Inference Rules and Proof Methods

Lucia Moura

Winter 2010

Rules of Inference and Formal Proofs

Proofs in mathematics are valid arguments that establish the truth of mathematical statements.

- An **argument** is a sequence of statements that end with a conclusion.
- The argument is **valid** if the conclusion (final statement) follows from the truth of the preceding statements (**premises**).

Rules of inference are templates for building valid arguments.

We will study rules of inferences for compound propositions, for quantified statements, and then see how to combine them.

These will be the main ingredients needed in **formal proofs**.

Proof methods and Informal Proofs

After studying how to write **formal proofs** using rules of inference for predicate logic and quantified statements, we will move to **informal proofs**.

Proving useful theorems using **formal proofs** would result in long and tedious proofs, where every single logical step must be provided.

Proofs used for human consumption (rather than for automated derivations by the computer) are usually **informal proofs**, where steps are combined or skipped, axioms or rules of inference are not explicitly provided.

The second part of these slides will cover methods for writing informal proofs.

Valid Arguments using Propositional Logic

Consider the following argument (sequence of propositions):

- If the prof offers chocolate for an answer, you answer the prof's question.
- The prof offers chocolate for an answer.
- Therefore, you answer the prof's question.

Let p be "the prof offers chocolate for an answer"
and q be "you answer the prof's question".

The *form* of the above argument is:

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

The argument is valid since $((p \rightarrow q) \wedge p) \rightarrow q$ is a tautology.

Arguments, argument forms and their validity

Definition

An *argument* in propositional logic is sequence of propositions. All but the final proposition are called *premises* and the final proposition is called the *conclusion*. An argument is *valid* if the truth of all its premises implies that the conclusion is true.
An *argument form* in propositional logic is a sequence of compound propositions involving propositional variables. An argument form is *valid* if no matter which propositions are substituted for the propositional variables in its premises, if the premises are all true, then the conclusion is true.

In other words, an argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion q is valid if and only if

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

is a tautology.

Rules of Inference for Propositional Logic I

inference rule	tautology	name
p $p \to q$ $\therefore\ q$	$(p \land (p \to q)) \to q$	Modus ponens (mode that affirms)
$\neg q$ $p \to q$ $\therefore\ \neg p$	$(\neg q \land (p \to q)) \to \neg p$	Modus tollens (mode that denies)
$p \to q$ $q \to r$ $\therefore\ p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	hypothetical syllogism
$p \lor q$ $\neg p$ $\therefore\ q$	$((p \lor q) \land (\neg p)) \to q$	disjunctive syllogism

Rules of Inference for Propositional Logic II

$\begin{array}{rl} & p \\ \hline \therefore & p \vee q \end{array}$	$p \rightarrow (p \vee q)$	addition
$\begin{array}{rl} & p \wedge q \\ \hline \therefore & p \end{array}$	$(p \wedge q) \rightarrow p$	simplification
$\begin{array}{rl} & p \\ & q \\ \hline \therefore & p \wedge q \end{array}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	conjunction
$\begin{array}{rl} & p \vee q \\ & \neg p \vee r \\ \hline \therefore & q \vee r \end{array}$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	resolution

Which rule of inference is used in each argument below?

- Alice is a Math major. Therefore, Alice is either a Math major or a CSI major.
- Jerry is a Math major and a CSI major. Therefore, Jerry is a Math major.
- If it is rainy, then the pool will be closed. It is rainy. Therefore, the pool is closed.
- If it snows today, the university will close. The university is not closed today. Therefore, it did not snow today.
- If I go swimming, then I will stay in the sun too long. If I stay in the sun too long, then I will sunburn. Therefore, if I go swimming, then I will sunburn.
- I go swimming or eat an ice cream. I did not go swimming. Therefore, I eat an ice cream.

Determine whether the argument is valid and whether the conclusion must be true

- If $\sqrt{2} > \frac{3}{2}$ then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$. Therefore, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$.

Determine whether the argument is valid and whether the conclusion must be true

- If $\sqrt{2} > \frac{3}{2}$ then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$. Therefore, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$.
- Is the argument valid?

