Discrete Structures: Introduction to Proofs

Amotz Bar-Noy

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

Five out of many definitions

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.
A story

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 itself.

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

Some history

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

End of Proof

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

Videos

- What is QED? https://www.youtube.com/watch?v=U6FmQP7fQw8
- Quite Easily Done: https://www.youtube.com/watch?v=oTkQD65XMwg
Cartoons


Some Major Techniques

Direct proofs: by construction and/or by exhaustion

Proof by contradiction

Proof by contrapositive

Proof by induction
Some Major Techniques

Direct proofs: by construction and/or by exhaustion
- **Goal**: prove that $P$ implies $Q$.
- Assume $P$ is true.
- Demonstrate that $Q$ **must** follow from $P$.

Proof by contradiction

Proof by contrapositive

Proof by induction
Some Major Techniques

Direct proofs: by construction and/or by exhaustion

Proof by contradiction
- **Goal**: prove that $P$ is true.
- Assume $P$ is false.
- Demonstrate a *contradiction*.

Proof by contrapositive

Proof by induction
Some Major Techniques

Direct proofs: by construction and/or by exhaustion

Proof by contradiction

Proof by contrapositive

- **Goal:** prove that \( P \) implies \( Q \).
- Assume \( Q \) is false.
- Demonstrate that \( P \) is false must follow from \( Q \) is false.
- Observe that (\( P \) is true implies \( Q \) is true) if-and-only-if (\( Q \) is false implies \( P \) is false).

Proof by induction
Some Major Techniques

Direct proofs: by construction and/or by exhaustion

Proof by contradiction

Proof by contrapositive

Proof by induction

- **Goal:** prove $P \implies Q$ for $P, Q$ as functions of some ordered set $S$.
- **Basis:** show $P \implies Q$ is valid for a specific element $k \in S$.
- **Inductive Hypothesis:** Assume $P \implies Q$ for some element $n \in S$.
- **Inductive step:** Demonstrate $P \implies Q$ for the element $n + 1$.
- Conclude $P \implies Q$ for all elements greater than or equal to $k$ in $S$. 
Resources

Lectures about logic & proofs from “Introduction to Higher Math”:

- **Problem Solving:**
  www.youtube.com/watch?v=CMWFmjlB8v0&list=PLZzHxk_TPOStgPtqRZ6KzmkUQBQ8TSWVX&index=1

- **Introduction to Proofs:**
  www.youtube.com/watch?v=_x65OJU8Uq4&index=2&list=PLZzHxk_TPOStgPtqRZ6KzmkUQBQ8TSWVX

- **Propositional Logic:**
  www.youtube.com/watch?v=3kzhDsSzKCU&index=3&list=PLZzHxk_TPOStgPtqRZ6KzmkUQBQ8TSWVX

- **Proof Techniques:**
  www.youtube.com/watch?v=WSb9q4Rj2Bg&index=4&list=PLZzHxk_TPOStgPtqRZ6KzmkUQBQ8TSWVX
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=YDKBEOrMuy8&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
A text book

- Section 1.7: “Introduction to Proofs” (pages 80-90):
  

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
A “Trivial” Proof

Theorem
- $n^2 \geq n$ for all integers $n$.

Examples
- $0^2 = 0 \geq 0$.
- $(-1)^2 = 1^2 = 1 \geq 1 > -1$.
- $(-2)^2 = 2^2 = 4 > 2 > -2$.

Proof
- Prove by case analysis:
  * $n^2 > 0 > n$ for $n \leq -1$.
  * $0^2 = 0 \geq 0 = n$ for $n = 0$.
  * $n \geq 1 \Rightarrow n \cdot n \geq n \cdot 1 \Rightarrow n^2 \geq n$ for $n \geq 1$.
- Q.E.D.
A “Non-Trivial” Proof

Theorem

- \( n^2 \) is the maximum possible product of two positive integers \( h \leq k \) such that \( h + k = 2n \).

Example: \( n = 6 \)

- For \( h = 1 \) and \( k = 11 \) the product is \( 11 = 1 \times 11 \).
- For \( h = 2 \) and \( k = 10 \) the product is \( 20 = 2 \times 10 \).
- For \( h = 3 \) and \( k = 9 \) the product is \( 27 = 3 \times 9 \).
- For \( h = 4 \) and \( k = 8 \) the product is \( 32 = 4 \times 8 \).
- For \( h = 5 \) and \( k = 7 \) the product is \( 35 = 5 \times 7 \).
- For \( h = 6 \) and \( k = 6 \) the product is \( 36 = 6 \times 6 \).
A “Non-Trivial” Proof

**Theorem**

- \( n^2 \) is the maximum possible product of two positive integers \( h \leq k \) such that \( h + k = 2n \).

