Introduction to Formal Proof

Bernard Sufrin

Trinity Term 2018

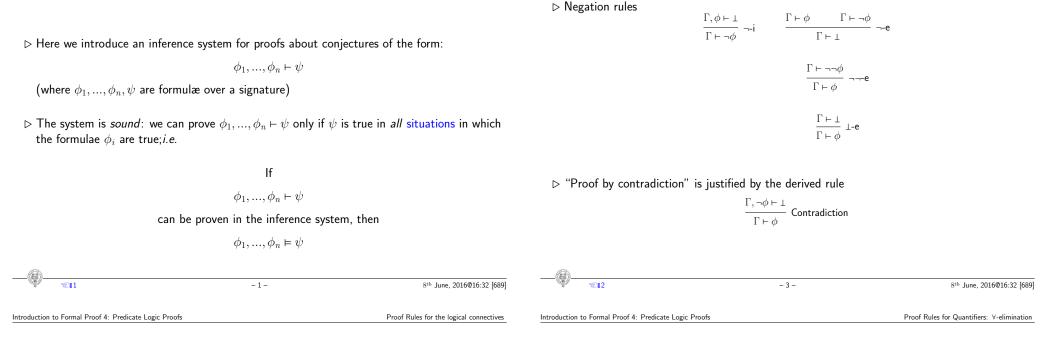


# 4: Predicate Logic Proofs

[04-folproof]

Introduction to Formal Proof 4: Predicate Logic Proofs

Proof Rules for the logical connectives



## Proof Rules for the logical connectives

Predicate Calculus Proofs

## We adopt (sequent calculus formulations of) the natural deduction rules:

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \rightarrow \psi} \rightarrow \mathbf{i} \qquad \qquad \frac{\Gamma \vdash \phi \qquad \Gamma \vdash \phi \rightarrow \psi}{\Gamma \vdash \psi} \rightarrow \mathbf{e}$$

$$\frac{\Gamma \vdash \phi \qquad \Gamma \vdash \psi}{\Gamma \vdash \phi \land \psi} \wedge \mathbf{i} \qquad \qquad \frac{\frac{\Gamma \vdash \phi \land \psi}{\Gamma \vdash \phi} \land \mathbf{e}_{L}}{\frac{\Gamma \vdash \phi \land \psi}{\Gamma \vdash \psi} \land \mathbf{e}_{R}}$$

$$\frac{\frac{\Gamma \vdash \phi}{\Gamma \vdash \psi} \lor \mathbf{v} \cdot \mathbf{i}_{L}}{\frac{\Gamma \vdash \psi}{\Gamma \vdash \phi} \lor \mathbf{v} \cdot \mathbf{i}_{R}} \qquad \frac{\Gamma \vdash \phi \lor \psi \qquad \Gamma, \phi \vdash \kappa \qquad \Gamma, \psi \vdash \kappa}{\Gamma \vdash \kappa} \lor \mathbf{v} \cdot \mathbf{e}$$

# **Proof Rules for Quantifiers:** $\forall$ -elimination

 $\triangleright$  Writing  $\phi(x)$  for a *formula* in which the variable x may appear free we can capture informally one natural way of reasoning from universally quantified formulæ as follows:

"In a context in which we accept  $\forall x \cdot \phi(x)$  we must accept  $\phi(T)$  (for any term T)"

(here  $\phi(T)$  means the result of substituting T for all free occurrences of x in  $\phi(x)$ ).

 $\triangleright$  For example: in a context in which we accept

$$\forall x \cdot \forall y \cdot succ \ y + x = succ(y + x)$$

we must accept

$$\forall y \cdot succ \ y + 0 = succ(y + 0)$$

(in this case the  $\phi(x)$  is  $\forall y \cdot succ \ y + x = succ(y + x)$ , and the T is 0)

- 2 -

- 4 -

we must accept

 $\triangleright$  This way of reasoning can be captured by the  $\forall$  elimination rule:

$$\frac{\Gamma \vdash \forall x \cdot \phi(x)}{\Gamma \vdash \phi(T)} \forall -\mathsf{e}$$

(T must be free for x in  $\phi(x)$ )

NB: This is a schematic (general) rule: the x stands for any variable, and the T for any term. All the other quantifier rules below will also be schematic.



