

CS208 (Semester 1) Topic 4 : Proof for Predicate Logic

Dr. Robert Atkey

Computer & Information Sciences

Proof for Predicate Logic, Part 1

Upgrading Natural Deduction

Tracking free variables

We are going to prove things like:

$$\vdash \forall x.(p(x) \wedge q(x)) \rightarrow p(x)$$

This will mean we will have proof states like:

$$\dots \vdash (p(x) \wedge q(x)) \rightarrow p(x)$$

We need to keep track of variables as well as assumed formulas to the left of the \vdash “turnstile”.

Judgements

Proving:

$$\underbrace{P_1, x_1, \dots, x_i, P_j, \dots, x_m, P_n}_{\text{assumptions and variables}} \vdash \underbrace{Q}_{\text{conclusion}}$$

Focused:

$$\underbrace{P_1, x_1, \dots, x_i, P_j, \dots, x_m, P_n}_{\text{assumptions and variables}} [\underbrace{P}_{\text{focus}}] \vdash \underbrace{Q}_{\text{conclusion}}$$

Note:

1. We never focus on a variable, only formulas
2. Each P_j only contains free variables that appear to the *left* of it

Well-scoped terms and formulas

If we have a list of variables and assumptions (a “context”)

$$\Gamma = P_1, x_1, \dots, x_i, P_j, \dots, x_m, P_n$$

Γ is the name we're giving to the list

- ▶ A formula P is *well-scoped in Γ* if all the free variables of P appear in Γ .
- ▶ A term t is *well-scoped in Γ* if all the variables of t appear in Γ .
- ▶ All formulas in Γ must be well-scoped by the variables to their left (same condition as previous slide).
- ▶ The focus and conclusion must always be well-scoped in Γ .

Well-scoped terms and formulas

Are the following well-scoped?

1. Context: x Formula: $\forall y. P(y) \rightarrow Q(y)$

Well-scoped terms and formulas

Are the following well-scoped?

1. Context: x Formula: $\forall y.P(y) \rightarrow Q(y)$
Yes. The variable y is bound in the formula.

Well-scoped terms and formulas

Are the following well-scoped?

1. Context: x Formula: $\forall y.P(y) \rightarrow Q(y)$
Yes. The variable y is bound in the formula.
2. Context: x Formula: $\forall y.P(y) \rightarrow Q(x, y)$

Well-scoped terms and formulas

Are the following well-scoped?

1. Context: x Formula: $\forall y.P(y) \rightarrow Q(y)$

Yes. The variable y is bound in the formula.

2. Context: x Formula: $\forall y.P(y) \rightarrow Q(x, y)$

Yes. The variable y is bound in the formula, and the free variable x is in the context.

Well-scoped terms and formulas

Are the following well-scoped?

1. Context: *empty* Formula: $\forall y. P(y) \rightarrow Q(x, y)$

Well-scoped terms and formulas

Are the following well-scoped?

1. Context: *empty* Formula: $\forall y. P(y) \rightarrow Q(x, y)$
No. The variable y is bound in the formula, but the free variable x is not in the context.

Well-scoped terms and formulas

Are the following well-scoped?

1. Context: *empty* Formula: $\forall y. P(y) \rightarrow Q(x, y)$
No. The variable y is bound in the formula, but the free variable x is not in the context.
2. Context: *empty* Term: $x + 1$

Well-scoped terms and formulas

Are the following well-scoped?

1. Context: *empty* Formula: $\forall y. P(y) \rightarrow Q(x, y)$

No. The variable y is bound in the formula, but the free variable x is not in the context.

2. Context: *empty* Term: $x + 1$

No. The variable x is free in the term but is not in the context.

Well-scoped terms and formulas

Are the following well-scoped?

1. Context: *empty* Formula: $\forall y. P(y) \rightarrow Q(x, y)$

No. The variable y is bound in the formula, but the free variable x is not in the context.

2. Context: *empty* Term: $x + 1$

No. The variable x is free in the term but is not in the context.

Well-scoped Judgements

Is the following well-scoped?