**Proof**

- Observe that \( k \geq n \) because \( k \geq h \) and \( k \leq 2n - 1 \) since \( h \geq 1 \).
- Assign \( k = n + i \) for \( 0 \leq i \leq n - 1 \).
- Since \( h + k = 2n \), it follows that \( h = n - i \).
- Therefore the product \( h \cdot k \) is
  \[
  (n - i)(n + i) = n^2 - i^2 \leq n^2
  \]
- The last inequality follows because \( i^2 \) is never negative.
- Q.E.D.
A More General Theorem

**Theorem**

\[ \left\lfloor \frac{m}{2} \right\rfloor \times \left\lceil \frac{m}{2} \right\rceil \] is the maximum possible product of two positive integers \( h \leq k \) such that \( h + k = m \).

**Remark**

For an even \( m \) this theorem is the same as the previous theorem.

**Example: \( m = 11 \)**

- For \( h = 1 \) and \( k = 10 \) the product is \( 10 = 1 \times 10 \).
- For \( h = 2 \) and \( k = 9 \) the product is \( 18 = 2 \times 9 \).
- For \( h = 3 \) and \( k = 8 \) the product is \( 24 = 3 \times 8 \).
- For \( h = 4 \) and \( k = 7 \) the product is \( 28 = 4 \times 7 \).
- For \( h = 5 \) and \( k = 6 \) the product is \( 30 = 5 \times 6 \).
Three Classic Proofs

From Hippasus about 2500 years ago
- The square root of 2 is an irrational number

From Euclid about 2300 years ago
- There are infinitely many prime numbers

From Pythagoras about 2550 years ago
- The Pythagorean Theorem
Hippasus’ proof:

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

Another proof

Assume towards \textit{contradiction} that \( \frac{p}{q} = \sqrt{2} \) for two positive integers \( p \) and \( q \) with the smallest possible positive integer \( q \).

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

It follows that
\[
(2q - p)^2 = 4q^2 - 4pq + p^2 = 2p^2 - 4pq + 2q^2 = 2(p - q)^2.
\]

Therefore, \( 2 = \frac{(2q - p)^2}{(p - q)^2} \).

Taking the square root of the equation implies \( \sqrt{2} = \frac{2q - p}{p - q} \).

Note that if \( p \geq 2q \) then \( \frac{p}{q} \geq 2 > \sqrt{2} \).

Therefore, \( p < 2q \) which is equivalent to \( p - q < q \).

A \textit{contradiction} to the minimality assumption about \( q \).
The square root of 2 is an irrational number

Another version of the second proof

- Assume towards **contradiction** that $\frac{p}{q} = \sqrt{2}$ for two positive integers $p$ and $q$ with the smallest possible positive integer $q$.
- $\sqrt{2} > 1$ implies that $q < p$.
- $\sqrt{2} < 2$ implies that $p < 2q$.
- The above inequality is equivalent to $p - q < q$.
- Hence, the fraction $r = \frac{2q - p}{p - q}$ is a fraction of two positive integers whose denominator is smaller than the fraction $\frac{p}{q}$.
- The **contradiction** is established by proving that $r = \sqrt{2}$.

$$r = \frac{2q - p}{p - q} = \frac{2}{\frac{q}{p}} - 1 = \frac{2 - \sqrt{2}}{\sqrt{2} - 1} = \sqrt{2}$$
What about $\sqrt{2}^{\sqrt{2}}$?

Theorem
There exist two irrational numbers $s$ and $t$ such that $s^t$ is rational.

Proof

- If $\sqrt{2}^{\sqrt{2}}$ is rational then set $s = t = \sqrt{2}$.
- Otherwise, set $s = \sqrt{2}^{\sqrt{2}}$ and $t = \sqrt{2}$.

$$s^t = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2} \cdot \sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$$
Resources

The original proof
- https://www.youtube.com/watch?v=sbGjr_aewePE

Five proofs with animation
- https://www.youtube.com/watch?v=zEXcsZo4hOQ

The story of $\sqrt{2}$

Approximating $\sqrt{2}$
- https://www.youtube.com/watch?v=f1yDExNAEMg&feature=youtu.be

Videos with longer explanations
- Original proof: https://www.youtube.com/watch?v=rOGqq1OlrzI&feature=youtu.be
- Original proof: https://www.youtube.com/watch?v=TwNfWgMHFmI
- Second proof: https://www.youtube.com/watch?v=VeZleYkcFus
There are infinitely many prime numbers

Euclid’s proof

- Let $p_1 < p_2 < \cdots < p_n$ be $n$ prime numbers.
- 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 prime numbers.
  - The Fundamental Theorem of Arithmetic.

None of these prime numbers can be $p_1, \ldots, p_n$ because each one of them divides $Q - 1$.

Therefore, the prime factors of $Q$ are new prime numbers.

