Recitation 1:
Rule Induction

15-312: Principles of Programming Languages

Wednesday, January 15, 2014

1 Inductive definitions and natural numbers

Inductive definitions are the basis for a lot of the work we will be doing this semester. Inductive definitions take the following form:

$$\frac{J_1 \quad J_2 \quad J_3 \quad \dots}{J}\ (\textsc{r})$$

Where the meaning of this is "If I can prove $J_1, J_2, \dots$ (the *premises*) then I can use rule $(\textsc{r})$ to prove J (the *conclusion*)."

1.1 Natural numbers

Let's begin with an inductive definition of natural numbers, which has two rules:

$$\frac{}{\mathsf{zero}\ \mathsf{nat}}\ (\textsc{z}) \qquad \frac{n\ \mathsf{nat}}{\mathsf{succ}(n)\ \mathsf{nat}}\ (\textsc{s})$$

The first rule can be read "zero is a natural number." The second rule can be read "If n is a natural number, then $\mathsf{succ}(n)$ is also a natural number."

We often want to prove a property about all natural numbers, $\mathcal{P}(n)$. We can use *rule induction* to do this. In the case of natural numbers, the induction principle is this:

In order to show $\mathcal{P}(n)$ whenever $n\ \mathsf{nat}$, it suffices to show:

- **Rule $(\textsc{z})$:** $\mathcal{P}(\mathsf{zero})$
- **Rule $(\textsc{s})$:** $\mathcal{P}(\mathsf{succ}(n))$ assuming $\mathcal{P}(n)$

1.2 The sum of two natural numbers

We can now give an inductive definition of $\mathsf{plus}(a, b, c)$, a judgment which means that $a + b = c$. There are, again, two rules:

$$\frac{n\ \mathsf{nat}}{\mathsf{plus}(\mathsf{zero}, n, n)}\ (\textsc{pz}) \qquad \frac{\mathsf{plus}(n, m, p)}{\mathsf{plus}(\mathsf{succ}(n), m, \mathsf{succ}(p))}\ (\textsc{ps})$$

The first rule can be read "If n is a natural number, then $0 + n = n$." The second rule can be read "If $n + m = p$, then $(n + 1) + m = (p + 1)$."

1.3 Proofs with inductive definitions

Now, say we want to prove "If n nat, then plus(zero, n, n)." This is easy!

To show: If n nat then plus(zero, n, n)
Apply rule (PZ)
To show: n nat
n nat by assumption

On the other hand the statement "If n nat, then plus(n, zero, n)," while just as true intuitively, is not possible to directly prove. We will prove the statement by a very simple induction! Take $\mathcal{P}(n)$ to be "plus(n, zero, n)." Then, if we prove the two cases of the induction principle in Section **??**, we will have shown that plus(n, zero, n) whenever n nat, which is exactly what we need to show!

- **Case (Z):** Prove $\mathcal{P}$(zero), i.e. prove plus(zero, zero, zero)

  To show: plus(zero, zero, zero)
  Apply rule (PZ).
  To show: zero nat (the premise of rule (PZ))
  Apply rule (Z).

- **Case (S):** Prove $\mathcal{P}$(succ(n)) assuming $\mathcal{P}(n)$, i.e. prove plus(succ(n), zero, succ(n)) assuming plus(n, zero, n) (the IH).

  To show: plus(succ(n), zero, succ(n))
  Apply rule (PS).
  To show: plus(n, zero, n) (the premise of rule (PS))
  Apply the IH.

1.4 Another proof

Inversion for zero: *For all m and p, if* plus(zero, m, p) *, then $m = p$*

Inversion for successor: *For all n, m, p, if* plus(succ(n), m, p)*, then there exists a p' such that $p =$* succ(p') *and* plus(n, m, p').

Lemma 1. *For all n, m, p, if* plus(n, m, p) *then* plus(n, succ(m), succ(p))

Proof. Consider for arbitrary n.

The induction principle tells us that, in order to show $\mathcal{P}(n)$, for any $\mathcal{P}$, it suffices to show

- $\mathcal{P}$(zero)
- For every n', if $\mathcal{P}(n')$, then $\mathcal{P}$(succ(n'))

We define the property $\mathcal{P}$ as follows, $\mathcal{P}(n)$ iff for all m and p, if plus(n, m, p) then plus(n, succ(m), succ(p))

We proceed by induction

- $\mathcal{P}(\mathsf{zero})$

  To show: ____
  Let m be arbitrary and fixed
  Let p be arbitrary and fixed
  1) Assume $\mathsf{plus}(\mathsf{zero}, m, p)$
  Suffices to show: ____
  2) $m = p$ By inversion for zero and (1)
  Suffices to show: $\mathsf{plus}(\mathsf{zero}, \mathsf{succ}(m), \mathsf{succ}(m))$ By (2)
  3) $\mathsf{plus}(\mathsf{zero}, \mathsf{succ}(m), \mathsf{succ}(p))$ By rule (PZ)

