15-317 Lecture 7: Heyting Arithmetic

- Natural numbers as a type
- Induction
- Equality of nats
- Primitive Recursion
- Proof Terms

Natural Numbers

- $t : \tau$ has an instance $n : nat$

$$\frac{}{z : nat}\, nat\, I_0$$

$(0 : nat)$

$$\frac{n : nat}{s\, n : nat}\, nat\, I_S$$

$$\frac{\dfrac{\dfrac{}{z : nat}\, I_0}{S(z) : nat}\, I_S}{S(S(z)) : nat}\, nat\, I_S$$

$$\frac{n : nat \qquad C(z)\ true \qquad \begin{array}{c} \overline{x : nat} \quad \overline{C(x)}^{u} \\ \vdots \\ C(s\, x) \end{array}}{C(n)\ true}\, nat\, E^{x,u}$$

$$\overline{w : nat} \qquad \overline{w = Z \vee \exists y{:}nat.\ w = sy \text{ bw}}^{\,u}$$

proven in 2 pages

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$x : nat$}
\AxiomC{}
\RightLabel{$=I_{ZZ}$}
\UnaryInfC{$Z = Z$}
\RightLabel{$\vee I_1$}
\UnaryInfC{$Z = Z \vee \exists \ldots$}
\AxiomC{}
\UnaryInfC{$w : nat$}
\AxiomC{$\forall x{:}nat\ x' = x' \text{ true}$}
\AxiomC{}
\RightLabel{w}
\UnaryInfC{$w : nat$}
\RightLabel{$\forall E$}
\BinaryInfC{$w = w$}
\RightLabel{$=I_{ss}$}
\UnaryInfC{$sw = sw$}
\RightLabel{$\exists I$}
\BinaryInfC{$\exists y{:}nat.\ sw = sy$}
\RightLabel{$\vee I_2$}
\UnaryInfC{$sw = Z \vee \exists y{:}nat.\ sw = sy$}
\RightLabel{$nat E^{w,u}$}
\TrinaryInfC{$x = Z \vee \exists \ldots \text{ true}$}
\RightLabel{$\forall I^{x}$}
\UnaryInfC{$\forall x{:}nat.\ x = Z \vee \exists y{:}nat.\ x = sy \text{ true}$}
\end{prooftree}
$$

Equality for nat

$$\frac{}{z = z \ \text{true}} =I_{zz}$$

$$\frac{x = y \ \text{true}}{s\,x = s\,y \ \text{true}} =I_{ss}$$

$$\cancel{\frac{}{s\,x = z \ \text{true}}} \ ??$$

No $=E_{zz}$

$$\frac{s\,x = s\,y \ \text{true}}{x = y \ \text{true}} =E_{ss}$$

$$\frac{s\,x = z \ \text{true}}{C \ \text{true}} =E_{sz} \qquad \frac{z = s\,x \ \text{true}}{C \ \text{true}} =E_{zs}$$

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ x = y \ \text{true}\end{array}}{s\,x = s\,y \ \text{true}} =I_{ss}}{x = y \ \text{true}} =E_{ss} \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{D}\\ x = y \ \text{true}\end{array}$$

$$\begin{array}{c}\mathcal{D}\\ s\,x = s\,y \ \text{true}\end{array} \quad \Longrightarrow_E$$

$$z = z \ \text{true}$$

$$\frac{}{y : nat} \qquad \frac{}{y = y \ true}\, u$$

$$\dfrac{\dfrac{}{x : nat} \qquad \dfrac{}{z = z \ true}\, {=}I_{zz} \qquad \dfrac{\dfrac{}{y = y}\, u}{s\,y = s\,y \ \ true}\, {=}I_{ss}}{\dfrac{x = x \ true}{\forall x : nat \,.\, x = x \ true}\, \forall I^{x}}\, nat\,E^{y,u}$$

Primitive Recursion

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

$$\begin{array}{c}\mathcal{D} \\ n : nat\end{array} \;\Longrightarrow_E\; \dfrac{\begin{array}{c}\mathcal{D} \\ n : nat\end{array} \qquad \dfrac{}{z : nat}\,nat\,I_z \qquad \dfrac{\overline{x : nat}}{s\,x : nat}\,nat\,I_s}{R(n, z, x.r.\,s\,x) : nat}$$

