Logic and Proofs

Sections 1.6, 1.7

Rules of Inference

Section 1.6

Video 10: Valid Arguments

- Arguments
- Argument Forms
- Inference Rules
- Valid Arguments

Example

Assume the following rule holds

“If I have passed AICC, I can advance to year 2 of the studies”

And assume that you know

“I have passed AICC”

Then you would conclude

“I can advance to year 2 of the studies”

This is a **valid argument**

Example

Assume the following rule holds

“If I have passed AICC, I can advance to year 2 of the studies”

And assume that you know

p := “I have passed AICC”

Then you would conclude

q : = “I can advance to year 2 of the studies”

Example

Assume the following rule holds

$p \rightarrow q$

And assume that you know

p

Then you would conclude

q

This is a **valid argument form**

- It is true for any *p* and *q*

It is written as

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

It is called **Modus Ponens**

Why is the Argument Form Valid?

We know that $(p \land (p \rightarrow q)) \rightarrow q$ is a tautology

So if we know that p and $p \rightarrow q$ are True, then the premise $(p \land (p \rightarrow q))$ is True, and therefore also q is True

This holds for any tautology of the form $(p_1 \land p_2 \land \ldots \land p_n) \rightarrow q$

Note: if at least one of the premises is not True, we **cannot conclude** that the conclusion is True

Arguments in Propositional Logic

- A **argument** in propositional logic is a sequence of propositions.
  - All but the final proposition are called **premises**.
  - The last statement is the **conclusion**.
  - The argument is valid if the premises imply the conclusion.

- An **argument form** is an argument that is valid no matter what propositions are substituted into its propositional variables

- **Inference rules** are simple argument forms that will be used to construct more complex argument forms

What is this good for?

Assume the following rule holds

> "If I have passed AICC and if I have passed Analysis 1 and if I have passed Linear Algebra and …. (list all your courses here), I can advance to year 2 of the studies"

And assume that you know

> p_1 := "I have passed AICC"
>
> p_2 := "I have passed Analysis 1"
>
> p_3 := "I have passed Linear Algebra"
>
> …
>
> (and all other courses here)

Then you would conclude

> q : = "I can advance to year 2 of the studies"

Using a Truth Table

Now build the truth table for $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$

to show that the argument holds

where n = 20 is the number of courses

The table will have 2^{20} = 1’048’576 rows, which is not very practical

Using Inference Rules

We have another inference rule: **Conjunction** Inference Rule
($p \land q \rightarrow p \land q$ is a tautology)

$$\begin{array}{l} p \\ q \\ \hline \therefore p \land q \end{array}$$

Now we can provide the argument in a much simpler way!

Building the Argument

Write down what we know (the premises)

p_1

p_2

…

p_n

$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$

Building the Argument

Apply the Conjunction Inference Rule to the first two premises

$\boldsymbol{p_1}$

$\boldsymbol{p_2}$

…

p_n

$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$

$\boldsymbol{p_1 \wedge p_2}$

Building the Argument

Apply the Conjunction Inference Rule to the new and the third premise

p_1

p_2

…

p_n

$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$

$p_1 \wedge p_2$

$\boldsymbol{p_1 \wedge p_2 \wedge p_3}$

Building the Argument

Repeat for all other p_i

p_1
p_2
…
$\boldsymbol{p_n}$

$(p_1 \land p_2 \land \ldots \land p_n) \rightarrow q$

$p_1 \land p_2$

…

$\boldsymbol{(p_1 \land p_2 \land \ldots \land p_n)}$

Building the Argument

Apply Modus Ponens and obtain the conclusion

p_1

p_2

…

p_n

$\boldsymbol{(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q}$

$p_1 \wedge p_2$

…

$\boldsymbol{(p_1 \wedge p_2 \wedge \ldots \wedge p_n)}$

$\boldsymbol{\therefore q}$

Using the Inference Rules to Build Valid Arguments

- A **valid argument** is a sequence of statements.
  - Each statement is either a premise or follows from previous statements by inference rules.
  - The last statement is called conclusion.
- A valid argument takes the following form:

$$\begin{array}{rl} & \text{Step}_1 \\ & \text{Step}_2 \\ & \quad\quad . \\ & \quad\quad . \\ & \quad\quad . \\ & \text{Step}_n \\ \hline \therefore & \text{Conclusion} \end{array}$$

