Lecture Notes on Quantifiers

15-836: Substructural Logics
Frank Pfenning

Lecture 13
October 10, 2023

1 Introduction

In the development of logical inference, we used propositions such as $\mathsf{path}(x, y)$ or $\mathsf{proc}(P)$ in the rules, but we did not explicitly quantify over them. That's because the schematic variables in inference rules are *implicitly* universally quantified. The lack of quantifiers was then a problem when we tried to internalize the rules as logical propositions. For example, we'd like to translate the rule on the left to the proposition on the right.

$$\frac{\mathsf{path}(x, y) \quad \mathsf{path}(y, z)}{\mathsf{path}(x, z)} \qquad\qquad \forall x.\, \forall y.\, \forall z.\, \mathsf{path}(x, y) \wedge \mathsf{path}(y, z) \supset \mathsf{path}(x, z)$$

On the logical side, introducing quantifiers is interesting and not particularly disturbing. When we think of propositions as types (and proofs as programs), then there are multiple ways to think about quantifiers, and none are particularly canonical unless we go all the way to type theory in which we can talk (and therefore quantify) over proofs. Even there, matters are complicated specifically when we consider substructural type theories.

Today, we'll stay comfortably in logic and logical inference. We'll go with ordered logic as our base because this is the context we have thought the most about cut elimination. Our considerations carry over to linear, structural, and adjoint logics.

2 Universal Quantification

One tricky aspect of quantification is the *domain* we quantify over. For example, in the reachability example of the introduction, the quantifiers range over nodes in a graph. Or we may quantify over natural numbers, or trees, etc. When we go to a full type theory, this issue must be faced and deeply considered. In predicate calculus (or first-order logic, as it is often called) it is convenient to consider the laws of the quantifiers independently from the domain of quantification. In other words, we'd like to investigate the rules of logical reasoning *independently* of the individuals we quantify over. This is not unlike the step we took when we investigated the logical connectives. We postulated some atomic propositions P, but the our reasoning did not depend on them. Once we fix a domain of interest, say, the natural numbers, we are no longer in the pure predicate calculus; instead we are reasoning in *arithmetic*, or the theory of lists, or trees, etc.

Diving in now: when can we prove $\forall i.\, A(i)$, not considering the domain of quantification? We can prove it if we can prove $A(a)$ for an arbitrary individual n. So we could write

$$\frac{\Omega \vdash A(n)}{\Omega \vdash \forall i.\, A(i)}\ \forall R^n$$

where the superscript n means that n must be *fresh*: it cannot already occur in Ω or $\forall i.\, A(i)$. This condition is crucial. Otherwise, we could for example prove that $A(n) \supset \forall i.\, A(i)$, that is, if A holds for some individual n then it holds for all individuals. This concept is so important it has its own name: n is an *eigenvariable* of the inference, and the proof of the premise is *parametric in* n.

Similar freshness conditions applied to proof terms that introduced variables, and we managed them through explicit naming of all antecedents. We stick here to the same form of variable hygiene and introduce a structural context naming all the individuals that may appear in a sequent.

$$\underbrace{i_1\ \mathit{ind}, \ldots, i_k\ \mathit{ind}}_{\Gamma}\ ; \Omega \vdash A$$

Our *presupposition* is that all variables $i_1, \ldots, i_k$ are distinct, and that all variables occurring in Ω and A are declared in Γ. We then obtain the rule

$$\frac{\Gamma, i\ \mathit{ind}\ ; \Omega \vdash A(i)}{\Gamma\ ; \Omega \vdash \forall i.\, A(i)}\ \forall R$$

Since the condition on the eigenvariable is now enforced by our presupposition we no longer annotate the rule. As for proof terms, we write the same variable name i, but bound variables (as in $\forall i.\, A(i)$) can be silently renamed in order to make the rule applicable in the form presented.

