Complexity Theory

Kya Hai Computers Ke Liye Mushkil?

National Science Day Celebration, 2020

Anamay Tengse STCS, TIFR - Mumbai































Studying Computation

Computers: Solve Problems using Programs

Can all programs be made fast?

- Can all programs be made **fast**?
- What makes problems difficult to solve fast?

- Can all programs be made fast?
- What makes problems difficult to solve fast?
- Can we prove something is difficult?

- Can all programs be made **fast**?
- What makes problems difficult to solve fast?
- Can we prove something is difficult?

What do all these words mean?



Humare Zamaane Mein...

Part I What is a *Computer*?







1936

8 – 1 British India Germany

1936





Automatic Computers





Automatic Computers





Automatic Computers





- Input: (a, b)
 1. Set P = 0, c = b
 2. If c is 0
 then Go-to 5.
 3. Set P = P + a.
 4. Set c = c 1, Go-to 2.
 - 5. **Output** *P*.











Input: (a, b)
1. Set P = 0, c = b
2. If c is 0
then Go-to 5.
3. Set P = P + a.
4. Set c = c - 1, Go-to 2.



Input: (a, b)
1. Set P = 0, c = b
2. If c is 0
 then Go-to 5.
3. Set P = P + a.
4. Set c = c - 1, Go-to 2.

5. **Output** *P*.

[1] *P* = 0, *c* = 2

$$\begin{bmatrix} 1 \end{bmatrix} P = 0, c = 2 \\ \begin{bmatrix} 3 \end{bmatrix} P = 12$$

 $(12 \ 2)$

Input: (a, b)
1. Set P = 0, c = b
2. If c is 0
 then Go-to 5.
3. Set P = P + a.

- 4. Set c = c 1, Go-to 2.
- 5. Output P.

[1]
$$P = 0, c = 2$$

[3] $P = 12$
[4] $c = 1$

[1]
$$P = 0, c = 2$$

[3] $P = 12$
[4] $c = 1$
[3] $P = 24$

[1]
$$P = 0, c = 2$$

[3] $P = 12$
[4] $c = 1$
[3] $P = 24$
[4] $c = 0$

5. **Output** *P*.

[1]
$$P = 0, c = 2$$

[3] $P = 12$
[4] $c = 1$
[3] $P = 24$
[4] $c = 0$
[5] **Output** P

24

Fixed sequence of simple steps For all inputs

Fixed sequence of simple steps
 For all inputs

Unlimited paper (memory)
 May depend on the input

What is easy?
Addition or Multiplication?

Addition or Multiplication?

Addition!

Addition or Multiplication?

Addition!

6712537 + 23421 or 2×3 ?

Addition or Multiplication?

Addition!

6712537 + 23421 or 2 × 3?

OH COME ON!!

Addition or Multiplication?

Addition!

6712537 + 23421 or 2×3 ?

OH COME ON!!

What? Why?

Addition or Multiplication?

Addition!

6712537 + 23421 or 2×3 ?

OH COME ON!!

What? Why?

Because...

Addition or Multiplication?

Addition!

6712537 + 23421 or 2×3 ?

OH COME ON!!

What? Why?

Because...

This needs some care...

Part II What does *easy* mean?













Goa is now in India!





Efficient (Fast) Solutions



Efficient (Fast) Solutions ↓



Efficient (Fast) Solutions ↓ Easy problems

$419 \times 42 = ?$

$419 \times 42 = ?$

 419×42





























Add 419 to 0, 42 times.

42

Add 419 to 0, 42 times.

6 simple operations. Add results, 6 steps.

42

12

Add 419 to 0, 42 times.

42

6 simple operations. Add results, 6 steps. 12

Q. What about 419000×4200 ?
Add 419 to 0, 42 times.

42

6 simple operations. Add results, 6 steps. 12

Q. What about 419000×4200 ?

Add 419000 to 0, 4200 times. 4200 6 simple operations. Add results, 6 steps. 12

Q. What about 419000×4200 ?

 Add 419000 to 0,
 24 simple operations.

 4200 times.
 Add results, 24 steps.

 4200
 48

Q. What about 419000×4200 ?

 Add 419000 to 0,
 24 simple operations.

 4200 times.
 Add results, 24 steps.

 4200
 48

Q. What about 419000 × 4200?

 $2 \times \text{size}, 4 \times \text{steps}!$

Fast Programs [Edmonds'65]

Steps grow steadily with size of input. 2× size, 50× steps.

Fast Programs [Edmonds'65]

Steps grow steadily with size of input.
 2× size, 50× steps.

Some steps can use other fast programs.
 e.g. Multiplication tables, addition.

