POLYNOMIAL TIME REDUCTIONS

~~A problem is NPC (NP complete) if we are able to solve that~~

$A \leq_p B$

if $\exists$ a function $f: \Sigma^* \longrightarrow \Sigma^*$ s.t.

$\forall x \quad A(x) \iff B(f(x))$

↳ iff

if $\exists$ a function $f: \Sigma^* \longrightarrow \Sigma^*$ s.t.

$\forall x, \quad x \in A \iff f(x) \in B$

then

$A \leq_m B$

↓

reduced mapping

then $A \leq_p B$ efficiently computable → polynomial time reducible

eg. A: satisfiability problem (or a variant of it)

You will be given a boolean formula ϕ in conjugtive normal form (CNF) such that it is satisfiable with exactly 3 literals per clause ~~and ϕ is satisfiable~~.

$3\text{-SAT} = \{ \phi \mid \phi$ is in CNF, with exactly 3 literals per change and ϕ is satisfiable $\}$

CNF is product of sums

$\phi : (x_1 \vee \bar{x_2} \vee x_3) \wedge (\bar{x_1} \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6)$

$\wedge (\quad) \wedge \ldots \wedge (\quad)$

Input : 3-CNF ϕ

Output : yes if ϕ is satisfiable
no otherwise

i.e. write a program that makes a truth table, outputs yes if one row satisfies

eg. (i) $\phi = (x_1 \vee x_2 \vee x_3)$

if x_1 = true, then ϕ is satisfiable

(ii) $\phi = (x_1 \vee x_2 \vee x_3) \wedge (\bar{x_1} \vee \bar{x_2} \vee \bar{x_3})$

is not satisfiable

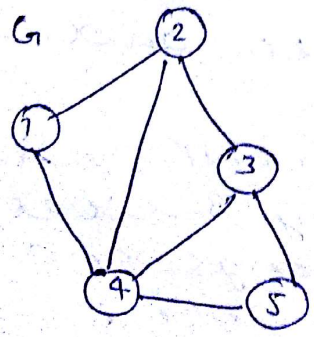
eg (i) $\phi \in$ 3-SAT

eg (ii) $\phi \notin$ 3-SAT

Consider problem B: Clique problem
Language is graph G and a +ve integer k such that G has a clique of size k (G has complete ~~graph~~ subgraph of size k)

CLIQUE = $\{\langle G, k\rangle$ / G has a clique of size k$\}$

eg.



$\langle G, 1\rangle \in$ Clique
$\langle G, 2\rangle \in$ Clique
$\langle G, 3\rangle \in$ "
$\langle G, 4\rangle \notin$ "

Write a program that outputs yes if there exists clique of size k.

If you can write a solution to B, you can solve A (satisfiability problem)

Theorem: $3\text{-SAT} \leq_p \text{CLIQUE}$

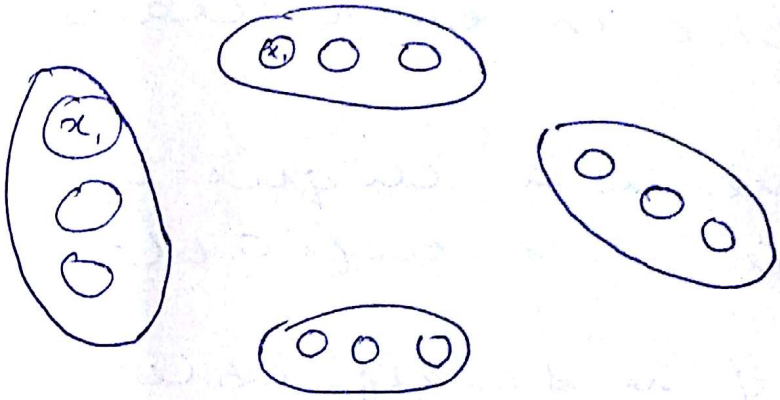
convert ϕ to $\langle G, k \rangle$

such that $\phi \in 3\text{-SAT} \iff \langle G, k \rangle \in \text{CLIQUE}$

consider $\phi : (x_1 \vee x_2 \vee \bar{x_3}) \wedge (\ . \vee . \vee .) \wedge \ldots \ldots \wedge (\ )$

with k clauses and n variables

create G on $3k$ vertices (due to $3k$ literals)



First define edges that should not be connected:

(i) There should be no edge between 2 vertices of the same clause

(ii) No edges between vertices that are complimentary to each other. i.e., no edge connects x & $\bar{x}$

All other edges exist.

