

Informal Proofs

David L. Dill
Department of Computer Science
Stanford University

1 / 30

Announcements

- Homework 1 due now.
- Homework 2 is assigned.

2 / 30

Clarification on predicate logic syntax

When I defined the syntax of predicate logic formulas a few lectures ago, I said:

Terms can contain function symbols, individual constants, and *variables*.

E.g., a , x , $f(a)$, $f(a, x)$

I should have added that, in some cases, there is special notation. For example, in $x + y$, $x \times y$, the functions are *infix*, as opposed to the generic prefix notation I used, which would have been: $+(x, y)$ and $\times(x, y)$.

This is just a different notation that exists for historical reasons. It doesn't change anything important about predicate logic.

3 / 30

Outline

- Simple proof rules for quantifiers.
- Rules involving subproofs
 - Conditional Introduction
 - Universal Introduction (Universal Generalization)
 - Negation Introduction (Proof by Contradiction)
 - Biconditional Introduction
 - Disjunction Elimination (Proof by Cases)
 - Existential Elimination (Existential Instantiation)

This lecture will give formal proof rules and examples of formal and informal proofs.

4 / 30

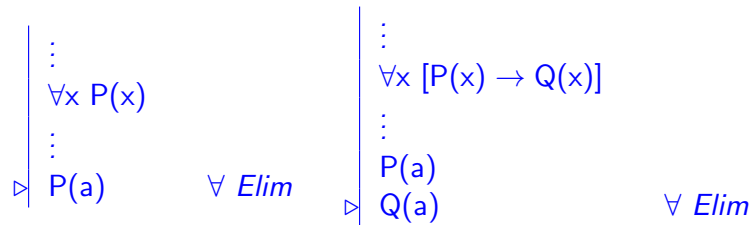
Universal Elimination

This is also called “Universal Instantiation.”

If $\forall x P(x)$ holds, then $P(a)$ holds for *any term* a .

More generally, if $\forall x (P(x) \rightarrow Q(x))$ holds and $P(a)$ holds for some term a , we may conclude $Q(a)$ holds.

Example: If “Every integer greater than 1 is a product of primes,” then “49 is a product of primes.”



5 / 30

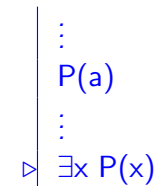
Existential Introduction

This is also called “Existential generalization.” a can be an arbitrary term.

If $P(a)$ holds for some term a , then $\exists x P(x)$ holds.

Since “2 is an even prime,” we can conclude “There is an even prime.”

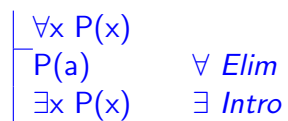
\exists Introduction



6 / 30

Example Proof with Simple Quantifier Rules

Let’s prove $\forall x P(x) \Rightarrow \exists x P(x)$.



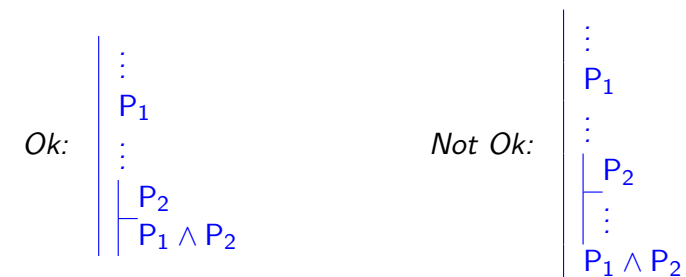
System F assumes the domain of discourse is non-empty, otherwise this would not be valid.

7 / 30

Subproofs

In all but the simplest proof, it is necessary to prove simpler claims inside the proof.

This is formalized as a *subproof* in System F.



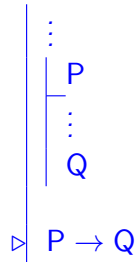
You can use previous sentences in enclosing proofs, but you can’t use sentences that only occur inside non-enclosing proofs.

8 / 30

Conditional Introduction

If, by assuming P , you can prove Q , then $P \rightarrow Q$ holds.

\rightarrow *Introduction*



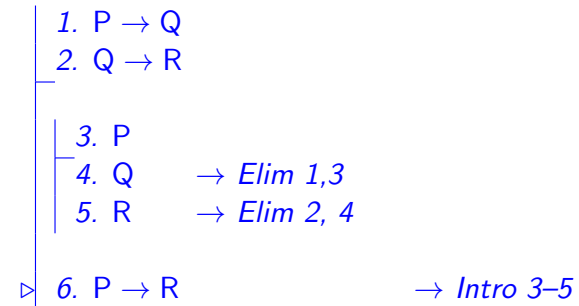
This rule allows you to “lift” a conclusion out of a subproof by qualifying it with the premises of the subproof.

This is one of the basic techniques used in informal proofs, called “Conditional Proof.”

9 / 30

Example Proof

This is a proof of a simple and important property of \rightarrow : it is *transitive*.



10 / 30

Conditional introduction in informal proofs

\rightarrow Intro is very frequently used in proofs. Here is the style we want you to use.

