6.1200J/18.062J *Mathematics for Computer Science* Tuesday 6th February, 2024
Massachusetts Institute of Technology, Spring 2024
Z. Abel, B. Chapman, E. Demaine
revised Saturday 10th February, 2024

Lecture 01: Predicates, Sets, and Proofs

1 Administrivia

Please see Course Information handout!

- Lectures Tu/Th
- Rec W/F, attendance taken (10%), focus on solving problems in groups
- WU before every rec: instant feedback, unlimited tries until deadline, please do before rec.
- Psets due Mondays, released Tuesdays
- Collab policy
  - Solve psets in small groups
  - List collaborators per problem, or Collab: None
  - Write solutions on your own: don't look at other solutions (from friends, internet, OR chat gpt), don't reference communal notes while composing your own proof, and don't show your solutions to others
  - Why? P vs NP fallacy: understanding someone else's proof is easier that piecing together your own argument from scratch. When we say "in your own words", we want to see how *you* piece together the proof yourself.
- Late psets: briefly, late psets allowed for half credit until last day of classes! In truth, n hours late will get $100 - n$ percent of earned points, unless $n \geq 50$, in which case you'll get 50% of earned points. So don't worry about being a few hours late, it's nbd.
- Will talk more about late psets next time.

2 Proofs

Q: What is a proof?
A: A method of ascertaining the truth

Examples:

- Experiment / observation (physics)
- Sampling (statistics)
- Legal (judge / jury)
- Public opinion
- Business (authority)
- School (Professor says so!)
- Religion (Word of God)
- Inner Conviction
- "Why not?"

In mathematics:

Definition 1. *A* mathematical proof *is a verification of a* ***proposition*** *by a chain of* ***logical deductions*** *from a base set of* ***axioms****.*

Over the next two lectures, we will delve into *predicate logic* (also called *first-order logic*), break down this definition, and see what each of these three bolded components means.

3 Propositions

Definition 2. *A* proposition *is a statement that is either True or False.*

Definition 3. *A* predicate *is a proposition whose truth depends on variables.*

Examples:

Proposition 1 (True)**.** $2 + 3 = 5$

Proposition 2 (False)**.** $2 + 3 = 6$

Proposition 3. $\forall n \in \mathbb{N}.\ n^2 + n + 41$ *is prime*

Some non-examples:

- Hello.
- Who are you?

- This statement is false. (What does it mean for statements to reference themselves? Doesn't always make sense. Not something we're going to handle in this class.)

Some notation:

- $\forall$ ("for all"): universal quantifier, followed by the predicate "$n^2 + n + 41$ is prime"
- $\in$ ("in"): element of a set
- $\mathbb{N}$ ("the natural numbers"): the set of non-negative integers $0, 1, 2, \ldots$

To see if Proposition 3 is true or false, we need to know whether the predicate is true for every choice of n. Let's check?

n	$n^2 + n + 41$	Prime?
0	41	True
1	43	True
2	47	True
3	53	True
4	61	True
5	71	True
⋮	⋮	⋮
20	461	True
⋮	⋮	⋮
39	1601	True

It's true for the first 40 examples, so probably true right? In some fields, this would be convincing: Engineering, Physics, CS (simulations often used in lieu of proof). But if $n = 41$, then $n^2 + n + 41 = 43 \times 41$. In mathematics, we call this a "Proof by Example", which is NOT a valid proof!

Some propositions in number theory are even more devious.

Proposition 4 (False)**.** *$a^4 + b^4 + c^4 = d^4$ has no positive integer solution.*

- Conjectured by Euler in 1769
- Ultimately disproved by Noam Elkies
- Solution: $a = 95800, b = 217519, c = 414560, d = 422481$

Proposition 5 (True)**.** $\exists a, b, c, d \in \mathbb{Z}^+.\ a^4 + b^4 + c^4 = d^4$

Proposition 6 (False)**.** *$313(x^3 + y^3) = z^3$ has no positive integer solution.*

- Smallest counterexample has over 1000 digits

- Why care...?
  - about $313(x^3 + y^3) = z^3$?
  - about 1000-digit numbers?
- In fact, this is an example of an *elliptic curve*. Elliptic curves are crucial to the understanding of how to factor large numbers. The ability to factor large numbers would give you access to most computer systems on the planet...

