axiom and the argue why it is true.

Hint: $A \Rightarrow B$ not saying that A causes B to happen. It is a boolean statement that is either true or false. It is saying that in every universe in which A is true, B is also true. How do you just use negation, ANDs, and ORs to state what needs to be true to give a counter example to $A \Rightarrow B$.

(b) Consider the following three statements.

i. $\forall n_0,\ \exists n > n_0,\ P(n)$.

ii. The set $S = \{n \mid P(n) \text{ is true }\}$ is finite and hence has a maximum value n_{max}.

iii. There is an infinite sequence $m_0, m_1, m_2, \ldots$ such that for each $i \geq 0$, $P(m_i)$ is true.

Prove that if the second statement is true, then the first statement is not true. Note that by the contra-positive (or proof by contradiction) this proves that if the first statement is true then there are an infinite number of values n for which the property $P(n)$ is true.

(c) Use loop invariants and/or induction to prove that if the first statement in the previous question is true, then so is the third. Note that this is a second proof that if the first statement is true then there are an infinite number of values n for which the property $P(n)$ is true.

3. A classic type of first order logic definitions and proofs are called "Epsilon Delta". The are key to calculus, analysis, and set theory.

Continuous: Let the function $f(x)$ be from reals to reals.
(We state this definition in a number of equivalent ways)
f is said to be *continuous* everywhere
iff $\forall x$, f is continuous at x
iff for an arbitrary definition of closeness, as x' approaches x, $f(x')$ eventually gets and stays close to $f(x)$.
iff $\forall x$, $\forall \epsilon > 0$, within a sufficiently small range near x, f does not vary by more than ϵ
iff $\forall x$, $\forall \epsilon > 0$, $\exists \delta > 0$, $\forall x' \in [x-\delta, x+\delta]$, $|f(x') - f(x)| \leq \epsilon$

Converge: Consider the infinite sequence $a_1, a_2, a_3, \ldots$.
It is said to *converge* to the value a
iff for an arbitrary definition of closeness, the sequence eventually gets and stays close to a
iff $\forall \epsilon > 0, \exists i, \forall i' \geq i, |a_{i'} - a| \leq \epsilon$.

Try to prove the follow.

(a) Assume that $f(x)$ is continuous everywhere. Define $a_i = f(\frac{1}{i})$. Prove that the infinite sequence $a_1, a_2, a_3, \ldots$ converges to the value $f(0)$.

(b) Give one sentence explaining either why the converse is true or why it is not. Namely, let $f(x)$ be a function from the reals to the reals. For every integer i, let $a_i = f(\frac{1}{i})$. Suppose the infinite sequence $a_1, a_2, \ldots$ converges. Do we know that f is continuous at $f(0)$?

4. Intermediate Value Theorem:
If $f(x)$ is a continuous function from the reals to the reals with $f(a) < 0$ and $f(b) > 0$, then there exists a real value $r \in [a, b]$ for which $f(r) = 0$.

More generally, if $g(x)$ is a continuous function and $u \in [g(a), g(b)]$, then there exists a real value $r \in [a, b]$ for which $g(r) = u$.
This is proved from the previous by setting $f(x) = g(x) - u$.

Our task is to prove the first using first order logic.

Binary Search: The algorithm for finding this r is to do binary search, i.e. check the value of $f(m)$ for $m = \frac{a+b}{2}$. But this just moves us "closer" to r. It does not actually move us closer to having a proof.

Continuous: (We state this definition in a number of equivalent ways)
f is said to be *continuous* everywhere
iff $\forall x$, f is continuous at x
iff $\forall x$, $\forall \epsilon > 0$, within a sufficiently small range near x, f does not vary by more than ϵ
iff $\forall x$, $\forall \epsilon > 0$, $\exists \delta > 0$, $\forall x' \in [x-\delta, x+\delta]$, $|f(x') - f(x)| \leq \epsilon$

A Missing Real: Suppose the reals was missing some value r. There are so many real values, surely we would not miss one. Here then is a counter example to the intermediate value theorem. Let $f(x) = -1$ for $x < r$ and $f(x) = 1$ for $x > r$. We would not have to define $f(r)$ because r is not a real. This function is continuous everywhere except at r. Though it is not continuous at r, this is not a problem because r is not a real. This forms a counter example to the intermediate value theorem.

Completeness = Existence of a Supremum: Intuitively, completeness implies that there are not any gaps or missing points in the real number line. We start with a few definitions (each expressed in a number of equivalent ways)

r *upper bounds* a set S of reals
iff $\forall x \in S$, $x \leq r$
iff $\forall x > r$, $x \notin S$.

r is the *maximum* of a set S of reals
iff it upper bounds S and is in S
iff $[\forall x > r, x \notin S]$ and $[r \in S]$.
For example, the maximum of $S = \{x \mid x \leq 5\}$ is 5, but the set $S = \{x \mid x < 5\}$ has no maximum.

A supremum of a set S of reals is supposed to be like a maximum
that does not itself need to be in the set.
For example, the supremum of $S = \{x \mid x < 5\}$ is 5.
r is the *supremum* of a set S of reals
iff it is the minimum of all upper bounds of S
iff $[\forall r' < r$, r' is not an upper bounds of $S]$ and $[r$ is an upper of $S]$
iff $[\forall r' < r, \neg\, [\forall x > r', x \notin S]]$ and $[\forall x' > r, x' \notin S]$
iff $[\forall r' < r, \exists x > r', x \in S]$ and $[\forall x' > r, x' \notin S]$
(but for $x \in S$, we have $x \leq r$.)
iff $[\forall r' < r, \exists x, r' < x \leq r$ and $x \in S]$ and $[\forall x' > r, x' \notin S]$

Our Axiom (stated a few equivalent ways) is that
Every non-empty bounded subset of the reals has a supremum
iff $\forall S \subset \mathcal{R}$, $[S$ is non-empty and $\exists r$, r bounds $S] \Rightarrow [\exists r$, r is a supremum of $S]$

Two Zeros: Suppose that the reals had two zeros, denoted 0 and $0'$. Here then is a counter example to the intermediate value theorem. Let $f(x) = x$, except that $f(0) = 0'$.

Defining Zero: We will need to prove that $f(r)$ is exactly equal to zero. To do this we need the following axiom.

The smallest non-negative number is zero
iff $[\forall \epsilon > 0, |q| \leq \epsilon]] \Rightarrow [q = 0]$.

Proof: Your job is to prove the intermediate value theorem:
If $f(x)$ is a continuous function with $f(a) < 0$ and $f(b) > 0$ and both axioms about the reals are true, then there exists a real value $r \in [a, b]$ for which $f(r) = 0$.
Hint: Let r be the supremum of $S = \{x \leq b \mid f(x) < 0\}$.