- Assume P (“Suppose P holds ...”)
- Prove Q follows from P in one or more steps.
- Conclude that $P \rightarrow Q$ holds.

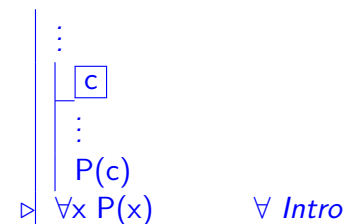
11 / 30

Universal Introduction

This rule is a bit more subtle.

Idea: To prove a universal statement, dream up a name about which nothing is known because it has never been used to name an object.

If you can prove something of that object, it is true of all objects.

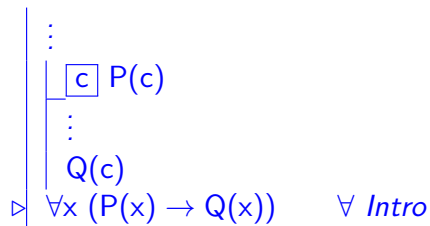


Note: c must not have appeared before the boxed occurrence.

12 / 30

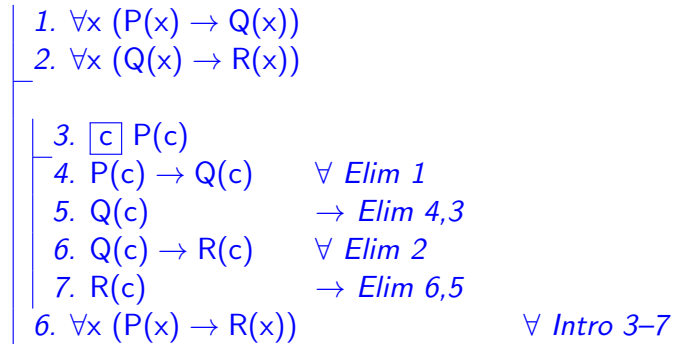
Alternate Universal Introduction Rule

This is a small variation.



13 / 30

Example Proof with Universal Generalization



14 / 30

General Conditional Proof

This is the informal proof method that corresponds to \forall Introduction in System F .

- “Let a be any (whatever) such that $P(a)$.” **Do this on homework 2 when using Universal Generalization**
- Prove $Q(a)$.
- Conclude “Since a was chosen arbitrarily, every $P(a)$ is a $Q(a)$.” (or, in many cases, “Hence, $P(x)$ implies $Q(x)$ for all x .”)

In mathematics, and in our informal examples, a will often be the same name as a universal variable in the formula.

System F doesn't allow the name to be the same as a quantified variable (names and variables are different), but the standard practice rarely leads to confusion.

15 / 30

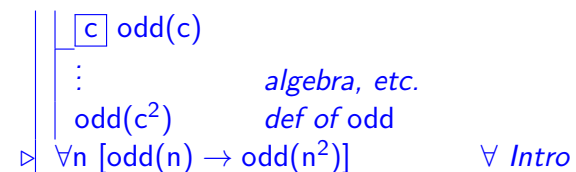
Formal vs. informal proof

Here is a theorem from the last lecture, without the fudging of quantifiers:

Theorem: For all integers n , if n is odd, then n^2 is odd.

Proof: Let n be an arbitrary odd integer. Then, by definition, $n = 2k + 1$. Therefore, $n^2 = 4k^2 + 4k + 1$. But then this can be written $2(2k^2 + 2k) + 1$, so n^2 is odd. Hence, the theorem holds for all integers. \square

Formally: $\forall n [\text{odd}(n) \rightarrow \text{odd}(n^2)]$

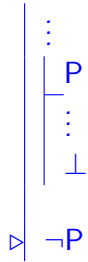


16 / 30

Negation Introduction in System F

In System F, proof by contradiction is captured in the negation introduction rule.

¬ Introduction



17 / 30

Proof by Contradiction

This is the informal version of negation introduction:

- Explain that you are proving by contradiction (“We prove by contradiction.” or “Suppose to the contrary ...”, etc.)
Always do this.
- Assume the negation of the desired conclusion.
- Prove that a contradiction results.
- Point out that this proves the desired conclusion.

18 / 30

Some Simple Integer Facts

Definition An integer n is *even* if it can be written as $n = 2k$ where k is an integer.

$$\forall n \text{ even}(n) \leftrightarrow \exists k n = 2k$$

Note: It is standard to use “if” in definitions, even though the logical meaning is really “iff”

Definition An integer n is *odd* if it can be written as $n = 2k + 1$ where k is an integer.

$$\forall n \text{ odd}(n) \leftrightarrow \exists k n = 2k + 1$$

An integer n is *odd* iff it is not even.

19 / 30

Informal Proof by Contradiction

Theorem: For every integer n , if n^2 is even, then n is even.

proof: Let n be any integer. Suppose to the contrary that n^2 is even but n is odd. Then $n = 2k + 1$ for some integer k , by definition. But then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, so it is odd, a contradiction.

Therefore, since n was chosen arbitrarily, when n^2 is even, n must also be even. \square

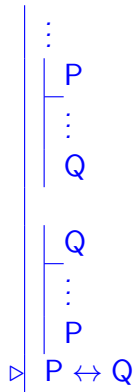
Note: We assume $\text{even}(n^2) \wedge \text{odd}(n)$ because it is $\neg[\text{even}(n^2) \rightarrow \text{even}(n)]$.

