Proofs

UC Berkeley – Summer 2025 – Steve Tate

Lecture 2

Note 2 / Lecture 2

Proofs!!!

Note 2 / Lecture 2

Proofs!!!

Note 2 / Lecture 2

Proofs!!!

Why Proofs?

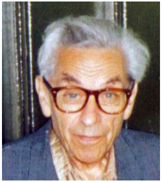
The objectives in creating a proof:

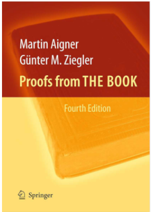
- Logical correctness that establishes truth of a claim
- Clarity – *why* it's true – often seems obvious in retrospect
- Beauty that comes from elegance and simplicity

“God has the Big Book, the beautiful proofs of mathematical theorems are listed here.”

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

— Paul Erdös





“Proofs from THE BOOK” – a collection of beautiful and elegant proofs.

About Proofs

"But I just want to write programs.."

- Building a habit of clarity of thought is broadly applicable
- Writing *correct* programs "is a good thing"
- *Writing proofs and writing programs are the same!*
  $\Rightarrow$ Curry-Howard Correspondence: Proofs $\equiv$ Programs!

Some broad tips on writing proofs:

- Start from definitions - *write them out!*
- Can work from both ends (claim to conclusion or vice-versa)
  $\Rightarrow$ Be careful not to assume the conclusion though!
- Consider your first (and second...) attempt a draft – refine!
  $\Rightarrow$ Seek elegance ("make things as simple as possible, but no simpler")
- *How To Prove It*: good book all about how to write proofs

Note 2 / Lecture 2

Proofs!!!

1. By Example (or Counterexample)
2. Direct (Prove $P \implies Q$: assume P, show Q)
3. By Contraposition (Prove $P \implies Q$ by proving $\neg Q \implies \neg P$)
4. By Contradiction (Prove P: assume $\neg P$ and reach a contradiction)
5. By Cases (enumerate an exhaustive set of cases)

Proof by Example

Existentially-quantified statements

General form: $\exists x\, P(x)$

How to prove? Identify an x that works – *and show it does!*

Theorem: $(\exists x \in \mathbb{N})(x = x^2)$

Proof: Let $x = 0$. *[Identify an x that works ...]*
Then $x = 0$ and $x^2 = 0$, so $x = x^2$. *[... and show it does]* □

What the heck is that □ ???

$\Rightarrow$ *Marks the end of a proof – like “Q.E.D.”*

Proof by Example

Negated universally-quantified statements

We want to prove that $x^2 - 10x + 28$ is *not* ≥ 4 for all $x \in \mathbb{Z}$

Let's try some values:

$$\begin{aligned} x = 0 &\;\rightarrow\; 0^2 - 10 \cdot 0 + 28 = 28 \\ x = 3 &\;\rightarrow\; 3^2 - 10 \cdot 3 + 28 = 9 - 30 + 28 = 7 \\ x = 8 &\;\rightarrow\; 8^2 - 10 \cdot 8 + 28 = 64 - 80 + 28 = 12 \end{aligned}$$

but... not *always!*

Theorem: $\neg(\forall x \in \mathbb{Z})\ (x^2 - 10x + 28 \geq 4)$

Note: This is equivalent to $(\exists x)\ (x^2 - 10x + 28 < 4)$ *– proof by example!*

Proof: Let $x = 5$. Then

$x^2 - 10x + 28 = 5^2 - 10 \cdot 5 + 28 = 25 - 50 + 28 = 3 < 4.$ □

A Brief Interlude For Some Definitions

More interesting proofs require some more interesting concepts...

Definition: We say "a divides b," and write $a \mid b$, iff $(\exists q \in \mathbb{Z})\ b = q\,a$.

Equivalent statements: "b is divisible by a" or "a divides evenly into b" or "b is a multiple of a"

Quick concept check:

$2 \mid 4$? Yes! (because $q = 2$ gives $4 = 2 \cdot 2$)

$7 \mid 23$? No!

$4 \mid 2$? No!

