Methods of Proof

1 Mathematical Proof

A mathematical proof is a valid argument that establishes the truth of a mathematical argument

A proof is generally constructed using:

- The hypothesis of the theorem
- Axioms known to be true
- Previously proved theorems
- Rules of inference

Up until now, we have been considering formal proofs (in logics)
Now we focus on informal proofs, as applied by humans

2 Theorems

Theorems are usually stated using an informal version of first-order logic and often have one of the following structures:

- ”Every x is a y”
- ”There is a x that is not y”
- ”If something is x then it is a y”

Consequently, in order to prove many theorems we utilize our knowledge of first order logic
Different proof methods are available to us, often depending on the structure of the theorem to be proved

3 Direct Proofs

A direct proof is used to prove theorems of the form

If such and such then such and such

More generally, theorems of the form

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

Essentially, a direct proof is a list of statements starting from P(x) and ending at Q(x), and where every statement in the list is

- An axiom
- A previously proved theorem, or
- An inference of such using a rule of inference

Direct proofs, once stated, tend to be easy to check, but often some insight is required to devise the proof in the first place

3.1 Example 1

3.1.1 Theorem

If n is an odd integer then so is n^2

3.1.2 Proof

- Suppose that n is an odd integer
- So, $n = 2k + 1$, for some integer k
- Thus, $n^2 = (2k + 1)^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1$
- When we divide n^2 by 2 we get $2k^2 + 2k$ remainder 1
- Thus, n^2 is odd

3.2 Example 2

3.2.1 Theorem

If m and n are perfect squares then so is mn

3.2.2 Proof

- Suppose that m and n are perfect squares
- So, $m = a^2$, for some integer a, and $n = b^2$, for some integer b
- Thus, $mn = a^2b^2 = (ab)^2$
- So mn is a perfect square

4 Proof by contraposition

Proofs by contraposition are generally used to prove theorems of the form:

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

The key to a proof by contraposition is the following argument from first-order logic

- M is a model of $\forall x(P(x) \Rightarrow Q(x))$
- Iff for every x, M is a model of $P(x) \Rightarrow Q(x)$
- Iff for every x, M is a model of $\neg Q(x) \Rightarrow \neg P(x)$
- Iff M is a model of $\forall x(\neg Q(x) \Rightarrow \neg P(x))$

Thus, if we wish to prove that $\forall x(P(x) \Rightarrow Q(x))$ is a theorem, then it suffices to prove that for any value of x, $\neg Q(x) \Rightarrow \neg P(x)$

4.1 Example 1

4.1.1 Theorem

If n is an integer and 3n+2 is odd then n is odd

4.1.2 Proof

Wanting to show that if n is even, then $3n + 2$ is even (the opposite)

- Assume the negation of what we want to prove; that is, assume that n is even
- So, n=2k, for some integer k
- Thus, $3n + 2 = 6k + 2$ is even
- Hence, if n is even then $3n + 2$ is even; that is, if $3n + 2$ is odd then n is odd

Let's try and prove the result above with a **direct proof**
Suppose that $3n + 2$ is odd; so, 3n+2=2k+1, for some integer k. So, $3n = 2k - 1$ is odd
It's not so clear as to how to proceed now, as we appear to be back where we started except we have that 3n is odd as opposed to 3n+2

4.2 Example 2

4.2.1 Theorem

If m and n are integers and mn is even then m is even or n is even

4.2.2 Proof

Wanting to prove that if m and n are odd then mn is odd
Assume that m is odd and n is odd.
So, $m = 2k + 1$, for some integer k, and $n = 2p + 1$, for some integer p
Thus,

$$mn = (2k + 1)(2p + 1) = 4kp + 2k + 2p + 1 = 2(2kp + k + p) + 1$$

Which is odd

4.3 Example 3

4.3.1 Theorem

If n is an integer and $n^3 + 5$ is odd then n is even

4.3.2 Proof

Wanting to prove that is n is off then $n^3 + 5$ is even
Assume that n is odd; so, $n = 2k + 1$, for some integer k
Thus,

$$\begin{aligned} n^3 + 5 &= (2k + 1)^3 + 5 \\ &= (2k + 1)\left(4k^2 + 4k + 1\right) + 5 \\ &= 8k^3 + 12k^2 + 6k + 6 \\ &= 2\left(4k^3 + 6k^2 + 3k + 3\right) \end{aligned}$$