Determine whether the argument is valid and whether the conclusion must be true

- If $\sqrt{2} > \frac{3}{2}$ then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$. Therefore, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$.
- Is the argument valid?
- Does the conclusion must be true?

Determine whether the argument is valid and whether the conclusion must be true

- If $\sqrt{2} > \frac{3}{2}$ then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$. Therefore, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$.
- Is the argument valid?
- Does the conclusion must be true?
- What is wrong?

Determine whether the argument is valid and whether the conclusion must be true

- If $\sqrt{2} > \frac{3}{2}$ then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$. Therefore, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$.
- Is the argument valid?
- Does the conclusion must be true?
- What is wrong?
- The argument is valid: modus ponens inference rule.

Determine whether the argument is valid and whether the conclusion must be true

- If $\sqrt{2} > \frac{3}{2}$ then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$. Therefore, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$.
- Is the argument valid?
- Does the conclusion must be true?
- What is wrong?
- The argument is valid: modus ponens inference rule.
- We cannot conclude that the conclusion is true, since one of its premises, $\sqrt{2} > \frac{3}{2}$, is false.

Determine whether the argument is valid and whether the conclusion must be true

- If $\sqrt{2} > \frac{3}{2}$ then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$. Therefore, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$.
- Is the argument valid?
- Does the conclusion must be true?
- What is wrong?
- The argument is valid: modus ponens inference rule.
- We cannot conclude that the conclusion is true, since one of its premises, $\sqrt{2} > \frac{3}{2}$, is false.
- Indeed, in this case the conclusion is false, since $2 \not> \frac{9}{4} = 2.25$.

Formal Proofs: using rules of inference to build arguments

Definition

A **formal proof** of a conclusion q given hypotheses $p_1, p_2, \ldots, p_n$ is a sequence of steps, each of which applies some inference rule to hypotheses or previously proven statements (antecedents) to yield a new true statement (the consequent).

A formal proof demonstrates that if the premises are true, then the conclusion is true.
Note that the word formal *here is not a synomym of rigorous.*
A formal proof is based simply on symbol manipulation (no need of thinking, just apply rules).
A formal proof is rigorous but so can be a proof that does not rely on symbols!

Formal proof example

Show that the 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.

lead to the conclusion:

- We will be home by the sunset.

Main steps:

1. Translate the statements into proposional logic.
2. Write a formal proof, a sequence of steps that state hypotheses or apply inference rules to previous steps.

Show that the hypotheses:

- It is not sunny this afternoon and it is colder than yesterday. $\neg s \wedge c$
- We will go swimming only if it is sunny. $w \rightarrow s$
- If we do not go swimming, then we will take a canoe trip. $\neg w \rightarrow t$
- If we take a canoe trip, then we will be home by sunset. $t \rightarrow h$

lead to the conclusion:

- We will be home by the sunset. h

Step	Reason
1. $\neg s \wedge c$	hypothesis
2. $\neg s$	simplification
3. $w \rightarrow s$	hypothesis
4. $\neg w$	modus tollens of 2 and 3
5. $\neg w \rightarrow t$	hypothesis
6. t	modus ponens of 4 and 5
7. $t \rightarrow h$	hypothesis
8. h	modus ponens of 6 and 7

Where:
s: "it is sunny this afternoon"
c: "it is colder than yesterday"
w: "we will go swimming"
t: "we will take a canoe trip.
h: "we will be home by the sunset."

Resolution and Automated Theorem Proving

We can build programs that automate the task of reasoning and proving theorems.

Recall that the rule of inference called **resolution** is based on the tautology:

$$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$$

If we express the hypotheses and the conclusion as **clauses** (possible by CNF, a conjunction of clauses), we can use **resolution** as the only inference rule to build proofs!

This is used in programming languages like **Prolog**.
It can be used in **automated theorem proving systems**.

