Introduction to Formal Proof

Bernard Sufrin

Trinity Term 2018

4: Predicate Logic Proofs

Predicate Calculus Proofs

▷ Here we introduce an inference system for proofs about conjectures of the form:

$$\phi_1, ..., \phi_n \vdash \psi$$

(where $\phi_1, ..., \phi_n, \psi$ are formulæ over a signature)

▷ The system is *sound*: we can prove $\phi_1, ..., \phi_n \vdash \psi$ only if ψ is true in *all* situations in which the formulae ϕ_i are true;*i.e.*

If

$$\phi_1, ..., \phi_n \vdash \psi$$

can be proven in the inference system, then

$$\phi_1, ..., \phi_n \vDash \psi$$

Proof Rules for the logical connectives

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

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

$$\frac{\Gamma \vdash \phi \qquad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi} \wedge\text{-i} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi} \wedge\text{-e}_L \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi} \wedge\text{-e}_R$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi} \vee\text{-i}_L \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi} \vee\text{-i}_R \qquad \frac{\Gamma \vdash \phi \vee \psi \qquad \Gamma, \phi \vdash \kappa \qquad \Gamma, \psi \vdash \kappa}{\Gamma \vdash \kappa} \vee\text{-e}$$

▷ Negation rules

$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg\phi} \neg\text{-i} \qquad \frac{\Gamma \vdash \phi \qquad \Gamma \vdash \neg\phi}{\Gamma \vdash \bot} \neg\text{-e}$$

$$\frac{\Gamma \vdash \neg\neg\phi}{\Gamma \vdash \phi} \neg\neg\text{-e}$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \phi} \bot\text{-e}$$

▷ “Proof by contradiction” is justified by the derived rule

$$\frac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \phi} \text{Contradiction}$$

Proof Rules for Quantifiers: ∀-elimination

▷ 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 occurences of x in $\phi(x)$).

▷ 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)

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

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

we must accept

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

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

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

▷ 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 $\exists y \cdot$

▷ In logic in general the *free for* x condition is taken care of by the detailed definition of substitution

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

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

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

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

(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.

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

$$\boxed{\text{the formula } \forall x \cdot \phi(x) \text{ means the same as } \phi(\delta_1) \wedge \dots \wedge \phi(\delta_n)}$$

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

▷ *Of course this is* **not a logically acceptable justification** *of the soundness of the rule in general.*

▷ Nevertheless, treating the quantifiers as generalized conjunction and disjunction can help us get to grips with what they mean in general.

Proof Rules for Quantifiers: $\exists$-introduction

▷ 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 $\exists x \cdot \phi(x)$"

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

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

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

Proof Rules for Quantifiers: $\exists$-elimination

"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*."

▷ It is captured formally by the $\exists$-elimination rule

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

▷ Exercise: write this rule in the natural deduction style

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

$$\boxed{\text{the formula } \exists x \cdot \phi(x) \text{ means the same as } \phi(\delta_1) \vee \ldots \vee \phi(\delta_n)}$$

The proof of κ from $\phi(\delta_1) \vee \ldots \vee \phi(\delta_n)$ using only $\vee$-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.

▷ *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.*

▷ 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 $P(v) \to Q(v)$ (specialising the $\forall$ premiss)
3. So $Q(v)$ (by the implication)
4. So $\exists x \cdot Q(x)$

▷ The completely formal proof is at least as convincing.

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

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

▷ Getting it wrong

- We want to prove $\exists x \cdot P(x) \wedge Q(x) \vdash \exists x \cdot P(x)$
- We guess (wrongly) that the proof will look like (for some unknown term ω):

1:	$\exists x \cdot P(x) \wedge Q(x)$	premiss
	$\cdots$	
n':	$P(\omega)$	
n:	$\exists x \cdot P(x)$	∃-i n'

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

▷ But the ∃-e rule must choose a *fresh* variable ν (which therefore cannot appear free in the term ω) and the proof is stuck

1:	$\exists x \cdot P(x) \wedge Q(x)$	premiss
	fresh ν	
2:	$P(\nu) \wedge Q(\nu)$	assumption (from n')
	$\cdots$	
n'':	$P(\omega)$	
n':	$P(\omega)$	∃-e 1, 2-n''
n:	$\exists x \cdot P(x)$	∃-i n'

▷ This suggests that our guess was wrong.