Compare with a recursive function f:

$$\left.\begin{array}{l} f(z) = t_0 \\ f(s\,y) = \underbrace{t_s(y, f(y))}\quad \text{or} \quad t_s[y/x, f(y)/r] \end{array}\right\}\; R(n, t_0, x.r.t_s)$$

$$R(z, t_0, x.r.\, t_s) \Longrightarrow_R t_0$$

$$R(s\,y, t_0, x.r.\, t_s) \Longrightarrow_R t_s\,[y/x]\,[R(y, t_0, x.r.\, t_s)/r]$$

$$\text{factorial}\ n = R(n, s\,z, x.r.\, n * r)$$

$$\begin{aligned}
\text{factorial}\ (s\,s\,z) &\Longrightarrow_R (s\,s\,z) * R(s\,z, s\,z, x.r.\, n * r) \\
&\Longrightarrow_R (s\,s\,z) * (s\,z) * R(z, s\,z, x.r.\, n * r) \\
&\Longrightarrow_R (s\,s\,z) * (s\,z) * (s\,z)
\end{aligned}$$

$$\dfrac{\begin{array}{c}\overline{x : \sigma} \\ \vdots \\ t : \tau\end{array}}{\lambda x.\, t : \sigma \to \tau} \to I \qquad \dfrac{f : \sigma \to \tau \qquad t : \sigma}{f(t) : \tau} \to E$$

$$\dfrac{t_1 : \tau_1 \qquad t_2 : \tau_2}{(t_1, t_2) : \tau_1 \times \tau_2} \times I$$

$$\text{double} = \lambda n{:}\text{nat}.\ R(n,\ z,\ x.r.\ ssr) \qquad \begin{cases} f(0) = 0 \\ f(n+1) = 2 + f(n) \end{cases}$$

$$\text{plus} = \lambda x{:}\text{nat}.\ \lambda y{:}\text{nat}.\ R(x,\ y,\ w.r.\ s(r))$$

$$\text{plus}' = \lambda x{:}\text{nat}.\ \underbrace{R(x,\ \lambda y.y,\ w.r.\ \lambda y.\ s(r(y)))}_{\text{nat} \to \text{nat}}$$

$$\text{zeros} = \lambda x{:}\text{nat}.\ R(x,\ [\,],\ w.r.\ z :: r) \qquad \text{(informally)}$$

$$\text{plus}'\ ssz \Rightarrow_K \lambda y'.\ s(R(sz,\ \ldots)\ y')$$

$$\Rightarrow_R \lambda y'.\ s(\lambda y''.\ s(R(z, \ldots)\ y'')\ y')$$

$$\Rightarrow_R \lambda y'.\ s(\lambda y''.\ s(\lambda y.y\ \ y''))\ y'$$

$$\Rightarrow_R \lambda y'.\ s((\lambda y''.\ s(y''))\ y')$$

$$\Rightarrow_R \lambda y'.\ ss\ y'$$

$$\dfrac{n : nat \qquad M_0 : C(0) \qquad \begin{array}{c} \overline{x : nat} \quad \overline{u : C(x)}^{\,u} \\ \vdots \\ M_s : C(s\,x) \end{array}}{R(n, M_0, x.u.M_s) : C(n)}\; natE^{x,u}$$

$$\dfrac{\dfrac{\begin{matrix}\mathcal{D}\\ n \text{ inat}\end{matrix}}{s\,n \text{ inat}}\,\text{nat}I_s \qquad \begin{matrix}\mathcal{E}\\ C(0) \text{ true}\end{matrix} \qquad \begin{matrix}\overline{x \text{ inat}} \quad \overline{C(x) \text{ true}}^{\,u}\\ \mathcal{F}\\ C(s\,x) \text{ true}\end{matrix}}{C(s\,n) \text{ true}}$$

$$\Longrightarrow_R$$

$$\begin{matrix}\dfrac{\begin{matrix}\mathcal{D}\\ n \text{ inat}\end{matrix} \qquad \begin{matrix}\mathcal{E}\\ C(0) \text{ true}\end{matrix} \qquad \begin{matrix}\overline{x \text{ inat}} \quad C(x) \text{ true}\\ \mathcal{F}\\ C(s\,x) \text{ true}\end{matrix}}{C(n) \text{ true}}\,\text{nat}E\\ \mathcal{F}\\ C(s\,n) \text{ true}\end{matrix}$$