-from MIT OCW 6.042J Week 1, date: August 19, 2025

1. What is a Proof?

A proof is...
a method of ascertaining truth
↳ differs among fields
Ex.) • Legal truth.
based on allowable evidence ← presented at trial
• Authoritative truth
by a trusted person or organization
• Scientific truth
hypothesized, and confirmed or refuted by experiments
• Probable truth
obtained from statiscal analysis
ex) public opinion
• Philosophical proof
involves careful exposition and persuasion based on consistency and plausibility
ex) "Cogito ergo sum" ("I think, therefore I am.")

in Mathematics...
A formal proof of a proposition is a chain of logical deductions leading to the proposition from a base set of axioms.

2. Propositions

A proposition is...
a statement that is either true or false.
↳ especially:
Mathematically meaningful propositions must be
• about well-defined mathematical objects
(like numbers, sets, functions, relations, etc.)
• stated using mathematically meaningful terminology
(like "AND" and "FORALL")

Ex.)

Proposition 2.1 $2+3=5$ $\Rightarrow$ True

Proposition 2.2

Let $p(n) := n^2+n+41$.

$\forall n \in \mathbb{N}.\ p(n)$ is a prime number.

($\forall$: is read "for all"

$\mathbb{N}$: the set of natural numbers $(0, 1, 2, 3, \dots)$)

$\Rightarrow$ False!

why? : if $n=40$, then $p(n) = 40^2+40+41 = 41 \cdot 41$ ← not prime!

$\therefore p(n)$ is not prime for all!

Proposition 2.3

$a^4+b^4+c^4=d^4$ has no solution when a, b, c, d are positive integers.

In logical notation, letting $\mathbb{Z}^+$ denote the positive integers, we have

$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \forall c \in \mathbb{Z}^+ \forall d \in \mathbb{Z}^+.\ a^4+b^4+c^4 \neq d^4$.

↳ $\forall a, b, c, d \in \mathbb{Z}^+.\ a^4+b^4+c^4 \neq d^4$.

$\Rightarrow$ True!

the solution: $a=95800,\ b=217519,\ c=414560,\ d=422481$

(found by Noam Elkies)

Proposition 2.4

$\exists z \exists (x^3+y^3) = z^3$ has no solution when $x, y, z \in \mathbb{N}$

$\Rightarrow$ False.

Proposition 2.5

Every map can be with 4 colors so that adjacent regions have different colors.

$\Rightarrow$ True

↳ known as "four-color theorem"

Proposition 2.6 (Goldbach)

Every even integer greater than 2 is the sum of two primes.

$\Rightarrow$ No one knows whether this proposition is true or false

↳ "Goldbach Conjecture"

* this lecture was in 2005, but this is still an unsolved issue.

3. The Axiomatic Method

The standard procedure for establishing Truth in mathematics
↳ invented by Euclid
↳ begin with five assumptions about geometry : seemed undeniable based on direct experience
(ex) "There is a straight line segment between every pair of points.")
Propositions like these that are simply accepted as true ··· axioms

A proof is...
a sequence of logical deductions from axioms and previously-proved statements that concludes with the proposition in question

Common terms for a proposition that has been proved:
- theorems : important propositions
- a lemma : a preliminary proposition useful for proving later propositions
- a corollary : an afterthought, a proposition that follows in just a few logical steps from a theorem

※ these definitions are not precise
↳ a good lemma turns out to be far more important than the theorem it was originally used to prove

the axiomatic method :
- Euclid's axiom-and-proof approach
- the foundation for mathematics today

↳ just a handful of axioms (ZFC) and a few logical deduction rules with them are enough to derive essentially all of mathematics

3.1 Our Axioms

The ZFC axioms are
- important in studying and justifying the foundations of Mathematics.
- × much too primitive for practical purposes
  ↳ (ex) proving that 2+2=4 requires more than 20,000 steps!

→ we're going to take a huge set of axioms

No. 4

Date

3.2 Proofs in Practice

many proofs follow one of a handful of standard templates!
→ we'll...
1. go through several of these standard patterns
2. learn more sophisticated proof techniques

The ZFC Axioms
- the axioms of Zermelo-Frankel Set Theory

Extensionality

Two sets are equal if they have the same members.
In formal logical notation, this would be stated as:
$(\forall z.(z \in x \longleftrightarrow z \in y)) \longrightarrow x = y$.

Pairing

For any two sets x and y, there is a set, $\{x, y\}$, with x and y as its only elements.

Union

The union of a collection, z, of sets is also a set.
$\exists u \forall x.(\exists y.x \in y \wedge y \in z) \longleftrightarrow x \in u$.

