Lecture 24. Review of logic.

A goal in CS: Can computers do mathematics? Now being achieved.

Subproblems:

- Check correctness of proofs/results eg. Lean
- Come up with plausible conjectures
  - humans use logic/symbolic computation to make conjectures
  - prove statements we believe are true.

Def (MIT- Math for CS notes) A mathematical proof of a proposition (a math statement) is a chain of logical deductions (↳ rules of logic) leading to a prop from a set of axioms.
↳ you need some 'truths' to begin with.

Simple statements to bigger/more complicated statements

Notation.

Plain English	Prop calc	Math
P AND Q	$P \wedge Q$	$A \cap B$
P OR Q	$P \vee Q$	$A \cup B$
NOT P	$\neg P$ or $\overline{P}$	A^c
P IMPLIES Q	$P \to Q$	$P \Rightarrow Q$
P IFF Q (if and only if)	$P \leftrightarrow Q$	$P \Longleftrightarrow Q$ (equivalent)

Calculate truth tables / implement basic stuff.

Eg. $P \to Q$.

P	Q	$P \to Q$
T	F	F
T	T	T
F	F	T
F	T	T

Q can be true even if P is false

Ex2. Prop. A false proposition implies any proposition.

P	$\neg P$	$P \wedge \neg P$	Q	$P \wedge \neg P \to Q$
T	F	F	T	T
			F	T
F	T	F	T	T
			F	T

This is the reason why we don't allow contradictions.
Contradiction: P and not P.

Ex. Show $P \to Q$ has same values as $\neg Q \to \neg P$ (contrapositive).

The point of truth tables is that you can program computers to calculate truth value of statements, knowing atomic statements.

More notation is needed for real math theorems.

Thm (Division Algo) Given $m, n \in \mathbb{N}$, there are q and r s.t. $n = mq + r$ and either $r = 0$ or $0 < r < m$.

This statement is about $m, n \in \mathbb{N}$ — 'Domain' or Universal set

Valid for all $m, n \in \mathbb{N}$ — $\forall$ ← for all
there exists q, r — $\exists$ ← there exist
either $r = 0$ or $0 < r < m$
↳ P OR Q and NOT (P and Q)
$0 < r < m \to r$ is > 0 and $r < m$

In real life we don't use prop calculus to learn to argue. This is why I didn't do in beginning. You need to learn as we did.

Predicate: Truth of statement may depend on values
- for all $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$
- for some values $x^2 + x + 1 = 0$

Ex. The eqn $ax + by = d$ has a soln $x, y \in \mathbb{Z}$ for any a, b, d. We know it is false: $2x + 6y = 3$ has no soln.

- ONLY ONE Counterexample is needed

$$\text{NOT } (\forall x, P(x)) = \exists x \text{ (s.t.) NOT } P(x)$$

Other rules:
$(A \cup B)^c = A^c \cap B^c$
$(A \cap B)^c = A^c \cup B^c$
→ translate to logic.

Valid statements – true regardless of truth value of component statements.

Satisfiable – if for some values it is true.
eg P and $\overline{Q}$ → True if $P = T$, $\overline{Q} = T$ or $Q = F$

The SAT problem → Check if a statement can be made true if some assignment of variables can make it true.
→ Doing so by truth tables takes 2^n steps
- Does SAT have poly algo? P vs NP problem
  - \$1 Mn if you solve it (+ eternal glory).

Rules for logic

1. if P Then Q, P — antecedents
   Q — conclusion
2. $P \to Q$, $Q \to R$
   $P \to R$
3. $P \to Q$, not Q
   not P.

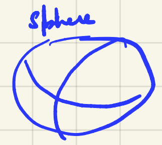
Proof ideas: To show P OR Q. Assume NOT P, show Q
$P \to Q$: Assume P show Q → direct proof
Assume not Q show not P → contrapositive
Assume P, not Q show $R \wedge \neg R$ → Contradiction

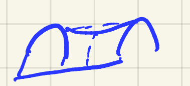
Ex. Go through all proofs. Have we used anything other than these?

Questions: Sp I have a list of axioms. I compute all possible theorems by applying rules of logic. Will I get all possible true statements?

History: Euclid's 5th axiom raised many doubts.
Given a line ℓ and pt P not on ℓ, there is exactly one line through P passing through ℓ.
- People tried to prove it
- Euclidean geometry is consistent – there is no contradiction in assuming this.

This axiom is independent – if we modify axiom we get different consistent geometries.

sphere

No line is ∥ ← Riemannian Geometry
△'s can be 270° > 180

saddle shaped

Many lines are ∥
← sum of ∠'s in △ < 180.

- Completeness: Will all true theorems be proved?
Ans: Gödel → No (Read: Smullyan (last ch.) Gödel, Escher Bach.

Next time: One or 2 pending theorems - review.