- For every n', if $\mathcal{P}(n')$, then $\mathcal{P}(\mathsf{succ}(n'))$

  Let n' be arbitrary and fixed
  1) For all m and p, if $\mathsf{plus}(n', m, p)$ then $\mathsf{plus}(n', \mathsf{succ}(m), \mathsf{succ}(p))$ By ________________
  To show: ____
  Let m be arbitrary and fixed
  Let p be arbitrary and fixed
  2) Assume $\mathsf{plus}(\mathsf{succ}(n'), m, p)$
  Suffices to show: ____
  3) Exists p' such that $p = \mathsf{succ}(p')$ and $\mathsf{plus}(n', m, p')$ By ________________
  Consider such a p'
  Suffices to show: ____ By (3)
  4) $\mathsf{plus}(n', m, p')$
  5) ______________________________ By (1), substituting m for m and p' for p, and (4)
  6) $\mathsf{plus}(\mathsf{succ}(n'), \mathsf{succ}(m), \mathsf{succ}(\mathsf{succ}(p')))$ By (PS) on (5)

Thus, we have established $\mathcal{P}(n)$, which is what we needed show □

2 Proving that $\mathsf{plus}(n, m, p)$ is a function

We intended the inductively defined relation $\mathsf{plus}(n, m, p)$, to be a *function* from n and m to p, that means "If n nat and m nat, there exists a *unique* p nat such that $\mathsf{plus}(n, m, p)$." This, is actually shorthand for two separate statements:

- **Existence:** If n nat and m nat, there exists p nat such that $\mathsf{plus}(n, m, p)$.
- **Uniqueness:** If n nat, m nat, p nat, p' nat, $\mathsf{plus}(n, m, p)$, and $\mathsf{plus}(n, m, p')$, then $p = p'$ nat.

We will consider each of these two proofs in turn.

2.1 Proving existence

We need to prove that if n nat and m nat, there exists p nat such that $\mathsf{plus}(n, m, p)$

We proceed by induction on n nat. Our property of interest, $\mathcal{P}(n)$ is "If m nat, there exists p nat such that $\mathsf{plus}(n, m, p)$."

- **Case** (Z)**:** Prove $\mathcal{P}(\mathsf{zero})$, i.e. prove that if $m\,\mathsf{nat}$, there exists $p\,\mathsf{nat}$ such that $\mathsf{plus}(\mathsf{zero}, m, p)$.

  To show: If $m\,\mathsf{nat}$, there exists $p\,\mathsf{nat}$ such that $\mathsf{plus}(\mathsf{zero}, m, p)$
  Take $p = m$.
  To show: if $m\,\mathsf{nat}$ then $p\,\mathsf{nat}$ and $\mathsf{plus}(\mathsf{zero}, m, m)$
  We took $p = m$, and $m\,\mathsf{nat}$ by assumption.
  To show: If $m\,\mathsf{nat}$, $\mathsf{plus}(\mathsf{zero}, m, m)$.
  Apply rule (PZ).
  To show: $a\,\mathsf{nat}$
  By assumption.

- **Case** (S)**:** Prove $\mathcal{P}(\mathsf{succ}(n))$ assuming $\mathcal{P}(n)$, i.e. prove that if $m\,\mathsf{nat}$, then there exists $p\,\mathsf{nat}$ such that $\mathsf{plus}(\mathsf{succ}(n), m, p)$ assuming that if $m\,\mathsf{nat}$, there exists $p\,\mathsf{nat}$ such that $\mathsf{plus}(n, m, p)$.

  To show: If $m\,\mathsf{nat}$, then there exists $p\,\mathsf{nat}$ such that $\mathsf{plus}(\mathsf{succ}(n), m, p)$
  Let p' be the p that exists by applying the IH
  (which we can apply because $m\,\mathsf{nat}$ by assumption.)
  Choose $p = \mathsf{succ}(p')$.
  To show: If $m\,\mathsf{nat}$, then $\mathsf{succ}(p')\,\mathsf{nat}$ and $\mathsf{plus}(\mathsf{succ}(n), m, \mathsf{succ}(p'))$.
  We have $\mathsf{succ}(p')\,\mathsf{nat}$ by applying the (S) rule, knowing $p'\,\mathsf{nat}$ by the IH as above.
  To show: If $m\,\mathsf{nat}$, then $\mathsf{plus}(\mathsf{succ}(n), m, \mathsf{succ}(p'))$.
  Apply rule (PS).
  To show: If $m\,\mathsf{nat}$, then $\mathsf{plus}(n, m, p')$.
  Apply the IH as above.

2.2 Proving uniqueness

. . . Later... . . .