Utrecht University

Logic for Computer Science

06 – Proof strategies

Wouter Swierstra

University of Utrecht

Last time

Predicate logic

This lecture

Proof strategies

Syntax and semantics

Whenever we study *formal* languages and logics, we typically distinguish between two different aspects:

- **syntax** describes what terms are well-formed;
- **semantics** describes the meaning of terms (or in the context of logic, what statements are true);

This is an important distinction to make.

Syntax and semantics of propositional logic

We defined the **syntax** of propositional logic:

- T and F are a propositions;
- an atomic propositional variable, such as P and Q
- if p is a proposition, so is $\neg p$
- if p and q are propositions, so are $p \wedge q$, $p \vee q$, $p \Rightarrow q$, and $p \Leftrightarrow q$

This fixes the language that we consider.

We can rule out non-sensical terms such as $\wedge p(\vee\neg)$ – but it doesn't tell us what the *meaning* is of a formula such as $p \vee q \Rightarrow p$.

Syntax and semantics of propositional logic

The **semantics** of propositional logic is given by truth tables.

We defined truth tables for all the operators, such as $\wedge$ and $\Rightarrow$, and showed how to use these to write a truth table for **any** syntactically valid formula in propositional logic.

Syntax and semantics of propositional logic

The **semantics** of propositional logic is given by truth tables.

We defined truth tables for all the operators, such as $\wedge$ and $\Rightarrow$, and showed how to use these to write a truth table for **any** syntactically valid formula in propositional logic.

But other 'semantics' exist:

- determining whether or not a propositional formula is a tautology;
- computing the set of atomic propositions a formula contains;
- mapping propositional formulas to a unique representation or *normal form*;
- ...

Each of these assign different kinds of meaning to the syntax of our propositional logic.

Syntax of predicate logic

In the previous lecture, we saw how to define the **syntax** of predicate logic, including:

- familiar operators from propositional logic;
- predicates;
- universal and existential quantifiers;
- careful treatment of scope and binding.

Syntax of predicate logic

In the previous lecture, we saw how to define the **syntax** of predicate logic, including:

- familiar operators from propositional logic;
- predicates;
- universal and existential quantifiers;
- careful treatment of scope and binding.

But what is the **semantics** associated with predicate logic?

Semantics of predicate logic

Predicate logic much more powerful than propositional logic.

To prove a propositional formula was a tautology, we could check all possible combinations of the truth values of its atomic propositions – for example, by writing out a truth table.

But how to prove a statement in predicate logic?

For example, how should we prove that there are three natural numbers a, b and c such that $a^2 + b^2 = c^2$?

Semantics of predicate logic

Predicate logic much more powerful than propositional logic.

To prove a propositional formula was a tautology, we could check all possible combinations of the truth values of its atomic propositions – for example, by writing out a truth table.

But how to prove a statement in predicate logic?

For example, how should we prove that there are three natural numbers a, b and c such that $a^2 + b^2 = c^2$?

After some head scratching, we can find that 3, 4 and 5 satisfy the required property – but how can we **decide** this in general?

Decidability

For any formula in propositional logic, a computer can check in finite time whether or not it is a tautology – for example, by generating the truth table.

We say that propositional logic is **decidable**.

But for an arbitrary formula in predicate logic, how can we check whether it is true or not?

We may need to check that all the inhabitants of an infinite set have some property!

There's no way to do that in finite time – proving the that an arbitrary statement in predicate logic holds is **not** decidable.

Semantics of predicate logic

Does that mean that there's no point in studying predicate logic?

Semantics of predicate logic

Does that mean that there's no point in studying predicate logic?

No! It simply means that the proofs are inherently more interesting and require human creativity.

Rather than give an 'algorithm' for proving propositional formulas, we'll study 'proof strategies' that give you a framework for performing proofs by hand.

These proof strategies *can* be given a precise logical formulation – and we'll do so later on in this course.

As it turns out, a computer *can* check whether or not a given proof adheres to these rules or not.

What is a proof?

Proofs exist in many different levels of rigour:

- Many mathematical textbooks and articles give hints how to construct the proof – ‘follows from lemma 4.3 and definition 4.1’ – but do not give the proof explicitly
- Many exercises when learning about logic and proofs, require students to be much more explicit about every single step done in the proof.
- Other proofs might sketch the key ideas, but not spell out every single detail.

Formal logic gives a precise set of rules that define what a valid proof object is.

A computer can then check that a given proof object can be constructed using these rules.