Proofs that use exclusively **resolution** as inference rule

Step 1: Convert hypotheses and conclusion into clauses:

Original hypothesis	equivalent CNF	Hypothesis as list of clauses
$(p \wedge q) \vee r$	$(p \vee r) \wedge (q \vee r)$	$(p \vee r)$, $(q \vee r)$
$r \rightarrow s$	$(\neg r \vee s)$	$(\neg r \vee s)$

Conclusion	equivalent CNF	Conclusion as list of clauses
$p \vee s$	$(p \vee s)$	$(p \vee s)$

Step 2: Write a proof based on resolution:

Step	Reason
1. $p \vee r$	hypothesis
2. $\neg r \vee s$	hypothesis
3. $p \vee s$	resolution of 1 and 2

Show that the hypotheses:

- $\neg s \wedge c$ translates to clauses: $\neg s$, c
- $w \rightarrow s$ translates to clause: $(\neg w \vee s)$
- $\neg w \rightarrow t$ translates to clause: $(w \vee t)$
- $t \rightarrow h$ translates to clause: $(\neg t \vee h)$

lead to the conclusion:

- h (it is already a trivial clause)

Note that the fact that p and $\neg p \vee q$ implies q (called disjunctive syllogism) is a special case of resolution, since $p \vee F$ and $\neg p \vee q$ give us $F \vee q$ which is equivalent to q.

Resolution-based proof:

Step	Reason
1. $\neg s$	hypothesis
2. $\neg w \vee s$	hypothesis
3. $\neg w$	resolution of 1 and 2
4. $w \vee t$	hypothesis
5. t	resolution of 3 and 4
6. $\neg t \vee h$	hypothesis
7. h	resolution of 5 and 6

Fallacies

Fallacy = misconception resulting from incorrect argument.

- **Fallacy of affirming the conclusion**
  Based on
  $$((p \to q) \land q) \to p$$
  which is NOT A TAUTOLOGY.
  Ex.: If prof gives chocolate, then you answer the question. You answer the question. We conclude the prof gave chocolate.

- **Fallacy of denying the hypothesis**
  Based on
  $$((p \to q) \land \neg p) \to \neg q$$
  which is NOT A TAUTOLOGY.
  Ex.: If prof gives chocolate, then you answer the question. Prof doesn't give chocolate. Therefore, you don't answer the question.

Rules of Inference for Quantified Statements

Rule of Inference	Name
$\dfrac{\forall x P(x)}{\therefore\ P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\ \forall x P(x)}$	Universal generalization
$\dfrac{\exists x P(x)}{\therefore\ P(c) \text{ for some element } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some element } c}{\therefore\ \exists x P(x)}$	Existencial generalization

Show that the premises:

- A student in Section A of the course has not read the book.
- Everyone in Section A of the course passed the first exam.

imply the conclusion

- Someone who passed the first exam has not read the book.

$A(x)$: "x is in Section A of the course"
$B(x)$: "x read the book"
$P(x)$: "x passed the first exam."

Hypotheses: $\exists x(A(x) \wedge \neg B(x))$ and $\forall x(A(x) \rightarrow P(x))$.
Conclusion: $\exists x(P(x) \wedge \neg B(x))$.

Hypotheses: $\exists x(A(x) \land \neg B(x))$ and $\forall x(A(x) \rightarrow P(x))$.
Conclusion: $\exists x(P(x) \land \neg B(x))$.

Step	Reason
1. $\exists x(A(x) \land \neg B(x))$	Hypothesis
2. $A(a) \land \neg B(a)$	Existencial instantiation from (1)
3. $A(a)$	Simplification from (2)
4. $\forall x(A(x) \rightarrow P(x))$	Hypothesis
5. $A(a) \rightarrow P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \land \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x(P(x) \land \neg B(x))$	Existential generalization from (8)

Combining Rules of Inference for Propositions and Quantified Statements

These inference rules are frequently used and combine propositions and quantified statements:

- **Universal Modus Ponens**

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

- **Universal Modus Tollens**

$$\begin{array}{rl} & \forall x(P(x) \to Q(x)) \\ & \neg Q(a), \text{ where } a \text{ is a particular element in the domain} \\ \hline \therefore & \neg P(a) \end{array}$$

Proof Methods

A proof is a valid argument that establishes the truth of a mathematical statement, using the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven theorems.

Using these ingredients and rules of inference, the proof establishes the truth of the statement being proved.

We move from formal proofs, as seen in the previous section, to **informal proofs**, where more than one inference rule may be used at each step, where steps may be skipped, and where axioms and rules of inference used are not explicitly stated.