Let $k = k$ and ask whether a clique of size k exists

prove that such a clique exists iff ϕ is satisfiable.

~~suppose that is a sigh~~

if you can have maximum size clique of size k. where one in each clause is connected. all of these will not be complimentary. make them all true.

if this has to imply that ϕ is satisfiable since atleast one in each clause is true.

∴ if there is a clique of size k, it is satisfiable.

suppose ϕ is satisfiable ~~you can assign~~ each clause is satisfiable and atleast one literal in every clause is true. pick the first literal that is true in every clause. you would have picked k literals. so you would have picked k literals in the graph. these k literals have to form a clique because there can't be a missing edge and satisfies (a) and (b)

$(\because \phi \in 3\text{-SAT} \iff \langle G, k \rangle \in \text{CLIQUE}$

$\forall L \in NP$, if $L \leq_p 3\text{-SAT}$

$\Rightarrow$ 3-SAT is NP Hard.

A is NP-Hard if $\forall L \in NP$, $L \leq_p A$ (Hardness of L is upper bounded by hardness of A)

A is NP complete ~~and~~ and NP Hard

$\Rightarrow$ A is NP complete.

$3\text{-SAT} \leq_p \text{CLIQUE}$

$L \leq_p 3\text{-SAT} \leq_p \text{CLIQUE}$

(It is transitive)

If you take an NP complete program and reduce it to your problem, then even that is NP hard.

~~it has proof~~

A problem x is interesting if ~~and~~ it has an efficient algorithm A such that $A(x,p) = 1$ iff $x \in L$

~~$\Rightarrow L$ is in P~~ $\Rightarrow L \in NP$

~~$\exists x \quad \forall x \quad \exists$ proof p~~

$\forall x \; \exists p$ | $\exists$ efficient algo A s.t. $A(x,p) = 1$ iff $x \in L$

NUMBER THEORETIC ALGORITHMS

- Primality testing (done)
- GCD, %b.
- Chinese remainder theorem

G.C.D

Input: a, b (a ≥ b)
Output: g = gcd(a, b)

Euclid's GCD:
Recursive algorithm

Euclid(a, b): (a ≥ b)
  if (b == 0) return a;
  else return (Euclid(b, a %. b));

TPT:
% g = gcd(a, b)
d = gcd(b, a %. b)
then g = d

g = gcd(a, b) => g | a & g | b

=> g | a %. b
(since a %. b = a - mb
= g.a₁ - mgb₁ (where a = ga₁, b = gb₁)
= g(a₁ - mb₁)
∴ g | a %. b)
=> g is gcd(b, a %. b)

$T(n) = 1 + T(m)$

where $n = \log_2 a$, $m = \log_2 (a \% b)$

But this is tough to solve.

$a \% b \leq \frac{a}{2}$

Proof:

if $b \leq a/2$, then it is true

else if $b \geq a/2$, then $a \% b = a - b \leq a/2$ (true)

$O(\log_2 a)$ time.

For a tighter bound,

if Euclid-algo takes k (recursion) steps, then $a \geq F_{k+2}$, $b \geq F_{k+1}$

At $k = 0$, $F_1 = 0$, $F_2 = 1$

Assume theorem is true upto $k-1$

So if it is true till Euclid $(b, a \% b)$

$\Rightarrow b \geq F_{(k-1)+2} = F_{k+1}$

$a \% b \geq F_{(k-1)+1} = F_k$.

Is $a \geq F_{k+2}$

Now $a \geq b + (a \% b)$

(since $a = mb + (a \% b)$ and $m \geq 1$)

$\Rightarrow a \geq F_{k+1} + F_k$ (from induction hypothesis)

$\Rightarrow a \geq F_{k+2}$

Q) show that this is tight i.e., if we start with $a = F_{k+2}$, $b = F_{k+1}$, then it takes k recursion.

