6c Lecture 12: May 8, 2014

10 A proof system for first-order logic

We begin with two definitions.

Definition 10.1. If ϕ is a formula, then a *generalization* of ϕ is a formula of the form $\forall x_1 \forall x_2 \dots \forall x_n \phi$.

So for example, if $\phi = x+y = y+x$, then $\forall x(x+y = y+x)$, $\forall x \forall y(x+y = y+x)$ and $\forall z(x + y = y + x)$ are all generalizations of ϕ.

Definition 10.2. If ϕ is a formula, x is a variable and t is a term, then ϕ_t^x is the formula where we replace each free instance of x by t.

So for instance, if $\phi = \exists z(x + z \cdot z = 0 \vee x = z \cdot z)$, then if $t = (1 + y)$, then $\phi_t^x = \exists z((1+y)+z \cdot z = 0 \vee (1+y) = z \cdot z)$. Similarly, if $\phi = R(x, y) \vee \exists x R(x, y, z)$, and $t = f(1, 0)$, then $\phi_t^x = R(f(1, 0), y) \vee \exists x R(x, y, z)$ (since the latter two instances of x are not free in ϕ).

We are now ready to define the logical axioms of our proof system. We note that from now on for the purposes of defining our proof system, we will only deal with universal (i.e. $\forall$) quantifiers. We will regard the quantifier $\exists x$ as an abbreviation for $\neg \forall x \neg$.

Definition 10.3. The logical axioms of our proof system consist of all generalizations of the following types of formulas.

1. $\phi' \to \psi'$, whenever ϕ and ψ are propositional formulas in the variables $p_1, \dots, p_n$ such that $\phi \to \psi$ is a tautology, $\theta_1 \dots, \theta_n$ are first-order formulas, and ϕ' and ψ' are the formulas obtained by replacing each instance of p_i with θ_i in ϕ and ψ respectively.

2. $\forall x \phi \to \phi_t^x$ whenever ϕ is a formula, x is a variable and t is a term, and t is *substitutable* for x in ϕ (we define this below).

3. $\forall x(\phi \to \psi) \to (\forall x \phi \to \forall x \psi)$, for all formulas ϕ and ψ.

4. $\phi \to \forall x \phi$ whenever ϕ is a formula such that x is not free in ϕ.

5. $t = t$ for any term t.

6. $r = s \wedge s = t \to r = t$ for any terms r, s, t.

7. $s = t \to t = s$ for any terms s and t.

8. $s_1 = t_1 \wedge s_2 = t_2 \wedge \ldots s_n = t_n \rightarrow (f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)$ for any terms s_i and t_i and any n-ary function f.

9. $s_1 = t_1 \wedge s_2 = t_2 \wedge \ldots s_n = t_n \rightarrow (R(s_1, \ldots, s_n) \rightarrow R(t_1, \ldots, t_n)$ for any terms s_i and t_i and any n-ary relation R.

Most of these axioms are straightforward. However, we discuss in some detail axiom 2, and define precisely what it means for a term to be substitutable. Roughly, we want axiom 2 to say that if $\forall x \phi$ is true, then we can substitute any term t for x in the formula ϕ and it will remain true. However, the following example illustrates that we need to be careful exactly how we do this.

Let $\phi = \exists y(x \neq y)$ and now consider the formula $\forall x \phi = \forall x \exists y(x \neq y)$, which says roughly "the universe has at least two different elements". If we substitute $t = y$ for x in ϕ, then we get the formula $\exists y(y \neq y)$ which is always false. The problem here is that in our original formula $\forall x \exists y(x \neq y)$, for each x we could pick in an arbitrary way a y depending upon x to satisfy the formula. When we substitute a term for x that involves y, then we alter this dependency, which is what changes the meaning of the formula. To address this issue, we define the notion of substitutability as follows:

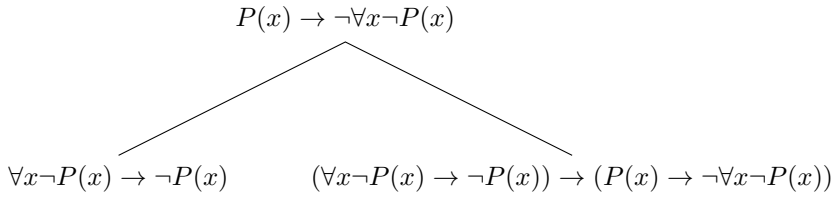
Definition 10.4. If ϕ is a formula, x is a variable and t is a term, then t *is substitutable for* x *in* ϕ if whenever a free occurrence of x is in the scope of a quantifier over another variable y, then the variable y does not occur in t.