1. Is this judgement well-scoped:

$$x, y [P(x, y)] \vdash Q(x)$$

Well-scoped Judgements

Is the following well-scoped?

1. Is this judgement well-scoped:

$$x, y [P(x, y)] \vdash Q(x)$$

Yes. The free variables of the focus and conclusion are x, y , which are in the context.

Well-scoped Judgements

Is the following well-scoped?

1. Is this judgement well-scoped:

$$x [P(x, y)] \vdash Q(x)$$

Well-scoped Judgements

Is the following well-scoped?

1. Is this judgement well-scoped:

$$x [P(x, y)] \vdash Q(x)$$

No. The free variables of the focus and conclusion are x, y , but y is not in the context.

Well-scoped Judgements

Is the following well-scoped?

1. Is this judgement well-scoped:

$$x, Q(x), y [P(x, y)] \vdash Q(y)$$

Well-scoped Judgements

Is the following well-scoped?

1. Is this judgement well-scoped:

$$x, Q(x), y [P(x, y)] \vdash Q(y)$$

Yes. Each variable appears before (reading left to right) it is used.

Well-scoped Judgements

Is the following well-scoped?

1. Is this judgement well-scoped:

$$\forall x.Q(x), y [P(x, y)] \vdash Q(y)$$

Well-scoped Judgements

Is the following well-scoped?

1. Is this judgement well-scoped:

$$\forall x.Q(x), y [P(x, y)] \vdash Q(y)$$

No. The x in the first $Q(x)$ is OK, but the x in $P(x, y)$ has not been declared in scope.

Summary

1. We started to upgrade Natural Deduction to Predicate Logic
2. We need to manage the *scope* of variables
3. To do so, we add them to the context
4. Variables may only be used by formulas to their right

Proof for Predicate Logic, Part 2

Rules for “Forall”

What does $\forall x.P$ mean?

(assuming a domain of discourse)



Answer 1 : it means for all individuals “a”, $P[x := a]$ is true.

(we think of “for all” as an infinite conjunction)

What does $\forall x.P$ mean?

(assuming a domain of discourse)

Answer 1 : it means for all individuals “a”, $P[x := a]$ is true.

(we think of “for all” as an infinite conjunction)

Answer 2 : thinking about proofs:

To *prove* a $\forall x.P$:

- ▶ We must prove $P[x := x_0]$ for a *general* x_0 .
- ▶ The x_0 stands in for any “a” that might be chosen.

To *use* a proof of $\forall x.P$:

- ▶ We can *choose* any t we like for x , and get $P[x := t]$

Introduction rule

$$\frac{\Gamma, x_0 \vdash Q[x := x_0]}{\Gamma \vdash \forall x. Q} \text{INTRODUCE}\forall$$

Introduction rule

$$\frac{\Gamma, x_0 \vdash Q[x := x_0]}{\Gamma \vdash \forall x. Q} \text{INTRODUCE}\forall$$

“To prove $\forall x. Q$, we prove $Q[x := x_0]$, assuming an arbitrary x_0 .”

$$\begin{array}{c}
 \frac{}{x, P(x) \wedge Q(x) [P(x)] \vdash P(x)} \text{ DONE} \\
 \frac{}{x, P(x) \wedge Q(x) [P(x) \wedge Q(x)] \vdash P(x)} \text{ FIRST} \\
 \frac{}{x, P(x) \wedge Q(x) \vdash P(x)} \text{ USE} \\
 \frac{}{x \vdash (P(x) \wedge Q(x)) \rightarrow P(x)} \text{ INTRODUCE} \\
 \frac{}{\vdash \forall x. (P(x) \wedge Q(x)) \rightarrow P(x)} \text{ INTRODUCE}
 \end{array}$$

Elimination

$$\frac{\Gamma [P[x := t]] \vdash Q}{\Gamma [\forall x.P] \vdash Q} \text{ INSTANTIATE}$$

(side condition: t is well-scoped in Γ)

Elimination

$$\frac{\Gamma [P[x := t]] \vdash Q}{\Gamma [\forall x.P] \vdash Q} \text{ INSTANTIATE}$$

