First-Order Logic

In this course, we have focused on using a specific logic (the ACL2 logic) for reasoning about programs written in ACL2. It turns out that much of what we learned in fact applies to "standard" logic, used to reason about a variety of things.

What do I mean by "standard" logic? Really, I mean *first-order logic*. The ACL2 logic we have seen is really a variant (fragment, depending on how you look at it) of first-order logic.[1] First-order logic looks just like the ACL2 logic, in the sense that it has the logical operators $\wedge$, $\vee$, $\neg$, $\Rightarrow$, as well as basic facts to reason about (not quite ACL2 expressions, but close, you'll see), but on top of those it also has *quantifiers*.

A quantified formula is a formula of the form $\forall x{\in}A.\varphi$ and $\exists x{\in}A.\varphi$, where φ is a formula, and A is a set of values. We often leave out the A when we mean "all possible values".

- Formula $\forall x{\in}A.\varphi$ is read "for all x in A, φ holds".
- Formula $\exists x{\in}A.\varphi$ is read "there exists an x in A such that φ holds".

We have already seen the first quantifier, $\forall$. It was *implicit* in all our ACL2 theorems. Indeed, a formula such as

```
(= (rev (app x y)) (app (rev y) (rev x)))
```

is really meant to be read as:

$$\forall \texttt{x}{\in}\mathit{Values}.\forall \texttt{y}{\in}\mathit{Values}.\texttt{(= (rev (app x y)) (app (rev y) (rev x)))},$$

where *Values* is the set of all ACL2 values. Note that this is how I used to "pronounce" the original formula anyways.

So how do you prove a formula such as $\forall x{\in}A.\varphi$ or $\exists x{\in}A.\varphi$? There are two rules to remember:

- To prove $\forall x{\in}A.\varphi$, it suffices to prove that $\varphi[x \mapsto v]$ for *any* choice of value v in A, where $\varphi[x \mapsto v]$ is the result of substituting v for x in φ.
- To prove $\exists x{\in}A.\varphi$, it suffices to prove that $\varphi[x \mapsto v]$ for *some* choice of value v in A.

[1] The full logic implemented by the ACL2s theorem prover is in fact full first-order logic, but we haven't seen that yet.

Let's illustrate quantification, as well as convince you that what we've learned about proving stuff in ACL2 carries over to other domains, by proving two facts about functions in mathematics. We will use the same techniques we used in our proofs.

Forget programs for a moment. In mathematics, a function f is a mapping from elements of some set A (called the domain of f) to some set B (called the range of f). We usually write $f : A \to B$ for a function with domain A and range B. Intuitively, $f : A \to B$ associates with every element x of A an element $f(x)$ of B. For example, we can define a function $f : \mathbb{N} \to \mathbb{N}$ by taking $f(n) = n + 1$—it maps every natural number in $\mathbb{N}$ to a natural number (its successor).

Given two functions $f : A \to B$ and $g : B \to C$, we can define their *composition* $g \circ f : A \to C$, by taking $(g \circ f)(x)$ to be $g(f(x))$.

Definition. *A function $f : A \to B$ is* injective *(or* one-to-one*) if it does not map different elements of A to the same element of B, that is, if $\forall x{\in}A.\forall y{\in}A.\,(f(x) = f(y) \Longrightarrow x = y)$.*

Injective functions are particularly well-behaved functions. The successor function above on the natural numbers is injective. In contrast, the absolute value function on the integers is not injective: both 1 and -1, for instance, map to 1.

This is what I want to prove:

Theorem 1. *If $f : A \to B$ is injective and $g : B \to C$ is injective, then $g \circ f : A \to C$ is injective.*

Proof. Let's first formalize this theorem more carefully:

$$(f \textit{ injective}) \wedge (g \textit{ injective}) \Longrightarrow (g \circ f \textit{ injective}).$$

This is an implication, and we know how to prove implications: isolate the context, and prove what's on the right-hand side of the implication. The context is:

A1: f injective, that is, $\forall x{\in}A.\forall y{\in}A.\,(f(x) = f(y) \Longrightarrow x = y)$

A2: g injective, that is, $\forall x{\in}B.\forall y{\in}B.\,(g(x) = g(y) \Longrightarrow x = y)$

In this context, we want to prove $g \circ f$ is injective, that is, we want to prove

$$\forall x{\in}A.\forall y{\in}A.\,(g \circ f)(x) = (g \circ f)(y) \Longrightarrow x = y)\,.$$

Remember, I told you how to prove $\forall$ formulas: show the body of the formula for all choices of values for the quantified variable.

So let's choose a value $x_0{\in}A$ and $y_0{\in}A$, and prove that $(g \circ f)(x_0) = (g \circ f)(y_0) \Longrightarrow x_0 = y_0)$. This x_0 and y_0 are arbitrary, this will show that the formula is true not matter what choices of x and y we take.

So we now want to prove that $(g \circ f)(x_0) = (g \circ f)(y_0) \Longrightarrow x_0 = y_0)$. This is an implication, so it suffices to prove the right-hand side $(x_0 = y_0)$ if we add the context of this formula to the general context above:

A3: $(g \circ f)(x_0) = (g \circ f)(y_0)$

By definitiion of $\circ$, we can rewrite A3 into the equivalent:

A4: $g(f(x_0)) = g(f(y_0))$

We want to prove $x_0 = y_0$, given A1–A4. It turns out that we can prove this by only working on the context. So let's derive interesting properties from the context.