Proofs

There is no single definition of ‘what is a proof’ – it depends on context.

- Who are you trying to convince? Fellow experts? A machine?
- How much detail can you omit?
- Are you working in a very formal setting?

And many other factors contribute to what might be considered a valid proof.

Proofs and natural language

Many proofs (and proof strategies) are written in *natural language* (English, Dutch, etc.)

But they are clearly structured – and the words they use ‘Assume A is a set’ or ‘From X we conclude Y’ – have a clear and particular ‘technical’ meaning.

These words matter! You cannot write arbitrary text – but instead need to learn to structure proofs clearly, constructing the argument you want to make in an unambiguous fashion.

Proof strategies

Proof strategies

Today I want to go through an example proof in great detail.

The steps I take in this proof can be generalized, turning them into ‘proof strategies’ that give you a reusable proof template whenever you need to prove a statement (or use an assumption) of a certain form.

This should give you some understanding of how to write a precise proof – but doing so takes practice!

Later on in the course, I’ll give a formal treatment of logic, making these proof sketches more precise.

How to write a proof

On the exam (or in the exercises), start *any* proof by:

- Writing down all the assumptions.
- Stating the statement (or goal) that you aim to prove.
- Using these assumptions to prove (intermediate) results.
- Establishing that the goal follows from your assumptions (and these intermediate results).

Even if you only write down the assumptions and goals – you can still get partial credit.

Example

Theorem For all sets A, B, and C we have that $A \subseteq C \land B \subseteq C \Rightarrow A \cup B \subseteq C$

If we unfold the definition of subsets and translate this statement to predicate logic, this gives rise to a sizeable formula:

$$\forall A \forall B \forall C \quad ((\forall a \quad (a \in A \Rightarrow a \in C)) \land (\forall b \quad (b \in B \Rightarrow b \in C)) \Rightarrow (\forall x \quad (x \in A \cup B \Rightarrow x \in C)))$$

How should we go about proving this?

Example

Theorem For all sets A, B, and C we have that $A \subseteq C \land B \subseteq C \Rightarrow A \cup B \subseteq C$

If we unfold the definition of subsets and translate this statement to predicate logic, this gives rise to a sizeable formula:

$$\forall A \forall B \forall C \quad ((\forall a \quad (a \in A \Rightarrow a \in C)) \land (\forall b \quad (b \in B \Rightarrow b \in C)) \Rightarrow (\forall x \quad (x \in A \cup B \Rightarrow x \in C)))$$

How should we go about proving this?

We could draw a Venn diagram to convince ourselves that this is true – but let's look at what a written proof looks like.

Example

Theorem Let A, B, and C be sets. Then $A \subseteq C \land B \subseteq C \Rightarrow A \cup B \subseteq C$

Example

Theorem Let A, B, and C be sets. Then $A \subseteq C \land B \subseteq C \Rightarrow A \cup B \subseteq C$

Proof

Let A, B, and C be arbitrary sets. Assume that $A \subseteq C \land B \subseteq C$.

We can deduce that $A \subseteq C$ and $B \subseteq C$.

We must show $A \cup B \subseteq C$. By definition of set inclusion, this amounts to proving:

$$\forall x \quad x \in A \cup B \Rightarrow x \in C$$

Let x be some element of $A \cup B$. We need to show that $x \in C$.

From $x \in A \cup B$, we know that either $x \in A$ or $x \in B$.

- if $x \in A$, we know that $x \in C$ by our earlier assumption that $A \subseteq C$
- if $x \in B$, we know that $x \in C$ by our earlier assumption that $B \subseteq C$

Hence, we can conclude that $x \in C$ as required.

Example – revisited

This example is a ‘semi-formal proof’:

- it is written in a mix of English and mathematics
- it is clearly structured and ‘easy’ to translate to a more formal logical setting;

Unfortunately, it is easy to make mistakes in these proofs – especially if you don’t have years of experience in logic.

On the other hand, you don’t yet have the experience to give the fully formal rules…

Proof strategies

Modelling computing systems presents a series of **proof strategies** – or proof templates – that can be used to write such (semi)formal proofs.

Given a theorem you would like to prove, these strategies give you a means to break the problem into smaller, more manageable proofs.

Given any proof – for example one written by a fellow student – you can check whether it has correctly applied these strategies or not.

It tries to strike a balance between ‘ease of use’ and precision.

Proof strategies

We'll see strategies for the logical operators and quantifiers we have learned about over the past weeks.

