CS 381 - A1

Martin Mueller

Due: Friday, February 14^{th}, 2020

1. (5 points) Assuming $c \in \mathbb{R}^+ - \{0\}$ and $N_0, N \in \{i \in \mathbb{Z} | i > 0\}$, use a **direct proof** to disprove the following statement:

$$\boxed{(\exists c, N_0)(\forall N)[N \geq N_0 \rightarrow N \geq c \cdot N^2]}$$

The best way to approach this is by negating the statement and trying to prove that true:

$$\begin{aligned} \neg(\exists c, N_0)(\forall N)[N \geq N_0 \rightarrow N \geq c \cdot N^2] &= \neg(\exists c, N_0)(\forall N)[\neg[N \geq N_0] \vee [N \geq c \cdot N^2]] \\ &= (\forall c, N_0)(\exists N)[N \geq N_0 \wedge N < c \cdot N^2] \end{aligned}$$

In order to prove this, we must select (a) value(s) of N such that for any arbitrary c and N_0, both $N \geq N_0$ *and* $N < c \cdot N^2$. Let's start with the inequality $N < c \cdot N^2$:

$$\begin{aligned} N < c \cdot N^2 &= \frac{N}{N} < c \cdot \frac{N^2}{N} \\ &= 1 < c \cdot N \\ &= \frac{1}{c} < N \end{aligned}$$

Let's now consider the case that $c > 1$. If this is the case, the constant on the left hand side will be smaller than 1. Since N cannot be smaller than 1, the case $c > 1$ works for any N greater than or equal to N_0. However, even if c is arbitrarily small such that the constant $\frac{1}{c}$ is arbitrarily large, we can always pick an N greater than that, as N is not bounded from above. Therefore, there will always be an N that satisfies those two conditions, making the negation of the statement true. This makes the original statement false.

2. (5 points) Recall that a number $q > 1$ is composite if there exists a positive integer d, such that, $d > 1$, $d < q$ and d divides q. Use a proof by contradiction to prove the following statement, assuming q is a positive integer greater than 1:

If, for all integers d, the sufficient conditions $d > 1$ and $d < q$ imply that either $1 = 0$ or d does not divide q, then q is not composite.

First, we'll rewrite the definition of composite. To do this, we'll define two functions: $C(x)$ and $D(x, y)$ to mean that x is composite and x divides y respectively. Incorporating this with the first statement, we get:

$$(q > 1 \wedge (\exists d \in \mathbb{Z}^+)[d > 1 \wedge d < q \wedge D(d, q)]) \rightarrow C(q)$$

Next, we'll also use these functions to restate the proposition we are trying to prove:

$$
\begin{aligned}
&(\forall q \in \mathbb{N} - \{1\}, d \in \mathbb{Z})[[d > 1 \wedge d < q \rightarrow 1 = 0 \vee \neg D(d, q)] \rightarrow \neg C(q)] \\
&= (\forall q \in \mathbb{N} - \{1\}, d \in \mathbb{Z})[[d > 1 \wedge d < q \rightarrow \neg D(d, q)] \rightarrow \neg C(q)]
\end{aligned}
$$

Now we'll rewrite the implications:

$$(\forall q \in \mathbb{N} - \{1\}, d \in \mathbb{Z})[\neg[\neg(d > 1 \wedge d < q) \vee \neg D(d, q)] \vee \neg C(q)]$$

Next we simplify:

$$(\forall q \in \mathbb{N} - \{1\}, d \in \mathbb{Z})[d > 1 \wedge d < q \wedge D(d, q) \vee \neg C(q)]$$

Notice that $d > 1 \wedge d < q \wedge D(d, q)$ for any $q > 1$ is the definition of composite. this means we can further simplify this to:

$$(\forall q \in \mathbb{N} - \{1\}, d \in \mathbb{Z})[C(q) \vee \neg C(q)]$$

For the sake of obtaining a contradiction, let's take this statement and negate it:

$$
\begin{aligned}
&\neg(\forall q \in \mathbb{N} - \{1\}, d \in \mathbb{Z})[C(q) \vee \neg C(q)] \\
&= (\exists q \in \mathbb{N} - \{1\}, d \in \mathbb{Z})[\neg C(q) \wedge C(q)]
\end{aligned}
$$

Here we can see that this is in the form of $\neg r \wedge r$: a contradiction. Since the negation of the statement reveals a contradiction, the statement must be a tautology and therefore is true.