Which is even

5 Which is the easiest method to use?

The previous examples show that using one proof method can be easier than using another; but how do we decide which proof method to use?
There is no canonical answer: a good approach is to try a direct proof and if you struggle, try proof by contraposition

5.1 Theorem

The sum of two rational numbers are rational

5.2 Proof

Try a direct proof. Let x and y be rational numbers; so, let $x = a/b$ and let $y = c/d$, where a,b,c and d are integers. Thus, $x + y = a/b + c/d = ad/bd + bc/bd = (ad + bc)/bd$, which is rational, and so the direct proof works

If we tried a proof by contraposition then we would start by considering the irrational sum of two numbers $x + y$. This would not be of very much help

6 Proof by contradiction

Suppose that we wish to prove that something, p say, is true.
Suppose we also know:

- Something else, q say, to be false
- $\neg p \Rightarrow q$ to be true

The only way that $\neg p \Rightarrow q$ can be true when q is false is for p to be true. The above state of affairs results in a proof by contradiction

Look more closely at a proof by contradiction
It proves that p is true but it does it non-constructively; that is, it does it not by building a proof that p is true but by showing that if p were false then we would be able to prove that something known to be false is true

6.1 Example 1

6.1.1 Theorem

$\sqrt{2}$ is irrational

6.1.2 Proof

Suppose that $\sqrt{2}$ is rational; that is, suppose that $\sqrt{2} = a/b$ where a and b are integers and where no integer apart from 1 divides both a and b.

So, $2 = a^2/b^2$, with $a^2 = 2b^2$ and a^2 even.

So we have that a is even; that is, $a = 2p$ for some integer p.

Hence, $4p^2 = 2b^2$ with $b^2 = 2p^2$; in particular, b^2 is even.

So b is even; so, $b = 2q$, for some integer q.

This, 2 divides a and 2 divides b, which yields a contradiction.

Hence, our original assumption that $\sqrt{2}$ is rational cannot be correct; that is, $\sqrt{2}$ is irrational

6.2 Example 2

6.2.1 Theorem

There is no rational number r for which $r^3 + r + 1 = 0$

6.2.2 Proof

Suppose that $r = a/b$ is rational, where a and b are integers having no common factor different from 1. So,

$$a^3/b^3 + a/b + 1 = 0$$

with

$$a^3 + ab^2 + b^3 = 0$$

As 0 is even

$$a^3 + ab^2 + b^3$$

is even
If a and b are odd then $a^3 + ab^2 + b^3$ is odd - contradiction
If a is odd and b is even, $a^3 + ab^2 + b^3$ is odd - contradiction
If a is even and b is odd, $a^3 + ab^2 + b^3$ is odd - contradiction
So, a and b have a common factor 2 - contradiction

7 Proof of equivalence

Proof of equivalence have the form $p \Leftrightarrow q$ and are usually structured into two parts $p \Rightarrow q$ and $q \Rightarrow p$

7.1 Example 1

7.1.1 Theorem

For any integer n, n if odd iff n^2 is odd

7.1.2 Proof

(Direct Proof): If n is odd then $n = 2k + 1$, for some integer k.
So, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is odd

(Proof by contraposition): Conversely, now we wish to prove that if n^2 is odd then n is odd.
Suppose than n is even; that is, $n = 2k$, for some integer k. Thus, $n^2 = (2k)^2 = 2(2k^2)$ is even

7.2 Example 2

7.2.1 Theorem

If x is a real number then the following are equivalent

(i) x is rational

(ii) $x/2$ is rational

(iii) $3x - 1$ is rational

7.2.2 Proof

- Suppose that (i) holds
  - So, $x = a/b$ is rational and $x/2 = a/2b$ is rational
  - So (ii) holds
- Suppose that (ii) holds
  - S, $x/2 = a/b$ is rational and $x = 2a/b$ is rational
  - So (i) holds
- Suppose that (i) holds
  - So, $x = a/b$ is rational and $3x - 1 = 3a/b = 1 = (3a - b)/b$ is rational
  - So (iii) holds
- Suppose that (iii) holds
  - So, $3x - 1 = a/b$ is rational and $x = (a + b)/3b$ is rational
  - So (i) holds

Thus:

- $(i) \Leftrightarrow (ii)$
- $(i) \Leftrightarrow (iii)$

Hence

- $(ii) \Rightarrow (i)$
- $(i) \Rightarrow (iii)$
- $(iii) \Rightarrow (i)$
- $(i) \Rightarrow (ii)$