Next, we need to consider the matching left rule. If we know $A(i)$ is true for an arbitrary individual i, we should be able to instantiate it with any individual.

$$\frac{\Gamma \vdash t\ \mathit{ind} \quad \Gamma\ ; \Omega_L\ A(t)\ \Omega_R \vdash C}{\Gamma\ ; \Omega_L\ (\forall i.\, A(i))\ \Omega_R \vdash C}\ \forall L$$

Here, t is a term in our logical language denoting an individual that uses only variable from Γ. This condition is necessary because otherwise the premise with $A(t)$ may no longer satisfy our presupposition. The minimal choice for the judgment $\Gamma \vdash t\ ind$ is that the term t is a variable declared in Γ. Depending on our intentions, we could also have other terms denoting individuals, such as $\mathsf{zero}, \mathsf{succ}(\mathsf{zero}), \mathsf{succ}(i)$, etc.

Also, we see that we treat Γ *structurally* rather than linearly or in an ordered fashion. Intuitively, that's because individuals are truly *used* in a proof, they are merely *mentioned* inside proposition. Therefore, terms that are meaningful (that is, in scope and well-formed) can be mentioned arbitrarily and are themselves not subject to a substructural discipline even if we are reasoning within one.

Of course, now we need to check for harmony.

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma, i\ ind\ ;\ \Omega \vdash A(i)\end{array}}{\Gamma\ ;\ \Omega \vdash \forall i.\, A(i)}\ \forall R \qquad \dfrac{\begin{array}{c}\mathcal{E}_1\\ \Gamma \vdash t\ ind\end{array} \quad \begin{array}{c}\mathcal{E}_2\\ \Gamma\ ;\ \Omega_L\ A(t)\ \Omega_R \vdash C\end{array}}{\Gamma\ ;\ \Omega_L\ (\forall i.\, A(i))\ \Omega_R \vdash C}\ \forall L}{\Gamma \vdash \Omega_L\ \Omega\ \Omega_R \vdash C}\ \mathsf{cut}_{\forall i.\, A(i)}$$

It is not immediately clear how to proceed because the propositions $A(i)$ and $A(t)$ in the premises do not match. This is precisely why we had to choose i to be fresh: so we could substitute t for i in the sequent and in fact in the whole derivation. Assuming for the moment this is possible, we obtain

$$\longrightarrow \qquad \dfrac{\begin{array}{c}[t/i]\mathcal{D}'\\ \Gamma\ ;\ \Omega \vdash A(t)\end{array} \quad \begin{array}{c}\mathcal{E}_2\\ \Gamma\ ;\ \Omega_L\ (A(t))\ \Omega_R \vdash C\end{array}}{\Gamma \vdash \Omega_L\ \Omega\ \Omega_R \vdash C}\ \mathsf{cut}_{A(t)}$$

First, we should see why $A(t)$ is smaller than $\forall i.\, A(i)$. The term t could contain constructors as indicated above so it could be arbitrarily large. On the other hand, in a predicate calculus/first-order logic we distinguish between individuals and propositions, so the term t cannot contain any propositions. Therefore, if we count quantifiers and logical connectives, then $A(t)$ is smaller than $\forall i.\, A(i)$.

Second, we should verify that $[t/i]\mathcal{D}'$ can always be constructed as a proof of $\Gamma\ ;\ \Omega \vdash A(t)$. This follows from the *substitution principle* for individuals:

$$\dfrac{\Gamma \vdash t\ ind \quad \Gamma, i\ ind\ ;\ \Omega(i) \vdash A(i)}{\Gamma\ ;\ \Omega(t) \vdash A(t)}\ \mathsf{subst}$$

We call this a substitution principle because we obtain the resulting derivation simply by substituting t for i. It is proved by induction over the second given derivation. The particular application of this rule here is:

$$\dfrac{\overset{\mathcal{E}_2}{\Gamma \vdash t\ ind} \quad \overset{\mathcal{D}'}{\Gamma, i\ ind\ ; \Omega \vdash A(i)}}{\Gamma\ ; \Omega \vdash A(t)}\ \mathsf{subst}$$

We know from the the shape of $\mathcal{D}$ and our presuppositions that the ordered antecedents in $\mathcal{D}'$ do not depend in i.