Summary

- Arguments
- Argument Forms
- Inference Rules
- Valid Arguments

Video 11: Inference Rules in Propositional Logic

- Important inference rules
- Examples
- Fallacies

Inference Rules

1. Propositional Logic: Inference Rules
2. Predicate Logic: Inference rules for propositional logic plus additional inference rules to handle variables and quantifiers

Conjunction and Modus Ponens

$$\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$$

Corresponding Tautology:
$(p \wedge q) \rightarrow (p \wedge q)$

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

Corresponding Tautology:
$(p \wedge (p \rightarrow q)) \rightarrow q$

Inference Rule: Modus Tollens

$$\begin{array}{l} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

Corresponding Tautology:

(¬q $\wedge$ (p →q)) → ¬p

Example:
p := “I have passed AICC”
q := “I can advance to year 2 of the studies”

Premises
“If I have passed AICC, I can advance to year 2 of the studies”
“I cannot advance to year 2 of the studies.”

Conclusion
“I did not pass AICC.”

Hypothetical Syllogism

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$

Corresponding Tautology:

$((p \to q) \wedge (q \to r)) \to (p \to r)$

Example:
r := "I can take Analysis 4"

Premises
"If I have passed AICC, I can advance to year 2 of the studies"
"If I can advance to year 2 of the studies, I can take Analysis 4"

Conclusion
"If I have passed AICC, I can take Analysis 4"

Resolution

$$\begin{array}{l} \neg p \lor r \\ p \lor q \\ \hline \therefore q \lor r \end{array}$$

Corresponding Tautology:

$((\neg p \lor r) \land (p \lor q)) \rightarrow (q \lor r)$

Example:
p := “The weather is nice
q := “I am at home”
r := “I am at the beach”

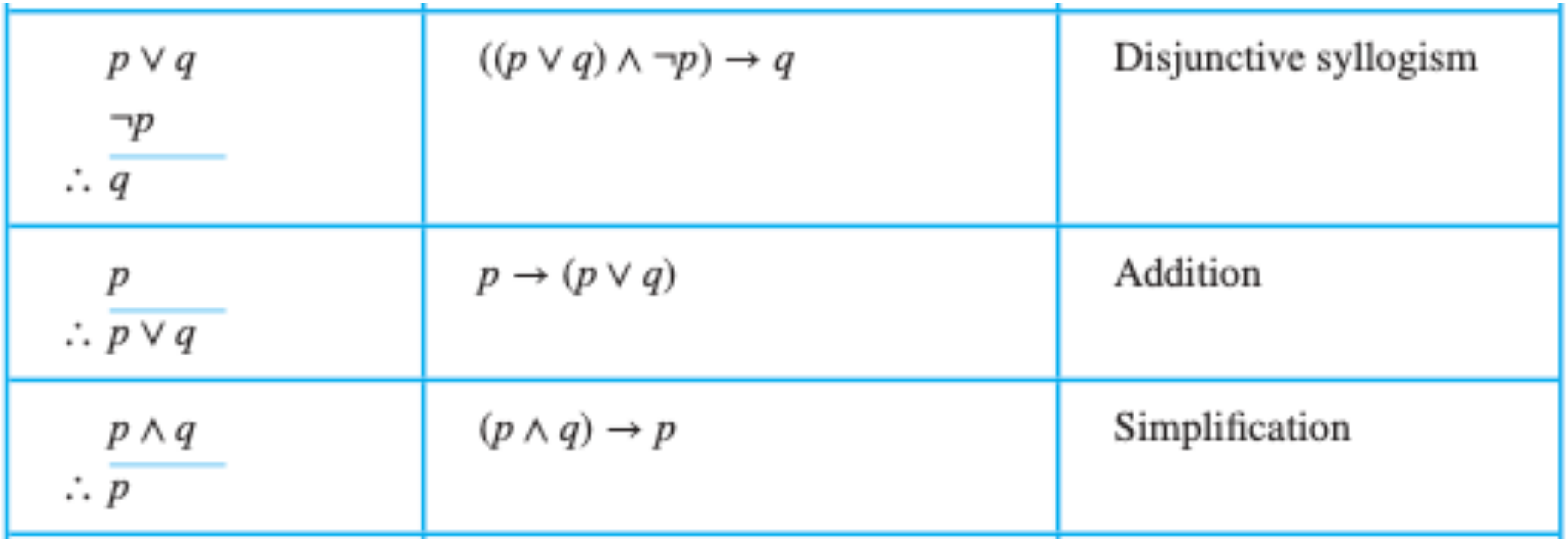
Premises:
“The weather is bad or I am at the beach”
“The weather is nice or I am at home”

