1+1 = 2

do we need a proof?

In mathematics, sometimes your intuition can be dead wrong.

We know that 1 ≠ 2

But here’s a theorem of Banach & Tarski:

A solid ball in 3-dimensions can be cut up into a finite number of pieces, so that these pieces can be moved around and assembled into two identical copies of the original ball.

Not possible in 1 or 2 dimensions, btw.

What is a proof?

So it really pays off to:

- Formalize concepts, give precise definitions
- Make implicit assumptions explicit
- Write careful proofs, where every step can be checked carefully.
- Even “mechanically” using a “computing machine”, if you will
Let’s ask the OED

1. a. Something that proves a statement; evidence or argument establishing a fact or the truth of anything, or belief in the certainty of something; an instance of this.

3. Math. and Logic. A sequence of steps by which a theorem or other statement is derived from given premises.

What is a proof?

Intuitively, a proof is a sequence of “statements”, each of which follows “logically” from some of the previous steps.

What are “statements”? What does it mean for one to follow “logically” from another?

We’ll lay the groundwork for these questions in today’s lecture...

But we will come back to these questions again later...

Propositions

A proposition is a statement that is either true or false.

snow

2+2

is xadk keosign sziable?

Complex Statements

If snow is white then the sun rises in the west

Socrates was bald and Cicero ate a pie

2 + 2 = 5 if and only if 4 + 4 = 9

Snow is not white

Propositions

A proposition is a statement that is either true or false.

snow

2+2

Socrates had six digits on his left hand

the summer solstice occurs on June 21st
Complex Statements

snow is white $\Rightarrow$ the sun rises in the west

Socrates was bald $\land$ Cicero ate a pie

$2 + 2 = 5 \iff 4 + 4 = 9$

$\neg$ (Snow is white)

Well-Formed Statements

Every “simple” proposition is a well-formed propositional statement

If $A$ and $B$ are well-formed

so are $(A \land B), (A \lor B), \neg A, (A \Rightarrow B), (A \Leftrightarrow B)$

and or not if... then if and only if

The “meaning” of these connectives

$(A \land B)$ “A and B”

true if both $A$ and $B$ are true

$\neg A$ “not A”

true if $A$ is false

$(A \lor B)$ “A or B”

true if at least one of $A$ and $B$ is true

The “meaning” of these connectives

$(A \Rightarrow B)$ “if A then B”

“A implies B”

what are the rules for this?

The “meaning” of these connectives

$(A \Leftrightarrow B)$ “A if and only if B”

same as $(A \Rightarrow B)$ and $(B \Rightarrow A)$

Which of the following are true?

Snow is white.

If snow is white then grass is green.

Therefore, grass is green.

Snow is white.

If snow is white then grass is green.

Therefore, grass is green.
Which of the following are true?

The orchestra will not play both Bach and Haydn.
The orchestra will not play Bach. Therefore, the orchestra will play Haydn.

Let’s abstract out the underlying mathematical structure…

Well-Formed Propositional Formulas

The truth values T and F are well-formed
All variables p, q, p₁, p₂, ... are well-formed
If A and B are well-formed
so are (A ∨ B), (A ∨ B), ¬A, (A⇒B), (A⇔B)

Is ¬(p ∨ ¬q) well formed? ✓ ♦

p? (p ∨ ¬q)? (p⇒q)⇒(¬p⇒q)?

(Well-Formed) Propositional Formulas

Each propositional formula B on n variables defines a function fₐ from (T,F)ⁿ to {T,F}.

How is this function defined?
Inductively.

Tautologies (a.k.a. Truths)

A propositional formula B is a tautology if it is true for every setting of the variables

T F p p ∩ q
p ∨ ¬p p ∨ p
¬p ∨ q ≡ (p⇒q) (p∨q) ≡ (q ∨ p)
(p⇒q) ≡ ((p⇒q) ∧ (q⇒p))

Checking for Tautologies

Evaluate the propositional formula B on every input in {T,F}ⁿ

How?
E.g., \( B = (p \land (p \Rightarrow q)) \Rightarrow q \)

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( p \Rightarrow q )</th>
<th>( p \land (p \Rightarrow q) )</th>
<th>( (p \land (p \Rightarrow q)) \Rightarrow q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

Truth Table for formula \( B \)

Create a table with \( 2^n \) rows

\[
\begin{align*}
p_1 = T, & \ p_2 = T, \ p_3 = T \ldots, \ p_n = T & \quad & B(T,T,T,\ldots,T) \\
p_1 = F, & \ p_2 = T, \ p_3 = T \ldots, \ p_n = T & \quad & B(F,T,T,\ldots,T) \\
p_1 = T, & \ p_2 = F, \ p_3 = T \ldots, \ p_n = T & \quad & B(T,F,T,\ldots,T) \\
\vdots & \quad & \vdots & \\
p_1 = F, & \ p_2 = F, \ p_3 = F \ldots, \ p_n = F & \quad & B(F,F,F,\ldots,F)
\end{align*}
\]