Infinity

There is an infinite set; specifically, a nonempty set, x, such that for any set $y \in x$, the set $\{y\}$ is also a member of x.

Subset

Given any set, x, and any proposition $P(y)$, there is a set containing precisely those elements $y \in x$ for which $P(y)$ holds.

Power Set

All the subsets of a set form another set.

Replacement

The image of a set under a function is a set.

Foundation

For every non-empty set, x, there is a set $y \in x$ such that x and y are disjoint.
(In particular, this axiom prevents a set from being a member of itself.)

Choice

We can choose one element form each set in a collection of nonempty sets. More precisely,

if f is a function on a set, and the result of applying f to any element in the set is always a nonempty set, then there is a "choice" function g such that $g(y) \in y$ for every y in the set.

4. Proving an Implication

4.1 Method #1

In order to prove that P implies Q:

1. Write "Assume P."
2. Show that Q logically follows.

Example

Theorem 4.1. if $0 \le x \le 2$, then $-x^3 + 4x + 1 > 0$.

Proof Assume $0 \le x \le 2$.

Then x, $2-x$, and $2+x$ are all nonnegative.

Therefore, the product of these terms is also nonnegative. Adding 1 to this product gives a positive number, so:

$$x(2-x)(2+x) + 1 > 0$$

Multiplying out on the left side proves that

$$-x^3 + 4x + 1 > 0$$

as claimed. □

Points

- Trying to figure out the logical steps of a proof, doing some scratchwork is meaningful. But we must keep our scratchwork separate from our final proof.
- Proofs typically...
  - begin with the word "Proof."
  - end with some sort of doohickey like □ or "q.e.d."

4.2 Method #2 - Prove the Contrapositive

An implication ("P implies Q") is logically equivalent to its contrapositive "not Q implies not P"; proving one is as good as proving the other. And often proving the contrapositive is easier than proving the original the original statement.

1. Write "We prove the contrapositive:" and then state the contrapositive.
2. Proceed as in Method #1.

→

→

Example

Theorem 4.2. if r is irrational, then $\sqrt{r}$ is also irrational.

Proof. We prove the contrapositive: if $\sqrt{r}$ is rational, then r is rational.

Assume that $\sqrt{r}$ is rational. Then there exists integers a and b such that:

$$\sqrt{r} = \frac{a}{b}$$

Squaring both sides gives:

$$r = \frac{a^2}{b^2}$$

Since a^2 and b^2 are integers, r is also rational. □

5. Proving an "If and Only If"

5.1 Method #1: Prove Each Statement Implies the Other

The statement "P if and only if Q" is equivalent to the two statements "P implies Q" and "Q implies P." So, to prove an "if and only if":

1. Write, "We prove P implies Q and vice-versa."
2. Write, "First, we show P implies Q." Do this by one of the methods in Section 4.
3. Write, "Now, we show Q implies P." Again, do this by one of the methods in Section 4.

Example

Theorem 5.1 (DeMorgan's Law for Sets).

Let A, B, and C be sets. Then:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Proof. We show $x \in A \cap (B \cup C)$ implies $x \in (A \cap B) \cup (A \cap C)$ and vice-versa.

First, we show $x \in A \cap (B \cup C)$ implies $x \in (A \cap B) \cup (A \cap C)$.

Assume $x \in A \cap (B \cup C)$. Then x is in A and x is also in B or C.

Thus, x is in either $A \cap B$ or $A \cap C$, which implies $x \in (A \cap B) \cup (A \cap C)$.

Now, we show $x \in (A \cap B) \cup (A \cap C)$ implies $x \in A \cap (B \cup C)$. Assume $x \in (A \cap B) \cup (A \cap C)$.

Then x is in both A and B or else x is in both A and C.

Thus, x is in A and x is also B or C. This implies $x \in A \cap (B \cup C)$. □

5.2 Method #2: Construct a Chain of Iffs

In order to prove that P is true if and only if Q is true:

1. Write, "We construct a chain of if-and-only-if implications."
2. Prove P is equivalent to a second statement which is equivalent to a third statement and so forth until reach Q.

→

Example

Theorem 5.2. The standard deviation of a sequence of values $x_1, \dots, x_n$ is zero if and only if all the values are equal to the mean.

Proof. We construct a chain of "if and only if" implications.