$3 \mid 15$? Yes! (because $q = 5$ gives $15 = 3 \cdot 5$)

Some definitions related to divisibility:

An integer x is even if and only if $2 \mid x$ (or $x = 2k$ for some $k \in \mathbb{Z}$)

An integer x is odd if and only if $x = 2k + 1$ for some $k \in \mathbb{Z}$

A Brief Interlude For Some More Definitions

Definition: A natural number $n > 1$ is **composite** if $n = ab$ for $a, b \in \mathbb{N}$ with $2 \leq a, b \leq n-1$.

Definition: A natural number $p > 1$ is **prime** if it is not composite (or: it is divisible only by 1 and itself).

Definition: A set S is closed under binary operator $\circ$ if $(\forall a, b \in S)(a \circ b \in S)$.

Quick concept check:

Are the natural numbers closed under addition? Yes!

Are the natural numbers closed under subtraction? No!

Are the integers closed under subtraction? Yes!

Are the integers closed under multiplication? Yes!

Are the integers closed under division? No!

Direct Proof

General form: Prove $P \implies Q$ by assuming P and showing Q

Theorem: For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$ then $a \mid (b - c)$.

Proof: Assume $a \mid b$ and $a \mid c$, so there exist $q, q' \in \mathbb{Z}$ such that $b = qa$ and $c = q'a$. Then $b - c = qa - q'a = (q - q')a$. Since $\mathbb{Z}$ is closed under subtraction, $q - q' \in \mathbb{Z}$, so $a \mid (b - c)$. □

Let's break this proof down:

Assume P

Use definitions

Do some algebra

Use properties of integers

Therefore Q (using definitions again!)

Another Direct Proof

Theorem: Let D_3 be the set of 3-digit natural numbers. For all $n \in D_3$, if the alternating sum of digits of n is divisible by 11, than $11|n$.

The "alternating sum" alternates adding and subtracting.

Logically: $\forall n \in D_3\big((11\,|\,\text{alt. sum of digits of } n) \implies 11\,|\,n\big)$

Examples:

$n = 121$: Alt Sum: $1 - 2 + 1 = 0$. Divisible by 11, as is 121.

$n = 605$: Alt Sum: $6 - 0 + 5 = 11$. Divisible by 11, as is $605 = 11 \cdot 55$.

Proof: For $n \in D_3$, let a, b, c be the three decimal digits in n, so $n = 100a + 10b + c$. Assuming 11 divides the alternating sum of the digits, we have $a - b + c = 11k$ for some $k \in \mathbb{Z}$.

Add $99a + 11b$ to both sides, to get

$$100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b)$$

The LHS is n, and $k + 9a + b$ on the RHS side is an integer, so $11\,|\,n$. □

Assumed P $(11\,|\,a - b + c)$. Proved Q $(11\,|\,n)$.

What About The Converse?

The converse is:

Theorem: $\forall n \in D_3, \big((11 \mid n) \implies (11 \mid \text{alt. sum of digits of } n)\big)$

Example: $n = 264$. $11 \mid n$ (since $264 = 11 \cdot 24$), and $11 \mid (2 - 6 + 4)$

Proof: Assume $11 \mid n$, so $n = 11k$ for some $k \in \mathbb{Z}$, and if a, b, c represent the decimal digits of n, then $100a + 10b + c = 11k$. Then

$$\begin{aligned} n = 100a + 10b + c = 11k &\implies \\ 99a + 11b + (a - b + c) = 11k &\implies \\ a - b + c = 11k - 99a - 11b &\implies \\ a - b + c = 11(k - 9a - b) & \end{aligned}$$

$a - b + c$ is the alternating sum of the digits of n, and $k - 9a - b$ is an integer, so we conclude that $11 \mid$ alt. sum of digits of n. □

Note: Make the logic clear! Include $\implies$ (or $\impliedby$ or $\iff$). Don't just write algebraic formulas with no connectives. *Break bad high school proof habits!*

In this case, every $\implies$ could be $\iff$ (proving both directions at once).

Another Proof?

Or: Just because something is true doesn't mean all "proofs" are valid!

