RECITATION 5: INDUCTION, PRIMITIVE RECURSION, & MIDTERM REVIEW

RYAN KAVANAGH

1. Induction & Primitive Recursion

1.1. A brief recapitulation of Lecture 8. In Lecture 8 (and yesterday's review!), we saw two different elimination rules for natural numbers. The first, which captures induction, is a judgmental form of the principle of induction:

$$\dfrac{n : \mathsf{nat} \quad C(0)\ \mathit{true} \quad \begin{array}{c} \overline{x : \mathsf{nat}} \quad \overline{C(x)\ \mathit{true}}^{\,u} \\ \vdots \\ C(\mathsf{s}\,x)\ \mathit{true} \end{array}}{C(n)\ \mathit{true}}\ \mathsf{natE}^{x,u}$$

The other was the *rule of primitive recursion*, which introduces a new term constructor R for each type τ:

$$\dfrac{n : \mathsf{nat} \quad t_0 : \tau \quad \begin{array}{c} \overline{x : \mathsf{nat}} \quad \overline{r : \tau} \\ \vdots \\ t_s : \tau \end{array}}{R(n, t_0, x.\,r.\,t_s) : \tau}\ \mathsf{natE}^{x,r}$$

Its behaviour is captured by the following reduction rules:

$$\begin{aligned} R(0, t_0, x.\,r.\,t_s) &\Longrightarrow_R t_0, \\ R(\mathsf{s}\,n', t_0, x.\,r.\,t_s) &\Longrightarrow_R [R(n', t_0, x.\,r.\,t_s)/r][n'/x]\,t_s. \end{aligned}$$

These rules R indicate that R describes a recursive function "$R(n)$" on the first parameter, with value t_0 when $n = 0$, and value $[R(n')/r][n'/x]t_s$ when $n = \mathsf{s}\,n'$. This motivates the more readable *schema of primitive recursion*, where we define the function (call it "f" to avoid confusion) f by cases:

$$\begin{aligned} f(0) &= t_0, \\ f(\mathsf{s}\,x) &= t_s(x, f(x)). \end{aligned}$$

We can recover the recursor version of the definition as follows:

$$f = (\mathsf{fn}\ n \Rightarrow R(n, t_0, x.r.t_s(x, r))).$$

1.2. Working with these ideas.

Exercise 1. *The judgmental form of the principle of induction can be used to show the following more traditional formulation that uses universal quantification:*

$$\forall n : \mathsf{nat}.\, C(0) \supset (\forall x : \mathsf{nat}.\, C(x) \supset C(\mathsf{s}\,x)) \supset C(n)\ \mathit{true}.$$

What is the corresponding proof term?

Date: 27 September 2017.

Solution.

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{n : nat} \quad \dfrac{}{C(0)}\,u \quad \dfrac{\dfrac{\dfrac{}{\forall x : \mathsf{nat}.\, C(x) \supset C(\mathsf{s}\,x)}\,v \quad \dfrac{}{x : \mathsf{nat}}}{C(x) \supset C(\mathsf{s}\,x)}\,\forall\mathsf{E} \quad \dfrac{}{C(x)}\,w}{C(\mathsf{s}\,x)}\,\supset\mathsf{E}}{C(n)}\,\mathsf{natE}^{x,w}}{(\forall x : \mathsf{nat}.\, C(x) \supset C(\mathsf{s}\,x)) \supset C(n)}\,\supset\mathsf{I}^{v}}{C(0) \supset (\forall x : \mathsf{nat}.\, C(x) \supset C(\mathsf{s}\,x)) \supset C(n)}\,\supset\mathsf{I}^{u}}{\forall n : \mathsf{nat}.\, C(0) \supset (\forall x : \mathsf{nat}.\, C(x) \supset C(\mathsf{s}\,x)) \supset C(n)}\,\forall\mathsf{I}^{n}
$$

The corresponding proof term is $\mathsf{fn}\ n \Rightarrow \mathsf{fn}\ u \Rightarrow \mathsf{fn}\ v \Rightarrow R(n, u, x.w.(vx)w)$. □

The *total predecessor function* is the primitive recursive function given by the primitive recursion schema

$$
\begin{aligned}
\mathsf{pred}(0) &= 0 \\
\mathsf{pred}(\mathsf{s}\,x) &= x,
\end{aligned}
$$

or equivalently,

$$
\mathsf{pred}(n) = R(n, 0, x.r.x).
$$

Exercise 2. *Informally prove* $\forall x : nat.\, x = 0 \vee \mathsf{s}\,(\mathsf{pred}\ x) = x$. *Extract the corresponding function, assuming we already have a proof term* $p : \forall x.\, \mathsf{pred}\ (\mathsf{s}\,x) = x$.

