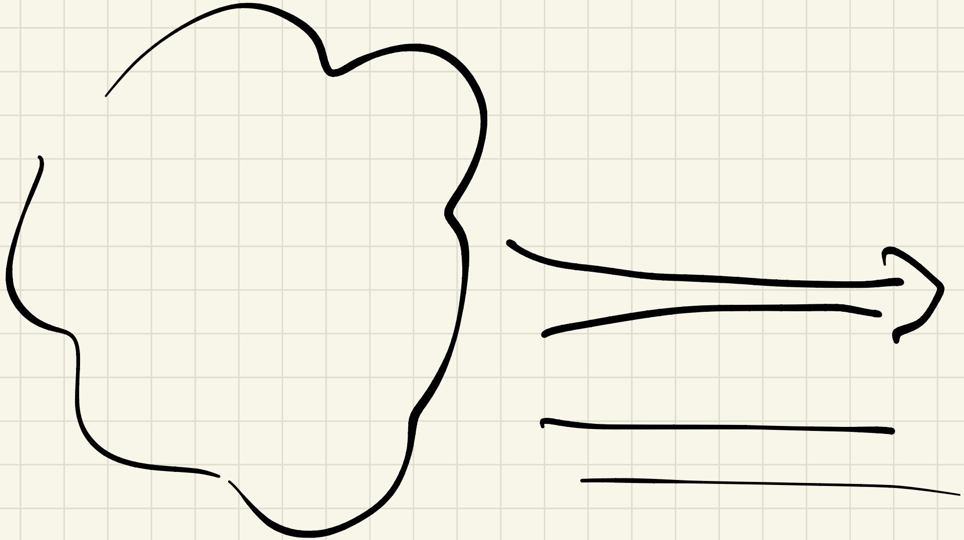
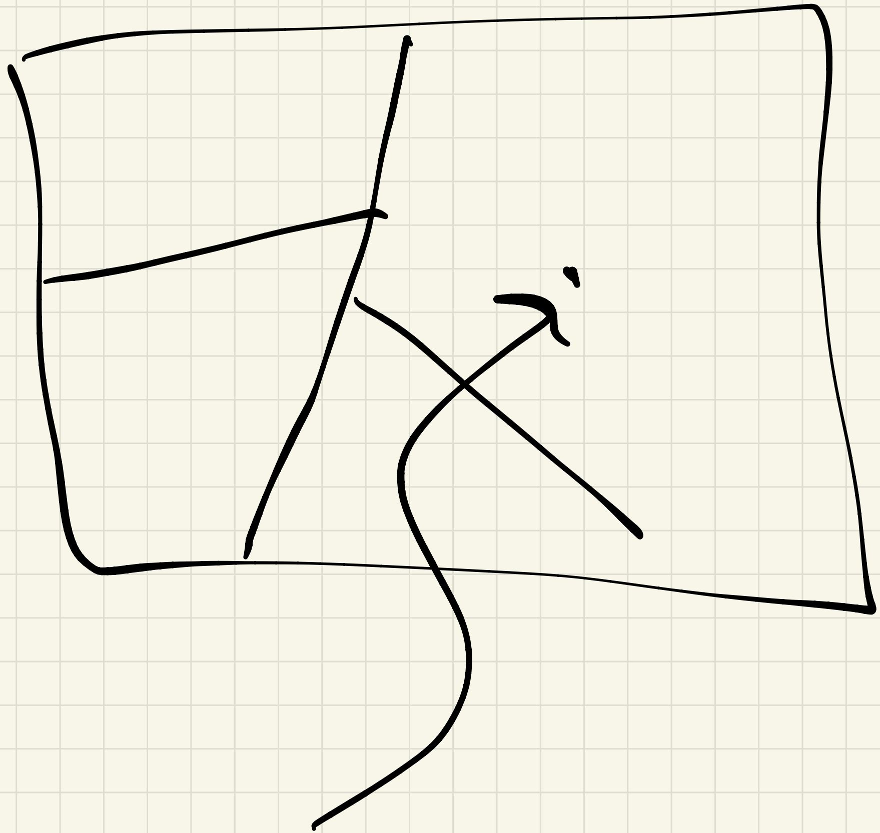
Indirect proofs



• Conjecture



$\forall n$ if n is even then n^2 is even

$\forall n$ if n is an integer s.t. n^2 is even

then n is even

n	0	1	2	3	4	5
n^2	0	1	4	9	16	25

Suppose that m is a particular but arbitrarily chosen integer s.t m^2 is even

Then $m^2 = 2k$ for some k

$\sqrt{2k}$?

