Discrete Structures: Introduction to Proofs

Amotz Bar-Noy

Department of Computer and Information Science
Brooklyn College
What is a Proof?

1. The cogency of evidence that compels acceptance by the mind of a truth or a fact.

2. A formal series of statements showing that if one thing is true something else necessarily follows from it.

3. The process or an instance of establishing the validity of a statement especially by derivation from other statements in accordance with principles of reasoning.

4. A sequence of statements, each of which is either validly derived from those preceding it or is an axiom or assumption, and the final member of which, the conclusion, is the statement of which the truth is thereby established.

5. A chain of reasoning using rules of inference, ultimately based on a set of axioms, that lead to a conclusion.
Paul Erdős, although an atheist, spoke of “The Book”, an imaginary book in which God had written down the best and most elegant proofs for mathematical theorems.

He said, “You don’t have to believe in God, but you should believe in The Book”.

He accused God of keeping the most elegant mathematical proofs to himself.

When he saw a particularly beautiful mathematical proof he would exclaim, “This ones from The Book”.
Proofs and End of Proofs

End of Proof:
- Q.E.D. or □
- Latin: Quod Erat Demonstrandum
- English: Which Was to be Demonstrated
Proofs and End of Proofs

End of Proof:

- Q.E.D. or 
- Latin: Quod Erat Demonstrandum
- English: Which Was to be Demonstrated

Some history:

https://www.youtube.com/watch?v=S0DSM-EkQE8
Some Major Techniques

- Direct Proofs
- Proof by contradiction
- Proof by contrapositive
- Proof by induction
Direct Proofs

Proof by construction and/or proof by exhaustion

Goal: prove $P \Rightarrow Q$.

Assume $P$ is true.

Demonstrate $Q$ must follow from $P$. 
Goal: prove $P \Rightarrow Q$.
Assume $P$ is true.
Assume $\neg Q$ is true.
Demonstrate a contradiction.
Proof By Contrapositive

- **Goal:** prove $P \implies Q$.
- **Assume** $\neg Q$ is true.
- **Demonstrate** $\neg P$ must follow from $\neg Q$.
- **Observe** $(P \implies Q) \iff (\neg Q \implies \neg P)$. 
Goal: prove $P \Rightarrow Q$ for $P$ and $Q$ expressed as a function of some ordered set $S$.

Basis: show $P \Rightarrow Q$ is valid for a specific element $k \in S$.

Inductive Hypothesis: Assume $P \Rightarrow Q$ for some element $n \in S$.

Demonstrate $P \Rightarrow Q$ for the element $n + 1$.

Conclude $P \Rightarrow Q$ for all elements greater than or equal to $k$ in $S$. 
4 lectures about logic and proofs from “Introduction to Higher Math”:

- **Problem Solving**: https://www.youtube.com/watch?v=CMWFmjlB8v0&list=PLZzHxk_TPOStgPtqRZ6KzmkUQBQ8TSWVX&index=1
- **Introduction to Proofs**: https://www.youtube.com/watch?v=_x65OJU8Uq4&index=2&list=PLZzHxk_TPOStgPtqRZ6KzmkUQBQ8TSWVX
- **Propositional Logic**: https://www.youtube.com/watch?v=3kzhDsSzKCU&index=3&list=PLZzHxk_TPOStgPtqRZ6KzmkUQBQ8TSWVX
- **Proof Techniques**: https://www.youtube.com/watch?v=WSb9q4Rj2Bg&index=4&list=PLZzHxk_TPOStgPtqRZ6KzmkUQBQ8TSWVX
Resources II

4 lectures about proofs from TrevTutor:

- **Direct Proofs:**
  https://www.youtube.com/watch?v=YFZzLQN5qOU&feature=youtu.be

- **Proof by Case:**
  https://www.youtube.com/watch?v=YDKBE0U6ucy&feature=youtu.be

- **Proof by Contraposition:**
  https://www.youtube.com/watch?v=X-hJ7krLBn0&feature=youtu.be