Proof. By induction on x.

- Case $x = 0$. Need to show: $0 = 0 \vee \mathsf{s}\,(\mathsf{pred}\ 0)) = 0$. We are done by $=\mathsf{I}_{00}$ and $\vee\mathsf{I}_1$.
- Case $x = \mathsf{s}\,x'$. Assume: $x' = 0 \vee \mathsf{s}\,(\mathsf{pred}\ x') = \mathsf{s}\,x'$. By definition of pred, we have $\mathsf{pred}\,\mathsf{s}\,x' = x'$. By $=\mathsf{I}_{ss}$, $\mathsf{s}\,(\mathsf{pred}\ \mathsf{s}\,x') = \mathsf{s}\,x'$. By $\vee\mathsf{I}_2$, $\mathsf{s}\,x' = 0 \vee \mathsf{s}\,(\mathsf{pred}\ \mathsf{s}\,x') = \mathsf{s}\,x'$. This is what we wanted to show.

The corresponding proof term is: $\mathsf{fn}\ x \Rightarrow R(x, \mathsf{inl}(=\mathsf{I}_{00}), x'.r.\mathsf{inr}(=\mathsf{I}_{\mathsf{ss}}\,(px')))$. □

We define *proper subtraction* for the natural numbers as follows to be the function

$$
a \dot{-} b = \begin{cases} a - b & a \geq b \\ 0 & a < b. \end{cases}
$$

Exercise 3. *Give a primitive recursive definition for* pminus.

Solution. We are trying to define a function

$$
\mathsf{pminus} : \mathsf{nat} \to \mathsf{nat} \to \mathsf{nat}
$$

by primitive recursion such that "$\mathsf{pminus}\ a\ b$" encodes $a \dot{-} b$. We make use of the following (informal) observation:

$$
\forall a : \mathsf{nat}.\, \forall b : \mathsf{nat}.\, \mathsf{s}\,b \dot{-} \mathsf{s}\,c = b \dot{-} c.
$$

When solving these examples, it is often useful to informally write out what the function should look like, before trying to find a primitive recursive definition:

$$
\begin{aligned}
(\mathsf{pminus}\ 0)(0) &= 0, \\
(\mathsf{pminus}\ \mathsf{s}\,x)(0) &= \mathsf{s}\,x, \\
(\mathsf{pminus}\ 0)(\mathsf{s}\,y) &= 0, \\
(\mathsf{pminus}\ \mathsf{s}\,x)(\mathsf{s}\,y) &= (\mathsf{pminus}\ x)(y).
\end{aligned}
$$

We can define pminus by primitive recursion on the second argument using the primitive recursion schema as follows:

$$\begin{aligned}(\mathsf{pminus}\ a)(\mathsf{0}) &= a,\\ (\mathsf{pminus}\ a)(\mathsf{s}\,y) &= (\mathsf{pminus}\ (\mathsf{pred}\,a))(y),\end{aligned}$$

or using the recursor:

$$\mathsf{pminus}\ a\ b = R(b, a, x.r.\,\mathsf{pminus}\ (\mathsf{pred}\,a)\ x).$$

Alternatively, we can define pminus by primitive recursion on the first argument:

$$\begin{aligned}\mathsf{pminus}\ \mathsf{0} &= \mathsf{fn}\ b \Rightarrow \mathsf{0},\\ \mathsf{pminus}\ \mathsf{s}\,x &= \mathsf{fn}\ b \Rightarrow R(b, \mathsf{s}\,x, y.r.\,\mathsf{pminus}\,x\,y),\end{aligned}$$

or using the recursor:

$$\mathsf{pminus}\ a = \mathsf{fn}\ b \Rightarrow R(a, \mathsf{0}, x.r.R(b, \mathsf{s}\,x, y.t.\,\mathsf{pminus}\,x\,y)).$$