Look at A2. It says: no matter what values from B you choose for x and y, if $g(x) = g(y)$, then $x = y$. Let's instantiate A2 to two specific values of x and y in B, namely $f(x_0)$ and $f(y_0)$. (Question: how do you know those values are in B?)

A5: $g(f(x_0)) = g(f(y_0)) \Longrightarrow f(x_0) = f(y_0)$

Putting together A4 and A5, we can derive, by Modus Ponens:

A6: $f(x_0) = f(y_0)$

So we're learning stuff about x_0 and y_0.

Look at A1 now. It says: no matter what values from A you choose for x and y, if $f(x) = f(y)$, then $x = y$. Let's instantiate A1 to two specific values of x and y, namely x_0 and y_0.

A7: $f(x_0) = f(y_0) \Longrightarrow x_0 = y_0$

Putting together A6 and A7, we can derive, by Modus Ponens:

A8: $x_0 = y_0$

Now it's extremely easy to prove $x_0 = y_0$—remember, that's what we wanted to prove: $x_0 = y_0$ is true simply by virtue of A8. □

The proof is long simply because we're being extra careful. Once you get more practice proving theorems in general, the above can be shortened tremendously.

Let's look at a proof that requires handling existentials ($\exists$).

Definition. *A function $f : A \to B$ is* surjective *(or* onto*) if every element in B is mapped to by an element in A, that is, if $\forall y{\in}B.\exists x{\in}A.(f(z) = y)$.*

Proof. Let's first formalize this theorem more carefully:

$$(f \textit{ surjective}) \wedge (g \textit{ surjective}) \Longrightarrow (g \circ f \textit{ surjective}).$$

Let's isolate the context, and prove what's on the right-hand side of the implication. The context is:

A1: f surjective, that is, $\forall y{\in}B.\exists x{\in}A.f(x) = y$

A2: g surjective, that is, $\forall y{\in}C.\exists x{\in}B.g(x) = y$

In this context, we want to prove $g \circ f$ is surjective, that is, we want to prove

$$\forall y{\in}C.\exists x{\in}A.(g \circ f)(x) = y.$$

To prove this formula, we choose an arbirary value $y_0{\in}C$, and prove that $\exists x{\in}A.(g \circ f)(x) = y_0$. By definition of $\circ$, $\exists x{\in}A.(g \circ f)(x) = y_0$ is equivalent to $\exists x{\in}A.g(f(x)) = y_0$.

To prove the latter formula, we work a bit on the context. Consider A2. It says: for any choice of y in C, $\exists x{\in}B.g(x) = y$. Let's instantiate A2 to our choice $y_0{\in}C$:

A3: $\exists x{\in}B.g(x) = y_0$

A3 says that there is some choice of value for x in B that makes $g(x) = y_0$ true. So let's call that choice $x_0{\in}B$, and we can instantiate A3 to:

A4: $g(x_0) = y_0$.

Look at A1 now. It says: for any choice of y in B, $\exists x{\in}A.f(x) = y$. Let's instantiate A1 to our $x_0 \in B$:

A5: $\exists x{\in}A.f(x) = x_0$

A5 says that there is some choice of value for x in A that makes $f(x) = x_0$ true. So let's call that choice $x_0'{\in}A$, and we can instantiate A5 to:

A6: $f(x_0') = x_0$

Now, substitute $f(x_0')$ for x_0 in A4, and we get:

A7: $g(f(x_0')) = y_0$.

Back to our proof. We want to prove $\exists x{\in}A.g(f(x)) = y_0$. It suffices to show that there is a choice of x that makes $g(f(x)) = y_0$ true. But A7 tells us that $x_0'{\in}A$ is such a choice for x, since $g(f(x_0')) = y_0$. That completes the proof. □

Addendum

Now, the two results above are often proved in a much more informal way.

Theorem 2. *If $f : A \to B$ is injective and $g : B \to C$ is injective, then $g \circ f : A \to C$ is injective.*

Proof. To prove an implication, we assume the left-hand side, and we prove the right-hand side. Therefore, we assume that $f : A \to B$ is injective and that $g : B \to C$ is injective. We want to prove that $g \circ f : A \to C$ is injective, that is, for all choices of $x, y \in A$, if $g(f(x)) = g(f(y))$, then $x = y$. Pick $x_0, y_0 \in A$, and we now only need to prove $g(f(x_0)) = g(f(y_0))) \implies x_0 = y_0$. Assume $g(f(x_0)) = g(f(y_0))$. We want to show that $x_0 = y_0$. Because g is injective, $g(f(x_0)) = g(f(y_0))$ implies that $f(x_0) = f(y_0)$, and therefore $f(x_0) = f(y_0)$. Because f is injective, $f(x_0) = f(y_0)$ implies that $x_0 = y_0$, and therefore $x_0 = y_0$, as required. □

Theorem 3. *If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is surjective.*

Proof. We assume that $f : A \to B$ is surjective and that $g : B \to C$ is surjective. We want to prove that $g \circ f : A \to C$ is surjective, that is, for all choices of $z \in C$, there exists $x \in A$ such that $g(f(x)) = z$. Pick $z_0 \in C$. We need to exhibit some $x_0 \in A$ such that $g(f(x_0)) = z_0$. Because g is injective, there exists some $y_0 \in B$ such that $g(y_0) = z_0$. Because f is surjective, there exists some $x_0 \in A$ such that $f(x_0) = y_0$. I claim that this x_0 is the one we're looking for; indeed, $g(f(x_0)) = g(y_0) = z_0$, as required. □