Fibonacci no.

Input : n
Output : Fib_n

```
Fib(n)
    if n == 0 return 0
    if n == 1 return 1
    else return (Fib(n-1) + Fib(n-2))
```

$T(n) = T(n-1) + T(n-2) + 1$

This is exponential

```
Fib(n)
    if n == 0, F[0] = 0
    if n == 1, F[1] = 1
    for i = 2 to n
        F[i] ← F[i-1] + F[i-2]
Print F[n]
```

This is linear time.

To do better use linear algebra.

$F_0 = 0$

$F_1 = 1$

$$\begin{bmatrix} F_1 \\ F_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} F_0 \\ F_1 \end{bmatrix}$$

$$\begin{bmatrix} F_2 \\ F_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} F_1 \\ F_2 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^2 \begin{bmatrix} F_0 \\ F_1 \end{bmatrix}$$

$$\begin{bmatrix} F_3 \\ F_4 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^3 \begin{bmatrix} F_0 \\ F_1 \end{bmatrix}$$

$$\vdots$$

$$\begin{bmatrix} F_{n} \\ F_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^n \begin{bmatrix} F_0 \\ F_1 \end{bmatrix}$$

$O(\log n)$

(since we can calculate $(\text{matrix})^2$, $(\text{matrix})^4 \ldots$)

But the nos: can be very large and can't be stored in that cell.

~~Ab~~

$Fib(0) = 0$, $Fib(1) = 1$

$Fib(n) = Fib(n-1) + Fib(n-2)$

Assume $fib(n) = \rho^n$

$\rho^n = \rho^{n-1} + \rho^{n-2}$ where $\rho > 0$

~~in the lowest case~~

$\Rightarrow \rho^2 = \rho + 1$ (dividing by ρ^{n-2})

$\rho^2 - \rho - 1 = 0$

$\Rightarrow \rho = \frac{1 \pm \sqrt{5}}{2}$

$\therefore fib(n) = \lambda_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \lambda_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$

$\therefore fib(0) = \lambda_1 + \lambda_2 = 0 \Rightarrow \lambda_2 = -\lambda_1$

$fib(1) = \lambda_1 \left(\frac{1+\sqrt{5}}{2}\right) + \lambda_2 \left(\frac{1-\sqrt{5}}{2}\right) = 1$

$\Rightarrow \lambda_1 \left(\frac{1+\sqrt{5}}{2}\right) - \lambda_1 \left(\frac{1-\sqrt{5}}{2}\right) = 1$

$\Rightarrow \lambda_1 = \frac{1}{\sqrt{5}}, \quad \lambda_2 = -\frac{1}{\sqrt{5}}$

$\therefore fib(n) = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n$

Chinese remainder theorem

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

$\vdots$

$x \equiv a_k \pmod{n_k}$

solve for x given n_i and a_i

eg. $x \equiv 1 \mod 3$

$x \equiv 2 \mod 5$

$x \equiv 3 \mod 7$

$x = 52 + m105$

$\therefore x = M + m \prod_{i=1}^{k} n_i$

now to find M?

Let $x \equiv 1 \mod n_1$

$x \equiv 0 \mod n_2$

$\vdots$

$x \equiv 0 \mod n_k$

$\left(\prod_{j=2}^{k} n_j\right) V$

$V = \left[\left(\prod_{j=2}^{k} n_j\right)^{-1} \mod n_1\right]$

$[1, 0, \ldots 0] = M_1$

$[0, 1, \ldots .0] = M_2$

$\vdots$

$[0, \ldots . 1] = M_k$

so solution will be

$a_1 M_1 + a_2 M_2 + \ldots + a_k M_k \mod \prod_{i=1}^{k} n_i$

$= \left[\sum_{i=1}^{k} \left\{a_i \left\{\left[\prod_{j=1}^{k} n_j\right] / n_i\right] \left[\left(\frac{\prod_{j=1}^{k} n_j}{n_i}\right)^{-1} \mod n_i\right]\right\}\right] \mod \prod_{i=1}^{k} n_k$

inverse must exist, so there must be no common factor with n_i.