So, $(ii) \Leftrightarrow (iii)$

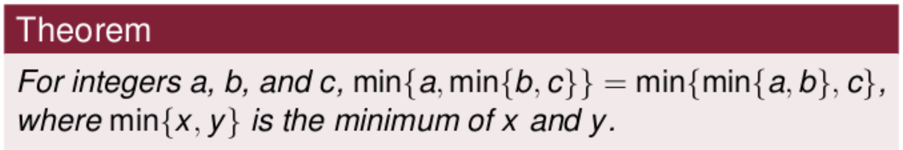
8 Proof by cases

Sometimes the proof of a theorem can be split up into the separate proofs of a small number of different cases

8.1 Example

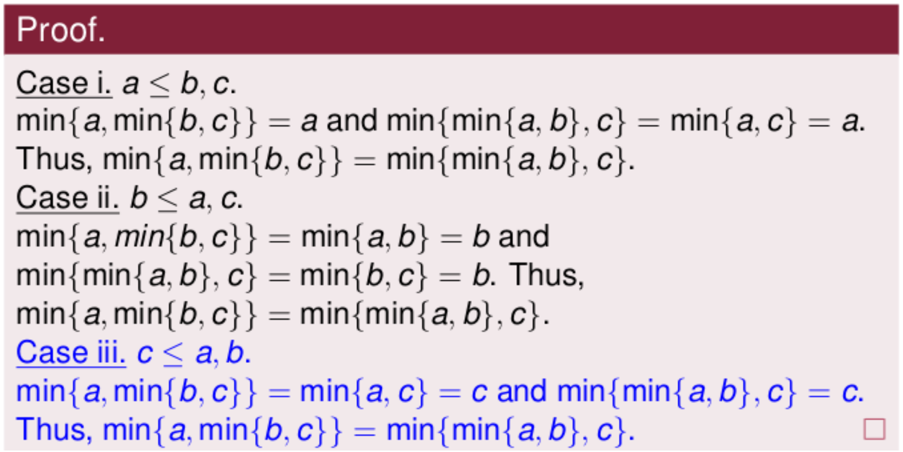
8.1.1 Theorem

For integers a,b and c



Theorem

For integers a, b, and c, $\min\{a, \min\{b, c\}\} = \min\{\min\{a, b\}, c\}$*, where* $\min\{x, y\}$ *is the minimum of* x *and* y*.*



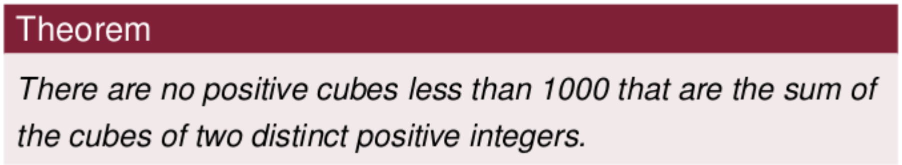
Proof.

Case i. $a \leq b, c$.
$\min\{a, \min\{b, c\}\} = a$ and $\min\{\min\{a, b\}, c\} = \min\{a, c\} = a$.
Thus, $\min\{a, \min\{b, c\}\} = \min\{\min\{a, b\}, c\}$.
Case ii. $b \leq a, c$.
$\min\{a, min\{b, c\}\} = \min\{a, b\} = b$ and
$\min\{\min\{a, b\}, c\} = \min\{b, c\} = b$. Thus,
$\min\{a, \min\{b, c\}\} = \min\{\min\{a, b\}, c\}$.
Case iii. $c \leq a, b$.
$\min\{a, \min\{b, c\}\} = \min\{a, c\} = c$ and $\min\{\min\{a, b\}, c\} = c$.
Thus, $\min\{a, \min\{b, c\}\} = \min\{\min\{a, b\}, c\}$. □