Fast Programs [Edmonds'65]

Steps grow steadily with size of input.
 2× size, 50× steps.

Some steps can use other fast programs.
 e.g. Multiplication tables, addition.

P - Polynomial time - fast programs.

What is *Hard*?

What is *Hard*?

▶ No fast program → hard problem?

- ▶ No fast program \rightarrow hard problem?
- ▶ New methods, new fast programs.

- ▶ No fast program \rightarrow hard problem?
- ▶ New methods, new fast programs.
- What problems are provably hard?









Return gifts for a party.



Possible with 4 colours?

Return gifts for a party.



Possible with 4 colours?

```
"Graph Colouring Problem"
```

Can you find P, Q such that $N = P \times Q$?

Can you find P, Q such that $N = P \times Q$? How?

Can you find P, Q such that $N = P \times Q$? How? What about 100 digit N?

Can you find P, Q such that $N = P \times Q$? How? What about 100 digit N?

"Factoring Problem"

- Party planning
- Ulta multiplication

- Party planning
- Ulta multiplication
- ▶ Sudoku (*Hatke*)

- Party planning
- Ulta multiplication
- ▶ Sudoku (*Hatke*)

"Easy to verify a solution"

- Party planning
- Ulta multiplication
- ▶ Sudoku (*Hatke*)

"Easy to verify a solution" - NP

"Hard" problems [Cook'71][Levin'73]

NP hard - Problems at least as hard as NP

"Hard" problems [Cook'71][Levin'73]

NP hard - Problems at least as hard as NP

$\mathbf{P} \neq \mathbf{NP}$ wins you 1,000,000 USD!

"Hard" problems [Cook'71][Levin'73]

NP hard - Problems at least as hard as NP

$\mathbf{P} \neq \mathbf{NP}$ wins you 1,000,000 USD!

Why confirm a "bad news"?

Part III Are Hard Problems Bad?












Wood





Hard to break \rightarrow Safe from *attackers*.

Hard Problems for Safety

Hard Problems for Safety

Veeru

Basanti

Hard Problems for Safety

Veeru

Basanti



Hard Problems for Safety

Veeru

Basanti



Jay

Hard Problems for Safety

Veeru

Basanti



Jay

Hard Problems for Safety

Veeru

Basanti



Solve Hard Problem!!

Jay

Hard Problems for Safety

Veeru

Basanti



Solve Hard Problem!!

Jay

Idea: By the time Jay solves the problem, information is useless.

Hard Problems for Safety

Veeru

Basanti





Solve Hard Problem!!

Jay

Idea: By the time Jay solves the problem, information is useless.

Hard problem: Given *N*, find *P*, *Q* for which $P \times Q = N$.

Given *N*, find *P*, *Q* for which $P \times Q = N$. E.g. $15 = 3 \times 5$, $407 = 11 \times 37$, $6893297 = 2297 \times 3001$.

Given *N*, find *P*, *Q* for which $P \times Q = N$. E.g. $15 = 3 \times 5$, $407 = 11 \times 37$, $6893297 = 2297 \times 3001$.

Standards for Factoring: *N* has around 150 digits.

Given *N*, find *P*, *Q* for which $P \times Q = N$. E.g. $15 = 3 \times 5$, $407 = 11 \times 37$, $6893297 = 2297 \times 3001$.

Standards for Factoring: *N* has around 150 digits.

Using the *fastest* computer **available**, at least *a million years*.

When is Computation Difficult?

• Goal: *Prove* problems are hard, confirm beliefs.

- Goal: *Prove* problems are hard, confirm beliefs.
- **Tools**: Mathematics and Logic.

- **Goal**: *Prove* problems are hard, confirm beliefs.
- **Tools**: Mathematics and Logic.
- Status: Significant progress.

- Goal: *Prove* problems are hard, confirm beliefs.
- **Tools**: Mathematics and Logic.
- Status: Significant progress.
 Unsolved basic questions (P vs NP).

When is Computation Difficult?

- **Goal**: *Prove* problems are hard, confirm beliefs.
- **Tools**: Mathematics and Logic.
- Status: Significant progress.
 Unsolved basic questions (P vs NP).

Need More People! Please join us. ©

Research in Complexity Theory

TIFR complexity theory group.

Research in Complexity Theory

- ▶ TIFR complexity theory group.
- Successful Indian researchers worldwide.

Research in Complexity Theory

- ► TIFR complexity theory group.
- Successful Indian researchers worldwide.
- Pick your role model!

Thanks to...

 Content: Prerona Chatterjee (TIFR), Kshitij Gajjar (Technion), Tulasi mohan Molli (TIFR).

- Feedback: TIFR Outreach, Volunteers for NSD.
- ▶ You, for your attention. ☺