Lecture Notes on Quantification

15-317: Constructive Logic

Frank Pfenning*

Lecture 5
September 15, 2016

1 Introduction

In this lecture, we introduce universal and existential quantification, making the transition from purely propositional logic to first-order intuitionistic logic. As usual, we follow the method of using introduction and elimination rules to explain the meaning of the connectives. An important aspect of the treatment of quantifiers is that it should be completely independent of the domain of quantification. We want to capture what is true of all quantifiers, rather than those applying to natural numbers or integers or rationals or lists or other type of data. We will therefore quantify over objects of an unspecified (arbitrary) type τ. Whatever we derive, will of course also hold for specific domain (for example, $\tau = \mathsf{nat}$). The basic judgment connecting objects t to types τ is $t : \tau$. We will refer to this judgment here, but not define any specific instances until later in the course when discussing data types. What emerges as a important judgmental principle is that of a parametric judgment and the associated substitution principle for objects.

2 Universal Quantification

First, universal quantification, written as $\forall x{:}\tau.\ A(x)$ and pronounced "for all x of type τ, $A(x)$". Here x is a bound variable and can therefore be

*Edits by André Platzer.

renamed so that $\forall x{:}\tau.\ A(x)$ and $\forall y{:}\tau.\ A(y)$ are equivalent. When we write $A(x)$ we mean an arbitrary proposition which may depend on x.

For the introduction rule we require that $A(a)$ be true for arbitrary a. In other words, the premise contains a *parametric judgment*, explained in more detail below.

$$\dfrac{\begin{array}{c}\overline{a : \tau}\\ \vdots \\ A(a)\ \mathit{true}\end{array}}{\forall x{:}\tau.\ A(x)\ \mathit{true}}\ \forall I^a$$

It is important that a be a *new* parameter, not used outside of its scope, which is the derivation between the new hypothesis $a : \tau$ and the conclusion $A(a)$ *true*. In particular, it may not occur in $\forall x{:}\tau.\ A(x)$. The rule makes sense: A proof that $A(x)$ holds for all x of type τ considers any arbitrary a of type τ and shows that $A(a)$ *true*. But it is important that a was indeed arbitrary and not constrained by anything other than its type τ. Observe that the parameter a is of a different kind than the label for the assumption a in the implication introduction rule $\supset I$, because a is a parameter for objects of type τ while u is a label of a proposition, and in fact the rules use different judgments. As a notational reminder for this difference, we not only use different names but also do not attach the parameter a to the rule bar.

If we think of this rule as the defining property of universal quantification, then a verification of $\forall x{:}\tau.\ A(x)$ describes a construction by which an arbitrary $t : \tau$ can be transformed into a proof of $A(t)$ *true*. The corresponding elimination rule $\forall E$, thus, accepts some $t{:}\tau$ and concludes that $A(t)$ *true*:

$$\dfrac{\forall x{:}\tau.\ A(x)\ \mathit{true} \quad t : \tau}{A(t)\ \mathit{true}}\ \forall E$$

We must verify that $t : \tau$ so that $A(t)$ is a well-formed proposition. The elimination rule makes sense: if $A(x)$ is true for all x of type τ, and if t is a particular term of type τ, then $A(t)$ is true as well for this particular t of type τ.

The local reduction uses the following *substitution principle for parametric judgments*:

$$\text{If}\quad \begin{array}{c} a : \tau \\ \mathcal{D} \\ J(a)\end{array} \quad\text{and}\quad \begin{array}{c}\mathcal{E}\\ t : \tau\end{array} \quad\text{then}\quad \begin{array}{c}\mathcal{E}\\ \overline{t : \tau}\\ {[t/a]\mathcal{D}}\\ J(t)\end{array}$$

That is, if $\mathcal{D}$ is a deduction deducing $J(a)$ from the judgment $a : \tau$ about parameter a, and if $\mathcal{E}$ is a deduction that term t is of type τ, we can substitute the term t for parameter a throughout the derivation $\mathcal{D}$ to obtain the derivation on the right that no longer depends on parameter a and uses the deduction $\mathcal{E}$ to show that t has the appropriate type. The right hand side is constructed by systematically substituting t for a in $\mathcal{D}$ and the judgments occurring in it. As usual, this substitution must be *capture avoiding* to be meaningful. It is the substitution into the judgments themselves which distinguishes substitution for parameters from substitution for hypotheses. The substitution into the judgments is necessary here since the propositions in the judgments in $\mathcal{D}$ may still mention parameter a, which needs to be substituted to become t instead.