▷ A correct proof will "start with" (*i.e.* be rooted at) ∃-e

1:	$\exists x \cdot P(x) \wedge Q(x)$	premiss
	fresh ν	
2:	$P(\nu) \wedge Q(\nu)$	assumption (from 5)
3:	$P(\nu)$	$\wedge$-e_L
4:	$\exists x \cdot P(x)$	∃-i 3
5:	$\exists x \cdot P(x)$	∃-e 1,2-4

▷ this rooting of the proof corresponds to the form of words:

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

Proof Rules for Quantifiers: ∀-introduction

▷ "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 $\phi(v)$."

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

▷ Exercise: construct an informal argument in support of ∀-i.

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

1:	$\forall x \cdot P(x) \to Q(x)$	premiss
2:	$\forall x \cdot P(x)$	premiss
	$\cdots$	
n:	$\forall x \cdot Q(x)$	

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

1:	$\forall x \cdot P(x) \to Q(x)$	premiss
2:	$\forall x \cdot P(x)$	premiss
	fresh w	
3:	$\ldots$	
n':	$Q(w)$	
n:	$\forall x \cdot Q(x)$	∀-i 3-n'

▷ We can now use ∀-e on either of the premisses, and then again on the other.
In both cases, the term used for the specialisation is w

1:	$\forall x \cdot P(x) \to Q(x)$	premiss
2:	$\forall x \cdot P(x)$	premiss
	fresh w	
3:	$P(w)$	∀-e 2
4:	$P(w) \to Q(w)$	∀-e 1
	$\cdots$	
n':	$Q(w)$	
n:	$\forall x \cdot Q(x)$	∀-i 3-n'

▷ The gap is now filled by an application of $\to e$

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

▷ Exercise: does this version of the proof satisfy the freshness stipulation of ∀-i?

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

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
	$\ldots$	
n:	$\forall y \cdot \exists x \cdot x < y$	

(Exercise: find an informal proof)

▷ Suppose we start the search by removing the quantifiers from the conclusion, using an (unknown) term μ (to be decided upon later) in ∃-i

1:	$\exists x \cdot \forall y \cdot x < y$	premiss
	fresh v	
	$\ldots$	
n'':	$\mu < v$	
n':	$\exists x \cdot x < v$	∃-i n'' (μ should be a term free for x in $x < v$)
n:	$\forall y \cdot \exists x \cdot x < y$	∀-i n'

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

1:	$\exists x \cdot \forall y \cdot x < y$	premiss
	fresh v	
	fresh w	
2:	$\forall y \cdot w < y$	assumption
3:	$w < v$	∀-e 2
	$\ldots$	
n''':	$\mu < v$	
n'':	$\mu < v$	∃-e(1) 2-n''' $*$
n':	$\exists x \cdot x < v$	∃-i n'' (μ should be a term free for x in $x < v$)
n:	$\forall y \cdot \exists x \cdot x < y$	∀-i n'

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

▷ **But the freshness proviso for w means it could not have been free in μ**

The problem is that we used ∃-i *too early* in our search!

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

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

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

1:	$\exists x \cdot \forall y \cdot x < y$	premiss
	fresh v	
	fresh w	
2:	$\forall y \cdot w < y$	assumption
	$\ldots$	
n'':	$\exists x \cdot x < v$	
n':	$\exists x \cdot x < v$	∃-e(1) 2-n''
n:	$\forall y \cdot \exists x \cdot x < y$	∀-i n'

▷ There are two ways to meet the proof obligation. Here is one

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

Exercises:

1. What is the other way to meet the proof obligation?
2. Is there a proof that ends with ∃-e?
3. Is there a proof that ends with ∃-i?

Summary of the Quantifier Rules

▷ Here we present the rules again, this time using explicit substitution notation.