We can check that our transcription of the inference rules is correct. Recall that top-down inference is turned into bottom-up inference among the antecedents. In this example, we ignore issues of order.

$$\dfrac{\mathsf{path}(a, b) \quad \mathsf{path}(b, c)}{\mathsf{path}(a, c)}\ \mathsf{trans}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathsf{path}(a,b) \vdash \mathsf{path}(a,b)}\ \mathsf{id} \quad \dfrac{}{\mathsf{path}(b,c) \vdash \mathsf{path}(b,c)}\ \mathsf{id}}{\mathsf{path}(a,b), \mathsf{path}(b,c) \vdash \mathsf{path}(a,b) \wedge \mathsf{path}(b,c)}\ {\wedge}R \quad \mathsf{path}(a,c) \vdash C}{\mathsf{path}(a,b) \wedge \mathsf{path}(b,c) \supset \mathsf{path}(a,c), \quad \mathsf{path}(a,b), \mathsf{path}(b,c), \vdash C}\ {\supset}L}{\forall z.\, \mathsf{path}(a,b) \wedge \mathsf{path}(b,z) \supset \mathsf{path}(a,z), \quad \mathsf{path}(a,b), \mathsf{path}(b,c) \vdash C}\ \forall L}{\forall y.\, \forall z.\, \mathsf{path}(a,y) \wedge \mathsf{path}(y,z) \supset \mathsf{path}(a,z), \quad \mathsf{path}(a,b), \mathsf{path}(b,c), \vdash C}\ \forall L}{\forall x.\, \forall y.\, \forall z.\, \mathsf{path}(x,y) \wedge \mathsf{path}(y,z) \supset \mathsf{path}(x,z), \quad \mathsf{path}(a,b), \mathsf{path}(b,c) \vdash C}\ \forall L$$

3 Existential Quantification

We expect the rules for existential quantification to mirror those for universal quantification, reversing the role of the antecedent and succedent.

$$\dfrac{\Gamma \vdash t\ \mathsf{ind} \quad \Gamma\ ; \Omega \vdash A(t)}{\Gamma\ ; \Omega \vdash \exists i.\, A(i)}\ \exists R \qquad \dfrac{\Gamma, i\ ind\ ; \Omega_L\ A(i)\ \Omega_R \vdash C}{\Gamma\ ; \Omega_L\ (\exists i.\, A(i))\ \Omega_R \vdash C}\ \exists L$$

We show the reduction, even if it is straightforward after what we discussed for the universal.

$$\dfrac{\dfrac{\begin{matrix}\mathcal{D}_1 \\ \Gamma \vdash t\ \mathsf{ind}\end{matrix} \quad \begin{matrix}\mathcal{D}_2 \\ \Gamma\ ;\ \Omega \vdash A(t)\end{matrix}}{\Gamma\ ;\ \Omega \vdash \exists i.\, A(i)}\ \exists R \qquad \dfrac{\begin{matrix}\mathcal{E}' \\ \Gamma, i\ ind\ ;\ \Omega_L\ A(i)\ \Omega_R \vdash C\end{matrix}}{\Gamma\ ;\ \Omega_L\ (\exists i.\, A(i))\ \Omega_R \vdash C}\ \exists L}{\Gamma\ ;\ \Omega_L\ \Omega\ \Omega_R \vdash C}\ \mathsf{cut}_{\exists i.\, A(i)}$$

$$\longrightarrow \quad \dfrac{\begin{matrix}\mathcal{D}_2 \\ \Gamma\ ;\ \Omega \vdash A(t)\end{matrix} \qquad \dfrac{\begin{matrix}\mathcal{D}_1 \\ \Gamma \vdash t\ \mathsf{ind}\end{matrix} \quad \begin{matrix}\mathcal{E}' \\ \Gamma, i\ \mathsf{ind}\ ;\ \Omega_L\ A(i)\ \Omega_R \vdash C\end{matrix}}{\Gamma\ ;\ \Omega_L\ A(t)\ \Omega_R \vdash C}\ \mathsf{subst}}{\Gamma\ ;\ \Omega_L\ \Omega\ \Omega_R \vdash C}\ \mathsf{cut}_{A(t)}$$