The local reduction showing local soundness of universal quantification then exploits this substitution principle.

$$\dfrac{\dfrac{\begin{array}{c}\overline{a : \tau}\\ \mathcal{D}\\ A(a)\ \mathit{true}\end{array}}{\forall x{:}\tau.\ A(x)\ \mathit{true}}\ \forall I^a \quad \begin{array}{c}\mathcal{E}\\ t : \tau\end{array}}{A(t)\ \mathit{true}}\ \forall E \quad \Longrightarrow_R \quad \begin{array}{c}\dfrac{\mathcal{E}}{t : \tau}\\ {[t/a]\mathcal{D}}\\ A(t)\ \mathit{true}\end{array}$$

The local expansion showing local completeness of universal quantification introduces a parameter which we can use to eliminate the universal quantifier.

$$\begin{array}{c}\mathcal{D}\\ \forall x{:}\tau.\ A(x)\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ \forall x{:}\tau.\ A(x)\ \mathit{true}\end{array} \quad \overline{a : \tau}}{A(a)\ \mathit{true}}\ \forall E}{\forall x{:}\tau.\ A(x)\ \mathit{true}}\ \forall I^a$$

As a simple example, consider the proof that universal quantifiers distribute over conjunction.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{\forall x{:}\tau.\ (A(x) \wedge B(x))\ \mathit{true}}^{\ u} \quad \overline{a : \tau}}{A(a) \wedge B(a)\ \mathit{true}}\ \forall E}{A(a)\ \mathit{true}}\ \wedge E_1}{\forall x{:}\tau.\ A(x)\ \mathit{true}}\ \forall I^a \quad \dfrac{\dfrac{\dfrac{\overline{\forall x{:}\tau.\ (A(x) \wedge B(x))\ \mathit{true}}^{\ u} \quad \overline{b : \tau}}{A(b) \wedge B(b)\ \mathit{true}}\ \forall E}{B(b)\ \mathit{true}}\ \wedge E_2}{\forall x{:}\tau.\ B(x)\ \mathit{true}}\ \forall I^b}{(\forall x{:}\tau.\ A(x)) \wedge (\forall x{:}\tau.\ B(x))\ \mathit{true}}\ \wedge I}{(\forall x{:}\tau.\ (A(x) \wedge B(x))) \supset (\forall x{:}\tau.\ A(x)) \wedge (\forall x{:}\tau.\ B(x))\ \mathit{true}}\ \supset I^u$$

Note how crucial it is that the parameter a in $\forall I^a$ is new, otherwise, the rules would unsoundly prove that a predicate C that is reflexive (i.e., $C(x,x)$ holds for all x) holds for all x, y, which is clearly not the case:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x{:}\tau.\ C(x,x)\ \mathit{true}}\,u \quad \dfrac{}{a:\tau}}{C(a,a)\ \mathit{true}}\,\forall E}{\forall y{:}\tau.\ C(a,y)\ \mathit{true}}\,\forall I^a??}{\forall x{:}\tau.\ \forall y{:}\tau.\ C(x,y)\ \mathit{true}}\,\forall I^a}{(\forall x{:}\tau.\ C(x,x)) \supset (\forall x{:}\tau.\ \forall y{:}\tau.\ C(x,y))\ \mathit{true}}\,\supset I^u$$

3 Existential Quantification

The existential quantifier is more difficult to specify, although the introduction rule seems innocuous enough. If there is a t of type τ for which a proof of $A(t)$ *true* succeeds, then there is a proof of $\exists x{:}\tau.\ A(x)$ *true* witnessed by said t.

$$\dfrac{t:\tau \quad A(t)\ \mathit{true}}{\exists x{:}\tau.\ A(x)\ \mathit{true}}\,\exists I$$

The elimination rules creates some difficulties. We cannot write

$$\dfrac{\exists x{:}\tau.\ A(x)\ \mathit{true}}{A(t)\ \mathit{true}}\,\exists E?$$

because we do not know for which t is is the case that $A(t)$ holds. It is easy to see that local soundness would fail with this rule, because we would prove $\exists x{:}\tau.\ A(x)$ with one witness t and then eliminate the quantifier using another object t' about which we have no reason to believe it would satisfy $A(t')$ *true*.

The best we can do is to assume that $A(a)$ is true for some new parameter a that, because it is new, we do not know anything about. The scope of this assumption is limited to the proof of some conclusion C *true* which does not mention a (which must be new).

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

Here, the scope of the hypotheses a and u is the deduction on the right, indicated by the vertical dots. In particular, C may not depend on a since a would otherwise escape its scope. We use this crucially in the local reduction for local soundness to see that C is unaffected when substituting t for a in the proof.

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ t : \tau\end{array} \quad \begin{array}{c}\mathcal{E}\\ A(t)\ \mathit{true}\end{array}}{\exists x{:}\tau.\ A(x)\ \mathit{true}}\ \exists I \qquad \begin{array}{c}\overline{a : \tau} \quad \overline{A(a)\ \mathit{true}}^{\,u}\\ \mathcal{F}\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\ \exists E^{a,u} \qquad \Longrightarrow_R \qquad \begin{array}{c}\dfrac{\mathcal{D}}{t : \tau} \quad \dfrac{\mathcal{E}}{A(t)\ \mathit{true}}\ u\\ {[t/a]\mathcal{F}}\\ C\ \mathit{true}\end{array}$$

The reduction requires two substitutions, one for a parameter a and one for a hypothesis u.