Typically, there will be **two proof strategies** for each such logical operator and quantifier:

- a introduction strategy tells you how to *prove a goal* of the form …
- a elimination strategy tells you how to *use an assumption* of the form …

To find a proof, you

- write down all you assumptions and apply elimination strategies.
- write down the conclusion you wish to prove and use introduction strategies.

By repeating these two steps, the proof goals should get simpler – until the proof is finished.

Proof strategies – implication introduction example

In our example proof, we showed that $A \subseteq C \land B \subseteq C \Rightarrow A \cup B \subseteq C$ in the following fashion:

Assume that $A \subseteq C \land B \subseteq C$ holds.

> Using this assumption, we prove that $A \cup B \subseteq C$ holds ...

Therefore we conclude that $A \subseteq C \land B \subseteq C \Rightarrow A \cup B \subseteq C$ as desired.

Let's generalize this to our first proof strategy.

Proof strategies – implication introduction

$\Rightarrow$-*I*

Assume P.

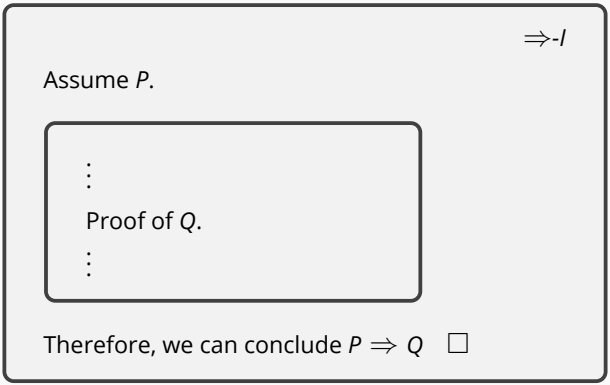
⋮

Proof of Q.

⋮

Therefore, we can conclude $P \Rightarrow Q$ □

Proof strategies – implication introduction



I've added an explicit label, ⇒-*I*, indicating that the *introduction rule* is being used.

The book leaves out such labels – but it can be useful to be explicit about which rule is being applied.

Example: implication introduction

We call a number a **even** if $a = 2 \times k$ for some number k.

Theorem: The product of two even numbers is also even.

Question

Make this statement precise and finish this proof. Be explicit about the proof strategy used.

Example: implication introduction

We call a number a **even** if $a = 2 \times k$ for some number k.

Theorem: The product of two even numbers is also even.

Question

Make this statement precise and finish this proof. Be explicit about the proof strategy used.

Proof

We need to show that if a and b are even, then so is $a \times b$.

Assume a and b are even.

By definition, we know $a = 2 \times n$ and $b = 2 \times m$.

The product of a and b is $(2 \times n) \times (2 \times m)$.

Using simple arithmetic, we can rewrite this as: $2 \times (2 \times n \times m)$.

Therefore the product of a and b can be written in the form $2 \times k$ and is also even.

Example: implication elimination example

As part of the proof done earlier, we showed that if $a \in A$ and $A \subseteq C$, we can conclude that $a \in C$.

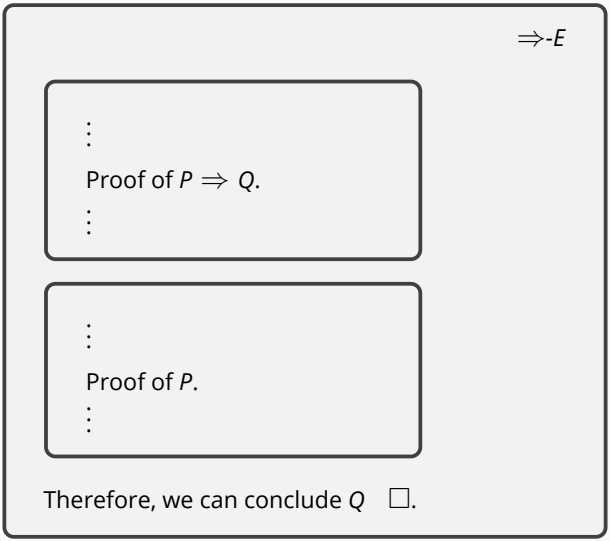
$A \subseteq C$ means that $\forall x \quad x \in A \Rightarrow x \in C$

So in particular, we know that $a \in A \Rightarrow a \in C$.

By assumption we know that $a \in A$.

So we may conclude that $a \in C$.

Proof strategies – implication elimination



Proof strategies

This covers the main proof strategies for implication.