Some terminology

- **Theorem**: a statement that can be shown to be true (sometimes referred to as **facts** or **results**). Less important theorems are often called **propositions**.
- A **lemma** is a less important theorem, used as an auxiliary result to prove a more important theorem.
- A **corollary** is a theorem proven as an easy consequence of a theorem.
- A **conjecture** is a statement that is being proposed as a true statement. If later proven, it becomes a theorem, but it may be false.
- **Axiom** (or **postulates**) are statements that we assume to be true (algebraic axioms specify rules for arithmetic like commutative laws).
- A **proof** is a valid argument that establishes the truth of a theorem. The statements used in a proof include axioms, hypotheses (or premises), and previously proven theorems. Rules of inference, together with definition of terms, are used to draw conclusions from other assertions, tying together the steps of a proof.

Understanding how theorems are stated

Many theorems assert that a property holds for all elements in a domain. However, the universal quantifier is often not explicitly stated.

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 $x^2 > y^2$."

That is, in formal logic under the domain of positive real numbers this is the same as $\forall x \forall y((x > y) \rightarrow (x^2 > y^2))$.

Methods of proving theorems

To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, we use the steps:

- Take an arbitrary element c of the domain and show that $(P(c) \rightarrow Q(c))$ is true.
- Apply universal generalization to conclude $\forall x(P(x) \rightarrow Q(x))$. (Normally we not even bother with this final step.)

3 methods of showing statements of the type $p \rightarrow q$ are true:

1. **Direct proofs:** Assume p is true; the last step establishes q is true.
2. **Proof by Contraposition:** Uses a direct proof of the contrapositive of $p \rightarrow q$, which is $\neg q \rightarrow \neg p$. That is, assume $\neg q$ is true; the last step established $\neg p$ is true.
3. **Proof by Contradiction:** To prove that P is true, we assume $\neg P$ is true and reach a contradiction, that is that $(r \wedge \neg r)$ is true for some proposition r. In particular, to prove $(p \rightarrow q)$, we assume $(p \rightarrow q)$ is false, and get as a consequence a contradiction. Assuming that $(p \rightarrow q)$ is false $= (\neg p \vee q)$ is false $= (p \wedge \neg q)$ is true.

Direct Proofs

A **formal direct proof** of a conditional statement $p \rightarrow q$ works as follows: assume p is true, build steps using inference rules, with the final step showing that q is true.

In a **(informal) direct proof**, we assume that p is true, and use axioms, definitions and previous theorems, together with rules of inference to show that q must be true.

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 $n = 2k + 1$.

Give a direct proof of the following theorem.

Theorem

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

Theorem

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

Observations: We want to show that $\forall n(P(n) \rightarrow Q(n))$, where $P(n)$ is "n is an odd integer" and $Q(n)$ is "n^2 is odd".
We show this by proving that for an arbitrary n, $P(n)$ implies $Q(n)$, without invoking the universal generalization.

Proof:
Let n be an odd integer.
By definition of odd, we know that there exists an integer k such that $n = 2k + 1$.
Squaring both sides of the equation, we get
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
Since $n^2 = 2k' + 1$, where $k' = 2k^2 + 2k$, by the definition of odd we conclude n^2 is odd. $\square$

Definition

An integer a is a *perfect square* if there is an integer b such that $a = b^2$.

Exercise:

Prove the following theorem using a direct proof.

Theorem

If m and n are both perfect squares, then mn is also a perfect square.

Proof by Contraposition

This method of proof makes use of the equivalence $(p \to q) \equiv (\neg q \to \neg p)$. In a proof by contraposition that $p \to q$, we assume $\neg q$ is true, and using axioms, definitions and previously proven theorems, together with inference rules, we show that $\neg p$ must be true. (It is a direct proof of the contrapositive statement!)