Conclusion:
“I am at home or at the beach”

Resolution plays an important role in automated theorem proofing and AI

It allows to eliminate propositional variables from the premises

Other Inference Rules



$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism
p $\therefore p \vee q$	$p \rightarrow (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \rightarrow p$	Simplification

Simpler form of resolution

Dual to Conjunction

Simpler form of Modus Ponens

Valid Arguments

Attention: even seemingly “obvious” conclusions imply an argument

Example: From *p* $\wedge$ *(p →q)* conclude *q*

Argument:

Step	**Reason**
1. $p \wedge (p \rightarrow q)$	Premise
2. p	Simplification using (1)
3. $p \rightarrow q$	Simplification using (1)
4. q	Modus Ponens using (2) and (3)

Example

With these hypotheses:

“It is not sunny this afternoon and it is colder than yesterday.”

“We will go swimming only if it is sunny.”

“If we do not go swimming, then we will take a canoe trip.”

“If we take a canoe trip, then we will be home by sunset.”

Using the inference rules, construct a valid argument for the conclusion:

“We will be home by sunset.”

Example

1. Choose propositional variables:

p := “It is sunny this afternoon.”
r := “We will go swimming.”
t := “We will be home by sunset.”
q := “It is colder than yesterday.”
s := “We will take a canoe trip.”

2. Translate into propositional logic:

$$\text{Hypotheses: } \neg p \wedge q,\ r \to p,\ \neg r \to s,\ s \to t$$
$$\text{Conclusion: } t$$

Example

3. Construct the Valid Argument

Step	**Reason**
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens using (6) and (7)

Fallacies!

$((p \to q) \land q) \to p$ *is not a tautology*

- **fallacy of affirming the conclusion**

Example:

- If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics.
- Therefore, you did every problem in this book?

Fallacies!

- $((p \to q) \land \neg p) \to \neg q$ is not a tautology
    - **fallacy of denying the hypothesis**

Example:

- If you do every problem in this book, then you will learn discrete mathematics. You did not do every problem in this book.
- Therefore, you did not learn discrete mathematics?

Summary

- Modus Ponens, Modus Tollens
- Hypothetical Syllogism
- Resolution
- How to build valid arguments
- Fallacies
  - affirming the conclusion
  - denying the hypothesis

Video 12: Arguments in Predicate Logic

- Inference Rules for Quantifiers
- Building valid arguments

Handling Quantified Statements

- Valid arguments for quantified statements are a sequence of statements.
- Each statement is either a premise or follows from previous statements by rules of inference which include:
  - Rules of Inference for Propositional Logic
  - Rules of Inference for Quantified Statements

Universal Instantiation (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Example: The domain consists of all Men and Socrates is a Man

Premise:
“All men are mortal.”

Conclusion:
“Therefore, Socrates is mortal.”

Solution for Socrates Example

If we choose a more general domain, e.g. all beings, including gods and spirits, we need a more elaborate proof to build a valid argument

- Both rules for propositional logic and quantifiers

Step	**Reason**
1. $\forall x(Man(x) \rightarrow Mortal(x))$	Premise
2. $Man(Socrates) \rightarrow Mortal(Socrates)$	UI from (1)
3. $Man(Socrates)$	Premise
4. $Mortal(Socrates)$	MP from (2) and (3)

Universal Generalization (UG)

$$\begin{array}{l} P(c) \text{ for an arbitrary } c \\ \hline \therefore \forall x P(x) \end{array}$$

Used often implicitly in Mathematical Proofs.