What about:

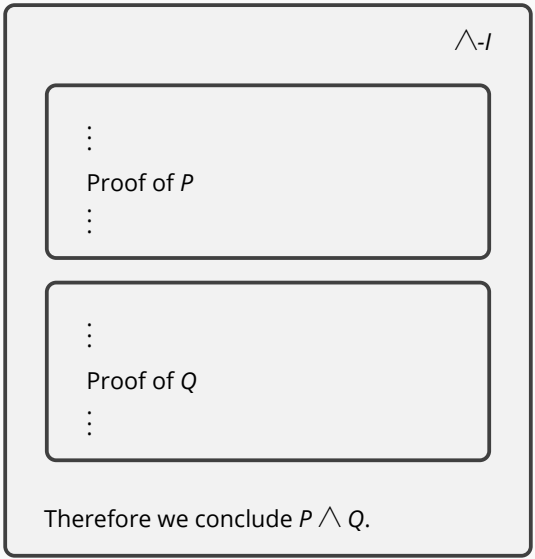
- negation;
- conjunction;
- disjunction;
- logical equivalence;
- universal quantification;
- existential quantification.

We'll look at each of these in turn and illustrate the proof strategies with examples.

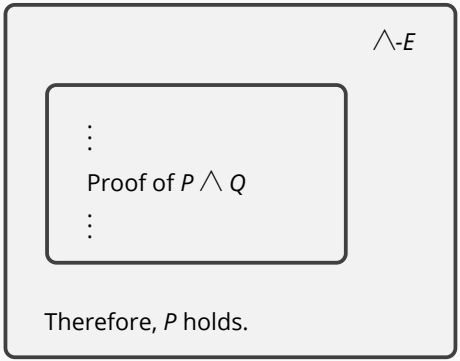
I'll also try to give some examples of common mistakes and pitfalls that you may encounter when applying these strategies.

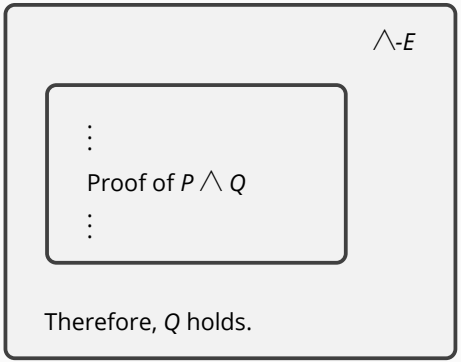
Strategies for logical operators

Proof strategies – conjunction introduction



Proof strategies – conjunction elimination





Example: conjunction elimination and introduction

Theorem: If $x \in A \cap B$, then $x \in B \cap A$.

I'll go through the proof step-by-step, explicitly identifying all the strategies used.

I've chosen to highlight the unfinished parts of the proof to distinguish them from the parts that have been completed.

Example: use implication introduction

Theorem: If $x \in A \cap B$, then $x \in B \cap A$.

$\Rightarrow$-*I*

Assume $x \in A \cap B$

$\vdots$

Proof of $x \in B \cap A$

$\vdots$

Hence $(x \in A \cap B) \Rightarrow (x \in B \cap A)$

Example: use conjunction introduction

$\Rightarrow$-*I*

Assume $x \in A \cap B$

$\bigwedge$-*I*

Proof of $x \in A$

Proof of $x \in B$

Because we have shown $x \in B \bigwedge x \in A$, we conclude $x \in B \cap A$

Hence $(x \in A \cap B) \Rightarrow (x \in B \cap A)$

Example: expand definition of intersection

Assume $x \in A \cap B$. $\Rightarrow$-*I*

By definition of $\cap$, it follows that $x \in A \wedge x \in B$

$\wedge$-*I*

Proof of $x \in A$

Proof of $x \in B$

Because we have shown $x \in B \wedge x \in A$, we conclude $x \in B \cap A$

Hence $(x \in A \cap B) \Rightarrow (x \in B \cap A)$

Assume $x \in A \cap B$. $\Rightarrow$-I

By definition of $\cap$, it follows that $x \in A \bigwedge x \in B$

$\bigwedge$-I

$\bigwedge$-E

From $x \in A \bigwedge x \in B$, we conclude $x \in A$

$\bigwedge$-E

From $x \in A \bigwedge x \in B$, we conclude $x \in B$

Because we have shown $x \in B \bigwedge x \in A$, we conclude $x \in B \cap A$

Hence $(x \in A \cap B) \Rightarrow (x \in B \cap A)$

Example: completing the proof

Theorem: If $x \in A \cap B$, then $x \in B \cap A$.

