Lecture Notes on Predicate Calculus

15-317: Constructive Logic
Frank Pfenning

Lecture 13
Tuesday, February 28, 2023

1 Introduction

So far, we have mainly covered *propositional logic* (which deals with conjunction, implication, disjunction, truth, and falsehood) and *arithmetic* (which deals with natural numbers and equality). To capture more of mathematics and computer science we also need *quantification*. Its simplest form is the *predicate calculus* that extends our propositional investigations in two ways: it generalizes *propositions* to *predicates*, and it introduces *quantification*. In the predicate calculus we abstract away entirely from the domain of quantification. In other words, we are concerned with what is true for *all* domains of quantification and we just write $\forall x.\, A(x)$ and $\exists x.\, A(x)$. It goes without saying that we use the verificationist approach to give constructive meaning to these new ways of forming propositions.

From these, it is a small but practically important step to specify the domain of quantification. For example, in arithmetic the quantifiers would range over natural numbers, in the (polymorphic) theory of lists they would range over lists, in the theory of lists of natural numbers we would have both, etc. This line of investigation would inevitably lead us down to *type theory*: Since we already know that propositions correspond to types and types to propositions, the most natural course of action is to generalize further to quantifiers $\forall x{:}A.\, B(x)$ and $\exists x{:}A.\, B(x)$. This generality comes at a price because it introduces new complications. Because this is a course on constructive *logic*, I do not think we will go very far down this fascinating path, and certainly not in today's lecture. In any case, understanding the fundamental logical laws concerning quantification is a natural step towards richer theories.

2 Universal Quantification

First, universal quantification, written as $\forall x.\, A(x)$ and pronounced "for all x, $A(x)$". Here x is a bound variable and can therefore be renamed so that $\forall x.\, A(x)$ and $\forall y.\, A(y)$ are identified. When we write $A(x)$ we mean an arbitrary proposition which may depend on x. We will also say that A is *predicate*.

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

purpose, we need a new judgment a *elem* stating that a is an element of our (purposely unspecified) domain.

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

It is important that a be a *new* parameter, not used outside of its scope, which is the derivation between the new hypothesis a *elem* and the conclusion $A(a)$ *true*. In particular, a may not occur in $\forall x.\, A(x)$.

The rule makes sense: A proof that $A(x)$ holds for all x considers any arbitrary element a and shows that $A(a)$ *true*. But it is important that a was indeed arbitrary. 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 standing for an element 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 $\forall x.\, A(x)$ describes a construction by which an arbitrary element t can be transformed into a proof of $A(t)$ *true*. The corresponding elimination rule $\forall E$, thus, accepts some element t and concludes that $A(t)$ *true*:

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

We must verify that t *elem* so that $A(t)$ is a well-formed proposition. The elimination rule makes sense: if $A(x)$ is true for all elements x, and if t is a particular element then $A(t)$ is true as well for this particular element.

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

$$\text{If}\quad \begin{array}{c}a\ \mathit{elem}\\ \mathcal{D}\\ C(a)\ \mathit{true}\end{array}\quad\text{and}\quad \begin{array}{c}\mathcal{E}\\ t\ \mathit{elem}\end{array}\quad\text{then}\quad \begin{array}{c}\dfrac{\mathcal{E}}{t\ \mathit{elem}}\\ [t/a]\mathcal{D}\\ C(t)\ \mathit{true}\end{array}$$

That is, if $\mathcal{D}$ is a derivation of $C(a)$ from the judgment a *elem* about parameter a, and if $\mathcal{E}$ is a deduction that t is indeed an element, then we can substitute t for the 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 is an element.

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.

For this substitution to work properly, we also need to substitute into derivations for judgments of the form t *elem*. That is, we also have the following substitution principle:

$$\text{If} \quad \begin{array}{c} a\ \mathit{elem} \\ \mathcal{D} \\ s\ \mathit{elem} \end{array} \quad \text{and} \quad \begin{array}{c} \mathcal{E} \\ t\ \mathit{elem} \end{array} \quad \text{then} \quad \begin{array}{c} \dfrac{\mathcal{E}}{t\ \mathit{elem}} \\ [t/a]\mathcal{D} \\ [t/a]s\ \mathit{elem} \end{array}$$

In the pure predicate calculus the only way to derive t *elem* is to have $t = b$ for some parameter b and have the *hypothesis* b *elem*, so this property is trivialized. In the more general, abstract form given above it will carry over to theories with data constructors such as arithmetic where expressions such as $\mathsf{s}(\mathsf{s}(a))$ arise.