 $\triangleright$  For this to work properly, T must be *free for* x in  $\phi(x)$ .

```
\triangleright For example: suppose we have \forall x \cdot \exists y \cdot x < y
```

```
then \phi(x) is \exists y \cdot x < y
```

and 
$$\phi(y)$$
 is  $\exists y \cdot y < y$ 

- So y is not free for x in  $\phi(x)$  because it is "captured" by  $\exists y \cdot$
- $\triangleright$  In logic in general the *free for* x condition is taken care of by the detailed definition of substitution

 $\triangleright$  The formula  $\phi(x)$  can be a logical composite. For example, in a context in which we accept

 $\forall x \cdot \begin{pmatrix} 0 + x = x & \land \\ \forall y \cdot succ \ y + x = succ(y + x) \end{pmatrix}$ 

 $\begin{pmatrix} 0 + succ(succ(0)) = succ(succ(0)) & \land \\ \forall y \cdot succ \ y + succ(succ(0)) = succ(y + succ(succ(0))) \end{pmatrix}$ 

 $\triangleright \text{ Here } T \text{ is } succ(succ(0)) \text{ and } \phi(x) \text{ is } \begin{pmatrix} 0+x=x & \land \\ \forall y \cdot succ \ y+x = succ(y+x) \end{pmatrix}$ 

- $\circ$  either variable-capturing substitutions are forbidden
- $\circ$  or bound variables are systematically renamed to avoid capture, *e.g.*

$$\phi(y)$$
 would be  $\exists y_1 \cdot y < y_1$ 

 $\triangleright$  One argument in favour of the soundness of the  $\forall$ -e rule starts from the observation that for a (non-empty) finite domain of discourse whose values are  $\delta_1, ... \delta_n$ 

the formula  $\forall x \cdot \phi(x)$  means the same as  $\phi(\delta_1) \wedge ... \wedge \phi(\delta_n)$ 

Now the term T must denote one of the values in the domain (say  $\delta_k$ ), and  $\phi(\delta_k)$  can be inferred from  $\phi(\delta_1) \wedge \ldots \wedge \phi(\delta_n)$  using an appropriate number of  $\wedge$ -e steps.

- ▷ Of course this is **not a logically acceptable justification** of the soundness of the rule in general.
- $\triangleright$  Nevertheless, treating the quantifiers as generalized conjunction and disjunction can help us get to grips with what they mean in general.

```
- б -
```

1 1 1 1 - 8 -

Proof Rules for Quantifiers: 3-introduction

Introduction to Formal Proof 4: Predicate Logic Proofs

Proof Rules for Quantifiers: 3-elimination

**Proof Rules for Quantifiers:** ∃-introduction

 $\triangleright$  Again writing  $\phi(x)$  for a *formula* in which the variable x may appear free, it seems natural to say that

"In a context in which we accept  $\phi(T)$  (for some term T) we must accept  $\exists x \cdot \phi(x)$ "

 $\triangleright$  This is captured by the  $\exists$ -introduction rule

$$\frac{\Gamma \vdash \phi(T)}{\Gamma \vdash \exists x \cdot \phi(x)} \exists -i$$

(T must be free for x in  $\phi(x)$ )

 $\triangleright$  An informal argument in support of  $\exists$ -e starts from the observation that for a (nonempty) finite domain whose values are  $\delta_1, ..., \delta_n$ ,

the formula  $\exists x \cdot \phi(x)$  means the same as  $\phi(\delta_1) \lor ... \lor \phi(\delta_n)$ 

The proof of  $\kappa$  from  $\phi(\delta_1) \lor ... \lor \phi(\delta_n)$  using only  $\lor$ -e would require us to make the n subproofs  $\phi(\delta_i) \vdash \kappa$  (for i = 1, 2, ..., n) Choosing a new variable v allows us to provide a general form for these proofs.

 $\triangleright$  Of course this is no more a logically acceptable justification of the soundness of the rule in general than was our earlier argument in support of  $\forall$ -e.





"In a context in which we accept  $\exists x \cdot \phi(x)$ , we can choose a name for an object that satisfies  $\phi(x)$  providing that the name does not appear anywhere in the context or the conclusion."