MID II

1. Dynamic Programming
2. Linear "
3. Polynomial time reduction
4. Primality testing & number testing algo.

A. Longest common subsequence (LCS)
B. Polygon triangulation
C. Optimal rod cutting
D. Longest path in a weighted tree.

B) Polygon triangulation:
Find optimum triangulation of a polygon (smallest perimeter)

C) eg: Rod of length 5

(i) Cutting first at 4 then at 2,
cost = 9

(ii) Cutting first at 2, then at 4,
cost = 8

E) 3-SAT $\leq_P$ Vertex cover
Given a graph, vertex cover is a subgraph where every edge is incident on

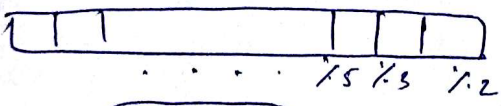
atleast one vertex is the cover.
Find vertex cover of min size ~~(if you know)~~
(Binary search)

(F) 3-SAT $\leq_p$ Subset sum
whether a there exists a subset in a given set that add up to a given no.

~~$\{\langle x_1, x_2, x_3, \ldots, x_n \rangle, T$~~

(h) Residue number system (RNS)
store ~~no~~ ~~no. % 2, no. % 3~~,
$n \% 2, n \% 3, \ldots$ ~~$n \% i$~~

~~you~~ n digit unique representation.



Sum

7 5 3 2
5 2 0 1
4 0 0 0
2 2 0 1

add digits and mod by respective

multiply

13 11 7 5 3 2
0 0 0 5 2 0 1
0 0 0 4 0 0 0
0 0 0 6 0 0 0

multiply and mod by respective

Hence sum and multiply are linear
However to compare you need Chinese remainder theorem

Representation	<	+	*
Binary	fast	fast	medium
RNS	M	F	F
Product of prime	S	S	F

(H) GCD

give a divide and conquer algo to get GCD ($O(\log n)$)

(split by LSB)

Assuming every character is distinct, solve

column no: ① ② ③ ④ ⑤

```
  SEND
+ MORE
------
MONEY
------
```

for unique solution. Find d.

M = 1

```
  SEND
+ 1ORE
------
1ONEY
------
```

S = 8 or S = 9

↳ (since there can be carry)

⇒ O = 0 or O = 1

↳ but M = 1

⇒ O = 0

⇒ S = 9 (since there can't be a carry in ~~second~~ third column)

```
  9END
  1ORE
------
1ONEY
------
```

N = E + 1 (since N can't be equal to E)

N + R = (E + 1) + R + Carry

⇒ 9 = R + Carry

Carry = 0 or Carry = 1, but it can't be 0 since R ≠ 9 ⇒ R = 8

```
  9END
+ 108E
------
 10NEY
------
```

~~N = E+1~~

$D + E \geq 12$ (since Y can't be 0 or 1 and there is a carry)

$\Rightarrow D = 7, E = 5$

```
  95ND
+ 1085
------
 10N5Y
------
```

$\Rightarrow N = 6, D = 7$

```
  9567
+ 1085
------
 10652
------
```

Q) (~~will~~ might come for endsem)

```
    I
 LIKE
  THE
+ SILK
------
 SHIRT
------
```

Q)

```
  GO
* GO
------
 COME
------
```

$O \neq 0, 1, 5, 6$

G is atleast 3

$$\begin{array}{r} 73 \\ \times\ 73 \\ \hline 529 \\ \hline \end{array}$$

Q) Consider a chessboard (8×8)
Remove top left corner and bottom right corner.
You are given a 1×2 rectangular object
Prove that it is impossible to place 31 such objects such that it ~~does not~~ covers the entire board

Q) Solve $1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}$

$$x = 1 + \frac{1}{x}$$

$$\Rightarrow 1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}} = \frac{1+\sqrt{5}}{2}$$

Q) Prove $e = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}}}}$

Q) Pg $e = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6}}}}}}$ ...