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

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

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

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

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

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

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:

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

3 Existential Quantification

The existential quantifier is more difficult to specify, although the introduction rule seems innocuous enough. If there is an element t for which we have a derivation of $A(t)$ *true*, then there is a proof of $\exists x.\, A(x)$ *true* witnessed by said t.

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

The elimination rules creates some difficulties. We cannot write

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

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 $\exists x.\, A(x)$ with one witness t and then eliminate the quantifier using another object s about which we have no reason to believe it would satisfy $A(s)$ *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 else 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).

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

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

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

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

The local expansion showing local completeness is patterned after the disjunction

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

As an example of quantifiers we show the equivalence of $\forall x.\, A(x) \supset C$ and $(\exists x.\, A(x)) \supset C$, 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.

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

The first three steps can be taken without hesitation, because we can *always* apply implication and universal introduction from the bottom up (something captured, as before, in the nature of verifications in Section 4).

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

At this point the conclusion is an unknown proposition, 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, which gives us a new subgoal.

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

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

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

We now consider the reverse implication.

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

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

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

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

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

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.

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

Now we can fill the gap with an implication elimination.

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

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 derive propositions that aren't true. The following would be such an example, expressing that there is at most one element!

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

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:

$$\dfrac{\dfrac{\dfrac{}{a\ \mathit{elem}}}{\vdots}}{\dfrac{A(a)\uparrow}{\forall x.\, A(x)\uparrow}\,\forall I^{a}} \qquad \dfrac{\forall x.\, A(x)\downarrow \quad t\ \mathit{elem}}{A(t)\downarrow}\,\forall E$$

We do not assign a direction to the judgment for typing objects, $t\ \mathit{elem}$.

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

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

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 (somewhat informally) that $(\exists x.\, A(x)) \supset (\forall x.\, A(x))$ is not true in general. After the first two steps of constructing a verification, we arrive at

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

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

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

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 $c\ \mathit{elem}$ 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 $A(a)$.

Such an argument is most rigorously carried out in the sequent calculus, so we show this next.

5 Quantification in Sequent Calculus

In natural deduction, we had two forms of hypotheses: $A\ \mathit{true}$ and $a\ \mathit{elem}$ for parameters a. The latter form was introduced into deductions by the $\forall I$ and $\exists E$ rules. In the sequent calculus we make all assumptions explicit on the left-hand side of sequents. In order to

model parameters we therefore need a second kind of judgment on the left, for which we reuse a *elem*. It is customary to collect all such hypotheses in a different context, denoted Σ for *signature*, but we will not do so here, just mixing A *ante* for propositions A and a *elem* for elements. We then have

$$\text{Antecedents} \quad \Gamma \quad ::= \quad \cdot \mid \Gamma, A\,\mathit{ante} \mid \Gamma, a\,\mathit{elem}$$

As usual, we will just write A instead of A *ante* and C instead of C *succ* for succedents. We assume that all parameters declared in a sequent are distinct. Sometimes this requires us to choose a parameter with a name that has not yet been used. When writing down a sequent $\Gamma \Longrightarrow C$ we presuppose that all parameters occurring in propositions are declared in Γ and are "in scope": in a sequent $\Gamma, a\,\mathit{elem}, \Gamma' \Longrightarrow C$, all occurrences of a are in Γ' and C. We maintain this presupposition as an invariant when reading rules bottom-up, as we (almost) always do in the sequent calculus.

We also have a new judgment $\Gamma \vdash a\ \mathit{elem}$ which holds if $a\,\mathit{elem}$ is in Γ. As for natural deduction, if we enrich the language of elements this judgment may become more complicated. For example, in arithmetic we might have $a\,\mathit{elem} \vdash \mathsf{s}\,(\mathsf{s}\,a)\ \mathit{elem}$.

In order to derive the rules for the quantifiers, we reexamine verifications for guidance, as we did for the propositional rules.

Universal quantification. We show the verification on the left and with the corresponding right rule.

$$\dfrac{\dfrac{\overline{a\ \mathit{elem}}}{\vdots}\ A(a)\uparrow}{\forall x.\, A(x)\uparrow}\ \forall I^a \qquad \dfrac{\Gamma, a\,\mathit{elem} \Longrightarrow A(a)}{\Gamma \Longrightarrow \forall x.\, A(x)}\ \forall R^a$$

Our general assumption that the signature declares every parameter at most once means that a cannot occur in Γ already or the rule would not apply.