So where do we use the existential? It turns out it allows us to express freshness conditions in multiset rewriting rules. We consider the dynamics of cut, written

$$\dfrac{\mathsf{proc}(x \leftarrow P(x)\ ;\ Q(x))}{\mathsf{proc}(P(a)) \quad \mathsf{proc}(Q(a))}\ (a \text{ fresh})$$

As mentioned in an earlier lecture, the freshness condition here is somewhat strange: a must be *globally fresh* for the whole configuration, not just with respect to $P(x)$ and $Q(x)$. When transcribed into a logical proposition, this freshness condition turns into an *existential* quantifier.

$$\forall P.\, \forall Q.\, \mathsf{proc}(x \leftarrow P(x)\ ;\ Q(x)) \multimap \exists a.\, \mathsf{proc}(P(a)) \otimes \mathsf{proc}(Q(a))$$

Here, P and Q act as abstractions over channels, a detail we ignore until maybe a future lecture. The point is that when using this proposition as an antecedent, we will arrive at a sequent

$$\Gamma\ ;\ \exists a.\, \mathsf{proc}(P(a)) \otimes \mathsf{proc}(Q(a)), \Delta \vdash C$$

where $\Gamma = (a_1\ ind, \ldots, a_k\ ind)$ covers all the channels that might occur in P, Q, Δ, or C. The variable a is still bound, and now the left rule will have to pick a globally fresh parameter for it and then break down the tensor.

$$\dfrac{\dfrac{\Gamma, a\ ind\ ;\ \mathsf{proc}(P(a)), \mathsf{proc}(Q(a)), \Delta \vdash C}{\Gamma, a\ ind\ ;\ \mathsf{proc}(P(a)) \otimes \mathsf{proc}(Q(a)), \Delta \vdash C}\ \otimes L}{\Gamma\ ;\ \exists a.\, \mathsf{proc}(P(a)) \otimes \mathsf{proc}(Q(a)), \Delta \vdash C}\ \exists L$$

This reasoning points out several things. First, the freshness condition in our dynamics is a manifestation of the existential quantifier at the propositional level. Second, in our formulation of the dynamics of MPASS we could have been more explicit by keeping, on the side, a collection of all the channels in the configuration.

4 Polarities

We can apply our quick test for the polarities, which is to check the first step in the identity expansion.

$$\dfrac{}{\Gamma \,;\, \forall j.\, A(j) \vdash \forall i.\, A(i)}\ \mathsf{id}_{\forall i.\, A(i)} \quad \longrightarrow_E \quad \dfrac{\dfrac{\dfrac{}{\Gamma, i\ ind \vdash i\ ind} \quad \dfrac{}{\Gamma, i\ ind \,;\, A(i) \vdash A(i)}\ \mathsf{id}_{A(i)}}{\Gamma, i\ ind \,;\, \forall j.\, A(j) \vdash A(i)}\ \forall L}{\Gamma \,;\, \forall j.\, A(j) \vdash \forall i.\, A(i)}\ \forall R$$

While not proof, this indicates that the universal quantifier is *negative*. It does show that it is not positive, because the left rules for universal quantification is not invertible: we cannot instantiate the quantifier in the antecedent with a term until we have such a term.

By the way, we had to add Γ to the statement of the identity because our presupposition requires that all free variables in the sequent are collected in Γ. Without Γ the identity would be restricted to closed propositions A, which is far from general enough.

We expect that the existential, somehow symmetric to the universal, would be positive and invertible on the left, and this is indeed the case although we don't bother showing the details here.