We can quickly check that the recursor definition matches the above informal description. To help you figure out what's going on, we colour-code a and b. The results of substitutions are determined by blue and Apricot colour-coding:

$$\begin{aligned}
R(\mathsf{0}, \mathsf{0}, x.r.R(b, \mathsf{s}\,x, y.t.\,\mathsf{pminus}\ x\ y)) &\Longrightarrow_R \mathsf{0},\\
R(\mathsf{s}\,x, \mathsf{0}, x.r.R(\mathsf{0}, \mathsf{s}\,x, y.t.\,\mathsf{pminus}\ x\ y)) &\Longrightarrow_R R(\mathsf{0}, \mathsf{s}\,x, y.t.\,\mathsf{pminus}\ x\ y)\\
&\Longrightarrow_R \mathsf{s}\,x,\\
R(\mathsf{s}\,x, \mathsf{0}, x.r.R(\mathsf{s}\,y, \mathsf{s}\,x, y.t.\,\mathsf{pminus}\ x\ y)) &\Longrightarrow_R R(\mathsf{s}\,y, \mathsf{s}\,x, y.t.\,\mathsf{pminus}\ x\ y)\\
&\Longrightarrow_R \mathsf{pminus}\ x\ y.
\end{aligned}$$

□

2. Midterm Review

We spend the remainder of the recitation answering the questions that were submitted via Piazza for the review. We will address them in quasi-logical order.

2.1. **Scoping.**

Colour-code boxes indicate the scope of each assumption or parametric judgment. Nested coloured boxes indicate that each of the corresponding judgments is in scope.

$$\dfrac{\begin{array}{c}\overline{B\ \mathit{true}}^{\,u}\\ \vdots\\ A\ \mathit{true}\end{array}}{A \supset B\ \mathit{true}}\ {\supset}\mathsf{I}^{u}
\qquad
\dfrac{A \vee B\ \mathit{true} \quad \begin{array}{c}\overline{A\ \mathit{true}}^{\,u}\\ \vdots\\ C\ \mathit{true}\end{array} \quad \begin{array}{c}\overline{B\ \mathit{true}}^{\,v}\\ \vdots\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\ {\vee}\mathsf{I}^{u,v}$$

$$\dfrac{\begin{array}{c}\overline{x : \tau}\\ \vdots\\ A(x)\ \mathit{true}\end{array}}{\forall x : \tau.\, A(x)\ \mathit{true}}\ \forall\mathsf{I}^{x}
\qquad
\dfrac{\exists x : \tau.\, A(x)\ \mathit{true} \quad \begin{array}{c}\overline{a : \tau} \quad \overline{A(a)\ \mathit{true}}^{\,u}\\ \vdots\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\ \exists\mathsf{E}^{a,u}$$

We would like to emphasise that you are *not* required to use an assumption or parametric judgment. Indeed, when such judgments are in scope, you are free to use them as many times as you wish, including *zero times*. To underscore this point, consider the following exercise:

Exercise 4. *Prove $A \supset \top$ true.*

Solution. Observe that the assumption

$$\dfrac{}{A\ \mathit{true}}\ u$$

is *not used anywhere* in the following proof:

$$\dfrac{\dfrac{}{\top}\ \top\mathsf{I}}{A \supset \top\ \mathit{true}}\ \supset\mathsf{I}^u. \qquad \square$$

2.2. **Quantifiers.** By popular demand, we prove properties similar to those you proved on homework 3.

Exercise 5. *Prove and give the corresponding proof term for* $(\forall x : \tau.A(x)) \supset \neg\exists x.\neg A(x)$ *true.*

Solution.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x : \tau.\neg A(x)\ \mathit{true}}\ v \qquad \dfrac{\dfrac{}{\neg A(a)\ \mathit{true}}\ w \qquad \dfrac{\dfrac{}{\forall x : \tau.A(x)\ \mathit{true}}\ u \qquad \dfrac{}{a : \tau}}{A(a)\ \mathit{true}}\ \forall E}{\bot\ \mathit{true}}\ \supset E}{\bot\ \mathit{true}}\ \exists E^{a,w}}{\neg\exists x.\neg A(x)\ \mathit{true}}\ \neg I^v}{(\forall x : \tau.A(x)) \supset \neg\exists x.\neg A(x)\ \mathit{true}}\ \supset I^u$$