The elimination rule that uses a universally quantified assumption corresponds to a left rule.

$$\dfrac{\forall x.\, A(x)\downarrow \quad t\ \mathit{elem}}{A(t)\downarrow}\ \forall E \qquad \dfrac{\Gamma \vdash t\ \mathit{elem} \quad \Gamma, \forall x.\, A(x), A(t) \Longrightarrow C}{\Gamma, \forall x.\, A(x) \Longrightarrow C}\ \forall L$$

If we know that $A(x)$ holds for all elements x, then $A(t)$ for any element t.

Existential quantification. Again, we derive the sequent calculus rules from the introduction and elimination rules.

$$\dfrac{t\ \mathit{elem} \quad A(t)\uparrow}{\exists x.\, A(x)\uparrow}\ \exists I \qquad \dfrac{\Gamma \vdash t\ \mathit{elem} \quad \Gamma \Longrightarrow A(t)}{\Gamma \Longrightarrow \exists x.\, A(x)}\ \exists R$$

As for disjunction elimination, the natural deduction rule already has somewhat of the flavor of the sequent calculus.

$$\dfrac{\exists x.\, A(x)\!\downarrow \qquad \begin{array}{c}\overline{a\ \mathit{elem}} \quad \overline{A(a)\!\downarrow}^{\,u} \\ \vdots \\ C\!\uparrow\end{array}}{C\!\uparrow}\ \exists E^{a,u} \qquad\qquad \dfrac{\Gamma, \exists x.\, A(x), a\ \mathit{elem}, A(a) \Longrightarrow C}{\Gamma, \exists x.\, A(x) \Longrightarrow C}\ \exists L^{a}$$

It is worth noting that the new a (not already in Γ, $\exists x.\, A(x)$, or C) is declared in Γ before its occurrence in $A(a)$, preserving our presuppositions regarding scope.

6 Admissibility of Cut with Quantification

The proof of the admissibility of cut extends to the case where we add quantifiers. A crucial property we need is substitution for parameters, which corresponds to a similar substitution principle on natural deductions:

Parameter substitution

1. If $\Gamma \vdash t\ \mathit{elem}$ and $\Gamma, a\ \mathit{elem} \vdash s\ \mathit{elem}$ then $\Gamma \vdash [t/a]s\ \mathit{elem}$
2. If $\Gamma \vdash t\ \mathit{elem}$ and $\Gamma, a\ \mathit{elem}, \Gamma' \Longrightarrow C$ then $\Gamma, [t/a]\Gamma' \Longrightarrow [t/a]C$.

The first is trivial on our current language, since s must be one of the parameters in Γ. The second follows by a straightforward induction over the structure of the second deduction, appealing to some elementary properties such as weakening where necessary.

We show only two cases of the extended proof of cut, where an existential (or universal) formula is cut and was just introduced on the right and left, respectively.

Subcase:

$$\mathcal{D} = \dfrac{\begin{array}{cc}\mathcal{T} & \mathcal{D}_1 \\ \Gamma \vdash t\ \mathit{elem} & \Gamma \Longrightarrow A_1(t)\end{array}}{\Gamma \Longrightarrow \exists x.\, A_1(x)}\ \exists R$$

$$\text{and} \quad \mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}_1 \\ \Gamma, \exists x.\, A_1(x), a\ \mathit{elem}, A_1(a) \Longrightarrow C\end{array}}{\Gamma, \exists x.\, A_1(x) \Longrightarrow C}\ \exists L$$

where $A = \exists x.A_1(x)$. Then

$\Gamma, \exists x.\, A_1(x), A_1(t) \Longrightarrow C$	By substitution $[t/a]\mathcal{E}_1$ using $\mathcal{T}$
$\Gamma, A_1(t) \Longrightarrow C$	By i.h. on $\exists x.\, A_1(x)$, $\mathcal{D}$, and $[t/a]\mathcal{E}_1$
$\Gamma \Longrightarrow C$	By i.h. on $A_1(t)$, $\mathcal{D}_1$, and above

The induction requires that $A_1(t)$ is considered smaller than $\exists x.\, A_1(x)$. Formally, this can be justified by counting the number of quantifiers and logical connectives in a proposition and noting that the term t does not contain any. A similar remark applies to check that the proof $[t/a]\mathcal{E}_1$ is smaller than $\mathcal{E}$. Also note how the side condition that a must be a new parameter in the $\exists L$ rule is required in the substitution step to conclude that, $[t/a]A_1(a) = A(t) = [t/x]A_1(x)$, and $[t/c]C = C$.