Theorem: $\forall n \in D_3, \big((11 \mid n) \implies (11|\text{alt. sum of digits of } n)\big)$

"Proof": Assume $11 \mid n$, so $n = 11k$ for some $k \in \mathbb{Z}$, and if a, b, c represent the decimal digits of n.

Now, let's calculate the alternating sum of digits:

Alternating sum $= a - b + c$

Since $n = 11k$, we have: $a - b + c = 11k$

This shows that the alternating sum of digits is equal to 11 times some integer k, and therefore, it is divisible by 11. *QED*?

What's wrong with this?

This just popped up out of nowhere with no justification.

Happens more than you might expect: the prover knows where they want to end up, and just write it down.

"Proof by stating confidently" is not legit (ChatGPT "proof"?)

Proof by Contraposition

Theorem: For $d, n \in \mathbb{N}$ with $d \mid n$, if n is odd then d is odd.

Try direct – what do we know/assume? $n = kd$ and $n = 2k' + 1$ for $k, k' \in \mathbb{Z}$

Now what???

If stuck with $P \implies Q$, try (the logically equivalent) $\neg Q \implies \neg P$.

Contrapositive: For $d, n \in \mathbb{N}$ with $d \mid n$, if d is even then n is even.

$\Rightarrow$ Contrapositives are straightforward, so you don't need to explicitly give this.

Proof: We proceed by contraposition. Assume d is even, so $d = 2k$ for some $k \in \mathbb{Z}$. Since $d \mid n$, there is a $k' \in \mathbb{Z}$ such that $n = dk' = (2k)k' = 2(kk')$. Since kk' is an integer, so we conclude that n is even. □

Another Contraposition

Theorem: For every $n \in \mathbb{N}$, if n^2 is even then n is even.

Try direct – what do we know/assume? $n^2 = 2k$ for some $k \in \mathbb{Z}$, so $n = \sqrt{2k}$

Now what??? Show $\sqrt{2k}$ is even?!?!?

Proof: We proceed by contraposition. Assume n is odd, so $n = 2k+1$ for some $k \in \mathbb{Z}$. Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Since $2k^2 + 2k$ is an integer, we conclude that n^2 is odd. □

Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.

Must show: $\forall a, b \in \mathbb{Z}$, $\frac{a}{b} \neq \sqrt{2}$

Proof by example? Direct? Contraposition? *None seem to work...*

New technique: proof by contradiction. General idea:

Theorem: P.

Assume for the sake of contradiction: $\neg P$.

Show $\neg P \implies P_1 \cdots \implies R$ (all valid derivations)

Show $\neg P \implies Q_1 \cdots \implies \neg R$ (all valid derivations)

So $R \wedge \neg R$ – impossible! So original assumption cannot be true.

$\neg P$ is false, so P is true. □

Assuming is dangerous – make sure you are clear!

Contradiction – Back To The Proof!

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume of the sake of contradiction that $\sqrt{2}$ is rational, so there exist integers $a, b \in \mathbb{Z}$ such that $\sqrt{2} = a/b$ and a/b is in reduced form (i.e., a and b have no common factors). Then

$$\sqrt{2} = a/b \implies \sqrt{2}b = a \implies 2b^2 = a^2$$

b^2 is an integer, so a^2 is 2 times an integer – so a^2 is even. Since a^2 is even, a is even (we just proved this!), so say $a = 2k$ for $k \in \mathbb{Z}$.

Then $2b^2 = a^2 = (2k)^2 = 4k^2$, which implies $b^2 = 2k^2$. Therefore, b^2 is even, and then so is b. We have concluded that both a and b are even, which means they are both divisible by 2. This is impossible if they share no common factors. Contradiction! Therefore, $\sqrt{2}$ is irrational. □

$$\left.\begin{array}{l} R = \text{"}a\text{ and }b\text{ have no common factor"} \\ \neg R = \text{"}a\text{ and }b\text{ have a common factor"} \end{array}\right\} \textbf{Contradiction!}$$

Proof by Contradiction: Another Example

Theorem: There are infinitely many primes.