Q) Pg $\tan x = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \ddots}}}$

Q) Represent $\sqrt{2}$ in terms of $x = \alpha + \cfrac{\beta}{x}$

Ans) $\Rightarrow x^2 - \alpha x - \beta = 0$

$\Rightarrow x = \cfrac{\alpha \pm \sqrt{\alpha^2 + 4\beta}}{2}$

$x = \sqrt{2}$

$1 + \sqrt{2} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}$

$\Rightarrow \sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}$

Q) How would you find continued fraction for a $\sqrt{x}$

INTRO TO Q

three Pol

Qubits

has 2

a spectr

it is a

$|\psi\rangle =$

C

eg. $|\psi\rangle =$

$|\psi\rangle =$

$|a^2| +$

If you

concaps

will b

vector

Expec

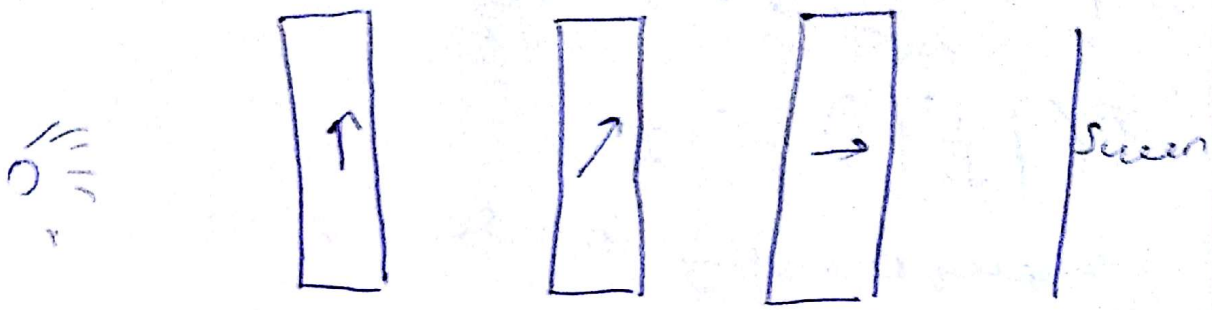
in the

first

to th

INTRO TO QUANTUM ALGORITHMS

three Polarizers experiment



Qubits

has 2 possible outcomes in a spectrum.
It is a state vector in $\mathbb{C}^2$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

($|0\rangle$: state (a times), $|1\rangle$: state (b time))

eg. $|\psi\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$

$|\psi\rangle = a|\nearrow\rangle + b|\nwarrow\rangle$

$|a^2| + |b^2| = 1$

If you measure, it will collapse to ~~it~~ basis vector. state vector will be measured by basis vector.

Expected value of $|a^2| = 1/2$

In three polarizers, for the first polarizer $1|\uparrow\rangle + 0|\rightarrow\rangle$, ~~so 100%~~ 50% of light

passes through
second polarizer

$|\nearrow\rangle = \frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{1}{\sqrt{2}} |\rightarrow\rangle$

$P\left(\left|\frac{1}{\sqrt{2}}\right|^2\right) = \frac{1}{2}$

Therefore $\frac{1}{2}$ of 50% pass through

25% pass through

similarly, $\frac{1}{2}$ of 25% pass through third

12.5% reach screen

In a 2 Qubit system, there are 4 possible combination

$|0\rangle, |0\rangle$

$|0\rangle, |1\rangle$

$|1\rangle, |0\rangle$

$|1\rangle, |1\rangle$

Superposition of all is a possibility

$\therefore a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

For a n-Qubit system, no. of amplitudes required to describe current state $= 2^n$

In 1 mole of gas, it's a 6.023×10^{23} Qubit system

That many combinations can't

realistically be stored in a computer.

EPR Paradox

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

$$|a^2| + |b^2| + |c^2| + |d^2| = 1$$

consider,

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

(other coefficients are zero)

it's a 2 Qubit system. One is on earth, other is taken to mars.

measure the electron state. If one Qubit 'A' on earth is measured to get $|0\rangle$, you get

$$1|00\rangle + 0|11\rangle$$

so one Qubit depends on the other however far they are.

so you measure something on Earth, and other state collapses.