Evaluate the function for each setting

Takes at least \( 2^n \) time

Recursive Evaluation for \( B \)

\[
\text{eval(formula } B, \text{ setting } M) \\
\{ \\
\quad \text{if } (B = "T") \text{ return } T; \\
\quad \text{if } (B = "F") \text{ return } F; \\
\quad \text{if } (B = "B_1 \land B_2") \\
\qquad \text{return eval}(B_1,M) \land \text{eval}(B_2,M); \\
\quad \quad \quad \ldots \\
\quad \quad \quad \ldots \\
\quad \}\n\]

OK, quick recap

propositional formulas

a formula maps each possible “world” in \((T,F)^n\) into either \( T \) or \( F \)

some formulas are “truths” (tautologies):
they are true in all possible \( 2^n \) worlds

can check if a formula is a tautology in \( \approx 2^n \) time.

What is a proof?

The truth table gives us a “proof” that a propositional formula is a tautology

What are the pros of this proof technique?

What are the cons?
Does not give much “intuition”

Even simple things have very long proofs

\[(p_1 \Rightarrow p_2) \land (p_2 \Rightarrow p_3) \land \ldots \land (p_{n-1} \Rightarrow p_n)\]

\[\Rightarrow (p_1 \Rightarrow p_n)\]

has truth-table of size \(2^n\)

Does not scale to non-Boolean proofs.

Later we will want to prove things about all the naturals, then we’re in trouble with brute-force.

A “more natural” way to prove things…

Let us start with a simple tautology

\[(-A \lor A)\]

we’ll call this an “axiom”

And use one of these rules at each step:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[A \lor (B \lor C)]</td>
<td>expansion</td>
</tr>
<tr>
<td>[(A \lor B) \lor C]</td>
<td>associativity</td>
</tr>
<tr>
<td>[A \lor A]</td>
<td>contraction</td>
</tr>
<tr>
<td>[A \land B]</td>
<td>cut rule</td>
</tr>
<tr>
<td>[(A \lor B), (-A \land C)]</td>
<td>“inference rules”</td>
</tr>
</tbody>
</table>

Whatever we can prove, we’ll call “theorems”

Proof of commutativity rule

\[
\begin{align*}
A \lor B & \quad \text{(hypothesis)} \quad (1) \\
\neg A \lor A & \quad \text{(axiom)} \quad (2) \\
B \lor A & \quad \text{(cut rule to 1,2)}
\end{align*}
\]

Proof of new expansion rule

\[
\begin{align*}
A & \quad \text{(hypothesis)} \\
B \lor A & \quad \text{(expansion rule)} \\
A \lor B & \quad \text{(commutativity)}
\end{align*}
\]

Proof of “modus ponens”

\[
\begin{align*}
A, A \Rightarrow B & \quad \text{Since the logical system does not have “⇒”} \\
\neg A \lor B & \quad \text{we define it to be } \neg A \lor B \\
A & \quad \text{(hypothesis)} \quad (1) \\
A \Rightarrow B & \quad \text{(hypothesis)} \\
\neg A \lor B & \quad \text{(def. of ⇒)} \quad (2) \\
A \lor B & \quad \text{(apply expansion to 1)} \quad (3) \\
B \lor B & \quad \text{(cut rule to 2,3)} \\
B & \quad \text{(contraction)}
\end{align*}
\]

What is a proof?

A sequence of statements, each of which

is an axiom,

or a hypothesis,

or follows from previous statements using an inference rule
Another recap

(well-formed) propositional formulas

some formulas are tautologies ("truths")
- \( p \lor \neg p \)
- \((p \land (p \Rightarrow q)) \Rightarrow q \)
can check by truth-table

some formulas are "theorems"
- \( p \lor \neg p \)
- \((p \land (p \Rightarrow q)) \Rightarrow q \)
these are formulas for which we can give proofs

For this logical system and Boolean formulas

Are all theorems “true” (i.e., tautologies)?
- Yes. (easy proof by induction)

Yay! Our logical system is “sound”.
We only prove truths.

Are all tautologies theorems?
- Yes. (much more involved proof)

Double yay! Our logical system is “complete”.
We can prove all the truths via inference rules.

The high-level picture

A Logical System

A “logic” consists of:
1) A collection \( S \) of well-formed sentences
2) Some sentences in \( S \) called “axioms”
3) A set of “rules of inference”

A “truth concept” consists of:
1) A collection \( S \) of well-formed sentences
2) Some sentences in \( S \) called “truths”

A Logical System for Propositions

Axiom:
- \( (\neg A \lor A) \)

Inference Rules:
- \( \frac{A \lor (B \lor C)}{(A \lor B) \lor C} \)
- \( \frac{A \lor A}{A} \) contraction
- \( \frac{A \lor \neg A}{B \lor A} \) expansion

associativity

\( \frac{(A \lor B), (\neg A \lor C)}{(B \lor C)} \) cut rule

This logical system is

sound “all theorems are true”
and

complete “all truths are theorems”

for propositional truths (tautologies)
Another (Toy) Example

Example: Balanced Parens

Consider strings of parentheses

Well-formed string:

Has an equal number of "("s and ")"s

E.g., ))))))(((). ()()(), ϵ

Truths:

The parens are balanced.