- **Proof by Contradiction:**
  https://www.youtube.com/watch?v=sRDwsfNDXak&feature=youtu.be
Section 1.7 “Introduction to Proofs” (pages 80-90) from the book “Discrete Mathematics and its Applications,” by Kenneth H. Rosen:


Two articles about proofs:

- Basic Proof Techniques:
  https://www.cse.wustl.edu/~cytron/547Pages/f14/IntroToProofs_Final.pdf

- Mathematical proof (Wikipedia):
  https://en.wikipedia.org/wiki/Mathematical_proof
Three Classic Proofs

- The square root of 2 is an irrational number
- There are infinitely many prime numbers
- The Pythagorean Theorem
The square root of 2 is an irrational number

Proof:

Assume towards contradiction that \( \frac{p}{q} = \sqrt{2} \) for two positive integers \( p \) and \( q \) that have no common divisor.

Squaring the equation implies \( p^2 = 2q^2 \).

Therefore, \( p \) must be even.

Let \( p = 2r \) for a positive integer \( r \).

It follows that \( 2q^2 = (2r)^2 = 4r^2 \) ⇒ \( q^2 = 2r^2 \).

Therefore, \( q \) must be even.

A contradiction since both \( p \) and \( q \) are even.
The square root of 2 is an irrational number

Proof:

Assume towards \textbf{contradiction} that $\frac{p}{q} = \sqrt{2}$ for two positive integers $p$ and $q$ that have no common divisor.
The square root of 2 is an irrational number

Proof:

- Assume towards contradiction that \( \frac{p}{q} = \sqrt{2} \) for two positive integers \( p \) and \( q \) that have no common divisor.
- Squaring the equation implies \( p^2 = 2q^2 \).
The square root of 2 is an irrational number

Proof:

- Assume towards contradiction that \( \frac{p}{q} = \sqrt{2} \) for two positive integers \( p \) and \( q \) that have no common divisor.
- Squaring the equation implies \( p^2 = 2q^2 \).
- Therefore, \( p \) must be even.

The square root of 2 is an irrational number

Proof:

- Assume towards **contradiction** that \( \frac{p}{q} = \sqrt{2} \) for two positive integers \( p \) and \( q \) that have no common divisor.

- Squaring the equation implies \( p^2 = 2q^2 \).

- Therefore, \( p \) must be even.

- Let \( p = 2r \) for a positive integer \( r \).
The square root of 2 is an irrational number

Proof:

- Assume towards contradiction that \( \frac{p}{q} = \sqrt{2} \) for two positive integers \( p \) and \( q \) that have no common divisor.

- Squaring the equation implies \( p^2 = 2q^2 \).

- Therefore, \( p \) must be even.

- Let \( p = 2r \) for a positive integer \( r \).

- It follows that \( 2q^2 = (2r)^2 = 4r^2 \Rightarrow q^2 = 2r^2 \).
The square root of 2 is an irrational number

Proof:

- Assume towards contradiction that \( \frac{p}{q} = \sqrt{2} \) for two positive integers \( p \) and \( q \) that have no common divisor.
- Squaring the equation implies \( p^2 = 2q^2 \).
- Therefore, \( p \) must be even.
- Let \( p = 2r \) for a positive integer \( r \).
- It follows that \( 2q^2 = (2r)^2 = 4r^2 \Rightarrow q^2 = 2r^2 \).
- Therefore, \( q \) must be even.
The square root of 2 is an irrational number

Proof:

Assume towards **contradiction** that \( \frac{p}{q} = \sqrt{2} \) for two positive integers \( p \) and \( q \) that have no common divisor.

Squaring the equation implies \( p^2 = 2q^2 \).

Therefore, \( p \) must be even.

Let \( p = 2r \) for a positive integer \( r \).

It follows that \( 2q^2 = (2r)^2 = 4r^2 \Rightarrow q^2 = 2r^2 \).

Therefore, \( q \) must be even.