(side condition: t is well-scoped in Γ)

“If we have P for all x , then we can pick any well-scoped t we like to stand in for it.”

$$\begin{array}{c}
 \frac{}{\Gamma [h(s())] \vdash h(s())} \text{ DONE} \\
 \frac{}{\Gamma \vdash h(s())} \text{ USE} \qquad \frac{}{\Gamma [m(s())] \vdash m(s())} \text{ DONE} \\
 \frac{}{\Gamma [h(s()) \rightarrow m(s())] \vdash m(s())} \text{ APPLY} \\
 \frac{}{\Gamma [\forall x.h(x) \rightarrow m(x)] \vdash m(s())} \text{ INSTANTIATE} \\
 \frac{}{\Gamma \vdash m(s())} \text{ USE} \\
 \frac{}{\forall x.h(x) \rightarrow m(x) \vdash h(s()) \rightarrow m(s())} \text{ INTRODUCE} \\
 \frac{}{\vdash (\forall x.h(x) \rightarrow m(x)) \rightarrow h(s()) \rightarrow m(s())} \text{ INTRODUCE}
 \end{array}$$

where $\Gamma = \forall x.h(x) \rightarrow m(x), h(s())$

Summary

- ▶ To prove $\forall x.P(x)$, we must prove $P(x_0)$ for a fresh x_0 .
- ▶ To use $\forall x.P(x)$, we get to choose the t we use for x .

Proof for Predicate Logic, Part 3

Rules for “Exists”

What does $\exists x.P$ mean?

(assuming a domain of discourse)



Answer 1 : there is at least one “a” such that $P[x := a]$ is true.

(we think of “exists” as an infinite disjunction)

What does $\exists x.P$ mean?

(assuming a domain of discourse)

Answer 1 : there is at least one “a” such that $P[x := a]$ is true.

(we think of “exists” as an infinite disjunction)

Answer 2 : thinking about proofs:

To *prove* a $\exists x.P$:

- ▶ We must provide a *witness* term t such that $P[x := t]$.

To *use* a proof of $\exists x.P$:

- ▶ We have to work with an arbitrary x_0 and all we know is $P[x := x_0]$.

Introduction

$$\frac{\Gamma \vdash P[x := t]}{\Gamma \vdash \exists x.P} \text{ EXISTS}$$

(side condition: t is well-scoped in Γ)

“To prove $\exists x.P$, we have to provide a witness t for x , and show that $P[x := t]$ ”

$\frac{\text{human}(\text{socrates}()) [\text{human}(\text{socrates}())] \vdash \text{human}(\text{socrates}())}{\text{human}(\text{socrates}()) \vdash \text{human}(\text{socrates}())}$	DONE
$\frac{\text{human}(\text{socrates}()) \vdash \text{human}(\text{socrates}())}{\text{human}(\text{socrates}()) \vdash \exists x.\text{human}(x)}$	USE
$\frac{\text{human}(\text{socrates}()) \vdash \exists x.\text{human}(x)}{\vdash \text{human}(\text{socrates}()) \rightarrow (\exists x.\text{human}(x))}$	EXISTS
	INTRODUCE

Elimination

$$\frac{\Gamma, x_0, P[x := x_0] \vdash Q}{\Gamma [\exists x.P] \vdash Q} \text{UNPACK}$$

“To use $\exists x.P$, we get some arbitrary x_0 that we know $P[x := x_0]$ about.”