The above process can continue forever to find infinitely many prime numbers.
There are infinitely many prime numbers

A similar proof

- Assume towards contradiction that $p$ is the largest prime number.
- Let $Q = p! + 1$.
- If $Q$ is a prime, then a new prime is found.
- Otherwise, $Q$ is a product of two or more prime numbers.
  - The Fundamental Theorem of Arithmetic.
- None of the numbers 2, 3, ..., $p$ can divide $Q$ because each one of them divides $Q - 1$.
- Therefore, the prime factors of $Q$ are larger than $p$.
- A contradiction to the assumption about $p$. 
Resources

The original proof by Euclid

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

The second proof

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

Illustrations
- https://miro.medium.com/max/700/1*SsN2DG__Z5DyOI0uf7hbwQ.png
- https://image.shutterstock.com/shutterstock/photos/754219900/display_1500/photo.jpg

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

An “experimental” proof
- https://www.youtube.com/watch?v=CAkMUdeB06o
- https://www.youtube.com/watch?v=_e6w5GtkcGI
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=T2K1leFepcs
- https://www.youtube.com/watch?v=8vHO-tFx3K0

Euclid’s Proof
- 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=fACgdCHgv9I
Algebraic Proofs

The “popular” algebraic proof
- https://www.youtube.com/watch?v=BNCj-K2hd_k
- https://www.youtube.com/watch?v=VjI4LtotC2o

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

An Origami Proof
- https://www.youtube.com/watch?v=z6lL83w131E

Moving objects proofs
- https://www.youtube.com/watch?v=6HbmSRU0uDE
- https://www.youtube.com/watch?v=odfhF5nLaaw
- https://www.youtube.com/watch?v=o1L86rJWkBc

Six proofs without words
- https://www.youtube.com/watch?v=COkhrDbNcuA

Proofs and beyond
- https://www.youtube.com/watch?v=p-0SOwBzUYI
370 proofs from 900 B.C. to 1940 A.D.

- An 1940 book: “The Pythagorean Proposition” by Elisha S. Loonis
  

Online list of 122 proofs

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

Some proofs

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

Wikipedia: More about the Theorem and its proofs

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

Constructing the 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.

Resources

- https://en.wikipedia.org/wiki/Pythagoras_tree_(fractal)#/media/File:Pythagoras_tree_1_1_13.svg
- https://www.youtube.com/watch?v=0Ih8LuIJ_go
The 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,
  \[
  \sin^2(\theta) + \cos^2(\theta) = 1 \iff c^2 = a^2 + b^2
  \]

Resources

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

1 = 2

\[
\begin{align*}
a &= b \\
a^2 &= ab \\
a^2 + a^2 &= a^2 + ab \\
2a^2 &= a^2 + ab \\
2a^2 - 2ab &= a^2 + ab - 2ab \\
2a^2 - 2ab &= a^2 - ab \\
2(a^2 - ab) &= 1(a^2 - ab) \\
2 &= 1
\end{align*}
\]

What is wrong?

Division by zero is forbidden!
False Proofs

1 = 2

\[
\begin{align*}
a &= b \\
a^2 &= ab \\
a^2 + a^2 &= a^2 + ab \\
2a^2 &= a^2 + ab \\
2a^2 - 2ab &= a^2 + ab - 2ab \\
2a^2 - 2ab &= a^2 - ab \\
2(a^2 - ab) &= 1(a^2 - ab) \\
2 &= 1
\end{align*}
\]

What is wrong?

- Division by zero is forbidden!
False Proofs

\[ a = b \text{ for two real numbers } a > b \]

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

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!
False Proofs

2 + 2 = 5

What is wrong?

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

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

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

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 = a² doesn’t imply that −a = a.

0 = 1

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

\[ 2 + 2 = 5 \]

What is wrong?

\[ (\neg a)^2 = a^2 \] doesn’t imply that \( \neg a = a \).

\[ 0 = 1 \]

What is wrong?

Cannot manipulate a non-convergent infinite sequence!
“Harder” to Explain False Proofs

The infinite tower function \( f(x) = x^{x^{x^{\ddots}}} \):

- Find the value of \( x \) for which \( f(x) = 2 \).
- If \( f(x) = a \) then \( x^a = a \).
- For \( a = 2 \) and \( a = 4 \), it follows that \( x = \sqrt{2} \) and therefore \( 2 = 4 \).

https://www.youtube.com/watch?v=DmP3sFIZ0XE&feature=youtu.be

What is wrong?

- The monotonically increasing function \( f(x) \) converges only for \( \frac{1}{e^e} \leq x \leq e^{\frac{1}{e}} \). Consequently, \( a \) cannot be \( 4 \geq e \).

Two more “tricky” examples

- \( 2 = 0 \): https://www.youtube.com/watch?v=lirvvZzbJkU
- \( 3 = 0 \): https://www.youtube.com/watch?v=SGUZ-8u10xM&feature=youtu.be