Quantum Computing Since Democritus

Scott Aaronson

Chapter 3: Gödel, Turing and Friends

Saumya Chaturvedi

Table of Contents

Gödel's Completeness Theorem

- First Order Logic is all you need.
- If, starting from some set of axioms, you can't derive a contradiction using these rules, then the axioms must have a model.
- Everything from Fermat's Last Theorem can be proved by applying these rules over and over again.

Proof

- “extracting semantics from syntax.”
- We cook up objects to order as the axioms request them!
- If inconsistency found, it suggests inconsistency in the original axioms.

Application

- Löwenheim-Skolem Theorem: If a countable theory has a model, it has a countable model.
- Every consistent set of axioms has a model of at most countable cardinality.
- Because you can only cook up objects to order a countably infinite number of times!

Gödel's (In)completeness Theorem

- For a computable (finite axioms), consistent (no contradictions) set of axioms, there's a true statement within those axioms which cannot be proven from those axioms.
- Proof: 30 pages vs 2 lines.

Proof Method 1: Encoding

- Similar to Scott's friend's method of realizing arrays.
- Very cool demonstration on whiteboard.

Turing Machine and Assumptions

- In 1936, ”computer” meant a woman.
- Realising a computer machine which does the following:
  - Writes calculations on a square paper, each symbol per square.
  - Reads 1 symbol at a time, and is able to go back and forth on the tape.
- How does it make instantaneous decisions?
  - Depends on the symbol currently being read,
  - and the machine’s current “internal configuration” or “state.”

- What should the machine do?
  1. Write a new symbol in the current square, overwriting whatever symbol is there,
  2. Move backward or forward one square, and
  3. Switch to a new state or halt.

- The number of possible internal states should be finite.

Implications

- Universal programmable computers can exist.
- Inventing the Halting Problem
- Hard problem, solving this solves other problems like Goldbach's Conjecture

Halting Problem and Proof

- Given a program, can we determine if it halts ever?
- Proof by contradiction that a program P to solve Turing problem exists.
- Modify P to produce a new program P' that:
  - runs forever if Q halts given its own code as input, or
  - halts if Q runs forever given its own code as input.
- Feed P' its own code as input.
- P' will run forever if it halts, and halt if it runs forever. So it doesn't exist.

Halting Proving Incompleteness

- Suppose: A consistent, computable proof system F proving/disproving any statement about the integers.
- Halting Problem: about integers, find proof within F.

Halting Proving Incompleteness

- Suppose: A consistent, computable proof system F proving/disproving any statement about the integers.
- Halting Problem: about integers, find proof within F.
- But program to solve Halting Problem can't exist.

Halting Proving Incompleteness

- Suppose: A consistent, computable proof system F proving/disproving any statement about the integers.
- Halting Problem: about integers, find proof within F.
- But program to solve Halting Problem can't exist.
- F can't exist.

Second Incompleteness Theorem

- Back to program P' fed to itself, why not use this program as proof?
- Hidden assumption behind it: F is consistent.
- If F was inconsistent, it could prove P halting even if it ran forever.
- But if F could prove its consistency, it could also prove P halting or running forever.
- Only possible conclusion: F is consistent but can't prove its own consistency.
- To prove consistency of powerful theories, we need even more powerful theories. (Illustration on whiteboard)

Implications

- Finding bigger infinities (large Cardinals) to prove consistencies. Example: PA and ZF.
- A quick question to test your understanding: while we can't prove in PA that Con(PA), can we least prove in PA that Con(PA) implies Con(ZF)?

Implications

- Finding bigger infinities (large Cardinals) to prove consistencies. Example: PA and ZF.
- A quick question to test your understanding: while we can't prove in PA that Con(PA), can we least prove in PA that Con(PA) implies Con(ZF)?
- No! Because then we could prove in ZF that Con(PA) implies Con(ZF).

Peano Arithmetic's example

- "self-hating theory": PA + the assertion of its own inconsistency. (whiteboard)
- Axioms keep cooking up large fictitious numbers to create a model for theories.
- The point of the Completeness Theorem is that the whole infinite set of fictitious numbers the axioms cook up will constitute a model for PA – just not from ordinary positive integers!
- For the latter, we move to Incompleteness theorem.

Just Believe in Yourself!

- Puzzle from last chapter
- Let's assume we can prove the Riemann Hypothesis!
- $\zeta(s) = 1 + \frac{1}{2^s} + 1/3s + 1/4s + ...$
- Löb's Theorem: a mathematical system cannot assert its own soundness without becoming inconsistent.

How does AC and CH fit into this?

- Is continuum (cardinality of the real numbers) true or false?
- Godel 1939: assuming the Axiom of Choice (AC) or the Continuum Hypothesis (CH) can never lead to an inconsistency.
- Can we also assume AC and CH are false?
- Paul Cohen 1963: CH is not provable from the axioms of set theory. (”forcing”)
- The independence of AC and CH from ZF set theory is itself a theorem of Peano Arithmetic.
- Do we ever really talk about the continuum, or do we only ever talk about finite sequences of symbols that talk about the continuum?

Physically Meaningless

- How many different positions of a pen on paper? $\aleph_1$? $2^{\aleph_0}$?
- A physically meaningless question, but requires a physical theory!
- Quantum mechnanics is somehow ”quantized” yet continuous.
- Scott’s assumption: Hilbert space(the space of all possible quantum states of some system) is finite-dimensional.
- There are continuous parameters (probabilities or amplitudes) but not directly observable, we’re ”shielded” from them. (waveforms collapsing on measurement.)

Exercises and Further Reading

exerciseAndRe