Theorem

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

Proof: We prove the statement by contraposition.
Assume n is even (assuming $\neg q$). Then, by definition, $n = 2k$ for some integer k. Thus, $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. So, we have that $3n + 2 = 2k'$ where $k' = 3k + 1$, which means $3n + 2$ is an even number. This is the negation of the hypothesis of the theorem $(\neg p)$, which concludes our proof by contraposition. □

Exercises: proof by contraposition

- Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
- Show that the proposition $P(0)$ is true where the domain consists of the integer numbers and $P(n)$ is "If $n \geq 1$ then $n^2 > n$."
  Note: vacuous proof: when p is false $p \rightarrow q$ is true, regardless of the value of q.

When to use each type of proof?

Usually try a direct proof. If it doesn't work, try a proof by contraposition.

Definition

A real number r is *rational* if there exists integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called *irrational*

Prove that the sum of two rational numbers is rational. (For all $r, s \in \mathbb{R}$, if r and s are rational numbers, then $r + s$ is rational.)
Let r and s be rational numbers. Then, there exist integers p, q, t, u with $q \neq 0$ and $u \neq 0$ such that $r = p/q$ and $s = t/u$. So,

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

Since $q \neq 0$ and $u \neq 0$, we have $qu \neq 0$. Therefore, we expressed $r + s$ as the ratio of two integers $pu + qt$ and qu, where $qu \neq 0$. This means that $r + s$ is rational. (The direct proof succeeded!)

Prove that for any integer number n, if n^2 is odd, then n is odd.

Trying a direct proof...
Let n be an integer number. Assume that n^2 is odd. We get next that there exists an integer k such that $n^2 = 2k + 1$. Solving for n produces the equation $n = \pm\sqrt{2k+1}$, which is not very useful to show that n is odd.

Try a prove by contraposition...
Let n be an integer number. Assume n is not odd. This means that n is even, and so there exists an integer k such that $n = 2k$. Thus, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. So, taking $k' = 2k^2$, we see that $n^2 = 2k'$ and so n^2 is even. This concludes our proof by contraposition.

Proof by Contradiction

In a proof by contradiction, we prove that a proposition p is true, by showing that there exists a contradiction q such that $\neg p \rightarrow q$.

We can prove that p is true by showing for instance that $\neg p \rightarrow (r \wedge \neg r)$, for some proposition r.

Prove that $\sqrt{2}$ is irrational.

A direct proof is difficult, as it means to show that there exists no two integer a and b with $b \neq 0$ such that $\sqrt{2} = a/b$. Nonexistence proofs are usually hard.

Let's try a proof by contradiction...

Theorem

$\sqrt{2}$ is irrational.

Proof: We prove by means of contradiction. Assume $\sqrt{2}$ is a rational number. So, there exists a' and b' integers with $b' \neq 0$ with $\sqrt{2} = a'/b'$. We select such integers a and b with the additional property that a and b have no common factors, i.e. the fraction a/b is in lowest terms (this is always possible to obtain, for we can keep dividing by common factors). So, $\sqrt{2} = a/b$ so $2 = a^2/b^2$. This implies $2b^2 = a^2$ (1). By the definition of even, we know that a^2 is even. Next we use a theorem that states that if a^2 is even then a is even (prove it as an exercise). Now, since a is even, we know that there exists c such that $a = 2c$. Substituting in the formula (1) above, we get that $2b^2 = (2c)^2 = 4c^2$. Dividing both sides by 2 we get $b^2 = 2c^2$. By the definition of even, we see that b is even. Therefore, we got that a is even and b is even, and so 2 is a common factor of a and b. But we also had that a and b had no common factors. We just reached a contradiction! □

Other types of proof statements

- **Proof of equivalences:**
  To prove a statement $p \leftrightarrow q$, we show that both $p \rightarrow q$ and $q \rightarrow p$ are true.

  Example: Prove that if n is a positive integer, then n is odd if and only if n^2 is odd.

- Showing that a statement of the form $\forall x P(x)$ is false:
  In this case, we need to find a **counterexample**.

  Example: Show that the statement "Every positive integer is the sum of the squares of two integers." is false.
  We argue that 3 is a counterexample. The only perfect squares smaller than 3 are 0 and 1, and clearly, 3 cannot be written as a sum of two terms each being 0 or 1.

Mistakes in Proofs

What is the problem with he following proof that $1 = 2$?

Use the following steps, where a and b are two equal positive integers.