The local expansion showing local completeness is patterned after the disjunction, which also—somewhat surprisingly—uses the elimination rule below the introduction rule.

$$\begin{array}{c}\mathcal{D}\\ \exists x{:}\tau.\ A(x)\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\begin{array}{c}\mathcal{D}\\ \exists x{:}\tau.\ A(x)\ \mathit{true}\end{array} \quad \dfrac{\overline{a : \tau} \quad \overline{A(a)\ \mathit{true}}^{\,u}}{\exists x{:}\tau.\ A(x)\ \mathit{true}}\ \exists I}{\exists x{:}\tau.\ A(x)\ \mathit{true}}\ \exists E^{a,u}$$

As an example of quantifiers we show the equivalence of $\forall x{:}\tau.\ A(x) \supset C$ and $(\exists x{:}\tau.\ A(x)) \supset C$, where C does not depend on x. Generally, in our propositions, any possible dependence on a bound variable is indicated by writing a general *predicate* $A(x_1, \ldots, x_n)$. We do not make explicit when such propositions are well-formed, although appropriate rules for explicit A could be given.

When looking at a proof, the static representation on the page is an inadequate image for the dynamics of proof construction. As we did earlier, we give two examples where we show the various stages of proof construction.

$$\begin{array}{c}\vdots\\ ((\exists x{:}\tau.\ A(x)) \supset C) \supset \forall x{:}\tau.\ (A(x) \supset C)\ \mathit{true}\end{array}$$

The first three steps can be taken without hesitation, because we can always apply implication and universal introduction from the bottom up without possibly missing a proof.

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

At this point the conclusion is atomic, so we must apply an elimination to an assumption if we follow the strategy of *introductions bottom-up* and *eliminations top-down*. The only possibility is implication elimination, since $a : \tau$ and $A(a)$ *true* are atomic. This gives us a new subgoal.

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

At this point it is easy to see how to complete the proof with an existential introduction.

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

We now consider the reverse implication.

$$\begin{array}{c}\vdots \\ (\forall x{:}\tau.\ (A(x) \supset C)) \supset ((\exists x{:}\tau.\ A(x)) \supset C)\ \mathit{true}\end{array}$$

From the initial goal, we can blindly carry out two implication introductions, bottom-up, which yields the following situation.

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

No we have two choices: existential elimination applied to w or universal elimination applied to u. However, we have not introduced any terms, so only the existential elimination can go forward.

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

At this point we need to apply another elimination rule to an assumption. We don't have much to work with, so we try universal elimination.

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

Now we can fill the gap with an implication elimination.

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

Finally, note again how crucial it is that the parameter a is actually new and does not occur in the conclusion C, otherwise we could prove unsound things:

$$\dfrac{\dfrac{\dfrac{}{\exists x{:}\tau.\ C(x)\ \mathit{true}}\ u \qquad \dfrac{}{a : \tau} \quad \dfrac{}{C(a)\ \mathit{true}}\ w}{C(a)\ \mathit{true}}\ \forall E^{a,w}??}{(\exists x{:}\tau.\ C(x)) \supset C(a)\ \mathit{true}}\ {\supset}I^u$$

4 Verifications and Uses

In order to formalize the proof search strategy, we use the judgments A has a verification ($A\uparrow$) and A may be used ($A\downarrow$) as we did in the propositional case. Universal quantification is straightforward:

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

We do not assign a direction to the judgment for typing objects, $t : \tau$.

Verifications for the existential elimination are patterned after the disjunction: we translate a usable $\exists x{:}\tau.\ A(x)$ into a usable $A(a)$ with a limited scope, both in the verification of some C.

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

As before, the fact that every true proposition has a verification is a kind of global version of the local soundness and completeness properties. If we take this for granted (since we do not prove it until later), then we can use this to demonstrate that certain propositions are not true, parametrically.

For example, we show that $(\exists x{:}\tau.\ A(x)) \supset (\forall x{:}\tau.\ A(x))$ is not true in general. After the first two steps of constructing a verification, we arrive at

$$
\dfrac{\dfrac{\begin{array}{c}\dfrac{}{\exists x{:}\tau.\ A(x)\downarrow}u \quad \dfrac{}{a:\tau} \\ \vdots \\ A(a)\uparrow\end{array}}{\forall x{:}\tau.\ A(x)\uparrow}\forall I^a}{(\exists x{:}\tau.\ A(x)) \supset (\forall x{:}\tau.\ A(x))\uparrow}\supset I^u
$$

At this point we can only apply existential elimination, which leads to

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x{:}\tau.\ A(x)\downarrow}u \quad \begin{array}{c}\dfrac{}{b:\tau} \quad \dfrac{}{A(b)\downarrow}v \quad \dfrac{}{a:\tau} \\ \vdots \\ A(a)\uparrow\end{array}}{A(a)\uparrow}\exists E^{b,v}}{\forall x{:}\tau.\ A(x)\uparrow}\forall I^a}{(\exists x{:}\tau.\ A(x)) \supset (\forall x{:}\tau.\ A(x))\uparrow}\supset I^u
$$

We cannot close the gap, because a and b are different parameters. We can only apply existential elimination to assumption u again. But this only creates $c : \tau$ and $A(c)\downarrow$ for some new c, so have made no progress. No matter how often we apply existential elimination, since the parameter introduced must be new, we can never prove $A(a)$.