The corresponding proof term is: $\mathsf{fn}\ u \Rightarrow \mathsf{fn}\ v \Rightarrow \mathsf{let}\ (a, w) = v\ \mathsf{in}\ w(ua)$. $\square$

Exercise 6. *Give the proof and proof term for*

$$(\forall x : \tau.\, P(x) \supset Q(x)) \supset (\exists x : \tau.\, \neg Q(x)) \supset \neg\forall x : \tau.\, P(x)\ \mathit{true}.$$

Solution.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x : \tau.\, \neg Q(x)}\ v \qquad \dfrac{\dfrac{\dfrac{}{\neg Q(a)}\ w \qquad \dfrac{\dfrac{\dfrac{}{\forall x : \tau.\, P(x) \supset Q(x)}\ u \qquad \dfrac{}{a : \tau}}{P(a) \supset Q(a)}\ \forall\mathsf{E} \qquad \dfrac{\dfrac{}{\forall x : \tau.\, P(x)}\ r \qquad \dfrac{}{a : \tau}}{P(a)}\ \forall\mathsf{E}}{Q(a)}\ \supset\mathsf{E}}{\bot}\ \supset\mathsf{E}}{\neg\forall x : \tau.\, P(x)}\ \supset\mathsf{I}^r}{\neg\forall x : \tau.\, P(x)}\ \exists\mathsf{E}^{a,w}}{(\exists x : \tau.\, \neg Q(x)) \supset \neg\forall x : \tau.\, P(x)}\ \supset\mathsf{I}^v}{(\forall x : \tau.\, P(x) \supset Q(x)) \supset (\exists x : \tau.\, \neg Q(x)) \supset \neg\forall x : \tau.\, P(x)}\ \supset\mathsf{I}^u$$

The corresponding proof term is: $\mathsf{fn}\ u \Rightarrow \mathsf{fn}\ v \Rightarrow \mathsf{let}\ (a, w) = v\ \mathsf{in}\ \mathsf{fn}\ r \Rightarrow w((ua)(ra))$. $\square$

2.3. **Harmony.** Consider the "?" connective, defined by its elimination rule:

$$\dfrac{?(A, B, C)\ \mathit{true} \quad A\ \mathit{true} \quad B\ \mathit{true}}{C\ \mathit{true}}\ ?\mathsf{E}.$$

Exercise 7. *Give an introduction rule for* $?(A, B, C)$ *and show it to be locally sound and complete.*

Solution.

$$\dfrac{\begin{array}{c}\dfrac{}{A\ \mathit{true}}\ u \quad \dfrac{}{B\ \mathit{true}}\ v \\ \vdots \\ C\ \mathit{true}\end{array}}{?(A, B, C)\ \mathit{true}}\ ?\mathsf{I}^{u,v}$$

Locally sound:

$$\cfrac{\cfrac{\begin{array}{c}\overline{A\ \mathit{true}}\ u \quad \overline{B\ \mathit{true}}\ v\\ \mathcal{F}\\ C\ \mathit{true}\end{array}}{?(A,B,C)}\ ?\mathsf{I}^{u,v} \quad \begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \quad \begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}}{C}\ ?\mathsf{E} \Longrightarrow_R \begin{array}{c}\cfrac{\mathcal{D}}{A\ \mathit{true}}\ u \quad \cfrac{\mathcal{E}}{B\ \mathit{true}}\ v\\ \mathcal{F}\\ C\ \mathit{true}\end{array}$$

Locally complete:

$$\begin{array}{c}\mathcal{D}\\ ?(A,B,C)\ \mathit{true}\end{array} \Longrightarrow_E \cfrac{\cfrac{\begin{array}{c}\mathcal{D}\\ ?(A,B,C)\end{array} \quad \overline{A\ \mathit{true}}\ u \quad \overline{B\ \mathit{true}}\ v}{C\ \mathit{true}}\ ?\mathsf{E}}{?(A,B,C)\ \mathit{true}}\ ?\mathsf{I}^{u,v}$$

□