Attention: you must not make any assumptions about c

Existential Instantiation (EI)

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

Example:

“There is someone who knows Java in the class.”
“Let’s call her *a* and say that *a* knows Java”

Existential Generalization (EG)

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

Example:

“Michelle knows Java in the class.”
“Therefore, someone knows Java in the class.”

Example

Use the rules of inference to construct a valid argument showing that the conclusion

“Someone who passed the first exam has not read the book.”

follows from the premises

“A student in this class has not read the book.”

“Everyone in this class passed the first exam.”

Example

Let

C(*x*) := “*x* is in this class”

B(*x*) := “ *x* has read the book”

P(*x*) := “*x* passed the first exam”

Translate the premises and conclusion into predicate logic

$$\begin{array}{l} \exists x(C(x) \land \neg B(x)) \\ \forall x(C(x) \to P(x)) \\ \hline \therefore\ \exists x(P(x) \land \neg B(x)) \end{array}$$

Example

Construct the valid argument

Step	**Reason**
1. $\exists x(C(x) \land \neg B(x))$	Premise
2. $C(a) \land \neg B(a)$	EI from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \to P(x))$	Premise
5. $C(a) \to P(a)$	UI from (4)
6. $P(a)$	MP from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \land \neg B(a)$	Conj from (6) and (7)
9. $\exists x(P(x) \land \neg B(x))$	EG from (8)

Universal Modus Ponens

$$\begin{array}{l} \forall x(P(x) \rightarrow Q(x)) \\ P(a), \text{where } a \text{ is a particular} \\ \quad\text{element in the domain} \\ \hline \therefore Q(a) \end{array}$$

Universal Modus Ponens combines universal instantiation and modus ponens into one rule.

This rule could be used in the Socrates example.

Summary

- Inference Rules for Quantifiers
    - Universal Instantiation
    - Universal Generalization
    - Existential Instantiation
    - Existential Generalization
    - Universal Modus Ponens

Introduction to Proofs

Section 1.7, 1.8.2, 1.8.6

Video 13: Introduction to Proofs

- Theorems
- Mathematical Proofs
- Types of Proofs

Proofs of Mathematical Statements

- An **axiom** is a statement which is given as true

- A **theorem** is a statement that can be shown to be true using
  - definitions
  - axioms
  - other theorems
  - rules of inference

- A **mathematical proof** is a **valid argument** that establishes the truth of a statement
  - in particular of a theorem

Informal Proofs

- In mathematics, computer science, and other disciplines, **informal proofs**, which are generally shorter, are often used
  - More than one rule of inference is used in a step
  - Steps may be skipped
  - The rules of inference used are not explicitly stated
  - Easier for to understand and to explain to people
  - **But it is also easier to introduce errors**

Applications of Proofs

- Apart from being at the core of mathematics, proofs have many practical applications as well
  - verification that computer programs are correct
  - establishing that operating systems are secure
  - enabling programs to make inferences in artificial intelligence
  - showing that system specifications are consistent

Terminology

- A **lemma** is a ‘helping theorem’ or a result which is needed to prove a theorem
- A **corollary** is a result which follows directly from a theorem
- Less important theorems are sometimes called **propositions**

- A **conjecture** is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.
  - Example: Fermat’s theorem has been a conjecture from 1634 - 1995

Forms of Theorems

Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or discrete structures

$$\forall x(P(x) \rightarrow Q(x))$$

Formulation of Theorems

Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

“If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ ”

really means

“For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$.”

Proving Theorems

To prove theorems of the form $\forall x(P(x) \rightarrow Q(x))$

we show that $P(c) \rightarrow Q(c)$

where *c* is an arbitrary element of the domain.

- By universal generalization the truth of the original formula follows.

- So, we must prove a statement of the form: $p \rightarrow q$

Proving Conditional Statements: *p* → *q*

Trivial Proof: If we know *q* is true, then *p* → *q* is true as well.

“If it is raining then 1 = 1.”

Vacuous Proof: If we know *p* is false then *p* → *q* is true as well.

“If I am both rich and poor then 2 + 2 = 5.”