$\frac{}{\exists x.h(x) \wedge m(x), \text{ali}, h(\text{ali}) \wedge m(\text{ali}) [h(\text{ali})] \vdash h(\text{ali})}$	DONE
$\frac{}{\exists x.h(x) \wedge m(x), \text{ali}, h(\text{ali}) \wedge m(\text{ali}) [h(\text{ali}) \wedge m(\text{ali})] \vdash h(\text{ali})}$	FIRST
$\frac{}{\exists x.h(x) \wedge m(x), \text{ali}, h(\text{ali}) \wedge m(\text{ali}) \vdash h(\text{ali})}$	USE
$\frac{}{\exists x.h(x) \wedge m(x), \text{ali}, h(\text{ali}) \wedge m(\text{ali}) \vdash \exists x.h(x)}$	EXISTS
$\frac{}{\exists x.h(x) \wedge m(x) [\exists x.h(x) \wedge m(x)] \vdash \exists x.h(x)}$	UNPACK
$\frac{}{\exists x.h(x) \wedge m(x) \vdash \exists x.h(x)}$	USE
$\frac{}{\vdash (\exists x.h(x) \wedge m(x)) \rightarrow (\exists x.h(x))}$	INTRODUCE

Comparing \wedge and \forall

Introduction

$$\frac{\Gamma \vdash P_1 \quad \Gamma \vdash P_2}{\Gamma \vdash P_1 \wedge P_2} \text{ SPLIT}$$

$$\frac{\Gamma, x_0 \vdash P[x := x_0]}{\Gamma \vdash \forall x. P} \forall\text{-I}$$

For \wedge , we have to prove P_i , no matter what i is. For \forall , we have to prove $P[x := x_0]$, no matter what x_0 is.

Comparing \wedge and \forall

Elimination

$$\frac{\Gamma [P_1] \vdash Q}{\Gamma [P_1 \wedge P_2] \vdash Q} \text{ FIRST}$$

$$\frac{\Gamma [P_2] \vdash Q}{\Gamma [P_1 \wedge P_2] \vdash Q} \text{ SECOND}$$

$$\frac{\Gamma [P[x := t]] \vdash Q}{\Gamma [\forall x.P] \vdash Q} \text{ INSTANTIATE}$$

For \wedge , we choose 1 or 2. For \forall , we choose t .

Comparing \vee and \exists

Introduction

$$\frac{\Gamma \vdash P_1}{\Gamma \vdash P_1 \vee P_2} \text{ LEFT}$$

$$\frac{\Gamma \vdash P_2}{\Gamma \vdash P_1 \vee P_2} \text{ RIGHT}$$

$$\frac{\Gamma \vdash P[x := t]}{\Gamma \vdash \exists x.P} \text{ EXISTS}$$

For \vee , we choose which of 1 or 2 we want. For \exists , we choose the witnessing term t .

Comparing \forall and \exists

Elimination

$$\frac{\Gamma, P_1 \vdash Q \quad \Gamma, P_2 \vdash Q}{\Gamma [P_1 \vee P_2] \vdash Q} \text{CASES}$$

$$\frac{\Gamma, x_0, P[x := x_0] \vdash Q}{\Gamma [\exists x.P] \vdash Q} \text{UNPACK}$$

For \forall , we must deal with 1 or 2. For \exists , we must cope with any x_0 .

Summary

- ▶ To prove $\exists x.P(x)$ we must give a witness t and prove $P(t)$.
- ▶ To use $\exists x.P(x)$ we get to assume there is some y and $P(y)$.

Proof for Predicate Logic, Part 4

Rules for Equality

What is Equality?

$$t_1 = t_2$$

What is Equality?

Some properties:

1. *Reflexivity*: for all x , $x = x$
2. *Symmetry*: for all x and y , if $x = y$ then $y = x$
3. *Transitivity*: for all x , y and z , if $x = y$ and $y = z$, then $x = z$

What is Equality?

Some properties:

1. *Reflexivity*: for all x , $x = x$
2. *Symmetry*: for all x and y , if $x = y$ then $y = x$
3. *Transitivity*: for all x , y and z , if $x = y$ and $y = z$, then $x = z$

Any binary relation that satisfies these properties is called an *equivalence relation*.

What is Equality?

The **special** property of equality is the following:

If $s = t$, then everything that is true about s is true about t .

What is Equality?

The **special** property of equality is the following:

If $s = t$, then everything that is true about s is true about t .

(and vice versa. but do we need to say this?)

What is Equality?

The **special** property of equality is the following:

If $s = t$, then everything that is true about s is true about t .

(and vice versa. but do we need to say this?)