A **contradiction** since both \( p \) and \( q \) are even.
The original proof and how to find a segment of length $\sqrt{k}$ for any integer $k \geq 2$:

- [https://www.youtube.com/watch?v=sbGjr_awePE](https://www.youtube.com/watch?v=sbGjr_awePE)

Five proofs:

- [https://www.youtube.com/watch?v=zEXcsZo4hOQ](https://www.youtube.com/watch?v=zEXcsZo4hOQ)

Visualizing irrationality with triangular squares:

- [https://www.youtube.com/watch?v=yk6wbvNPZW0](https://www.youtube.com/watch?v=yk6wbvNPZW0)

The original proof and the “story”:

There are infinitely many prime numbers

Proof:

Let \( p_1 < p_2 < \cdots < p_n \) be a set of \( n \) primes.

Let \( Q = p_1 p_2 \cdots p_n + 1 \).

If \( Q \) is a prime, then a new prime is found.

Otherwise, \( Q \) is a product of two or more primes.

The Fundamental Theorem of Arithmetic.

None of these primes can be \( p_1, \ldots, p_n \).

Therefore, a new prime is found.

This process can continue to find infinitely many primes.
There are infinitely many prime numbers

Proof:
- Let $p_1 < p_2 < \cdots < p_n$ be a set of $n$ primes.
There are infinitely many prime numbers

Proof:
- Let $p_1 < p_2 < \cdots < p_n$ be a set of $n$ primes.
- Let $Q = p_1 p_2 \cdots p_n + 1$. 

The Fundamental Theorem of Arithmetic.
Proof:

- Let $p_1 < p_2 < \cdots < p_n$ be a set of $n$ primes.
- Let $Q = p_1 p_2 \cdots p_n + 1$.
- If $Q$ is a prime, then a new prime is found.
There are infinitely many prime numbers

Proof:

Let \( p_1 < p_2 < \cdots < p_n \) be a set of \( n \) primes.

Let \( Q = p_1 p_2 \cdots p_n + 1 \).

If \( Q \) is a prime, then a new prime is found.

Otherwise, \( Q \) is a product of two or more primes.

The Fundamental Theorem of Arithmetic.
There are infinitely many prime numbers

Proof:
- Let $p_1 < p_2 < \cdots < p_n$ be a set of $n$ primes.
- Let $Q = p_1p_2 \cdots p_n + 1$.
- If $Q$ is a prime, then a new prime is found.
- Otherwise, $Q$ is a product of two or more primes.
  - The Fundamental Theorem of Arithmetic.
- None of these primes can be $p_1, \ldots, p_n$. 
There are infinitely many prime numbers

Proof:

- Let $p_1 < p_2 < \cdots < p_n$ be a set of $n$ primes.
- Let $Q = p_1 p_2 \cdots p_n + 1$.
- If $Q$ is a prime, then a new prime is found.
- Otherwise, $Q$ is a product of two or more primes.
  - The Fundamental Theorem of Arithmetic.
- None of these primes can be $p_1, \ldots, p_n$.
- Therefore, a new prime is found.
There are infinitely many prime numbers

Proof:

- Let $p_1 < p_2 < \cdots < p_n$ be a set of $n$ primes.
- Let $Q = p_1 p_2 \cdots p_n + 1$.
- If $Q$ is a prime, then a new prime is found.
- Otherwise, $Q$ is a product of two or more primes.
  - The Fundamental Theorem of Arithmetic.
- None of these primes can be $p_1, \ldots, p_n$.
- Therefore, a new prime is found.
- This process can continue to find infinitely many primes.
Resources

The original proof by Euclid:
- https://www.youtube.com/watch?v=dQmdHpvyfJ5s

Another proof:
- https://www.youtube.com/watch?v=fOXZgcAsrP8
The Pythagorean Theorem

An illustration:
https://www.researchgate.net/profile/Elvar_Theodorsson/publication/311442050/figure/fig3/AS:436272582926338@1481026897487/
The-pythagorean-theorem-states-that-the-square-of-the-hypotenuse-the-side-opposite-the.png