E.g., (((())), (), ϵ

Example: Balanced Parens

A Logical System:

Axiom: ϵ

Rules of inference:

\[
\begin{array}{c|c}
&A \\
\hline
(A) & A \cdot B \\
\end{array}
\]

Theorems are those strings of parens that can obtained via this logical system

Example: Balanced Parens

Proof of theorem "((()))"

\[
\begin{array}{c|c}
&\epsilon \\
\hline
(A) & A \\
\end{array}
\]

Proof:

\[
\begin{align*}
\epsilon & \quad \text{(axiom)} \\
() & \quad \text{(rule 1)} \\
(() & \quad \text{(rule 1 again)} \\
(() & \quad \text{(rule 2)} \\
\end{align*}
\]

Example: Balanced Parens

Truth concept:
The parens are balanced.

The logical system with one axiom and two rules of inference

In HW2, you showed

this logical system is sound and complete for this truth concept!

You also showed: another system was sound, but not complete!

Onwards and Upwards!
Propositional logic is fine in its place but it does not capture too much...

E.g.,

Socrates is a human.

All humans are crazy.

Hence Socrates is crazy.

\[ H(s) \quad \forall x \ H(x) \Rightarrow C(x) \quad \therefore \ C(s) \]

Or

\[ \forall x, y \ ((x < y) \Rightarrow (x+1 < y+1) \]

First Order Logics

Have variables, and usual logical operators

But variables can range over more general structures

Can have functions, relations and predicates

and quantifiers

\[ \forall x \ \exists y \ P(x) \Rightarrow Q(y) \]

One concrete example

Let’s say we want a language for arithmetic that captures statements like:

16 is even

“∃ natural x such that 2^x = 16”

Every natural number is either even or odd

“∀ natural x ( (∀ natural y such that 2^y = x) \vee (∃ natural z such that 2^z+1 = x) )

Need quantifiers, “=”, “+”, “(−)”, “≤”, “<”

and we need the natural numbers 0, 1, 2, … too!

Peano Arithmetic

The Peano axioms formally define properties of the natural numbers

| \[ \mathbb{N} = \{ 0, 1, 2, 3, 4, \ldots \} \] |

| Peano Arithmetic |

a) 0 is a natural number.

b) For every natural number n, its “successor” S(n) is a natural number.

c) For every natural number n, S(n) ≠ 0.

d) For all natural numbers m and n, if S(m) = S(n), then m = n.

e) For every natural n, n = n

f) For all naturals, if n = m, then m = n.

g) For all naturals if k = m and m = n then k = n.

h) If n is a natural number and n = m, then m is also a natural number.
Peano: Inductive Definition of +
\[ \mathbb{N} = \{ 0, S0, SS0, SSS0, \ldots \} \]

Inductive definition of addition (+):
\[ X, Y \in \mathbb{N} \Rightarrow \]
\[ X \text{ “+” } 0 = X \]
\[ X \text{ “+” } SY = S(X \text{ “+” } Y) \]

S0 + S0 = SS0 (i.e., “1+1=2”)

Proof:
\[ S0 + S0 \]
\[ = S(S0 + 0) \]
\[ = S(S0) \]
\[ = SS0 \]

Peano: Inductive Definition of *
\[ \mathbb{N} = \{ 0, S0, SS0, SSS0, \ldots \} \]

Inductive definition of multiplication (*):
\[ X, Y \in \mathbb{N} \Rightarrow \]
\[ X \text{ “*” } 0 = X \]
\[ X \text{ “*” } SY = (X \text{ “*” } Y) \text{ “+” } X \]

Peano: Defining “<”

Defining < for \( \mathbb{N} \):
\[ \forall x, y \in \mathbb{N} \]
\[ “x > y” \text{ is TRUE } \Leftrightarrow “y < x” \text{ is FALSE} \]
\[ “x > y” \text{ is TRUE } \Leftrightarrow “y > x” \text{ is FALSE} \]

“x+1 > 0” is TRUE

“x+1 > y+1” is TRUE \( \Rightarrow “x > y” \text{ is TRUE} \)

Peano: Defining “minus”

Defining partial minus for \( \mathbb{N} \):
\[ \forall x, y \in \mathbb{N} \]
\[ x - 0 = x \]
\[ x > y \Rightarrow (x+1) - (y+1) = x - y \]

Peano: and so on...

You can build an edifice for arithmetic
and use this logical system
to conceivably prove all arithmetic truths

Thm: the Peano system is sound for arithmetic

Q: Is it complete?
We’ll be back...

Propositional Logic
- well-formed expressions
- truth tables
- tautologies

Logical Systems
- truths
- theorems
- soundness and completeness

Here’s What You Need to Know...

First-order Logics
- quantifiers
- Peano’s axioms