Proof: Assume $x \in A \cap B$.\ By definition of set intersection, it follows that $x \in A \bigwedge x \in B$

- From $x \in A \bigwedge x \in B$, we conclude $x \in A$
- From $x \in A \bigwedge x \in B$, we conclude $x \in B$

Hence we know that $x \in B \bigwedge x \in A$.

Because we have shown $x \in B \bigwedge x \in A$, we conclude $x \in B \cap A$ using the definition of set intersection.

Hence $(x \in A \cap B) \Rightarrow (x \in B \cap A)$ as required.

Proof strategies – conjunction

The proof strategies for conjunction are fairly ‘obvious’ – we typically use them without thinking twice.

But for other logical operations – such as negation and disjunction – the proof strategies are a bit more involved.

Let’s start considering an example and generalise from there.

Example: negation introduction

Theorem There is no largest natural number.

Proof:

Suppose that there is a largest natural number, N.

We can always construct a number $N + 1$ that is even larger.

This contradicts our assumption that N was the largest number.

Hence we can conclude that no such number exists.

Proof strategies – negation introduction

¬-*I*

Assume P

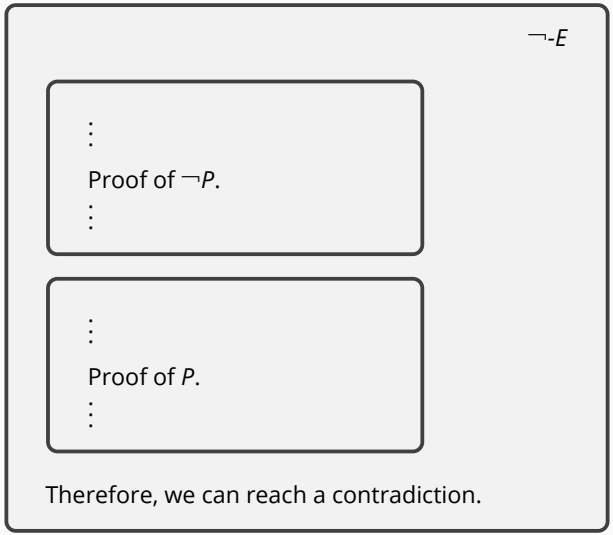
⋮

Proof of a contradiction

⋮

Therefore we conclude $\neg P$.

Proof strategies – negation elimination



Proof strategies – negation elimination

Pro tip: the negation rules have exactly the same structure as the implication rules.

You may want to read $\neg P$ as $P \Rightarrow \bot$

Proof strategies – negation elimination

Pro tip: the negation rules have exactly the same structure as the implication rules.

You may want to read $\neg P$ as $P \Rightarrow \bot$

We do need to say something about the rules for using and proving falsity.

- There is no rule to prove falsity – this would be a bad idea. You can only reach a contradiction by using other proof strategies.
- If you happen to have a false assumption, however, you can conclude whateever you like.

Example: falsity elimination

Theorem For any set *A*, the empty set is always a subset of *A*.

Put simply: $\emptyset \subseteq A$

Example: falsity elimination

Theorem For any set A, the empty set is always a subset of A.

Put simply: $\emptyset \subseteq A$

Proof

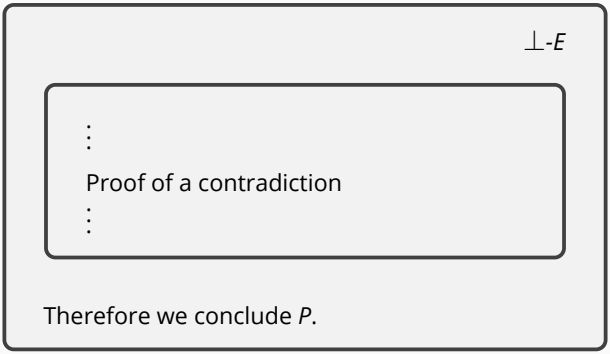
We need to show that $\forall x \quad x \in \emptyset \Rightarrow x \in A$

Assume that $x \in \emptyset$.

We have a contradiction: by definition there is no element x of the empty set.

Hence we can conclude that this (non-existent) x is also an element of A.

Proof strategies – falsity elimination



If we can somehow reach a contradiction from our assumptions, we can draw any conclusion we like – *ex falso sequitur quodlibet*.

Proof strategies – recap

This may seem like an overly complicated way to prove something trivial – and you're right!

