Natural deduction for predicate logic

Introduction

This is quite easy to set up. We keep the old propositional rules e.g., $A \vee \neg A$ for any first-order sentence A ('lemma') and add new ones for $\forall, \exists, =$.

You construct natural deduction proofs as for propositional logic: first think of a direct argument, then convert to ND.

This is even more important than for propositional logic. There's quite an art to it.

Validating arguments by predicate ND can sometimes be harder than for propositional ones, because the new rules give you wide choices, and at first you may make the wrong ones!

If you find this disconserting, remember, it's a hard problem, there's no computer program to do it (theorem 4.5)!

$\exists$-introduction, or $\exists I$

Notation 5.1

For a formula A, a variable x, and a term t, we write $A(t/x)$ for the formula got from A by replacing all free occurrences of x in A by t.

To prove a sentence $\exists x A$, you can prove $A(t/x)$, for some closed term t of your choice.

$$
\begin{array}{lll}
 & \vdots & \\
1 & A(t/x) & \text{we got this somehow...} \\
2 & \exists x A & \exists I(1)
\end{array}
$$

Recall a closed term (or ground term) is one with no variables.
This rule is reasonable. If in some structure, $A(t/x)$ is true, then so is $\exists x A$, because there exists an object in M (namely, the value in M of t) making A true.
But choosing the 'right' t can be hard — that's why it's such a good idea to think up a 'direct argument' first!

$\exists$-elimination, $\exists E$ (tricky!)

Let A be a formula. If you have managed to write down $\exists x A$, you can prove a sentence B from it by

- assuming $A(c/x)$, where c is a new constant not used in B or in the proof so far,
- proving B from this assumption.

During the proof, you can use anything already established.
But once you've proved B, you cannot use any part of the proof, including c, later on. So we isolate the proof of B from $A(c/x)$, in a box:

1	$\exists x A$	got this somehow
2	$A(c/x)$	ass
	$\langle$the proof$\rangle$	hard struggle
3	B	we made it!
4	B	$\exists E(1,2,3)$

c is often called a Skolem constant. Pandora uses sk1, sk2, ...

Justification of $\exists E$

Basically, 'we can give any object a name'.

Given any formula $A(x)$, if $\exists x A$ is true in some structure M, then there is an object a in $\mathrm{dom}(M)$ such that $M \models A(a)$.

Now a may not be named by a constant in M. But we can add a new constant to name it — say, c — and add the information to M that c names a.

c must be new — the other constants already in use may not name a in M.

And of course, if $M \models A(c/x)$ then $M \models \exists x A$.

So $A(c/x)$ for new c is really no better or worse than $\exists x A$.

Therefore, if we can prove B from the assumption $A(c/x)$, it counts as a proof of B from the already-proved $\exists x A$.

Example of $\exists$-rules

Show $\exists x(P(x) \wedge Q(x)) \vdash \exists x P(x) \wedge \exists x Q(x)$.

1	$\exists x(P(x) \wedge Q(x))$	given
2	$P(c) \wedge Q(c)$	ass
3	$P(c)$	$\wedge E(2)$
4	$\exists x P(x)$	$\exists I(3)$
5	$Q(c)$	$\exists I(3)$
6	$\exists x Q(x)$	$\exists I(5)$
7	$\exists x P(x) \wedge \exists x Q(x)$	$\wedge I(4, 6)$
8	$\exists x P(x) \wedge \exists x Q(x)$	$\exists E(1, 2, 7)$

In English, without the box (bad): Suppose $\exists x(P(x) \wedge Q(x))$.
Let c be some object such that $P(c) \wedge Q(c)$.
So $P(c)$ and $Q(c)$. So $\exists x P(x)$ and $\exists x Q(x)$.
So $\exists x P(x) \wedge \exists x Q(x)$, as required.

Note: only sentences occur in ND proofs. They should never involve formulas with free variables!

$\forall$-introduction, $\forall I$

To introduce the sentence $\forall x A$, for some $A(x)$, you introduce a *new* constant, say c, not used in the proof so far, and prove $A(c/x)$.

During the proof, you can use anything already established.

But once you've proved $A(c/x)$, you can no longer use the constant c later on.

So isolate the proof of $A(c/x)$, in a box:

1	c	$\forall I$ const
	$\langle$the proof$\rangle$	hard struggle
2	$A(c/x)$	we made it!
3	$\forall x A$	$\forall I(1, 2)$

This is the only time in ND that you write a line (1) containing a term, not a formula. And it's the only time a box doesn't start with a line labelled 'ass'.

Justification

To show $M \models \forall x A$, we must show $M \models A(a)$ for every object a in $\text{dom}(M)$.

So choose an arbitrary a, add a new constant c naming a, and prove $A(c/x)$. As a is arbitrary, this shows $\forall x A$.

c must be new, because the constants already in use may not name this particular a.