Subcase:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, a\,\mathit{elem} \Longrightarrow A_1(a)\end{array}}{\Gamma \Longrightarrow \forall x.\, A_1(x)}\ \forall R^a$$

$$\text{and}\quad \mathcal{E} = \dfrac{\begin{array}{cc}\mathcal{T} & \mathcal{E}_1\\ \Gamma \vdash t\,\mathit{elem} & \Gamma, \forall x.\, A_1(x), A_1(t) \Longrightarrow C\end{array}}{\Gamma, \forall x.\, A_1(x) \Longrightarrow C}\ \forall L$$

where $A = \forall x.\, A_1(x)$. Then

$\Gamma, A_1(t) \Longrightarrow C$	By i.h. on $\forall x.\, A_1(x)$, $\mathcal{D}$, $\mathcal{E}_1$
$\Gamma \Longrightarrow A_1(t)$	By substitution $[t/c]\mathcal{D}_1$ using $\mathcal{T}$
$\Gamma \Longrightarrow C$	By i.h. on $A_1(t)$ and the above two

It is again important that $A_1(t)$ is considered smaller than $\forall x.\, A_1(x)$. Similarly, the side condition that a must be a new parameter in $\forall R$ is needed to ensure that the substitution leaves Γ unchanged and that $[t/a]A_1(a) = A_1(t)$.

7 Example of Unprovability[1]

Let's reconsider $(\exists x.\, A(x)) \supset (\forall y.\, A(y))$. We cannot prove this for an arbitrary domain of quantification and predicate $A(x)$.

We construct a counterexample by postulating a domain with two elements, say, 0 and 1 and an atomic predicate P such that $P(0)$ is true and $P(1)$ is false. We quickly observe that

$$0\,\mathit{elem}, 1\,\mathit{elem}, P(0), \neg P(1) \Longrightarrow P(1)$$

is **not** provable (the only applicable rule $\supset L$ leads to the same subgoal in the first premise).

Furthermore

$$0\,\mathit{elem}, 1\,\mathit{elem}, P(0), \neg P(1) \Longrightarrow \exists x.\, P(x)$$

using 0 as the witness. If we also had

$$\exists x.\, P(x) \Longrightarrow \forall y.\, P(y)$$

[1] not covered in lecture

then using weakening and the admissibility of cut we would obtain

$$0\,\mathit{elem}, 1\,\mathit{elem}, P(0), \neg P(1) \Longrightarrow \forall y.\, P(y)$$

We can construct

$$\dfrac{\dfrac{}{1\,\mathit{elem} \vdash 1\,\mathit{elem}} \quad \dfrac{}{1\,\mathit{elem}, \forall y.\, P(y), P(1) \Longrightarrow P(1)}\ \mathsf{id}^*}{1\,\mathit{elem}, \forall y.\, P(y) \Longrightarrow P(1)}\ \forall L$$

so again, using admissibility of cut:

$$0\,\mathit{elem}, 1\,\mathit{elem}, P(0), \neg P(1) \Longrightarrow P(1)$$

This contradicts our earlier observation that this sequent cannot be provable.

One can also argue more syntactically, generalizing the induction hypothesis somewhat:

> No sequent of the form
>
> $$\exists x.\, P(x), b_1\,\mathit{elem}, P(b_1) \ldots, b_n\,\mathit{elem}, P(b_n), a\,\mathit{elem} \Longrightarrow P(a)$$
>
> is derivable.

Since we are proving a negation ("there exists no derivation") we assume there exists one (say $\mathcal{D}$) and prove a contradiction by induction over the structure of $\mathcal{D}$. By inversion, the only case we have to consider is that the last inference is $\exists L$, but then the premise has the same form and we can apply the induction hypothesis.

This means that we can also not derive any sequent

$$\exists x.\, P(x), b_1\,\mathit{elem}, P(b_1) \ldots, b_n\,\mathit{elem}, P(b_n) \Longrightarrow \forall x.\, P(x)$$

If we had such a proof, then the proof

$$a\,\mathit{elem}, \forall x.\, P(x) \Longrightarrow P(a)$$

and admissibility of cut would give us a proof of

$$\exists x.\, P(x), b_1\,\mathit{elem}, P(b_1) \ldots, b_n\,\mathit{elem}, P(b_n), a\,\mathit{elem} \Longrightarrow P(a)$$

which we already know is impossible.