It was experimentally verified that there was spooky effect despite however far it is and even if light hasn't moved yet. It is quantum

entanglement.

Represent qubit as vector.
unitary matrix - inverse of a matrix is its conjugate transpose
$U \cdot U^{\dagger} = I = U^{\dagger} U$
System can be transformed in any unitary way.
(Read up on postulates)

Quantum gates & circuits
Quantum teleportation
- Basic security algorithm - RSA

C-NOT ~~gate~~:
All single qubit unitary matrices (2×2)

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
$|0\rangle \rightarrow |0\rangle$
$|1\rangle \rightarrow |1\rangle$

$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
$|0\rangle \rightarrow |1\rangle$
$|1\rangle \rightarrow |0\rangle$

Z
$|0\rangle \rightarrow |0\rangle$
$|1\rangle \rightarrow |-1\rangle$

Y
$|0\rangle \rightarrow |-1\rangle$
$|1\rangle \rightarrow |0\rangle$

C-NOT
$|00\rangle$
$|01\rangle$
$|10\rangle$
$|11\rangle$

$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

H
$|0\rangle \rightarrow$
$|1\rangle \rightarrow \frac{1}{\sqrt{2}}$

Tele

$1^{+} q$

$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$|0\rangle \rightarrow |0\rangle$
$|1\rangle \rightarrow |-1\rangle$

$Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

$|0\rangle \rightarrow |-1\rangle$
$|1\rangle \rightarrow |0\rangle$

C-NOT is a 2×2 qubit matrix

$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ Hadamard transform

$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(\ \ )$

$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(\ \ )$

Teleportation :

A ——— channel ——— B

$|\psi\rangle$ ——— 2nd qubit of ψ

1st qubit of $|\psi\rangle$

code for A:

1. apply C-NOT to the two qubits
2. apply H to the first qubit
3. measure 2 qubits and get 2 bits of b_0 & b_1
4. send (b_0, b_1) to b.

eg $\psi = \alpha|0\rangle + \beta|1\rangle$,

Initial state is

$$(\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}$$

$$= \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$$

Apply C-NOT

$$\frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|110\rangle + \frac{\beta}{\sqrt{2}}|101\rangle$$

Apply H

$$\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle$$
$$+ \beta|011\rangle - \beta|110\rangle + \beta|001\rangle - \beta|111\rangle$$

b_0 b_1 can be 00, 01, 10, 11

b_0	b_1	$\alpha\|00\rangle + \beta\|\ \rangle$	$\alpha\|0\rangle + \beta\|1\rangle$
0	0		
0	1		
1	0		
1	1		

Code for B:

case $b_0 b_1$:

00 : apply I - gate

01 : apply X - gate

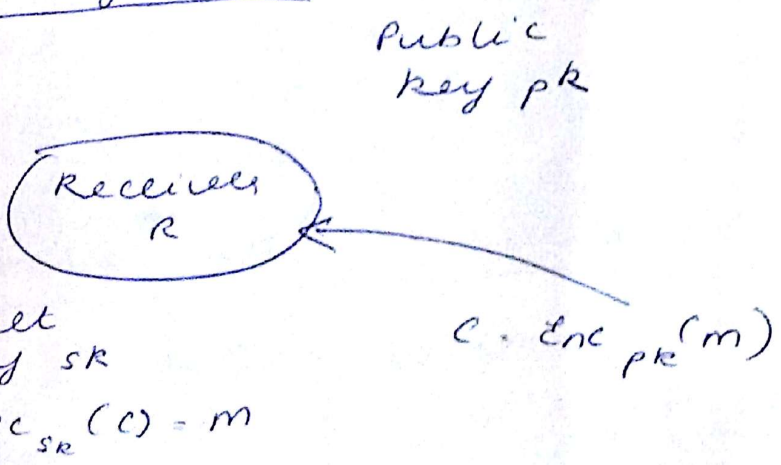
10 : apply Z - gate

11 : apply Y - gate

$\frac{\alpha}{2}|000\rangle + \frac{\alpha}{2}|100\rangle + \frac{\alpha}{2}|011\rangle + \frac{\alpha}{2}|111\rangle$

$+ \frac{\beta}{2}|010\rangle - \frac{\beta}{2}|110\rangle + \frac{\beta}{2}|001\rangle - \frac{\beta}{2}|101\rangle$

RSA algorithm



pk : N, e

sk : p, q → prime nos.