First Example:
http://www.learnalberta.ca/content/memg/Division03/Pythagorean%20Theorem/pythagex.gif

An “experimental” proof:
- https://www.youtube.com/watch?v=_e6w5GtkcGI
- https://www.youtube.com/watch?v=CAkMUdeB06o
The Pythagorean Theorem

Theorem:
Let $\triangle ABC$ be a right triangle with hypotenuse of length $c$ and two sides of lengths $a$ and $b$. Then $c^2 = a^2 + b^2$. 
“Famous” Proofs

Pythagoras’ proof:
- [https://www.youtube.com/watch?v=4yEyLZUEmQ8&feature=youtu.be](https://www.youtube.com/watch?v=4yEyLZUEmQ8&feature=youtu.be)
- [https://www.youtube.com/watch?v=T2K11eFepcs](https://www.youtube.com/watch?v=T2K11eFepcs)
- [https://www.youtube.com/watch?v=8vHO-tFx3K0](https://www.youtube.com/watch?v=8vHO-tFx3K0)

Euclid’s Proof:
- [https://www.youtube.com/watch?v=k2F56Vvlavs](https://www.youtube.com/watch?v=k2F56Vvlavs)
- [https://www.youtube.com/watch?v=nxi8gV6_50o](https://www.youtube.com/watch?v=nxi8gV6_50o)

Leonardo da Vinci’s Proof:
- [https://www.youtube.com/watch?v=70rJRV12MXM](https://www.youtube.com/watch?v=70rJRV12MXM)
- [https://www.youtube.com/watch?v=fACgdCHgv9I](https://www.youtube.com/watch?v=fACgdCHgv9I)
Algebraic Proofs

The “popular” algebraic proof:
- https://www.youtube.com/watch?v=BNCj-K2hd_k
- https://www.youtube.com/watch?v=VjI4ItotC2o

James Garfield’s Proof:
- https://www.youtube.com/watch?v=M-icQsRo4E8
- https://www.youtube.com/watch?v=tVwOSG4fXqM

Another algebraic proof:
- Proof #3: https://www.cut-the-knot.org/pythagoras/#3
Animated Proofs

Three proofs:

- [https://www.youtube.com/watch?v=YompsDlEdtc](https://www.youtube.com/watch?v=YompsDlEdtc)

An Origami Proof:

- [https://www.youtube.com/watch?v=z6lL83wl31E](https://www.youtube.com/watch?v=z6lL83wl31E)

Moving objects proofs:

- [https://www.youtube.com/watch?v=6HbmSRUOuDE](https://www.youtube.com/watch?v=6HbmSRUOuDE)
- [https://www.youtube.com/watch?v=odfhFSnLaaw](https://www.youtube.com/watch?v=odfhFSnLaaw)
- [https://www.youtube.com/watch?v=O1L86rJWkBc](https://www.youtube.com/watch?v=O1L86rJWkBc)

6 proofs without words:

- [https://www.youtube.com/watch?v=COkhrDbNcuA](https://www.youtube.com/watch?v=COkhrDbNcuA)
Texts About Proofs

Other proofs:

http://jwilson.coe.uga.edu/EMT668/EMT668.Student.Folders/HeadAngela/essay1/Pythagorean.html

122 proofs:

http://www.cut-the-knot.org/pythagoras/

More about the Theorem and its proofs:

https://en.wikipedia.org/wiki/Pythagorean_theorem
The Pythagorean Tree

The construction of the Pythagoras tree begins with a square. Upon this square are constructed two squares, each scaled down by a linear factor of $\sqrt{2}/2$, such that the corners of the squares coincide pairwise. The same procedure is then applied recursively to the two smaller squares, ad infinitum.

https://en.wikipedia.org/wiki/Pythagoras_tree_(fractal)#/media/File:Pythagoras_tree_1_1_13.svg

https://en.wikipedia.org/wiki/Pythagoras_tree_(fractal)#/media/File:Pythagoras_Tree_Colored.png

https://www.youtube.com/watch?v=0Ih8LuIJ_go
The Pythagorean Trigonometric Identity