Proposition 7 (Goldbach's Conjecture)**.** *Every even number greater than* 2 *is the sum of two primes.*

- T or F? Unknown!
- True for every even number ever checked...
- Generally believed
- Seems pretty hard, listed as one of the great unsolved mysteries on the front page of the Boston Globe in the mid 90s.

4 Combining Propositions

It's useful to construct new propositions by combining existing ones. For example,

- A AND B, aka $A \wedge B$, means "both A and B are true"
- A OR B, aka $A \vee B$, means "at least one of A or B is true". (Note: this is *inclusive* or, meaning it's also fine for A and B to *both* be true.)
- NOT A, aka $\overline{A}$, aka $\neg A$, means "A is false"

We can represent these as truth tables:

A	NOT A
T	F
F	T

A	B	A AND B	A OR B
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

Cautionary tale: math terms are precise, but English words often change meaning depending on context, and the two share a lot of terms. Even worse, we communicate math using English! When written in formulas, OR, etc., will always refer to the truth tables above. But in everyday lang

- Waiter at a wedding says that the dinner options were "chicken or pasta", and that word **or** is meant to communicate some set of allowable responses. In this case, you can say "chicken", or "pasta", but not "both" or "neither", since they've already seen all the RSVP cards. This isn't how we defined OR, it's *exclusive or*, denoted XOR.

- Waiter then says you can have "coffee or tea", and this time, you can say "just coffee", "just tea", or "neither", but not "both", since you only get one mug and they're not about to mix the two at a fancy party! This again isn't OR, it's NOT AND, sometimes called NAND.

- For your coffee, the waiter has "cream or sugar". This time, all 4 options are valid! Three uses of the English word "or", none of them actually meant OR.

5 Implication

One more important boolean operator: A IMPLIES B, also denoted $A \to B$ or $A \Rightarrow B$. Should be read "A implies B", aka "if A then B".

(Draw truth table, but take poll on the F IMPLIES T case:)

A	B	A IMPLIES B
T	T	T
T	F	F
F	T	T
F	F	T

The F IMPLIES T case might be less clear, so let's make it more concrete: "On Wednesdays we wear pink", aka, "if wednesday, wear pink", aka, "wednesday implies pink". Now F IMPLIES T being true makes sense: wearing pink on thursday doesn't violate the rule.

Note: A IMPLIES B is equivalent to its contrapositive, (NOT B) IMPLIES (NOT A), but not its converse B IMPLIES A.

Some examples that drive me crazy:

- You might be familiar with `<3`, the pre-emoji "heart" aka "I love you". I've also seen `<4` as an intensifier, "I really love you". But the latter is weaker! $x < 3$ IMPLIES $x < 4$, but not vice versa, so $x < 3$ is the stronger (i.e., more informative) statement. I guess it should be `<2`?

- Descartes: "I think therefore I am." This asserts T, but also T IMPLIES A. Internet meme: "I do not think therefore I do not am." This asserts NOT T but also NOT T IMPLIES NOT A. The implications are not equivalent! It's the ***inverse***, which is equivalent to the converse, but not equivalent to the original. If my shoe exists but doesn't think, Descartes would be fine with that, but the meme wouldn't. Should it be "I do not am therefore I do not think"?

Note: A IMPLIES B doesn't imply a *causal* relationship ("A causes B") or any connection with time ("A happened, which later caused B to happen"). Instead, A IMPLIES B is *defined* y this truth table.