The standard deviation of $x_1, \dots, x_n$ is zero if and only if:

$$\sqrt{(x_1-\mu)^2+(x_2-\mu)^2+\cdots+(x_n-\mu)^2}=0$$

where μ is the average of $x_1, \dots, x_n$. This equation holds if and only if

$$(x_1-\mu)^2+(x_2-\mu)^2+\cdots+(x_n-\mu)^2=0$$

since zero is the only number whose square root is zero. Every term in this equation is nonnegative, so this equation holds if and only every term is actually 0. But this is true if and only if every value x_i is equal to the mean μ. □

6. How to Write Good Proofs

- State your game plan.
  A good proof begins by explaining the general line of reasoning,
  e.g. "We use case analysis." or "We argue by contradiction."
- Keep a linear flow.
  The steps of your argument should follow one another in a sequential order.
- A proof is an essay, not a calculation.
  A good proof usually looks like an essay with some equations thrown in.
  Use complete sentences.
- Avoid excessive symbolism.
  Use words where you reasonably can.
- Simplify.
  A Proof with fewer logical steps is a better proof.
- Introduce notation thoughtfully.
  Sometimes an argument can be greatly simplified by introducing a variable, devising a special notation, or defining a new term.
  - ※ Do this sparingly.
  - ※ Remember to actually define the meanings of new variables, terms, or notations.
- Structure long proofs.
  - Facts needed in your proof that are easily stated, but not readily proved are best pulled out and proved in preliminary lemmas.

→

No. 8

Date

→

- If you are repeating essentially the same argument over and over, try to capture that argument in a general lemma, which you can cite repeatedly instead.
- Don't bully.
  Don't use phrases like "clearly" or "obviously" in an attempt to bully the reader into accepting something which you're having trouble proving.
- Finish.
  Tie everything together yourself and explain why the original claim follows.

↳ the analogy between good proofs and good programs extends beyond structure.

7. Propositional Formulas

7.1 Combining Propositions

7.1.1 "Not", "And" and "Or"

Using truth tables

example: not P

P	not P	
T	F	← P is true ⇒ "not P" is false
F	T	← P is false ⇒ "not P" is true

P and Q

P	Q	P and Q
T	T	T
T	F	F
F	T	F
F	F	F

the proposition "P and Q" is true when...
P and Q are both true.

P or Q

P	Q	P or Q
T	T	T
T	F	T
F	T	T
F	F	F

"P or Q" is true when...
- P is true
- Q is true
- both P and Q are true

7.1.2 "Implies"

"P implies Q" = "if P then Q"

P	Q	P implies Q / if P then Q
T	T	T
T	F	F
F	T	T
F	F	T

7.1.3 "If and Only if" (iff)

P	Q	P if and only Q
T	T	T
T	F	F
F	T	F
F	F	T

"P if and only Q"
= P and Q are logically equivalent
→ either both are true or both are false

7.2 Propositional Logic in Computer Programs

example (from C, C++ or Java:)

```
if (x>0 || (x <= 0 && y > 100))
    :
  (further instructions)
```

↳ || = "or"
&& = "and"
further instructions are carried out only if the proposition following "if" is true

⇒ A or ((not A) and B)

A	B	A or ((not A) and B)	A or B
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

No. 10

Date

7.3 A Cryptic Notation

English	Cryptic Notation
"not P"	$\neg P$ / $\overline{P}$
"P and Q"	$P \wedge Q$
"P or Q"	$P \vee Q$
"P implies Q" or "if P then Q"	$P \longrightarrow Q$
"P if and only if Q"	$P \longleftrightarrow Q$

7.4 Logically Equivalent Implications

the contrapositive of "P implies Q"
... "(not Q) implies (not P)"
↳ precisely equivalent

P	Q	P implies Q	(not Q) implies (not P)
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

the converse of "P implies Q"
... "Q implies P"
↳ not equivalent

P	Q	P implies Q	Q implies P
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

8 Logical Deductions

Logical deductions / inference rule:
used to prove new propositions using previously proved ones.

→

- modus ponens

  a proof of P together with a proof of $P \to Q$ is a proof of Q.

  $$\frac{P,\ P \to Q}{Q}$$

  ↳ the statements above the line (= antecedents) are proved

  ⇒ then we can consider statement below the line (= consequent) to also be proved

- $$\frac{P \to Q,\ Q \to R}{P \to R}$$
- $$\frac{\neg P \to Q,\ \neg Q}{P}$$
- $$\frac{\neg P \to \neg Q}{Q \to P}$$
- $$\frac{\neg P \to \neg Q}{P \to Q}$$

SAT

A proposition is satisfiable if...
same setting of the variables makes the proposition true
→ SAT: the general problem of deciding whether a proposition is satisfiable

Approaches to SAT
1. To construct a truth table and check whether or not a T (true) ever appears
   ↳ not very efficient
   (a proposition with n variables has a truth table with 2^n lines!)

Is there an efficient solution to SAT?

No one knows...