First-Order Logic and Proofs

Now that we're starting to explore more complex discrete structures, we're starting to see more and more definitions phrased in first-order logic. One major advantage of this approach is that first-order definitions, in some sense, give both a formal definition of a term and a sketch for how you might go about proving it.

Below is a table of all the quantifiers and connectives in first-order logic and how you should try to prove statements with each form:

Statement Form	Proof Approach
$\forall x.\ P$	***Direct proof:*** Consider an arbitrary x, then prove P is true for that choice of x. ***By contradiction:*** Suppose for the sake of contradiction that there is some x where P is false. Then derive a contradiction.
$\exists x.\ P$	***Direct proof:*** Do some exploring and find a choice of x where P is true. Then, write a proof explaining why P is true in that case. ***By contradiction:*** Suppose for the sake of contradiction that P is always false and derive a contradiction.
$\neg P$	***Direct proof:*** Simplify your formula by pushing the negation deeper, then apply the appropriate rule. ***By contradiction:*** Suppose for the sake of contradiction that P is true, then derive a contradiction.
$P \wedge Q$	***Direct proof:*** Prove each of P and Q independently. ***By contradiction:*** Assume $\neg P \vee \neg Q$. Then, try to derive a contradiction.
$P \vee Q$	***Direct proof:*** Prove that $\neg P \to Q$, or prove that $\neg Q \to P$. ***By contradiction:*** Assume $\neg P \wedge \neg Q$. Then, try to derive a contradiction.
$P \to Q$	***Direct proof:*** Assume P is true, then prove Q. ***By contradiction:*** Assume P is true and Q is false, then derive a contradiction. ***By contrapositive:*** Assume Q is false, then prove P is false.
$P \leftrightarrow Q$	Prove both $P \to Q$ and $Q \to P$.

The above might seem pretty abstract, so let's make things more concrete. Let's suppose we have a function $g : \mathbb{N} \to \mathbb{N}$ defined as $g(n) = 3n + 137$ and that we want to prove that g is injective. How exactly would we prove this? And what exactly is it that we need to prove?

Well, we happen to have a formal definition for injectivity. Specifically, a function $f : A \to B$ is injective if

$$\forall a_0 \in A.\ \forall a_1 \in A.\ (f(a_0) = f(a_1) \to a_0 = a_1)$$

If we want to prove that g is injective, we need to show that the above statement is true with respect to the function g from $\mathbb{N}$ to $\mathbb{N}$. Substituting that into the first-order definition above gives us

$$\forall n_0 \in \mathbb{N}.\ \forall n_1 \in \mathbb{N}.\ (g(n_0) = g(n_1) \to n_0 = n_1),$$

which is the statement we'll need to prove if we want to show that g is injective.

Now, how do we go about proving this? Well, we can see that this formula is a universal statement:

$$\forall n_0 \in \mathbb{N}.\ \forall n_1 \in \mathbb{N}.\ (g(n_0) = g(n_1) \to n_0 = n_1),$$

Consulting the table on the previous page, we see that the way to prove a statement like this is to choose arbitrary choices of natural numbers n_0 and n_1, then to go and prove the inside of the statement is true given those choices. Therefore, we could start our proof off like this:

> To prove that g is injective, consider arbitrary natural numbers n_0 and n_1.

We now need to prove that, for these choices of n_0 and n_1, that the following statement is true:

$$g(n_0) = g(n_1) \to n_0 = n_1$$

So how do we prove this? Consulting our table, we see that for a formula of the form $P \to Q$, we should assume P and prove Q. Here, this means assuming $g(n_0) = g(n_1)$, then proving $n_0 = n_1$. Let's write that out:

> To prove that g is injective, consider arbitrary natural numbers n_0 and n_1 where $g(n_0) = g(n_1)$. We need to prove that $n_0 = n_1$.

From here, the rest of the job is just showing that this statement is indeed true. To do so, it's probably best to expand out the definition of g to more specifically articulate what we're assuming and what we're going to prove:

> To prove that g is injective, consider arbitrary natural numbers n_0 and n_1 where $g(n_0) = g(n_1)$. In other words, we assume that $3n_0 + 137 = 3n_1 + 137$. We need to prove that $n_0 = n_1$.

Now, we've got a clear statement of what we need to prove. The rest of the proof is then just about filling in the details:

To prove that g is injective, consider arbitrary natural numbers n_0 and n_1 where $g(n_0) = g(n_1)$. In other words, we assume that $3n_0 + 137 = 3n_1 + 137$. We need to prove that $n_0 = n_1$.

Starting with $3n_0 + 137 = 3n_1 + 137$, we can apply some algebra to see that $3n_0 = 3n_1$, so $n_0 = n_1$, as required. ■

Notice how the first-order definition of the terms in question leads us to the shape of the proof we need to write. Without knowing anything about the behavior or properties of the function g, we could still see what we needed to assume, what we needed to prove, and what values were chosen arbitrarily. It's amazing that all of this information was packed into the small set of instructions "prove that g is injective," but that's often how math works: begin by "rehydrating" the statement to prove into something more concrete, then use that to determine how to approach the problem.