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

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

Proof Rules for Equality

▷ Introduction: “every term is equal to itself” (sometimes called “reflexivity of equality”)

$$\frac{}{\Gamma \vdash T = T}\ =\text{-i}$$

▷ Elimination: (sometimes called “substitutivity of equality”)

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

(where χ is a variable chosen so that T_1, T_2 are free for χ in ϕ)

Derived consequences of substitutivity

▷ Symmetry of equality

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

$$\frac{\dfrac{}{T_1 = T_2 \vdash T_1 = T_2}\ \text{hyp} \qquad \dfrac{}{T_1 = T_2 \vdash T_1 = T_1}\ =\text{-i}}{T_1 = T_2 \vdash T_2 = T_1}\ =\text{-e}$$

▷ How does the =-e work in this proof?

- 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 χ)

▷ Transitivity of equality

$$\frac{\dfrac{}{T_1 = T_2, T_2 = T_3 \vdash T_2 = T_3}\ \text{premiss} \qquad \dfrac{}{T_1 = T_2, T_2 = T_3 \vdash T_1 = T_2}\ \text{premiss}}{T_1 = T_2, T_2 = T_3 \vdash T_1 = T_3}\ =\text{-e}$$

▷ How does the =-e work in this proof?

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

(for *any* suitable variable χ)

Contents

Proof Rules for Predicate Calculus 1
Predicate Calculus Proofs 1
Proof Rules for the logical connectives 2
Proof Rules for Quantifiers: ∀-elimination 4
Proof Rules for Quantifiers: ∃-introduction 9
Proof Rules for Quantifiers: ∃-elimination 10
Proof Rules for Quantifiers: ∀-introduction 16
Freshness is important 21
Summary of the Quantifier Rules 25
Proof Rules for Equality 26
Derived consequences of substitutivity 27

Note 1: Situations 1 ☞

A *situation* is a *particular* model, together with a mapping from variables to the values of its domain. Establishing the truth of a formula "in all situations" cannot be done directly and mechanically by program, for such a program would have to enumerate all possible models for the signature, including non-finite models.

Note 2: Proof by contradiction 3 ☞

The law

$$\frac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \phi}\ \text{Contradiction}$$

is justified by the derivation

$$\frac{\dfrac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \neg\neg\phi}\ \neg - i}{\Gamma \vdash \phi}\ \neg\neg - e$$

Note 3: 7 ☞

It is a simple matter to show both that we can derive the "left-side" rule:

$$\frac{\Gamma, \forall x \cdot \phi(x), \phi(T) \vdash \psi}{\Gamma, \forall x \cdot \phi(x) \vdash \psi}\ \forall\vdash$$

from ∀-e; and that ∀-e would be derivable from $\forall \vdash$ if the latter were a rule. We leave these derivations as exercises for the interested reader. Unsurprisingly (in the light of the material relating left-side to elimination rules in chapter 2) the key to both derivations is the cut rule.

Note 4: 8 ☞

Suppose $\phi(x)$ is a formula, and δ 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.

Note 5: Fresh variables 10 ☞

A variable is fresh in a proof context if it doesn't appear free in any hypothesis or in the conclusion.

Note 6: 12 ☞

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{P(v) \vdash P(v)}\,\textsf{hyp} \qquad \dfrac{\dfrac{}{Q(v) \vdash Q(v)}\,\textsf{hyp}}{Q(v) \vdash \exists x \cdot Q(x)}\,\exists\textsf{-i}}{P(v) \to Q(v), P(v) \vdash \exists x \cdot Q(x)}\,{\to}{\vdash}}{\forall x \cdot P(x) \to Q(x), P(v) \vdash \exists x \cdot Q(x)}\,\forall{\vdash}}{\forall x \cdot P(x) \to Q(x), \exists x \cdot P(x) \vdash \exists x \cdot Q(x)}\,\exists\textsf{-e}$$

For conciseness here, we have silently used the weaken rule in several places, as well as the derived rules $\forall\vdash$ and $\to\vdash$ (from section 2).

Exercise: complete the proof tree by inserting appropriate instances of the weaken rule.