Proof: Assume for the sake of contradiction that there are finitely many primes, namely $p_1, \ldots, p_k$. Consider

$$q = p_1 \times p_2 \times \cdots p_k + 1.$$

q cannot be one of the primes as it is larger than any p_i. Since q is not prime, it has prime divisor $p > 1$, with $p \mid q$.

Since p is prime, it must be one of the p_i, and so if we define $r = p_1 \times p_2 \times \cdots p_k$ then $p \mid r$.

Since $p \mid q$ and $p \mid r$, we have $p \mid (q - r)$ (we proved this earlier!). However $q - r = 1$, so $p \leq 1$ which contradicts the fact that p is prime.
Therefore there are infinitely many primes. □

$$\left.\begin{array}{l} R = \text{“}p > 1\text{”} \\ \neg R = \text{“}p \leq 1\text{”} \end{array}\right\} \textbf{Contradiction!}$$

Product of first k primes..

Did we prove?

- "The product of the first k primes plus 1 is prime."
- No! The chain of reasoning started with a false statement.

Consider this example:

- $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$
- There is a prime *in between* 13 and $q = 30031$ that divides q.
- Proof assumed no primes *in between* p_k and q
  As it assumed the only primes were the first k primes

Proof By Cases (“divide-and-conquer” strategy)

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof: Follows from this:

Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in \mathbb{Z}$, then both a and b are even.

Theorem exhibits the same issue as the $\sqrt{2}$ proof – do you see it?

Proof (sketch) of lemma: Assume a solution of the form a/b.

$$\left(\frac{a}{b}\right)^5 - \frac{a}{b} + 1 = 0 \quad \Longrightarrow \quad a^5 - ab^4 + b^5 = 0$$

Consider possibilities for LHS of the last equation, for a and b:

Case 1: a odd, b odd: odd - odd + odd. Must be odd, so can’t be zero.
Case 2: a even, b odd: even - even + odd. Must be odd, so can’t be zero.
Case 3: a odd, b even: odd - even + even. Must be odd, so can’t be zero.
Case 4: a even, b even: even - even + even. Possible.

The fourth case is the only one possible, so the lemma follows. □

Proof By Cases – Another Example

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

Proof: Consider $\sqrt{2}^{\sqrt{2}}$.

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Done! Theorem holds with $x = y = \sqrt{2}$.
Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Let $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$, and consider

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}*\sqrt{2}} = \sqrt{2}^2 = 2.$$

Thus we have irrational x and y with a rational x^y (i.e., 2).

One of the cases must hold, so theorem holds. □

Note: If we knew whether $\sqrt{2}^{\sqrt{2}}$ is rational, we wouldn't need cases.

It actually *is* irrational, but proving that is complicated – and we can prove this result without needing to know!

Bad Proof! Be Careful!

Theorem: $3 = 4$.

"Proof": Assume $3 = 4$. Start with $12 = 12$.
Divide one side by 3 and the other by 4 to get $4 = 3$.
By commutativity the theorem holds. □

Don't assume what you want to prove!

Theorem: $1 = 2$.

"Proof": For variables x and y with $x = y$, we have

$$
\begin{aligned}
&(x^2 - xy) = x^2 - y^2 \\
\implies \quad & x(x-y) = (x+y)(x-y) \\
\implies \quad & x = (x+y) \\
\implies \quad & x = 2x \\
\implies \quad & 1 = 2
\end{aligned}
$$

□

Dividing by zero is no good.

Related: Beware of multiplying inequalities by a negative.

Summary

By Example:
To Prove: $(\exists x)P(x)$. Give such an x and prove $P(x)$.

Direct Proof:
To Prove: $P \implies Q$. Assume P. Reason forward, prove Q.

By Contraposition:
To Prove: $P \implies Q$. Assume $\neg Q$. Prove $\neg P$.

By Contradiction:
To Prove: P Assume $\neg P$. Find a contradiction showing $\neg P$ is false.

By Cases: informal.
Universal: show that statement holds in all cases.
Existence: used cases where one is true.
Either $\sqrt{2}$ and $\sqrt{2}$ worked.
or $\sqrt{2}$ and $\sqrt{2}^{\sqrt{2}}$ worked.

Careful when proving!
Don't assume the theorem or divide by zero. Watch out for converse.