 $\rhd$  It is captured formally by the  $\exists\text{-elimination rule}$ 

$$\frac{\Gamma, \phi(v) \vdash \kappa}{\Gamma, \exists x \cdot \phi(x) \vdash \kappa} \exists -e \text{ (where } v \text{ is fresh)}$$

 $\triangleright$  Exercise: write this rule in the natural deduction style

 $\triangleright$  Here's an example of "name choosing" in an (informal) proof of the sequent

$$\forall x \cdot P(x) \to Q(x), \exists x \cdot P(x) \vdash \exists x \cdot Q(x)$$

1. Let v be such that P(v) (using the  $\exists$  premiss)

2. Now  $P(v) \rightarrow Q(v)$  (specialising the  $\forall$  premiss)

3. So Q(v) (by the implication)

4. So  $\exists x \cdot Q(x)$ 

 $\triangleright$  The completely formal proof is at least as convincing.

	8			
1:	$\forall x \cdot P(x) \to Q(x)$	) premiss		
2:	$\exists x \cdot P(x)$	premiss		
	fresh v			
3:	P(v)	assumption		
4:	$P(v) \rightarrow Q(v)$	∀-e 1		
5:	Q(v)	→-e 3, 4		
6:	$\exists x \cdot Q(x)$	∃-i 5		
7:	$\exists x \cdot Q(x)$	∃-e(2) 3-6		

 $\triangleright$  The scope of the chosen name is the subproof 3-6.

10

- 12 -

Proof Rules for Quantifiers: 3-elimination

Introduction to Formal Proof 4: Predicate Logic Proofs

Proof Rules for Quantifiers: 3-elimination

▷ Getting it wrong

• We want to prove  $\exists x \cdot P(x) \land Q(x) \vdash \exists x \cdot P(x)$ 

 $\circ$  We guess (wrongly) that the proof will look like (for some unknown term  $\omega$ ):

 $\stackrel{_{1:}}{\longrightarrow} \exists x \cdot P(x) \land Q(x) \quad \text{premiss}$  $\begin{array}{ll} & \cdots & \\ & P(\omega) \\ & \exists x \cdot P(x) & \exists \text{-i n'} \end{array}$ 

 $\triangleright$  A correct proof will "start with" (*i.e.* be rooted at)  $\exists$ -e

1: 
$$\exists x \cdot P(x) \land Q(x)$$
 premiss  
2:  $\begin{bmatrix} \text{fresh } \nu \\ P(\nu) \land Q(\nu) \\ P(\nu) \\ \exists x \cdot P(x) \end{bmatrix}$  assumption (from 5)  
4:  $\exists x \cdot P(x) \\ \exists x \cdot P(x) \end{bmatrix}$   $\exists \text{-i } 3$   
5:  $\exists x \cdot P(x)$  $\exists \text{-e } 1,2\text{-4}$ 

 $\triangleright$  this rooting of the proof corresponds to the form of words:

"let  $\nu$  be such that  $P(\nu) \wedge Q(\nu)$ "



# Proof Rules for Quantifiers: ∀-introduction

 $\triangleright$  "To prove  $\forall x \cdot \phi(x)$  choose a fresh variable v, and prove  $\phi(v)$ . The scope of the variable v is limited to the proof of  $\phi(v)$ ."

$$\frac{\Gamma \vdash \phi(v)}{\Gamma \vdash \forall x \cdot \phi(x)} \forall \text{-i (where } v \text{ is fresh)}$$

 $\triangleright$  Exercise: construct an informal argument in support of  $\forall$ -i.

• At this point the only proof step that can possibly be taken is to use the premiss



 $\triangleright$  But the  $\exists$ -e rule must choose a *fresh* variable  $\nu$  (which therefore cannot appear free in the term  $\omega$ ) and the proof is stuck

$$\begin{array}{ccc} & \vdots & \exists x \cdot P(x) \land Q(x) & \text{premiss} \\ \\ & & fresh \nu \\ & P(\nu) \land Q(\nu) \\ & \vdots \\ & P(\omega) \\ \\ & n^{\circ} \vdots & P(\omega) \\ & n^{\circ} \vdots & P(\omega) \\ & \exists e 1, 2\text{-}n^{\circ} \\ & \exists x \cdot P(x) \\ \end{array}$$

 $\triangleright$  This suggests that our guess was wrong.