But these proof strategies give you a way to decompose your goal and use your assumptions – regardless of the proof itself.

Much harder theorems follow exactly the same pattern.

These proof strategies give you a foothold on how to tackle these theorems.

Exercise

Question

Prove that if $A \cap C \subseteq B$ and $a \in C$, then $a \notin A/B$.

Proof strategies – logical equivalence

Recall that $p \Leftrightarrow q$ is the same as $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

The corresponding proof strategies should not come as a surprise – they are a simple instance of the rules for conjunction.

Proof strategies – equivalence elimination

$\Leftrightarrow$-*I*

⋮

Proof of $P \Rightarrow Q$

⋮

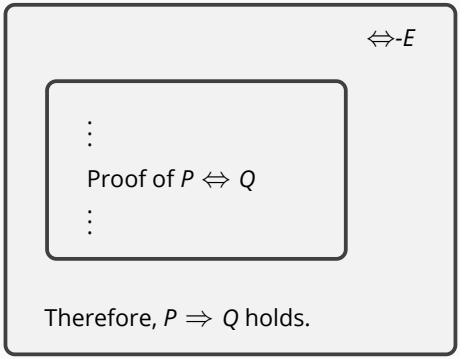
⋮

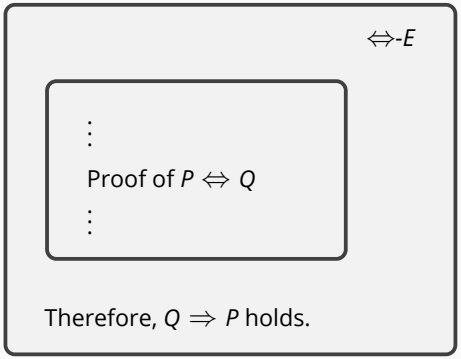
Proof of $Q \Rightarrow P$

⋮

Therefore we conclude $P \Leftrightarrow Q$.

Proof strategies – equivalence introduction



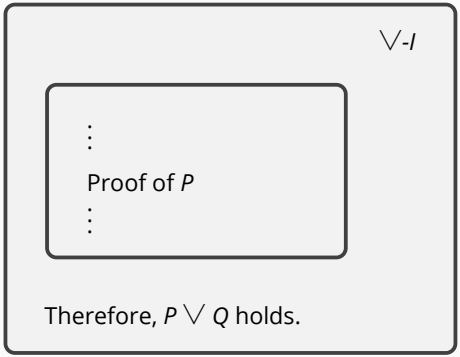


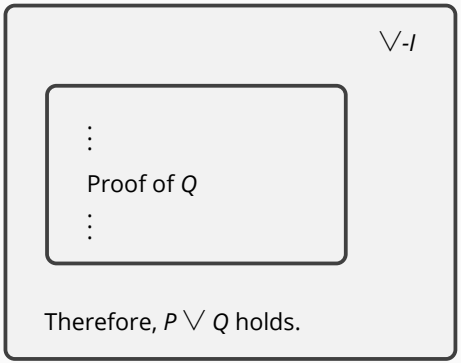
Proof strategies – disjunction

By now, the pattern should hopefully be familiar.

Disjunction and quantifiers, however, raise some new and subtle issues.

Proof strategies – disjunction introduction





By themselves, these rules are not very surprising (and do not to appear to be particularly useful).

Proof strategies – disjunction elimination

The rule for **disjunction elimination** is more complex.

Suppose we know that $P \vee Q$ holds – what can we conclude?

- We don't know for sure that P holds;
- We don't know for sure that Q holds;
- Concluding $P \vee Q$ doesn't tell us anything new…

Proof strategies – disjunction elimination

The rule for **disjunction elimination** is more complex.

Suppose we know that $P \vee Q$ holds – what can we conclude?

- We don't know for sure that P holds;
- We don't know for sure that Q holds;
- Concluding $P \vee Q$ doesn't tell us anything new...

The solution is to show that for some proposition R:

- if P holds, then R holds;
- and if Q holds, then R holds.

From these two proofs, we can conclude that whenever $P \vee Q$ holds, R must also hold.

Example: disjunction elimination

Theorem: Every square number has a remainder of 0 or 1 after division by 4.

Example: disjunction elimination

Theorem: Every square number has a remainder of 0 or 1 after division by 4.

Proof: Assume n is a natural number.

- If n is even, we know that $n = 2k$.

  Hence $n^2 = (2k)^2 = 4k^2$, which clearly is divisible by 4.

