Logic and Computation **Lecture 30**
CSU 290 Spring 2009 (Pucella) **Monday, Apr 13, 2009**

Informal Proofs by Induction

We saw in the course that a powerful way to prove theorems in the ACL2 logic that involve recursive functions over either the natural numbers or lists is to use induction. (In fact, recursive functions over any kind of data structures can lend themselves to proofs by induction.)

My goal in this lecture is to show you that the techinques we've learned for proving ACL2 formulas by induction carry over to more general settings.

Consider showing that the sum of the first n natural numbers can be computed by $\frac{n(n+1)}{2}$. Suppose we wanted to establish this result in ACL2. We could define

```
(defun sum-up-to (n)
  (if (zp n)
      0
    (+ n (sum-up-to (- n 1)))))
```

and then prove

```
(= (sum-up-to n) (/ (* n (+ n 1)) 2)).
```

You can do this—you should be able to do this. It's an easy proof by induction. Come up with the proof obligations, and go ahead and prove it.

It turns out that if you wanted to prove that the sum $0+1+\cdots+n$ is equal to $\frac{n(n+1)}{2}$ for all natural numbers n directly, without going through an ACL2 formalization, then the proof is still a proof by induction.

Theorem 1. *For all* $n \geq 0$, $0+1+\cdots+n = \frac{n(n+1)}{2}$.

Proof. We prove this by induction on n. Here are the two proof obligations:

(a) $(n = 0) \Longrightarrow (0+1+\cdots+n = \frac{n(n+1)}{2})$

(b) $(n > 0) \wedge (0+1+\cdots+(n-1) = \frac{(n-1)n}{2}) \Longrightarrow (0+1+\cdots+n = \frac{n(n+1)}{2})$

We prove the first proof obligation. Assume $n = 0$, then $0+1+\cdots+n = 0$, and $\frac{n(n+1)}{2} = 0$, so the equality $0+1+\cdots+n = \frac{n(n+1)}{2}$ holds.

We prove the second proof obligation. Assume $n > 0$ and $0+1+\cdots+(n-1) = \frac{(n-1)n}{2}$. We have the following equality:

$$\begin{aligned}
0+1+\cdots+n &= (0+1+\cdots+(n-1))+n \\
&= \frac{(n-1)n}{2}+n && \text{by assumption} \\
&= \frac{(n-1)n+2n}{2} && \text{by bringing to the same denominator} \\
&= \frac{n(n-1+2)}{2} && \text{by arithmetic} \\
&= \frac{n(n+1)}{2}
\end{aligned}$$

which is what we wanted. □

Let's look at another example. Define $\left(\begin{array}{c} n \\ k \end{array}\right)$ to be the number of ways in which you can choose k out of n elements. Using a simple counting argument, you can come up with the following recurrence for $\left(\begin{array}{c} n \\ k \end{array}\right)$:

$$\begin{aligned}
\left(\begin{array}{c} n \\ 0 \end{array}\right) &= 1 \\
\left(\begin{array}{c} n \\ n \end{array}\right) &= 1 \\
\left(\begin{array}{c} n \\ k \end{array}\right) &= \left(\begin{array}{c} n-1 \\ k \end{array}\right) + \left(\begin{array}{c} n-1 \\ k-1 \end{array}\right)
\end{aligned}$$

This gives you a recursive way of computing $\left(\begin{array}{c} n \\ k \end{array}\right)$. There is a direct way too: $\left(\begin{array}{c} n \\ k \end{array}\right)$ is given by $\frac{n!}{k!(n-k)!}$. That's not so obvious. So we want to prove that equality. Unsurprisingly, it's a proof by induction on n. The proof below uses the equality $n! = n(n-1)!$ (if $n \geq 1$).

Theorem 2. *For all $n \geq k \geq 0$, $\left(\begin{array}{c} n \\ k \end{array}\right) = \frac{n!}{k!(n-k)!}$*

Proof. We prove this by induction on n.

The first proof obligation is that the equality holds assuming $n = 0$ (and therefore $k = 0$). Note that $\left(\begin{array}{c} 0 \\ 0 \end{array}\right) = 1$, and $\frac{n!}{k!(n-k)!} = \frac{1}{1} = 1$, so the equality holds.

The second proof obligation is that the equality holds assuming $n > 0$ and the equality holds for $n - 1$. Let's work it out:

$$\begin{aligned}
\left(\begin{array}{c} n \\ k \end{array} \right) &= \left(\begin{array}{c} n-1 \\ k \end{array} \right) + \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) \\
&= \frac{(n-1)!}{k!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\
&= \frac{(n-k)(n-1)!}{k!(n-k)(n-k-1)!} + \frac{k(n-1)!}{k(k-1)!(n-k)!} \\
&= \frac{(n-k)(n-1)! + k(n-1)!}{k!(n-k)!} \\
&= \frac{(n-1)!(n-k+k)}{k!(n-k)!} \\
&= \frac{n(n-1)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!}
\end{aligned}$$

as required. □