$\forall$-elimination, or $\forall E$

Let $A(x)$ be a formula. If you have managed to write down $\forall x A$, you can go on to write down $A(t/x)$ for any closed term t. (It's your choice which t!)

$$\begin{array}{lll} & \vdots & \\ 1 & \forall x A & \text{we got this somehow...} \\ 2 & A(t/x) & \forall E(1) \end{array}$$

This is easily justified: if $\forall x A$ is true in a structure, then certainly $A(t/x)$ is true, for any closed term t.

However, choosing the 'right' t can be hard — that's why it's such a good idea to think up a 'direct argument' first!

Example of ∀-rules

Let's show $P \to \forall x Q(x) \vdash \forall x(P \to Q(x))$.
Here, P is a 0-ary relation symbol — that is, a propositional atom.

1	$P \to \forall x Q(x)$	given
2	c	$\forall I$ const
3	P	ass
4	$\forall x Q(x)$	$\to E(3,1)$
5	$Q(c)$	$\forall E(4)$
6	$P \to Q(c)$	$\to I(3,5)$
7	$\forall x(P \to Q(x))$	$\forall I(2,6)$

In English: Suppose $P \to \forall x Q(x)$. Then for any object a, if P then $\forall x Q(x)$, so $Q(a)$.

So for any object a, if P, then $Q(a)$.

That is, for any object a, we have $P \to Q(a)$. So $\forall x(P \to Q(x))$.

Example with all the quantifier rules

Show $\exists x \forall y G(x,y) \vdash \forall y \exists x G(x,y)$.

1	$\exists x \forall y G(x,y)$	given
2	d	$\forall I$ const
3	$\forall y G(c,y)$	ass
4	$G(c,d)$	$\forall E(3)$
5	$\exists x G(x,d)$	$\exists I(4)$
6	$\exists x G(x,d)$	$\exists E(1,3,5)$
7	$\forall y \exists x G(x,y)$	$\forall I(2,6)$

In English, without the boxes (bad): Suppose $\exists x \forall y G(x,y)$.

Let c be an object such that $\forall y G(c,y)$.

So for any object d, we have $G(c,d)$, so certainly $\exists x G(x,d)$.

Since d was arbitrary, we have $\forall y \exists x G(x,y)$.

Breaking the quantifier rules

I hope you know by now that $\forall x \exists y(x < y) \not\models \exists y \forall x(x < y)$.

E.g., in the natural numbers, $\forall x \exists y(x < y)$ is true; $\exists y \forall x(x < y)$ isn't.

So the following must be WRONG

$$
\begin{array}{lll}
1 & \forall x \exists y(x < y) & \text{given} \\
2 & c & \forall I \text{ const} \\
3 & \exists y(c < y) & \forall E(1) \\
4 & c < d & \text{ass} \\
5 & c < d & \checkmark\ (4) \\
6 & c < d & \exists E(3,4,5) \quad \leftarrow \text{WRONG} \\
7 & \forall x(x < d) & \forall I(2,6) \\
8 & \exists y \forall x(x < y) & \exists I(7)
\end{array}
$$

The 'Skolem constant' d, introduced on line 4, must not occur in the conclusion (lines 5, 6): see slide 122. So the $\exists E$ on line 6 is illegal.

Another wrong 'proof'
(often written by students in exams)

You may prefer a simpler $\exists E$ rule with no box. But...

$$
\begin{array}{lll}
1 & \forall x \exists y (x < y) & \text{given} \\
\hline
\quad 2 & c & \forall I \text{ const} \\
\quad 3 & \exists y (c < y) & \forall E(1) \\
\quad 4 & c < d & \exists E(3) \quad \leftarrow \text{WRONG} \\
\hline
5 & \forall x (x < d) & \forall I(2,4) \\
6 & \exists y \forall x (x < y) & \exists I(5)
\end{array}
$$

Again, this 'proves' an invalid argument:
$\forall x \exists y (x < y) \not\models \exists y \forall x (x < y)$.
So $\exists E$ does need its box.

The restrictions in the rules are necessary for sound proofs!

Derived rule $\forall{\to}E$

This is like PC: it collapses two steps into one. Useful, but not essential.

Idea: often we have proved $\forall x(A(x) \to B(x))$ and $A(t/x)$, for some formulas $A(x), B(x)$ and some closed term t.