Indirect proofs

- In a direct proof you start with the hypothesis of a statement and make one deduction after another until you reach the conclusion.
- Indirect proofs are more roundabout. One kind of indirect proof, argument by contradiction, is based on the fact that either a statement is true or it is false but not both.
- So if you can show that the assumption that a given statement is not true leads logically to a contradiction, impossibility, or absurdity, then that assumption must be false: and, hence, the given statement must be true.

Motivating example: Trial and error

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8	2	3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Motivating example: Proof beyond a reasonable doubt

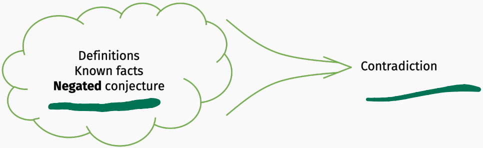
Proving that a defendant is guilty.

- Is it conceivable that the defendant is not guilty?
  - Is being not guilty compatible with the presented evidence?
  - If not, the defendant must be guilty

Direct proof vs proof by contradiction

- Direct proof:

- Proof by contradiction:

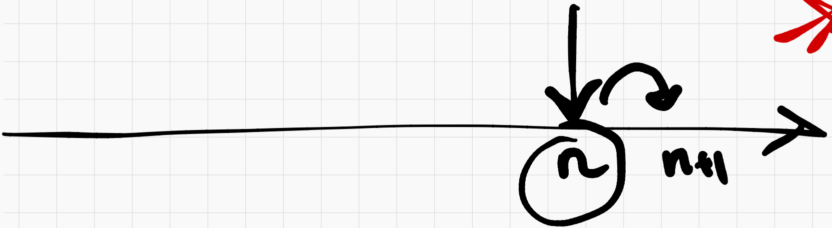


Use proof by contradiction to show that there is no greatest integer

Suppose for a proof by contradiction that there exists a greatest int. n

But $n+1 > n$, $n+1$ is an integer

so n is not a greatest integer



Use proof by contradiction to show that no integer can be both even and odd

Proof Suppose for a proof by contradiction that there exists an integer n s.t. n is both even and odd

So $n = 2k$ for some int. k.

and $n = 2l + 1$ for some integer l

So $2k = 2l + 1 \Rightarrow 1 = 2(k - l)$

But then 1 is even, a contradiction

Show for any integer m, if m^2 is even then m is even

Suppose for a proof by contradiction that there exists an integer m s.t m is not even and m^2 is even

Then m is odd. So $m = 2k+1$, for some integer k,

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

So m^2 is odd / not even. A contradiction

Proof by contraposition

To prove

$$\forall x \text{ if } P(x) \text{ then } Q(x)$$

it suffices to prove

$$\forall x \text{ if } \textbf{not } Q(x) \text{ then } \textbf{not } P(x)$$

Show that for any integer n if n^2 is even then n is even

Contrapositive

Show that for any integer n if n is not even then n^2 is not even

Two classic results

Use proof by contradiction to show that there is no greatest prime number

[1] Known to Euclid 300BC

proof continued

Recall: the real numbers

All (decimal) numbers — distances to points on a number line.

Examples.

- -3.0
- 0
- 1.6
- $\pi = 3.14159\ldots$

A real number that is not rational is called irrational.

But are there any irrational numbers?

Prove that $\sqrt{2}$ is not a rational number

Suppose for a proof by contradiction that $\sqrt{2}$ is a rational number [1]

Then $\sqrt{2} = \dfrac{m}{n}$ m, n are integers & $n \neq 0$

$\dfrac{m}{n}$ is irreducible

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \frac{8}{16} = \cdots$$

$$\left(\sqrt{2}\right)^2 = \left(\frac{m}{n}\right)^2$$

$$2 = \frac{m^2}{n^2} \Rightarrow 2n^2 = m^2 \Rightarrow m^2 \text{ is even}$$

$\Rightarrow m$ is even

[1] Known to Pythagoras 300BC

proof continued

$m = 2k$ for some int. k

so $m^2 = 4k^2$

$$2n^2 = m^2 = 4k^2$$

$$\Downarrow$$

$n^2 = 2k^2$ and n^2 is even

so n is even