Direct Proofs for $p \to q$

- **Direct Proof:** assume that *p* is true; then use definitions, axioms and theorems together with rules of inference till the statement *q* results

Indirect Proofs for $p \rightarrow q$

Proof by Contraposition: assume that ¬*q* is True; then use definitions, axiom and theorems together with rules of inference till the statement ¬*p* results

Since p → q ≡ ¬q → ¬p the statement is proven

This is one type of an **indirect proof**

Indirect Proofs for $p \rightarrow q$

Proof by Contradiction: assume that *p* and ¬*q* are true; then perform a direct proof to construct a contradiction, i.e., prove the statement ***F***

Since $p \rightarrow q \equiv (p \wedge \neg q) \rightarrow$ ***F*** the statement is proven.

AKA reductio ad absurdum, another type of indirect proof

Summary

- Axiom, Theorem, Proof
- Corollary, Lemma, Proposition, Conjecture
- Trivial and Vacuous Proof
- Direct Proof
- Indirect Proof: by contraposition and by contradiction

Video 14: Proof Examples

- Examples for direct and indirect proofs
- Other proof methods
- Mistakes in proofs

Theorem on Even and Odd Integers

Definition: The integer n is **even** if there exists an integer k such that $n = 2k$, and n is **odd** if there exists an integer k, such that $n = 2k + 1$.

Theorem: If n is an odd integer, then n^2 is odd.

Example: n = 3 is odd, then $3^2 = 9$ is odd.

Note: every integer is either even or odd and no integer is both even and odd. Strictly speaking, this requires a proof.

Direct Proof

Proof:

Assume that n is odd.

Then $n = 2k + 1$ for an integer k, according to the definition.

Squaring both sides of the equation, we get:

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

Setting $r = 2k^2 + 2k$, an integer, we obtain

$$n^2 = 2r + 1,$$

Thus, n^2 is an odd integer, according to the definition.

◀

(◀ marks the end of the proof. Sometimes **QED** is used instead.)

Theorem on Sum of Rational Numbers

Definition: The real number *r* is **rational** if there exist integers *p* and *q* where $q \neq 0$ such that $r = p/q$

Theorem: The sum of two rational numbers is rational.

Direct Proof

Proof*:*

Assume *r* and *s* are two rational numbers.

Then there must be integers *p, q, t, u* such that

$$r = \frac{p}{q}, s = \frac{t}{u}, q \neq 0, u \neq 0$$

Computing the sum, we obtain

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu+qt}{qu}$$

Setting $v = pu + qt$ and $w = qu \neq 0$, we have

$$r + s = \frac{v}{w}, \mathrm{w} \neq 0$$

Therefore, by definition, $r + s$ is a rational number.

◀

Proof by Contraposition

Theorem: If n is an integer and $3n + 2$ is odd, then n is odd.

Proof: Assume n is even. So, $n = 2k$ for some integer k.

Thus

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j \text{ for } j = 3k + 1$$

Therefore $3n + 2$ is even.

Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well. ◀

Proof by Contraposition

Theorem: For an integer n, if n^2 is odd, then n is odd.

Proof: Assume n is even.

Therefore, there exists an integer k such that $n = 2k$. Hence,

$$n^2 = 4k^2 = 2\,(2k^2)$$

and n^2 is even.

We have shown that if n is an even integer, then n^2 is even.

Therefore, by contraposition, for an integer n, if n^2 is odd, then n is odd.

◀

Proof by Contradiction

Theorem: If more than N items are distributed in any manner over N bins, there must be a bin containing at least two items (pigeonhole principle).

Proof:

Assume that each bin contains at most a single item ($\neg q$),

and that there are more than N items (p).

However, as we have only N bins and each bin contains at most one item, there are at most N items ($\neg p$).

This contradicts the assumption that there are more than N items (p).