Introduction to Formal Proof 4: Predicate Logic Proofs

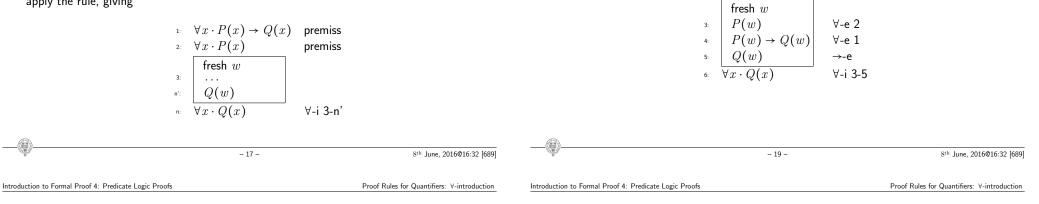
 $\triangleright$  The gap is now filled by an application of  $\rightarrow e$ 

Proof Rules for Quantifiers: ∀-introduction

 $\triangleright$  As an example of how we might use these rules, we shall complete the proof:

1:  $\forall x \cdot P(x) \rightarrow Q(x)$  premiss 2:  $\forall x \cdot P(x)$  premiss ... n:  $\forall x \cdot Q(x)$ 

 $\triangleright$  The form of the conclusion is such that we can confidently guess that the rule to be used there will be  $\forall$ -i. Although we could use x as our "fresh" variable (why?) we choose w and apply the rule, giving



# $\triangleright$ We can now use $\forall\text{-e}$ on either of the premisses, and then again on the other.

In both cases, the term used for the specialisation is w

1:  $\forall x \cdot P(x) \rightarrow Q(x)$  premiss 2:  $\forall x \cdot P(x)$  premiss 3: P(w)  $\forall -e 2$ 4:  $P(w) \rightarrow Q(w)$   $\forall -e 1$ ... n': Q(w)1:  $\forall x \cdot Q(x)$   $\forall -i 3-n'$   $\triangleright$  Exercise: does this version of the proof satisfy the freshness stipulation of  $\forall\mathchar`-i?$ 

1:  $\forall x \cdot P(x) \rightarrow Q(x)$ 

2:  $\forall x \cdot P(x)$ 

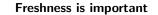
premiss

premiss

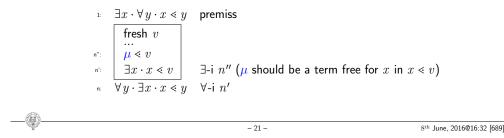
1: 2:	$ \forall x \cdot P(x) \to Q(x)  \forall x \cdot P(x) $	) premiss premiss
	fresh $x$ ?	
3:	P(x)	∀-е 2
4:	$P(x) \to Q(x)$	∀-e 1
5:	Q(x)	→-e
6:	$\overline{\forall x \cdot Q(x)}$	∀-i 3-5

Freshness is important

Freshness is important



- ▷ Example: Let < be a binary predicate. We will seek a formal proof of
  - 1:  $\exists x \cdot \forall y \cdot x < y$  premiss ... n:  $\forall y \cdot \exists x \cdot x < y$
  - (Exercise: find an informal proof)
- $\triangleright$  Suppose we start the search by removing the quantifiers from the conclusion, using an (unknown) term  $\mu$  (to be decided upon later) in  $\exists$ -i



Introduction to Formal Proof 4: Predicate Logic Proofs

 $\begin{cases} \text{fresh } w \\ \forall u \cdot w \leq z \end{cases}$ 

▷ It *appears* that we can use  $\exists$ -e at \* (with w as the variable) and specialize the assumption on line 2 to  $w \leq v$  using  $\forall$ -e (with term v)

> 1:  $\exists x \cdot \forall y \cdot x \lessdot y$ premiss fresh v fresh w  $\forall y \cdot w \lessdot y$ assumption 2:  $w \lessdot v$ ∀-е 2 3: n" ':  $\mu < v$ ∃-e(1) 2-n"'  $\boldsymbol{\mu} \lessdot \boldsymbol{v}$ n":  $\exists x \cdot x \lessdot v$  $\exists$ -i n" ( $\mu$  should be a term free for x in  $x \leq v$ ) n'·  $\forall y \cdot \exists x \cdot x \lessdot y$ ∀-in' n:

and, lastly, decide "retrospectively" that the  $\mu$  we had in mind all along was w.