By the way, if the F IMPLIES T case were swapped to what we wanted earlier, it's what we call "if and only if", abbreviated A IFF B, which asserts that A and B are both true or both false. It's equivalent to (A IMPLIES B) AND (B IMPLIES A), which is where it gets its name.

6 Brief Detour: Sets

A ***set*** is, roughly speaking, a collection of objects. Can be finite (e.g. $A = \{6, 1, 2, 0\}$), infinite (e.g., $\mathbb{N} = \{0, 1, 2, \ldots\}$, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, empty (the ***empty set*** is written as $\emptyset$ or $\{\}$ — same thing), can contain other sets as elements (B $= \{2, \{3, 4\}, \emptyset\}$), etc.

There is no such thing as duplicates (that would be a *multiset*), and the order of elements doesn't matter. So $\{1, 2, 2, 3\} = \{2, 3, 1\} = \{3, 1, 2\}$.

The set A has 4 ***elements***, and B has 3. Writtes as $6 \in A$. Is $\{1, 2\} \in A$? (no) Is $\{3, 4\} \in B$? (yes)

Sets can be subsets of each other: $S \subseteq T$ means all elements of S are also elements of T. Is $\{1, 2\} \subseteq A$? (yes) Is $\{0, 1, 2, 6\} \subseteq A$? (yes)

Often useful to use predicates to specify a subset, e.g., $\{n \in \mathbb{N} \mid \text{isPrime}(n)\} = \{2, 3, 5, 7, 11, \ldots, \}$. This is called ***set-builder notation***. Might also see this with a colon instead of |.

Also useful to be able to combine sets into other sets, e.g., intersection $A \cap B = \{2\}$, union $A \cup B = \{0, 1, 2, 6, \{3, 4\}, \emptyset\}$, difference $A - B = A \setminus B = \{0, 1, 6\}$ (the set of elements in A that are *not* elemenst of B).

By contrast, when order matters, we have *ordered tuples*, written with parentheses: $X = (6, 1, 2, 0)$ is not the same as $Y = (2, 1, 6, 0)$ (btw, 2.160 is *Identification, Estimation, and Learning* in Mech-E). Duplicates are also fine, e.g., $(6, 1, 2, 0, 0)$. Union, Interection, etc., don't make much sense for ordered tuples.

7 Axioms

The second component of a proof is the set of *axioms* on which it is based.

Definition 4. *An* axiom *is a proposition that is assumed to be True.*

- You may have heard: "Don't make assumptions in math"
- You *must* make assumptions!
- The key is to state them up front.

Examples:

Axiom 1. *If $a = b$ and $b = c$, then $a = c$.*

Axiom 2. *Given a line l and a point $p \notin l$, there is exactly one line through p parallel to l.*

Axiom 3. *Given a line l and a point $p \notin l$, there is no line through p parallel to l.*

Axiom 4. *Given a line l and a point $p \notin l$, there are infinitely many lines through p parallel to l.*

- These last three axioms are contradictory! Which is right?
- All are equally valid.
- Different axioms yield different proofs and theorems.
- Anyone who agrees with your axioms must accept theorems derived from them.
- Lines are just different objects in these three worlds...
- There is no "correct" set of axioms, but we would at least like:

Definition 5. *A set of axioms is* consistent *if no proposition can be both proved and disproved.*

Definition 6. *A set of axioms is* complete *if every proposition can be either proved or disproved.*

- Consistency and completeness are clearly desirable!
- Logicians Russell and Whitehead spent their entire careers trying to find a complete and consistent set of axioms for basic arithmetic.
- But:

Theorem 8 (Gödel's Incompleteness Theorem)**.** *No set of axioms is both complete and consistent.*

- Proved by Kurt Gödel in 1930s
- Shocked the field
- Bad day for Russell and Whitehead...
- Corollary: if you want consistency (necessary), then there are True statements that cannot be proved!
- Maybe: Goldbach's Conjecture is True, but there is no proof!
- Please let us know if we assign any of these as homework...

6.1200J Mathematics for Computer Science

Spring 2024