- If n is odd, we know that $n = 2k + 1$.

  Hence $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.

  $4(k^2 + k) + 1$ has a remainder of 1 after division by 4.

Therefore all squares have a remainder of 0 or 1 after division.

Proof strategies – disjunction elimination

$\vee$-*E*

Proof of $P \vee Q$

Assume that *P* is true.

… Proof of *R* …

Assume that *Q* is true.

…Proof of *R*…

Therefore, *R* is true, regardless of which of *P* or *Q* is true.

Proof strategies – recap

We have now seen proof strategies for all the operators from propositional logic.

Some of these strategies are obvious (like those for conjunction);

Others are easier to get wrong (like those for disjunction, negation, or implication).

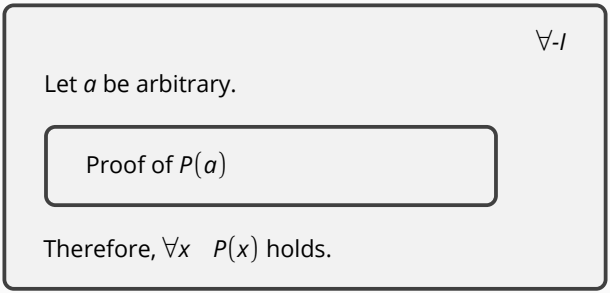
Practice writing proofs yourself using these strategies!

Go through the example proofs in the book and identify which strategy is used in every step.

Now we turn our attention to **quantifiers**.

Proof strategies for quantifiers

Proof strategies – universal quantification introduction

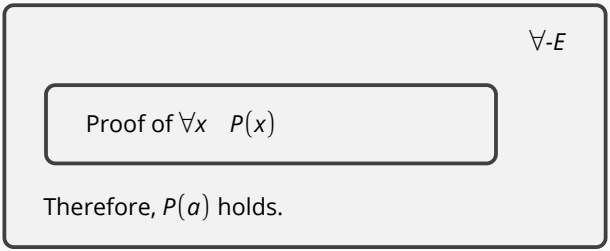


Intuitively

To prove $\forall x \quad P(x)$, we establish that $P(a)$ holds for *any* a.

Hence $P(x)$ must hold for **every** x.

Proof strategies – universal quantification elimination



Intuitively

If we know $\forall x \quad P(x)$ holds, we can conclude that $P(a)$ for whatever a we want.

Proof strategies – universal quantification

Both strategies seem reasonable.

The book argues that they generalise the strategies for conjunction.

We have already used them implicitly in previous proofs…

Subsets

Theorem

Let A, B, and C some arbitrary set. Then $A \subseteq C \land B \subseteq C \Rightarrow A \cup B \subseteq C$

Exercise

Question

Prove that for all sets A and B, if $A \cap B = A$ then $A \subseteq B$.

Where did you need to apply the strategies for the universal quantifier?

Proof strategies – existential quantification introduction

$\exists$-*I*

We choose a to be some value.

Proof of $P(a)$

Therefore, $\exists x \quad P(x)$ holds.

Example: existential quantification introduction

Lemma The function $f(x) = x^2 - 2x + 1$ intersects the x-axis.

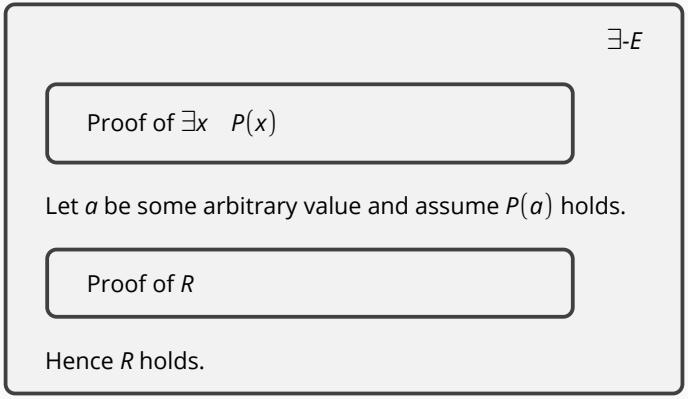
Example: existential quantification introduction

Lemma The function $f(x) = x^2 - 2x + 1$ intersects the x-axis.

Proof We need to show that $\exists a \quad f(a) = 0$

If we choose $a = 1$, we have $f(1) = 1 - 2 + 1 = 0$ as required.

Proof strategies – existential quantification elimination



Like we saw for the universal quantifier, these strategies generalise the strategy for disjunction.