For example, $t = 1+z$ is substitutable for x in the formula $\phi = \exists y(x+y = z)$. However, $t = 1 + y$ is not substitutable for x in this formula.

Having defined our logical axioms, our formal proofs are now made by combining them with our usual deduction rule of modus ponens.

Definition 10.5. If S is a set of formulas and ϕ is a formal, then a formal proof of ϕ from S is a finite tree whose vertices are labeled with formulas so that the root is labeled with ϕ, the leaves (vertices without children) are labeled with elements of S or logical axioms, and each vertex labeled ψ that is not a leaf has exactly two children labeled θ and $\theta \rightarrow \psi$ for some formula θ (corresponding to an instance of modus ponens).

We give an example of a proof of $P(x) \rightarrow \exists x P(x)$, recalling that $\exists x$ we regard as an abbreviation of $\neg \forall x \neg$.



Here, $\forall x \neg P(x) \rightarrow \neg P(x)$ is an instance of logical axiom 2 (with $t = x$ and $\phi = \neg P(x)$), and $(\forall x \neg P(x) \rightarrow \neg P(x)) \rightarrow (P(x) \rightarrow \neg\forall x \neg P(x))$ is an instance of logical axiom 1 coming from the propositional tautology $(p \rightarrow \neg q) \rightarrow (q \rightarrow \neg p)$.

As in propositional logic, we will often do proofs by induction the height of proofs.

Our next theorem says roughly that if we can prove a formula ϕ involving a variable x that we do not assume anything special about, then we can also prove $\forall x\phi$.

Theorem 10.6 (The generalization theorem)**.** *If $S \vdash \phi$, and S is a set of formulas that do not contain any free instance of the variable x, then $S \vdash \forall x\phi$.*

Proof. By induction on the height of proofs. If ϕ has a proof of height 0, then ϕ must be a logical axiom or an element of S. If ϕ is a logical axiom, then so is the generalization $\forall x\phi$ of ϕ. If ϕ is an element of S, then x does not occur as a free variable in ϕ, and hence $\phi \to \forall x\phi$ is instance of our logical axiom 4, and so by modus ponens $\forall x\phi$ is provable from S.

For our inductive step, assume ϕ has a proof of height $n+1$. Then ϕ arises from an instance of modus ponens from formulas θ and $\theta \to \phi$ for some θ. Now θ and $\theta \to \phi$ have proofs of height $\leq n$ from S so by our induction hypothesis, $S \vdash \forall x\theta$ and $S \vdash \forall x(\theta \to \phi)$ but now an instance of rule 3 is $\forall x(\theta \to \phi) \to (\forall x\theta \to \forall x\phi)$. Hence by modus ponens, $S \vdash \forall x\phi$. □

Many of our old results proved in the context of propositional logical will remain true here. For example, the deduction theorem that $S \cup \{\phi\} \vdash \psi$ iff $S \vdash \phi \to \psi$ will be assigned as homework.

We finish with one more example, showing $\vdash \forall x\forall y R(x,y) \to \forall y\forall x R(x,y)$. By the deduction theorem, it is enough to prove $\forall x\forall y R(x,y) \vdash \forall y\forall x R(x,y)$. By two instance of rule 2, since $\forall x\forall y R(x,y) \to \forall y R(x,y)$ and $\forall y R(x,y) \to R(x,y)$, we see $\forall x\forall y R(x,y) \vdash R(x,y)$. But then applying the generalization theorem twice, we see $\forall x\forall y R(x,y) \vdash \forall x R(x,y)$ and then $\forall x\forall y R(x,y) \vdash \forall y\forall x R(x,y)$.