Research in Theoretical Computer Science

Piyush P Kurur

February 18, 2023

What is a theory ?

A formal set of ideas that is intended to explain why something happens or exists — Oxford dictionary

Example: Gravity and Planetary motion

Abstraction Point mass

Vocabulary Mass, force, velocity, acceleration

Quantification/Measurement Equations of motion, Inverse square law of gravity etc

Prediction Position of planets, eclipses

Theoretical computer science ?

- Theory for "computer"

Theory A

- Data Structures, Algorithms, Complexity
- Quantum computing, Computational X

Theory B

- Logic
- Verification
- Model checking
- Programming languages and type theory

Algorithms and their efficiency

- What is an algorithm ?
- Algorithms for every problem ?
- Efficient algorithms ?
- Parallel algorithms ?

Unsolvable problems

- Check whether my C program terminates ?
- Check whether my C program reads illegal memory ?

Unsolvable problems

- Check whether my C program terminates ?
- Check whether my C program reads illegal memory ?

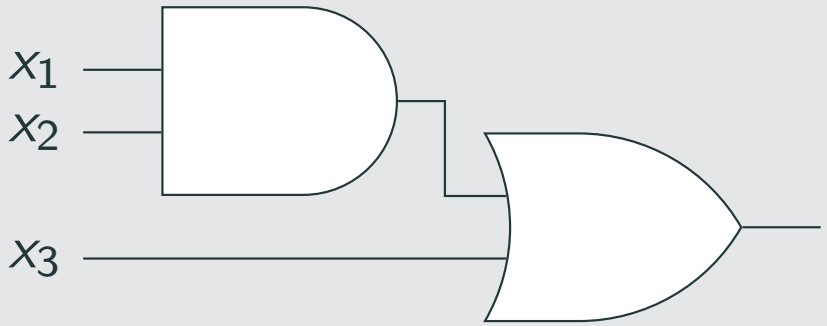
All of them are un-computable.

Theorem (Rice theorem)

Any non-trivial property about programs is uncomputatble

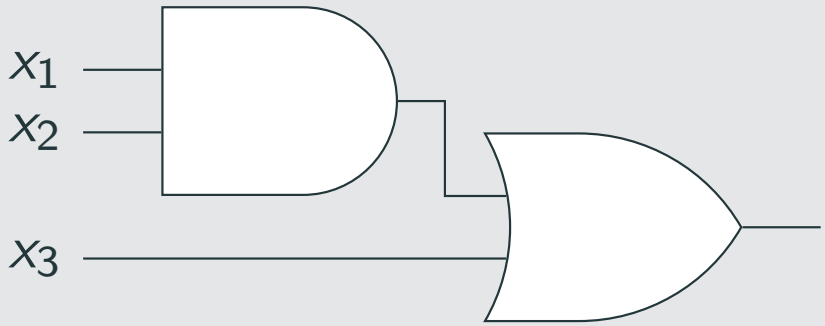
We can solve but

Boolean circuits



We can solve but

Boolean circuits



Two problems

- Is the circuit non-trivial ?
- Can we evaluate for a given input ?

Does throwing more computers help ?

Circuit evaluation problem is efficiently solvable but cannot be done in parallel efficiently.

Efficient parallel algorithms

- Arithmetic
- Determinant
- Linear algebra.

Summary so far

- Studying algorithms and algorithmic problems
- Classifying problems measured by hardness

Cryptography: When hardness is put into use

Scene Alice and Bob in a theater

Complication Seats are far apart, communicate via shouting.

Task Have an intimate conversation which no one else can understand.

Impossible ?

Key exchange (Diffie-Hellman)

- Alice shouts P (a big prime)

Alice

- Picks A, shouts $2^A mod\ P$
- From 2^B computes $(2^B)^A = 2^{AB} mod\ P$

Bob

- Picks B, shouts $2^B modP$
- From 2^A computes $(2^A)^B = 2^{AB}\ mod\ P$

Shared secret

$2^{AB} mod\ P$

Reasoning and Computer science

- What is truth and falsity ?
- When is something "proven" beyond doubt ?
- What is "meaning" ?

Logic and Computer Science

- Historic roots
- Reasoning about programs. Is this program correct ?
- Reasoning about concurrent process. Will this resource sharing mechanism deadlock?
- Modeling things like databases.

Often formulation is more interesting.

- Concurrent systems arriving at a consensus Paxos algorithm, Lamport clocks etc
- Design a correct C compiler
  - Meaning of C language
  - Meaning of processor instruction
  - Compiler should preserve meaning.

Many formulation of logic.

- The usual logic for reasoning in math
- Temporal logic (involving time)
- Linear logic (logic of resource)
- Separation logic (logic of heaps)
- Epistemic logic (logic of knowledge)
- Many more ..

Problems of interest

Give a formula φ

- Is it true ?
- Can I refute it ?
- Can a recognize a valid proof of it ?

Model checking and formal verification

- Automata to model statements
- To refute ψ, build a suitable automata and check emptiness

Programming languages and Type checking

- Type checking and proof checking in logic
- Write your programs and prove their correctness

Where to do research in India?

- IIT's
- IISER's
- CMI, IMSc, TIFRs

Blowing our own trumpets

- We work in diverse sub-areas of theory (More on it latter)

My own interests

- Formally certified hardware
- Cryptographic libraries with formal guarantees