Gottfried Leibniz (co-inventor of Calculus) took this as the *definition* of equality.

What is Equality?

With more symbols:

If $t_1 = t_2$, then for all P , if $P[x \mapsto t_1]$ then $P[x \mapsto t_2]$

What is Equality?

All we will need is:

1. Reflexivity: for every term t , $t = t$
2. Substitution: $t_1 = t_2$ and $P[x \mapsto t_1]$ implies $P[x \mapsto t_2]$

Amazingly, this is enough!

Symmetry

To prove that $x = y$ implies $y = x$:

1. We know that $x = x$ by reflexivity
2. So we use our assumption to replace the first x by y to get $y = x$.

Transitivity

To prove that $x = y$ and $y = z$ implies $x = z$:

1. Substitute the second assumption in the first to get $x = z$.

Rules for Equality: Introduction

$$\frac{}{\Gamma \vdash t = t} \text{ REFLEXIVITY}$$

Every term is equal to itself.

Rules for Equality: Elimination

$$\frac{\Gamma \vdash P[x \mapsto t_2]}{\Gamma [t_1 = t_2] \vdash P[x \mapsto t_1]} \text{ SUBST}$$

If we know that $t_1 = t_2$ then we can replace t_1 with t_2 in the goal. This is substitution backwards: if we know $P[x \mapsto t_2]$ and $t_1 = t_2$, then we know $P[x \mapsto t_1]$.

Example: Symmetry

$$\begin{array}{c} \frac{}{x, y, x = y \vdash y = y} \text{ REFLEXIVITY} \\ \frac{}{x, y, x = y [x = y] \vdash y = x} \text{ SUBST} \\ \frac{}{x, y, x = y \vdash y = x} \text{ USE} \\ \frac{}{x, y \vdash x = y \rightarrow y = x} \text{ INTRODUCE} \\ \frac{}{x \vdash \forall y. x = y \rightarrow y = x} \text{ INTRODUCE} \\ \frac{}{\vdash \forall x. \forall y. x = y \rightarrow y = x} \text{ INTRODUCE} \end{array}$$

Example: Transitivity

$x, y, z, x = y, y = z [y = z] \vdash y = z$	DONE
$x, y, z, x = y, y = z \vdash y = z$	USE
$x, y, z, x = y, y = z [x = y] \vdash x = z$	SUBST
$x, y, z, x = y, y = z \vdash x = z$	USE
$x, y, z, x = y \vdash y = z \rightarrow x = z$	INTRODUCE
$x, y, z \vdash x = y \rightarrow y = z \rightarrow x = z$	INTRODUCE
$x, y \vdash \forall z. x = y \rightarrow y = z \rightarrow x = z$	INTRODUCE
$x \vdash \forall y. \forall z. x = y \rightarrow y = z \rightarrow x = z$	INTRODUCE
$\vdash \forall x. \forall y. \forall z. x = y \rightarrow y = z \rightarrow x = z$	INTRODUCE

Rewriting

1. SUBST can be quite tricky to use because we have to give a formula P such that $P[x \mapsto t_1]$ is the one we start with, and $P[x \mapsto t_2]$ is the one we end up with.
2. Usually, we want to replace *every* occurrence of t_1 with t_2 . We write this as:

$$P\{t_1 \mapsto t_2\}$$

Rewriting

$$\frac{\Gamma \vdash P\{t_1 \mapsto t_2\}}{\Gamma [t_1 = t_2] \vdash P} \text{ REWRITE} \rightarrow$$

If we have $t_1 = t_2$ then we can replace t_1 with t_2 everywhere.

Rewriting

For convenience:

$$\frac{\Gamma \vdash P\{t_2 \mapsto t_1\}}{\Gamma [t_1 = t_2] \vdash P} \text{REWRITE} \leftarrow$$

If we have $t_1 = t_2$ then we can replace t_1 with t_2 everywhere.

Summary

Equality is characterised by two principles:

1. Everything is equal to itself (*reflexivity*)
2. If $s = t$, then everything that is true about s is true about t .