Recitation 4: Quantification and Arithmetic

Course Staff

1 Quantifiers

Up to now, we have been vague about what, exactly, our atomic propositions A are representing. In order to discuss quantification, however, we need to be precise over what, exactly, we are quantifying over. We do this via a new judgment $t : \tau$, where τ is some to-be-defined type. Oftentimes, we are interested in some particular type, like the type of natural numbers or the type of Turing Machines, but the meaning of the $\exists$ and $\forall$ connectives are independent of this.

The rules for verifying these are as follows:

$$\frac{\begin{array}{c}\overline{c : A}\\ \vdots\\ A(c)\uparrow\end{array}}{\forall x : \tau.\, A(x)\uparrow}\ \forall \mathsf{I}^c \qquad \frac{\forall x : \tau.\, A(x)\downarrow \quad t : \tau}{A(t)\downarrow}\ \forall \mathsf{E}$$

$$\frac{t : \tau \quad A(t)\uparrow}{\exists x : \tau.\, A(x)\uparrow}\ \exists \mathsf{I} \qquad \frac{\exists x : \tau.\, A(x)\downarrow \qquad \begin{array}{c}\overline{c : \tau} \quad \overline{A(c)\downarrow}^{\,u}\\ \vdots\\ C\uparrow\end{array}}{C\uparrow}\ \exists \mathsf{E}^{c,u}$$

By now, you should be comfortable with erasing the arrows to recover the rules defining these connectives for natural deduction. The intuition for these rules should be straightforward – to prove that some proposition $A(x)$ is true for all $x : \tau$, we should be able to derive $A(c)$ *true* for some arbitrary $c : \tau$. Similarly, we can introduce an existential by demonstrating some object satisfying the proposition.

Eliminating foralls is similarly simple. To eliminate an existential, however, we must do a little more work. If we have $\exists x : \tau.\, A(x)$, then we may not assume anything else about the witness! It must be an object of type τ, and also that it satisfies $A(x)$, but any other properties must be abstracted out, to be replaced with an arbitrary object with the known properties.

2 Examples with quantifiers

Consider predicates $A(x)$ and $B(x)$ which depend on $x : \tau$. We will show $\forall x : \tau.\, A(x) \wedge B(x) \supset \forall x : \tau.\, A(x) \wedge \forall x : \tau.\, B(x)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x : \tau.\, A(x) \wedge B(x)\ \mathit{true}}\,p \quad \dfrac{}{u : \tau}}{A(u) \wedge B(u)\ \mathit{true}}\ \forall \mathsf{E}}{A(u)\ \mathit{true}}\ \wedge \mathsf{E}_1}{\forall x : \tau.\, A(x)\ \mathit{true}}\ \forall \mathsf{I}_u \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x : \tau.\, A(x) \wedge B(x)\ \mathit{true}}\,p \quad \dfrac{}{v : \tau}}{A(v) \wedge B(v)\ \mathit{true}}\ \forall \mathsf{E}}{A(v)\ \mathit{true}}\ \wedge \mathsf{E}_2}{\forall x : \tau.\, B(x)\ \mathit{true}}\ \forall \mathsf{I}_v}{\forall x : \tau.\, A(x) \wedge \forall x : \tau.\, B(x)\ \mathit{true}}\ \wedge \mathsf{I}}{\forall x : \tau.\, A(x) \wedge B(x) \supset \forall x : \tau.\, A(x) \wedge \forall x : \tau.\, B(x)\ \mathit{true}}\ \supset \mathsf{I}^p$$

Next, let $A(x, y)$ be a formula with two variables $x : \tau$ and $y : \sigma$. We will show that you can "swap" an existential and universal.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\exists y : \tau. \forall x : \sigma. A(x, y) \downarrow}\, u \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\forall x : \sigma. A(x, d) \downarrow}\, v \quad \dfrac{}{c : \sigma}}{A(c, d) \downarrow}\, \forall \mathsf{E}}{A(c, d) \uparrow}\, \updownarrow \quad \dfrac{}{d : \tau}}{\exists y : \tau. A(c, y) \uparrow}\, \exists \mathsf{I}}{\exists y : \tau. A(c, y) \uparrow}\, \exists \mathsf{E}^{d,v}}{\forall x : \sigma. \exists y : \tau. A(x, y) \uparrow}\, \forall \mathsf{I}^{c}}{(\exists y : \tau. \forall x : \sigma. A(x, y)) \supset (\forall x : \sigma. \exists y : \tau. A(x, y)) \uparrow}\, \supset \mathsf{I}^{u}$$

3 Heyting Arithmetic

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

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

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

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

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:

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

3.1 Working with these ideas

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

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

As an exercise, try it before looking at the solution.

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