# $\triangleright$ But the freshness proviso for w means it could not have been free in $\mu$

The problem is that we used  $\exists$ -i too early in our search!

No variable chosen at \* could ever be fresh enough to complete this partial proof!

Freshness is important

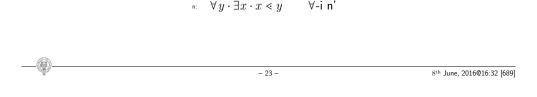
▷ One way of correcting this is to delay the use of  $\exists$ -i in the search for the proof, and to work forward from the premiss – choosing the name w for "an x for which  $\forall y \cdot x \leq y$ ".

premiss

This leaves us with a subproof obligation that is easy to meet.

 $\exists x \cdot \forall y \cdot x \lessdot y$ 

fresh v



Introduction to Formal Proof 4: Predicate Logic Proofs

 $\triangleright$  There are two ways to meet the proof obligation. Here is one

1:	$\exists x \cdot \forall y \cdot x \lessdot y$	premiss
	fresh $v$	
	fresh w	
2:	$\forall y \cdot w \lessdot y$	assumption
3:	$w \lessdot v$	∀-e(2) 3-4
4:	$\exists x \cdot x \lessdot v$	∃-i 3
5:	$\exists x \cdot x \lessdot v$	∃-e(1) 2-4
6:	$\overline{\forally\cdot\exists x\cdot x\lessdot y}$	∀-i 2-5

## Exercises:

1. What is the other way to meet the proof obligation?

- 2. Is there a proof that ends with  $\exists$ -e?
- 3. Is there a proof that ends with  $\exists$ -i?

Freshness is important

Summary of the Quantifier Rules

Introduction to Formal Proof 4: Predicate Logic Proofs

## Summary of the Quantifier Rules

 $\frac{\Gamma \vdash \phi[v/x]}{\Gamma \vdash \forall x \cdot \phi} \forall \text{-i } (v \text{ fresh}) \qquad \qquad \frac{\Gamma \vdash \forall x \cdot \phi}{\Gamma \vdash \phi[T/x]} \forall \text{-e } (T \text{ free for } x \text{ in } \phi)$ 

 $\frac{\Gamma \vdash \phi[T/x]}{\Gamma \vdash \exists x \cdot \phi} \exists \neg i \ (T \text{ free for } x \text{ in } \phi) \qquad \frac{\Gamma, \phi[v/x] \vdash \kappa}{\Gamma, \exists x \cdot \phi \vdash \kappa} \exists \neg e \ (v \text{ fresh})$ 

 $\triangleright$  Here we present the rules again, this time using explicit substitution notation.

# Derived consequences of substitutivity

 $\triangleright$  Symmetry of equality

1: 
$$T_1 = T_2$$
 premiss  
2:  $T_1 = T_1$  =-i  
3:  $T_2 = T_1$  =-e 1, 2

$$\frac{\overline{T_1 = T_2 \vdash T_1 = T_2}}{T_1 = T_2 \vdash T_2 = T_1} \stackrel{\text{hyp}}{=-e} = T_1$$

 $\triangleright$  How does the =-e work in this proof?

- $\circ$  the consequent conclusion  $T_2 = T_1$  is  $(\chi = T_1)[T_2/\chi]$
- the right hand antecedent conclusion is  $(\chi = T_1)[T_1/\chi]$

(for any suitable variable  $\chi$ )

- 25 - 8<sup>th</sup> June, 2016@16:32 [689] Introduction to Formal Proof 4: Predicate Logic Proofs Proof Rules for Equality

**Proof Rules for Equality** 

 $\triangleright$  Introduction: "every term is equal to itself" (sometimes called "reflexivity of equality")

 $\overline{\Gamma \vdash T} = \overline{T}^{=-i}$ 

 $8^{\rm th}$  June, 2016@16:32 [689]