We know we can derive $B(t/x)$ from this:

1	$\forall x(A(x) \to B(x))$	(got this somehow)
2	$A(t/x)$	(this too)
3	$A(t/x) \to B(t/x)$	$\forall E(1)$
4	$B(t/x)$	${\to}E(2,3)$

So let's just do it in 1 step:

1	$\forall x(A(x) \to B(x))$	(got this somehow)
2	$A(t/x)$	(this too)
4	$B(t/x)$	$\forall{\to}E(2,1)$

Example of $\forall{\rightarrow}E$ in action

Show $\quad \forall x \forall y (P(x,y) \rightarrow Q(x,y)), \exists x P(x,a) \quad \vdash \quad \exists y Q(y,a).$

1	$\forall x \forall y (P(x,y) \rightarrow Q(x,y))$	given
2	$\exists x P(x,a)$	given
3	$P(c,a)$	ass
4	$Q(c,a)$	$\forall{\rightarrow}E(3,1)$
5	$\exists y Q(y,a)$	$\exists I(4)$
6	$\exists y Q(y,a)$	$\exists E(2,3,5)$

We used $\forall{\rightarrow}E$ on 2 $\forall$s at once. This is even more useful. There is no limit to how many $\forall$s can be covered at once with $\forall{\rightarrow}E$!!

Rules for equality

There are two: refl and =sub. We also add a derived rule, =sym.

- Reflexivity of equality (refl).
  Whenever you feel like it, you can introduce the sentence $t = t$, for any closed L-term t and for any L you like.

	$\vdots$	bla bla bla
1	$t = t$	refl

(Idea: any L-structure makes $t = t$ true, so this is sound.)

More rules for equality

- Substitution of equal terms (=sub).
  If $A(x)$ is a formula, t, u are closed terms, you've proved $A(t/x)$, and you've also proved either $t = u$ or $u = t$, you can go on to write down $A(u/x)$.

1	$A(t/x)$	got this somehow...
2	$\vdots$	yada yada yada
3	$t = u$	...and this
4	$A(u/x)$	=sub(1,3)

  (Idea: if t, u are equal, there's no harm in replacing t by u as the value of x in A. Compare with the Leibniz principle, slide 116.)

Symmetry of $=$

Show $c = d \vdash d = c$. (c, d are constants.)

$$\begin{array}{lll} 1 & c = d & \text{given} \\ 2 & c = c & \text{refl} \\ 3 & d = c & \text{=sub(2,1)} \end{array}$$

Letting A be $x = c$, then line 2 is $A(c/x)$ and line 3 is $A(d/x)$.

This is often useful, so make it a derived rule 'symmetry of $=$':

1	c=d	given
2	d=c	=sym(1)

A hard-ish example

Show $\exists x \forall y (P(y) \to y = x), \forall x P(f(x)) \vdash \exists x (x = f(x))$.

1	$\exists x \forall y (P(y) \to y = x)$	given
2	$\forall x P(f(x))$	given
3	$\forall y (P(y) \to y = c)$	ass
4	$P(f(c))$	$\forall E(2)$
5	$f(c) = c$	$\forall{\to}E(4,3)$
6	$c = f(c)$	$=$sym(5)
7	$\exists x (x = f(x))$	$\exists I(6)$
8	$\exists x (x = f(x))$	$\exists E(1,3,7)$

English: assume there is an object c such that all objects a satisfying P (if any) are equal to c, and for any object b, $f(b)$ satisfies P.

Taking 'b' to be c, $f(c)$ satisfies P, so $f(c)$ is equal to c.

So c is equal to $f(c)$.

As $c = f(c)$, we obviously get $\exists x (x = f(x))$.

Soundness and completeness

Natural deduction is also sound and complete for predicate logic:

Theorem 5.2 (soundness)

Let $A_1, \ldots, A_n, B$ be any first-order sentences.
If $A_1, \ldots, A_n \vdash B$, then $A_1, \ldots, A_n \models B$.

'Any provable first-order sentence is valid.'

'Natural deduction never makes mistakes.'

Theorem 5.3 (completeness)

Let $A_1, \ldots, A_n, B$ be any first-order sentences.
If $A_1, \ldots, A_n \models B$, then $A_1, \ldots, A_n \vdash B$.

'Any first-order validity can be proved.' 'Natural deduction powerful enough to prove all valid first-order sentences'.

(We can use natural deduction to check validity.)

What we did...

Propositional logic

- Syntax - Literals, clauses (see Prolog in 2nd year!)
- Semantics
- English–logic translations
- Arguments, validity
    - †truth tables
    - direct reasoning
    - equivalences, †normal forms
    - natural deduction

Classical first-order predicate logic

same again (except *dag*), plus

- Many-sorted logic
- Specifications, pre- and post-conditions (continued in Reasoning about Programs)

Some of what we didn't do...

- normal forms for first-order logic
- proof of soundness or completeness for natural deduction
- theories, compactness, non-standard models, interpolation
- Gödel's theorems
- non-classical logics, eg. intuitionistic logic, linear logic, modal & temporal logic, model checking
- finite structures and computational complexity
- automated theorem proving

Some of these are covered in later years.