CMSC 27230

1-3-2024 | 1

HONORS THEORY OF ALGORITHMS

---

1. MODEL OF COMPUTATION
   COST

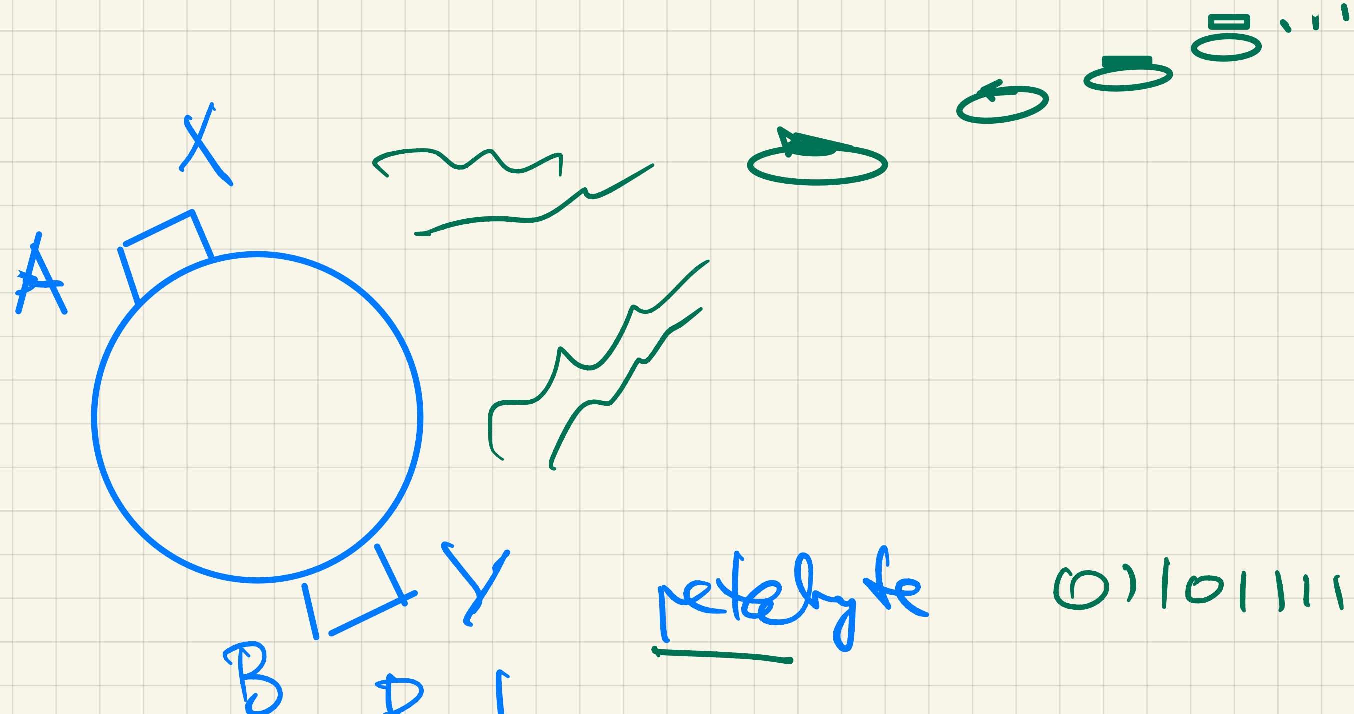
2. COMPUTATIONAL TASK

   input $\mapsto$ output function
   relation

---

upper bound on cost : algorithm analysis
lower bound : analysis of model
we are up against all conceivable algorithms

Alice



Bob

petabyte 0110111110 ...

TASK: $X \stackrel{?}{=} Y$

COST: # bits communicated $A \leftrightarrow B$

local computation: free

Comm. speed $\frac{1 \text{ Gbyte}}{\text{sec}}$

petabyte $\longrightarrow$ 27.4 years

3

$X, Y \in \{0,1\}^N$

$f(X,Y) \in \{0,1\}$

Alice & Bob collaboratively compute $f(X,Y)$

f known to both in advance

Cost: # bits of communication

---

analysis of model

Communication matrix $M_f = \big(f(X,Y)\big)_{X,Y}$

rows $\leftrightarrow X$

columns $\leftrightarrow Y$

(0,1) matrix

$2^N \times 2^N$

EXAMPLE

$X \stackrel{?}{=} Y$

$$f(X,Y) = \begin{cases} 1 & \text{if } X = Y \\ 0 & \text{if } X \neq Y \end{cases}$$

identity matrix

$$\begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots \; 1 \end{pmatrix} = I_{2^N}$$

Theorem (Mehlhorn-Schmidt)

for Deterministic communication

$$\underbrace{CC(f)}_{\text{min \#bits needed by the best communication protocol on worst input}} \geq \log_2 \operatorname{rk} M_f$$

cost of every algorithm is $\geq$ ...

$$\log_2 \operatorname{rk}(\underbrace{I_{2^N}}_{2^N}) = N$$

$$\operatorname{rk}(I_k) = k$$

Randomized solution

goal: min probability of error

Thm (Rabin - Yao - Simon)

$\exists$ randomized protocol
uses 400 bits communication
error prob $< 10^{-41}$

RYS protocol

Alice : generates a random prime $p < 2^{200}$

150 bits

Alice $\longrightarrow$ Bob : p 200 bits

$(X \bmod p)$ 200 bits

} 400 bits comm.

remainder of division by p

$(24 \bmod 7) = 3$

Bob :

if $(X \bmod p) \neq (Y \bmod p)$

Bob declares "$X \neq Y$" 100% confidence

else — " — "$X = Y$" hopes for the best

need to analyze probability of error

$\pi(x) = \#\text{primes } 1, \dots, x$

$\pi(10) = 4$

2, 3, 5, 7

$\pi(100) = 25$

check it

PRIME NUMBER THEOREM:

$$\boxed{\pi(x) \sim \frac{x}{\ln x}}$$

$$f(x) \sim g(x) \quad \text{if} \quad \lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$$

"asymptotically equal"

$\pi(2^{200})$

$$P(\text{error}) = \frac{\#\text{primes with} \le 200 \text{ bits dividing } X - Y}{\pi(2^{200})}$$

probability

when $X \neq Y$