20 / 30

Biconditional Introduction

Biconditional introduction basically requires proving implication in each direction, using subproofs.

\leftrightarrow *Introduction*



21 / 30

Informal Biconditional Introduction

When you need to prove something involving $P(x)$ iff $Q(x)$, the style is:

proof:

\Rightarrow : Suppose $P(x)$ Therefore, $Q(x)$.

\Leftarrow : Now suppose $Q(x)$ Therefore, $P(x)$.

Hence, $P(x)$ iff $Q(x)$. \square

Often, the theorem is actually $\forall x [P(x) \leftrightarrow Q(x)]$, and the universal elimination and introduction is implicit.

22 / 30

Example Informal Biconditional Proof

Theorem: n is even iff n^2 is even, for every integer n .

proof: Let n be an arbitrary integer. We prove both directions.

\Rightarrow : Proved earlier in this lecture.

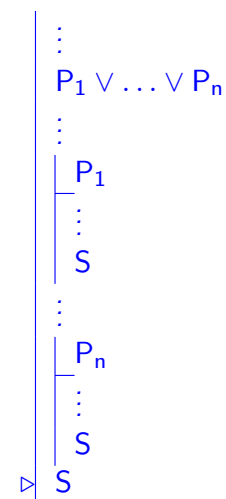
\Leftarrow : Also proved earlier.

Therefore, n is even iff n^2 is even, for all integers n . \square .

23 / 30

Disjunction Elimination

\vee *Elimination*



24 / 30

Informal Proof by Cases

This corresponds to \forall Elimination in System F .

1. Explain that you are doing a case analysis.
2. Show that a set of cases is exhaustive.
3. Show that the desired conclusion holds for each case.
4. Hence, the conclusion holds.

25 / 30

Proof by Cases

Theorem: $n^3 + n$ is even, for every integer n .

Proof: Let n be any integer.

Note that $n^3 + n = n(n^2 + 1)$.

n is even or odd, so there are two cases.

If n is even, then $n(n^2 + 1)$ must be even.

If n is odd, then n^2 is odd, so $n^2 + 1$ is even.

Hence, $n(n^2 + 1) = n^3 + n$ is even.

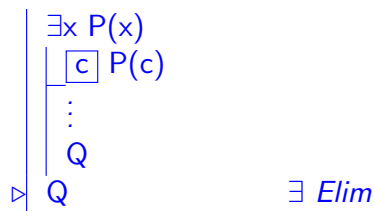
Since n was chosen arbitrarily, the theorem holds for all integers.

□

26 / 30

Existential Elimination

Also called Existential Instantiation.



Important: c must not appear in Q .

27 / 30

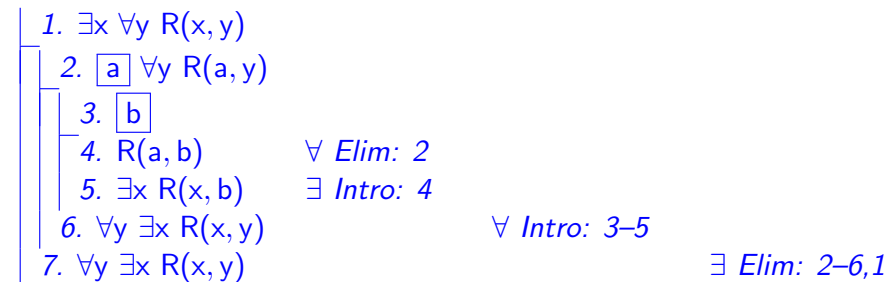
Example Proof Using Existential Elimination

This is true:

$$\exists x \forall y R(x, y) \Rightarrow \forall y \exists x R(x, y).$$

Intuition: If there is one person who likes everyone, then everyone is liked by someone.

It can be proved in System F :



28 / 30

Informal Proof Using Existential Instantiation

Facts:

By definition, n is rational if there exist integers p and q such that $n = p/q$.

For each pair of integers m and n , there exists a largest common factor k such that $m = ak$ and $n = bk$ for some integers a and b .

Theorem: Every rational number n can be written in the form p/q , where p and q are integers having no common factors.

proof: By definition, every rational number n there exist integers u and v such that $n = u/v$. Let k be the largest integer that evenly divides u and v . Then u/k and v/k are the desired p and q . \square

This proof used Existential Instantiation twice, once for each of the two facts at the top of the slide.

It also uses Existential Generalization, because it constructs the specific p and q to demonstrate their existence.

Existential Instantiation

Corresponds to Existential Elimination in Fitch.

- Observe that there exists something with property P.
- “Call it a,” where a is a new name (or “Let the even prime be a”).
- Prove Q.

Caution: Keep track of whether a depends on a previously instantiated universal variable.

Fallacious proof:

Let n be any number.

Since every number has a larger number, there is a number m such that $m > n$.

But, since n was chosen arbitrarily, every number must be less than m .

Problem: choice of m depended on prior choice of n .