Derived consequences of substitutivity

▷ Transitivity of equality

$$\frac{\overline{T_1 = T_2, T_2 = T_3 \vdash T_2 = T_3}_{\text{premiss}} \qquad \overline{T_1 = T_2, T_2 = T_3 \vdash T_1 = T_2}_{\text{remiss}} = e^{\text{premiss}}$$

▷ Elimination: (sometimes called "substitutivity of equality")

$$\frac{\Gamma \vdash T_1 = T_2 \qquad \Gamma \vdash \phi[T_1/\chi]}{\Gamma \vdash \phi[T_2/\chi]} = -\mathbf{e}$$

(where  $\chi$  is a variable chosen so that  $T_1, T_2$  are free for  $\chi$  in  $\phi$ )

 $\triangleright$  How does the =-e work in this proof?

- $\circ$  the consequent conclusion  $T_1$  =  $T_3$  is  $(T_1 = \chi)[T_3/\chi]$
- $\circ$  the right hand antecedent conclusion is (  $T_1$  =  $\chi)[\,T_2/\chi]$

(for any suitable variable  $\chi$ )

Contents	
Proof Rules for Predicate Calculus Proofs	Proof Rules for Quantifiers: V-introduction
- 29 -	<sup>8th</sup> June, 2016@16:32 [689]
Introduction to Formal Proof 4: Predicate Logic Proofs	Notes
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Note 2: Proof by contradiction	3 11
The law $\frac{\Gamma,\neg\phi\vdash \bot}{\Gamma\vdash\phi} \ \ {\rm Contra}$	Contradiction
is justified by the derivation $\frac{\Gamma, \neg \phi \vdash \bot}{\Gamma \vdash \neg \neg \phi}$	- i - e
<b>Note 3:</b> It is a simple matter to show both that we can derive the "left-side" rule:	ال€
$\frac{\Gamma, \forall x \cdot \phi(x), \phi(T) \vdash \psi}{\Gamma, \forall x \cdot \phi(x) \vdash \psi} \ \forall \vdash$	$\frac{1}{1-\frac{1}{2}}$ A <sup>L</sup>
from ∀-e; and that ∀-e would be derivable from ∀ ⊢ if the latter were a rule. We leave these derivations as exercises for i (in the light of the material relating left-side to elimination rules in chapter 2) the key to both derivations is the cut rule.	We leave these derivations as exercises for the interested reader. Unsurprisingly ) the key to both derivations is the cut rule.
Note 4: Suppose $\phi(x)$ is a formula, and $\delta$ an element of a domain. To save "formal clutter" we shall here and henceforth write $\phi(\delta)$ instead of the proper $\phi(\langle\!\langle\delta\rangle\!\rangle)$ when to do so will not cause any confusion.	8 $\mathbb{I}^{\cong}$ we shall here and henceforth write $\phi(\delta)$ instead of the proper $\phi(\langle\!\langle \delta \rangle\!\rangle)$

Logic Proofs
Predicate
Proof 4:
o Formal
Introduction to

Notes

10

12

**Note 5: Fresh variables** A variable is fresh in a proof context if it doesn't appear free in any hypothesis or in the conclusion.

Note 6: A sequent-tree presentation of the proof of

 $\forall x \cdot P(x) \to Q(x), \exists x \cdot P(x) \vdash \exists x \cdot Q(x)$ 

goes as follows

$\frac{d(v) \vdash Q(v)}{Q(v) \vdash \exists x \cdot Q(x)} \xrightarrow{\exists -1}_{a}$			$r \cdot P(x) \vdash \exists x \cdot Q(x)$
$\frac{1}{P(v) \vdash P(v)} hyp$	$P(v) \to Q(v), P(v) \vdash \exists x \cdot Q(x)$	$\forall x \cdot P(x) \to Q(x), P(v) \vdash \exists x \cdot Q(x)$	$\forall x \cdot P(x) \to Q(x), \exists x \cdot P(x) \vdash \exists x \cdot Q(x)$

For conciseness here, we have silently used the weaken rule in several places, as well as the derived rules  $\forall \vdash$  and  $\rightarrow \vdash$  (from section 2). Exercise: complete the proof tree by inserting appropriate instances of the weaken rule.  $8^{\rm th}$  June, 2016@16:32 [689]

- 31 -