1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a.
3. $a^2 - b^2 = ab - b^2$	Substract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factoring both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5), since $a = b$
7. $2 = 1$	Divide both sides of 6. by b.

Therefore $2 = 1$.

Proof by Cases

Sometimes it is difficult to use a single argument that holds for all cases. Proof by cases uses the following equivalence:

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q] \equiv [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$$

Example: Prove that if n is integer then $n^2 \geq n$.

We split the proof into three cases.

- Case (i) $n = 0$.
  In this case, $n^2 = 0^2 = 0 = n$.
- Case (ii) $n \geq 1$
  In this case, when we multiply both sides of $n \geq 1$ by n we obtain $n \cdot n \geq n \cdot 1$. This implies $n^2 \geq n$.
- Case (iii) $n \leq -1$
  In this case, $n \leq -1$, but $n^2 \geq 0$. Therefore, $n^2 \geq 0 \geq -1 \geq n$, and so $n^2 \geq n$.

□

Exhaustive proof

This is a special form of a proof by cases, when there is a finite and small number of examples for which we need to prove a fact.

Prove that $(n+1)^2 \geq 3^n$ if n is a positive integer with $n \leq 2$.

We use a proof by exhaustion, by examining the cases $n = 1, 2$.
For $n = 1$, $(n+1)^2 = 2^2 = 4 \geq 3 = 3^n$.
For $n = 2$, $(n+1)^2 = 3^2 = 9 \geq 3^2 = 3^n$.

Existence Proofs

Existence proofs prove statements of the form $\exists x P(x)$.

- **Constructive existence proof: find a such that $P(a)$ is true.**
  Example: Show that there is a positive integer that can be written as a sum of cubes of positive integers in two different ways.
  Proof: $1729 = 10^3 + 9^3$ and $1729 = 12^3 + 1^3$.

Existence Proofs

Existence proofs prove statements of the form $\exists x P(x)$.

- **Constructive existence proof: find a such that $P(a)$ is true.**
  Example: Show that there is a positive integer that can be written as a sum of cubes of positive integers in two different ways.
  Proof: $1729 = 10^3 + 9^3$ and $1729 = 12^3 + 1^3$.
- **Nonconstructive existence proof: show that $\exists x P(x)$ without explicitly giving a for which $P(a)$ is true.**
  Example: Show that there exist irrational numbers x and y such that x^y is rational.
  From a previous theorem we know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. There are two possible cases:

Existence Proofs

Existence proofs prove statements of the form $\exists x P(x)$.

- **Constructive existence proof: find a such that $P(a)$ is true.**
  Example: Show that there is a positive integer that can be written as a sum of cubes of positive integers in two different ways.
  Proof: $1729 = 10^3 + 9^3$ and $1729 = 12^3 + 1^3$.
- **Nonconstructive existence proof: show that $\exists x P(x)$ without explicitly giving a for which $P(a)$ is true.**
  Example: Show that there exist irrational numbers x and y such that x^y is rational.
  From a previous theorem we know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. There are two possible cases:
  - $\sqrt{2}^{\sqrt{2}}$ is rational: In this case, take $x = \sqrt{2}$ and $y = \sqrt{2}$.

Existence Proofs

Existence proofs prove statements of the form $\exists x P(x)$.

- **Constructive existence proof: find a such that $P(a)$ is true.**
  Example: Show that there is a positive integer that can be written as a sum of cubes of positive integers in two different ways.
  Proof: $1729 = 10^3 + 9^3$ and $1729 = 12^3 + 1^3$.
- **Nonconstructive existence proof: show that $\exists x P(x)$ without explicitly giving a for which $P(a)$ is true.**
  Example: Show that there exist irrational numbers x and y such that x^y is rational.
  From a previous theorem we know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. There are two possible cases:
  - $\sqrt{2}^{\sqrt{2}}$ is rational: In this case, take $x = \sqrt{2}$ and $y = \sqrt{2}$.
  - $\sqrt{2}^{\sqrt{2}}$ is irrational: In this case, take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Then $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.

The art of finding a proof method that works for a theorem

We need practice in order to recognize which type of proof to apply to a particular theorem/fact that we need to prove.

In the next topic "number theory", several theorems will be proven using different proof methods and strategies.