- Let $\theta$ be the angle between the side $a$ and the hypotenuse $c$.
- Then by definition $\sin \theta = b/c$ and $\cos \theta = a/c$.
- Consequently,
  \[
  \sin^2(\theta) + \cos^2(\theta) = \left(\frac{b}{c}\right)^2 + \left(\frac{a}{c}\right)^2 = \frac{a^2 + b^2}{c^2}
  \]
- Therefore,
  \[
  \sin^2(\theta) + \cos^2(\theta) = 1 \iff c^2 = a^2 + b^2
  \]
The Pythagorean Trigonometric Identity

Let $\theta$ be the angle between the side $a$ and the hypotenuse $c$.
Then by definition $\sin \theta = b/c$ and $\cos \theta = a/c$.
Consequently,

$$\sin^2(\theta) + \cos^2(\theta) = \left(\frac{b}{c}\right)^2 + \left(\frac{a}{c}\right)^2 = \frac{a^2 + b^2}{c^2}$$

Therefore,

$$\sin^2(\theta) + \cos^2(\theta) = 1 \iff c^2 = a^2 + b^2$$

https://www.youtube.com/watch?v=MyO2MFJbfi4
https://www.youtube.com/watch?v=Zb0An8dxDas
False Proofs

\[ a = b \] for two real numbers \( a > b \):

\[
\begin{align*}
    a &= b + c \\
    (a - b)a &= (a - b)(b + c) \\
    a^2 - ab &= ab + ac - b^2 - bc \\
    a^2 - ab - ac &= ab - b^2 - bc \\
    a(a - b - c) &= b(a - b - c) \\
    a &= b
\end{align*}
\]

What is wrong?

Division by zero is forbidden!
False Proofs

$a = b$ for two real numbers $a > b$:

\[
\begin{align*}
    a &= b + c \\
    (a - b)a &= (a - b)(b + c) \\
    a^2 - ab &= ab + ac - b^2 - bc \\
    a^2 - ab - ac &= ab - b^2 - bc \\
    a(a - b - c) &= b(a - b - c) \\
    a &= b
\end{align*}
\]

What is wrong?

- Division by zero is **forbidden**!
False Proofs

2 + 2 = 5:

https://www.youtube.com/watch?v=7eEUjvd3_I4

What is wrong?

(−a)^2 = a^2 doesn't imply that −a = a!

0 = 1:

https://www.youtube.com/watch?v=aOxMTgCORhA

What is wrong?

Cannot manipulate a non-convergent infinite sequence!

Amotz Bar-Noy (Brooklyn College)
False Proofs

2 + 2 = 5:

https://www.youtube.com/watch?v=7eEUjvd3_I4

What is wrong?

(-a)^2 = a^2 doesn’t imply that -a = a!
### False Proofs

#### 2 + 2 = 5:
- [https://www.youtube.com/watch?v=7eEUjvd3_I4](https://www.youtube.com/watch?v=7eEUjvd3_I4)

**What is wrong?**
- \((-a)^2 = a^2\) doesn’t imply that \(-a = a\)!

#### 0 = 1:
- [https://www.youtube.com/watch?v=aOxMTgCORhA](https://www.youtube.com/watch?v=aOxMTgCORhA)

**What is wrong?**
- Cannot manipulate a non-convergent infinite sequence!
False Proofs

2 + 2 = 5:

https://www.youtube.com/watch?v=7eEUjvd3_I4

What is wrong?

(-a)^2 = a^2 doesn’t imply that -a = a!

0 = 1:

https://www.youtube.com/watch?v=aOxMTgCORhA

What is wrong?

Cannot manipulate a non-convergent infinite sequence!
False Proofs

2 = 0:
- [link](https://www.youtube.com/watch?v=lirvvZzbJkU)

3 = 0:
- [link](https://www.youtube.com/watch?v=SGUZ-8ul0xM&feature=youtu.be)