8 Proof Terms

Going back to our very first lecture, we think of an intuitionistic proof of $\forall x.\, \exists y.\, A(x, y)$ as a function that, for every x constructs a witness y and a proof that $A(x, y)$ is true.

So the proof term for a universal quantifier should be a function and for an existential quantifier a pair consisting of a witness and a proof that the witness is correct.

We do not invent a new notation here, but reuse the notation for functions and applications.

$$\dfrac{\begin{array}{c}\overline{a\ \mathit{elem}}\\ \vdots\\ [a/x]M : A(a)\end{array}}{(\lambda x.\, M) : \forall x.\, A(x)}\ \forall I^a \qquad \dfrac{M : \forall x.\, A(x) \quad t\ \mathit{elem}}{M\,t : A(t)}\ \forall E$$

Note that the proof term M can of course depend on a, but we explicitly mark dependency only in propositions, using substitution notation on proof terms instead. The local reduction and expansions straightforwardly adapt the previous rules for functions.

$$\begin{array}{lll}(\lambda x.\, M)\,t & \Longrightarrow_R & [t/x]M \\ M : \forall x.\, A(x) & \Longrightarrow_E & (\lambda x.\, M\,x) \quad \text{for } x \text{ not in } M\end{array}$$

You should be able to correlate these reductions with the local reductions and expansions on proofs given earlier in this lecture.

For existential introduction the proof term is a pair, but the existential elimination is an interesting case because it does not just extract the first and second component of this pair. Instead, we have a new form that names the components of the pair, following the shape of the elimination rule.

$$\dfrac{t\ \mathit{elem} \quad M : A(t)}{\langle t, M\rangle : \exists x.\, A(x)}\ \exists I \qquad \dfrac{M : \exists x.\, A(x) \qquad \begin{array}{c}\overline{a\ \mathit{elem}} \quad \overline{u : A(a)}\ u\\ \vdots\\ [a/x]N : C\end{array}}{\mathbf{split}(M, x.\, u.\, N) : C}\ \exists E^{a,u}$$

The local reduction will decompose the pair as expected; the reduction decomposes it and then puts it back together.

$$\begin{array}{lll}\mathbf{split}(\langle t, M\rangle, x.\, u.\, N) & \Longrightarrow_R & [M/u][t/x]N \\ M : \exists x.\, A(x) & \Longrightarrow_E & \mathbf{split}(M, x.\, u.\, \langle x, u\rangle)\end{array}$$

9 Conclusion

Since we have constructed the rules in a systematic way following our earlier blueprint, the theorems from Lecture 9 relating natural deduction, verifications, and the sequent calculus carry over.

10 Rule Summary

Natural Deduction

$$\frac{\begin{array}{c}\overline{a\ elem}\\ \vdots\\ A(a)\ true\end{array}}{\forall x.\, A(x)\ true}\ \forall I^a \qquad \frac{\forall x.\, A(x)\ true \quad t\ elem}{A(t)\ true}\ \forall E$$

$$\frac{t\ elem \quad A(t)\ true}{\exists x.\, A(x)\ true}\ \exists I \qquad \frac{\exists x.\, A(x)\ true \qquad \begin{array}{c}\overline{a\ elem} \quad \overline{A(a)\ true}^{\,u}\\ \vdots\\ C\ true\end{array}}{C\ true}\ \exists E^{a,u}$$

Verifications.

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

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

Sequent Calculus

$$\frac{\Gamma, a\ elem \Longrightarrow A(a)}{\Gamma \Longrightarrow \forall x.\, A(x)}\ \forall R^a \qquad \frac{\Gamma \vdash t\ elem \quad \Gamma, \forall x.\, A(x), A(t) \Longrightarrow C}{\Gamma, \forall x.\, A(x) \Longrightarrow C}\ \forall L$$

$$\frac{\Gamma \vdash t\ elem \quad \Gamma \Longrightarrow A(t)}{\Gamma \Longrightarrow \exists x.\, A(x)}\ \exists R \qquad \frac{\Gamma, \exists x.\, A(x), a\ elem, A(a) \Longrightarrow C}{\Gamma, \exists x.\, A(x) \Longrightarrow C}\ \exists L^a$$