A wrong proof

Proof of $\exists x \quad P(x)$

Let a be some arbitrary value and assume $P(a)$ holds.

Proof of R

Hence R holds.

Question

Use the proof strategies to try to give a proof that

$$(\exists x \quad P(x)) \Rightarrow (\forall x \quad P(x))$$

What is wrong with the proof?

Derived proof strategies

Derived proof strategies: contraposition

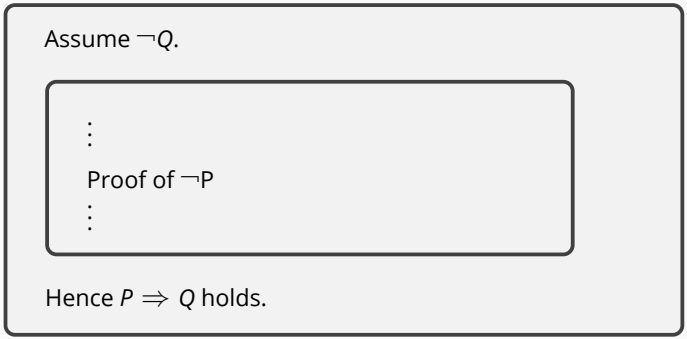
We have already seen a few examples of *derived* proof strategies, that capture some recurring pattern of usage of the more primitive strategies.

For example, there is the special case of the disjunction elimination rule where the disjunction being eliminated is of the form $P \bigvee \neg P$.

Another example is a so-called *proof by contraposition* that relies on $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$.

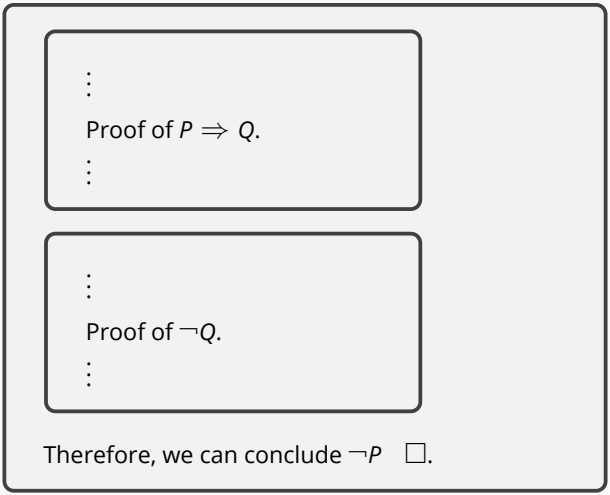
Instead of assuming P and deriving Q, we can also assume $\neg Q$ and derive $\neg P$ to conclude that $P \Rightarrow Q$.

Contraposition



A similar proof strategy exists for *implication elimination* that is sometimes called *modus tollens*.

Modus tollens



A wrong proof

Theorem: All numbers are equal to 0.

Proof:

Let n be a natural number.

If $n = 0$, then are goal holds.

If $n \neq 0$ – this contradicts our assumption that $n = 0$.

Hence, $n = 0$.

Question

What is wrong with this proof?

Other proof steps

These proof strategies give you the basic steps to help you break down a problem into smaller parts.

But there are many other steps in a proof that are not covered by these strategies:

- Unfolding definitions, for example replacing $A \subseteq B$ with $\forall x \quad x \in A \Rightarrow x \in B$
- Folding back definitions, for example replacing $\forall x \quad x \in A \Rightarrow x \in B$ with $A \subseteq B$.
- Arithmetic calculations.
- Algebraic properties, such as $a + b = b + a$.
- Choosing the right witness when trying to prove a property starting with an existential quantifier.
- Choosing the right property R when eliminating a disjunction;
- Any creative steps that require insight somehow.
- ...

Proof strategies: semi-formal

These proof strategies are a vehicle to teach proofs.

They give you enough of a formal framework to understand how to write proofs, identify which steps are allowed and which are not.

But they do not nail down exactly what constitutes a proof and what doesn't.

And they are not formal enough that they can be automatically checked by a computer, for instance.

Proof strategies: semi-formal

These proof strategies are a vehicle to teach proofs.

They give you enough of a formal framework to understand how to write proofs, identify which steps are allowed and which are not.

But they do not nail down exactly what constitutes a proof and what doesn't.

And they are not formal enough that they can be automatically checked by a computer, for instance.

But that's a story for another lecture...

Material

- Modelling Computing Systems Chapter 5
- Separate worksheet with exercises