9 Exhaustive checks

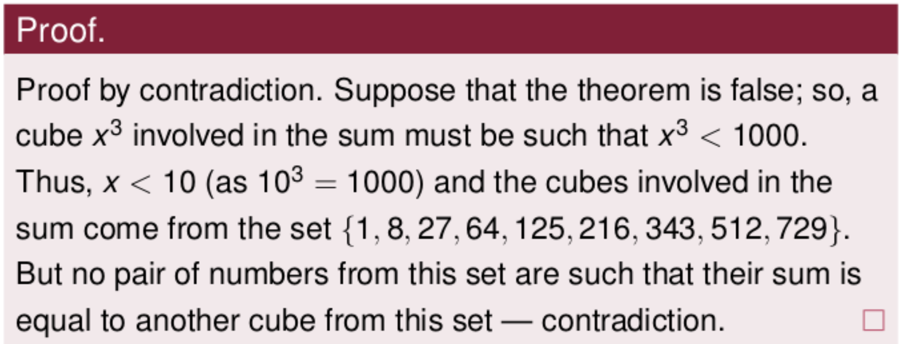
Sometimes a proof by cases is nothing other than an exhaustive check

9.1 Example



Theorem

There are no positive cubes less than 1000 that are the sum of the cubes of two distinct positive integers.



Proof.

Proof by contradiction. Suppose that the theorem is false; so, a cube x^3 involved in the sum must be such that $x^3 < 1000$. Thus, $x < 10$ (as $10^3 = 1000$) and the cubes involved in the sum come from the set $\{1, 8, 27, 64, 125, 216, 343, 512, 729\}$. But no pair of numbers from this set are such that their sum is equal to another cube from this set — contradiction. □

10 Existence proofs

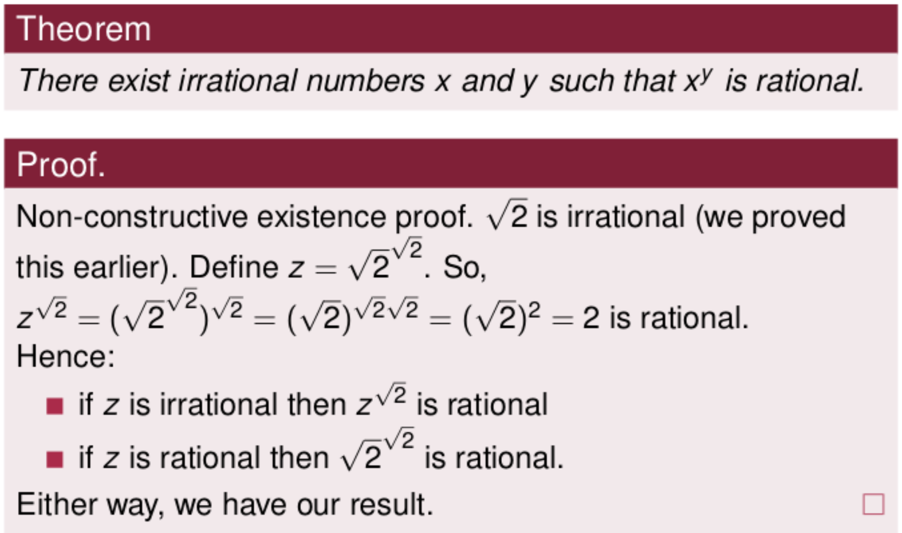
Existence proofs tend to be proofs of theorems in the form $\exists x P(x)$

In order to prove a theorem of the form $\exists x P(x)$ we can either construct an actual x such that $P(x)$ holds or we

can show that such an x must exist without actually constructing it
The former are called constructive proofs, the latter non-constructive proofs
For example, in order to prove the theorem:
Theorem:
There is a positive integer that is the sum of all positive integers less than it

We simply write 3 = 1 + 2 to constructively prove this

10.1 Non constructive existence proofs



Theorem

There exist irrational numbers x and y such that x^y is rational.

Proof.

Non-constructive existence proof. $\sqrt{2}$ is irrational (we proved this earlier). Define $z = \sqrt{2}^{\sqrt{2}}$. So,
$z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\sqrt{2}} = (\sqrt{2})^2 = 2$ is rational.
Hence:

- if z is irrational then $z^{\sqrt{2}}$ is rational
- if z is rational then $\sqrt{2}^{\sqrt{2}}$ is rational.

Either way, we have our result. □

11 Proof by counterexample

Consider a statement of the form $\forall x P(x)$
In order to prove it, we need to prove that for every x, P(x) holds
In order to disprove it, we need to find some x such that $\neg P(x)$ holds (or, at least, show that such an x exists). That is, find (the existence of) a counterexample.

For example, consider the statement

If a and b are rational numbers then a^b is rational

Refutation. Put $a = 2$ and $b = 1/2$. Then $a^b = \sqrt{2}$ is irrational.
Hence, the statement is not a theorem as we have found a counterexample