Constructive Logic (15-317), Spring 2021
Recitation 5: Recurse in proofs (2021-03-01)
André Platzer et al

1 Heyting Arithmetic

Now that we have fully explored the surrounding machinery, let's try and look at a more sophisticated system of logic.

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

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

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

Its behaviour is captured by the following reduction rules:

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

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 $n = S\ n'$. This motivates the more readable *schema of primitive recursion*, where we define the function (call it "f" to avoid confusion) f by cases:

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

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

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

1.1 All of the rules in one place!

Here are all of the Heyting arithmetic rules.

$$\dfrac{}{0 : \mathsf{nat}}\ \mathsf{nat}I_0 \qquad \dfrac{x : \mathsf{nat}}{\mathsf{s}\ x : \mathsf{nat}}\ \mathsf{nat}I_S$$

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

$$\dfrac{}{0 = 0\ \mathit{true}}\ {=}I_{00} \qquad \dfrac{x = y\ \mathit{true}}{\mathsf{s}\ x = \mathsf{s}\ y\ \mathit{true}}\ {=}I_{SS}$$

$$\dfrac{0 = \mathsf{s}\ x\ \mathit{true}}{C\ \mathit{true}}\ {=}E_{0S} \qquad \dfrac{\mathsf{s}\ x = 0\ \mathit{true}}{C\ \mathit{true}}\ {=}E_{S0} \qquad \dfrac{\mathsf{s}\ x = \mathsf{s}\ y\ \mathit{true}}{x = y\ \mathit{true}}\ {=}E_{SS}$$

$$\dfrac{}{R(0, t_0, x.r.t_S) \Rightarrow_R t_0}\ {\Rightarrow_R}\ I_0 \qquad \dfrac{}{R(\mathsf{s}\ n, t_0, x.r.t_S) \Rightarrow_R [R(n, t_0, x.r.t_S)/r][n/x]t_S}\ {\Rightarrow_R}\ I_S$$

$$\dfrac{A(x)\ \mathit{true} \quad x \Rightarrow_R y}{A(y)\ \mathit{true}}\ {\Rightarrow_R}\ E_1 \qquad \dfrac{A(y)\ \mathit{true} \quad x \Rightarrow_R y}{A(x)\ \mathit{true}}\ {\Rightarrow_R}\ E_2$$

1.2 Working with these ideas

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

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

Solution 1:

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

Task 2. Prove

$$\forall n : \mathsf{nat}.\, R(n, 0, x.r.S\ (S\ r)) = R(n, n, x.r.S\ r)\ \mathit{true}$$

You may assume for the purposes of this proof that $R(S\ y, S\ y, x.r.S\ r) \Rightarrow_R S\ (R(S\ y, y, x.r.S\ r))$ (note that while they are equivalent, neither side actually reduces to the other).
Furthermore, *although this is not a rule*, assume you may step underneath successors, as if you have a rule $\Rightarrow_R I^*$with the premise $x \Rightarrow_R y$ and conclusion $S\ x \Rightarrow_R S\ y$.

Solution 2: Let the following section be called X:

$$\dfrac{\dfrac{\dfrac{}{0 = 0\ \mathit{true}}\ {=}I_{00} \quad \dfrac{}{R(0, 0, x.r.S\ (S\ r)) \Rightarrow_R 0\ \mathit{true}}\ {\Rightarrow_R}\ I_0}{R(0, 0, x.r.S\ (S\ r)) = 0\ \mathit{true}}\ {\Rightarrow_R}\ E_2 \quad \dfrac{}{R(0, 0, x.r.S\ r) \Rightarrow_R 0\ \mathit{true}}\ {\Rightarrow_R}\ I_0}{R(0, 0, x.r.S\ (S\ r)) = R(0, 0, x.r.S\ r)\ \mathit{true}}\ {\Rightarrow_R}\ E_2$$

Let the following section be called Y:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{R(y,0,x.r.S\ (S\ r)) = R(y,y,x.r.S\ r)\ \mathit{true}}\ u}{S\ (R(y,0,x.r.S\ (S\ r))) = S\ (R(y,y,x.r.S\ r))\ \mathit{true}} = I_{SS}}{S\ (S\ (R(y,0,x.r.S\ (S\ r)))) = S\ (S\ (R(y,y,x.r.S\ r)))\ \mathit{true}} = I_{SS} \quad \dfrac{}{R(S\ y,0,x.r.S\ (S\ r)) \Rightarrow_R S\ (S\ (R(y,0,x.r.S\ (S\ r))))\ \mathit{true}} \Rightarrow_R I_S}{R(S\ y,0,x.r.S\ (S\ r)) = S\ (S\ (R(y,y,x.r.S\ r)))} \Rightarrow_R E_2$$

Let the following section be called Z:

$$\dfrac{\dfrac{Y \quad \dfrac{\dfrac{}{R(S\ y,y,x.r.S\ r) \Rightarrow_R S\ (R(y,y,x.r.S\ r))\ \mathit{true}} \Rightarrow_R I_S}{S\ (R(S\ y,y,x.r.S\ r)) \Rightarrow_R S\ (S\ (R(y,y,x.r.S\ r)))\ \mathit{true}} \Rightarrow_R I^*}{R(S\ y,0,x.r.S\ (S\ r)) = S\ (R(S\ y,y,x.r.S\ r))\ \mathit{true}} \Rightarrow_R E_2 \quad \dfrac{}{R(S\ y,S\ y,x.r.S\ r) \Rightarrow_R S\ (R(S\ y,y,x.r.S\ r))\ \mathit{true}}\ \text{given}}{R(S\ y,0,x.r.S\ (S\ r)) = R(S\ y,S\ y,x.r.S\ r)\ \mathit{true}} \Rightarrow_R E_2$$

The full proof is then:

$$\dfrac{\dfrac{\dfrac{}{a : \mathit{nat}} \quad X \quad Z}{R(a,0,x.r.S\ (S\ r)) = R(a,a,x.r.S\ r)\ \mathit{true}}\ \mathsf{natE}^{y,u}}{\forall n : \mathsf{nat}.\, R(n,0,x.r.S\ (S\ r)) = R(n,n,x.r.S\ r)\ \mathit{true}}\ \forall \mathsf{I}^n$$