◄

Contraposition vs. Contradiction

- The previous proof can also be interpreted as proof by contraposition.
- Assuming ¬q is true we made a direct proof of ¬p, and thus proved ¬q → ¬p
- More generally, any proof by contraposition can be tansformed in a proof by contradiction, but not vice versa:
  - If you assume that p and ¬q are true and you have a direct proof for ¬q → ¬p then you have shown that (p ∧ ¬q) → (p ∧ ¬p) ≡ **F**
- General proofs by contradiction use some other statement r that produces the contradiction, i.e., we prove (p ∧ ¬q) → (r ∧ ¬r)

Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational

Proof: Suppose $\sqrt{2}$ is rational. Then there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors. Then

$$2 = \frac{a^2}{b^2} \qquad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then a must be even (a theorem). Since a is even, $a = 2c$ for some integer c. Thus,

$$2b^2 = 4c^2$$

Therefore b^2 is even. Again then b must be even as well.

$$b^2 = 2c^2$$

But then 2 must divide both a and b. This contradicts our assumption that a and b have no common factors. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational .

Note: Statement r is that ”a and b have no common factors” ◀

Proofs for Biconditional Statements

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Theorem: If n is an integer, then n is odd if and only if n^2 is odd.

Proof:

We have already shown that both $p \rightarrow q$ and $q \rightarrow p$.

Therefore we can conclude $p \leftrightarrow q$.

Proof by Cases

To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

use the tautology

$$\begin{aligned}&[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow \\ &\qquad [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]\end{aligned}$$

Each of the implications $p_i \rightarrow q$ is a **case**.

Proof by Cases

Theorem: if *n* is an integer, then $n^2 \geq n$.

Proof*: C*onsider three cases: $n = 0$, $n \geq 1$, $n \leq -1$

Case (i): $n = 0$

Since $0^2 = 0$, we have $0^2 \geq 0$.
It follows that $n^2 \geq n$ in this case.

Case (ii): $n \geq 1$

We multiply both sides of the inequality $n \geq 1$ by the positive integer n, and obtain $n \cdot n \geq n \cdot 1$.
It follows that $n^2 \geq n$ in this case

Case (iii): $n \leq -1$
Since $n^2 \geq 0$, it follows that $n^2 \geq n$ in this case

Proof by Counterexample

To establish that $\neg\forall x P(x)$ is true (or $\forall x P(x)$ is false) find a *c* such that $\neg$*P*(*c*) is true or *P*(*c*) is false.

Reminder: $\exists x \neg P(x) \equiv \neg\forall x P(x)$

In this case *c* is called a **counterexample** to the assertion $\forall x P(x)$.

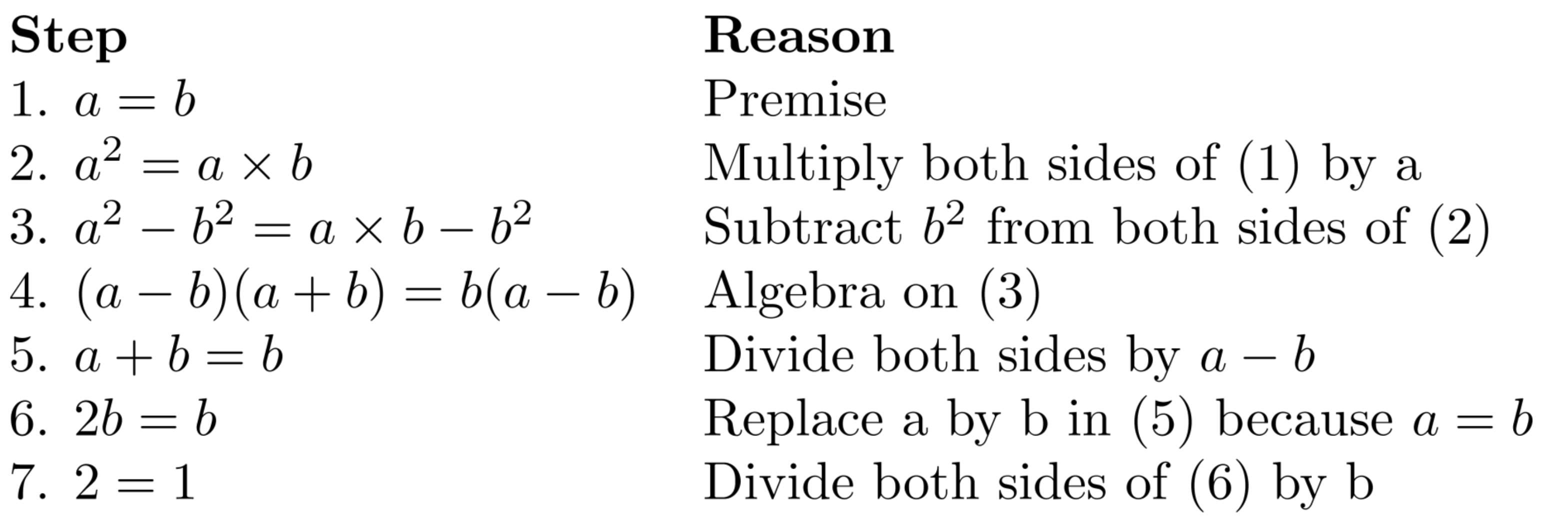
Example:

Show that the statement “Every positive integer is the sum of the squares of 2 integers.” is False.

The integer 3 is a counterexample. Why?

Mistakes in Proofs

“Proof” that *1 = 2*

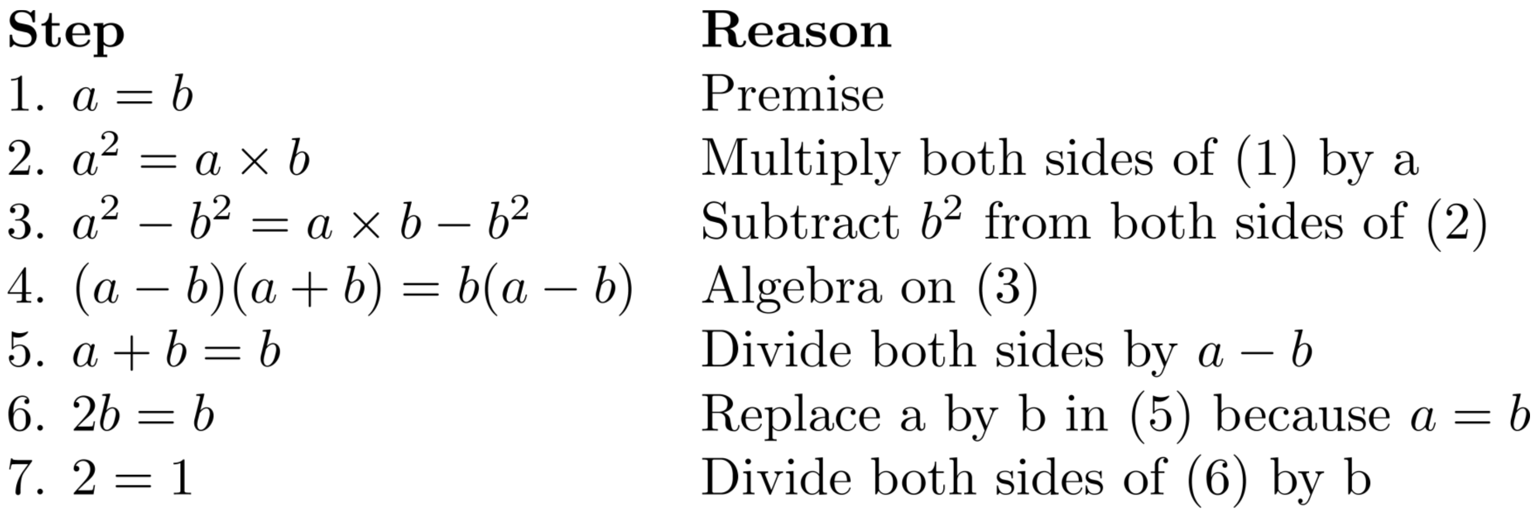


Step	**Reason**
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

Answer: Step 5. a - b = 0 by the premise and division by 0 is undefined.

Mistakes in Proofs

“Proof” that 2 = 1



Step	Reason
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

What went wrong?

Step 5: a - b = 0 by the premise and division by 0 is undefined.

Summary

- Examples of direct and indirect proofs
- Proofs for Biconditional Statements
- Proof by Cases
- Counterexamples
- Mistakes in Proofs