$N = pq$

$\gcd(e, (p-1)(q-1)) = 1$

$ed \equiv 1 \pmod{(p-1)(q-1)}$

Publish this and run the following encryption algorithm

$c = m^e \bmod N$

$m = c^d \bmod N$

$[m^e \bmod N]^d \bmod N$

$m^{ed} \bmod N$

$m^{ed} \bmod N$ (from Fermat's little theo

integer factorization

$\leq_1^*$ Non ~~trivial~~ trivial square roots of unity

$\leq_p^*$ Order of a random group element

$\leq_p^*$ (Quantum) Fourier sampling (Shor's algorithm)

integer factorization

Input : N (composite)

Output : $p \geq 2$, p divides n

Nontrivial ~~Natural~~ square roots of unity

Input : N (composite)

Output : $x \neq \pm 1$, $x^2 \equiv 1 \pmod N$

Order is a random group

Input : $x \in \mathbb{C}_n$

Output : Smallest integer r such that $x^r = 1$

$r = \text{order}(x)$

Quantum Fourier sampling

Input : $\alpha_0, \alpha_1, \alpha_2, \ldots \alpha_{n-1}$

Output : $[\beta_0, \beta_1, \beta_2, \ldots \beta_{n-1}] = DFT(\vec{\alpha})$

Index i we find $|\beta_i|^2$

For non trivial square root of unity

$(x^2-1) \equiv 0 \pmod N$

$(x+1)(x-1) \equiv 0 \bmod N$

$N \mid (x-1)(x+1)$

$\gcd(x+1, N) = p$ (Prime factor since N does not divide either $(x-1)$ or $(x+1)$ individually

$x^r \equiv 1 \bmod N$

If r is even, $[x^{r/2}]^2 - 1 \equiv 1 \bmod N$

$x^{r/2}$ will be a non trivial square root of 1

DFT:

$$\begin{bmatrix} & M & \end{bmatrix}_{N \times N} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} = \begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{bmatrix}$$

$M_{ij} = \omega^{ij}$

$\omega = \sqrt[N]{1}$

Suppose α's were periodic: Non-zeros at some location followed by periodic no. of zeros

If α's are non zero, only at multiples of k, what is β_j?

$$\beta_j = \sum_{l=0}^{N-1} w^{jl} \alpha_l$$

~~α_l is~~

$$\alpha_l = \begin{cases} 0 & \text{if } k \text{ doesn't divide } l \\ 1 & \text{otherwise} \end{cases}$$

$$\alpha_l = \begin{cases} 0 & \text{if } k \nmid l \\ 1 & \text{if } l = jk \end{cases} \quad [k \text{ is period of } \alpha]$$

$$\beta_j = \sum_{l=0}^{N-1/k} w^{jkl} \cdot \alpha_{kl}$$

$$= \alpha \sum_{l=0}^{N-1/k-1} w^{jkl}$$

→ summation of geometric

[If these values of α are equal - called the normalization factor]

$$= \alpha \left[\frac{1 - w^{j(N)}}{1 - w^{jk}} \right]$$

$$= \alpha \left[\frac{1 - w^{jkk}}{1 - w^{jk}} \right] \quad \text{where } K = \frac{N-1}{k}$$

$$\beta_j = \begin{cases} 0 & \text{if } jk \not\equiv 0 \pmod N \\ 1 & \text{if } jk \equiv 0 \pmod N \end{cases}$$

β has period K

Whatever is ~~time~~ period in α is frequency in β and vice versa

$f(a) = x^a \bmod N$

$f(a+r) = x^a \bmod N$ [since r is period]

$f(a+2r) = x^a \bmod N$

$\vdots$

$|\psi\rangle = \sum |i\rangle |f(i)\rangle$

measure some $f(a)$

$|\psi\rangle = \sum (|a\rangle + |a+r\rangle + |a+2r\rangle + \ldots)$ $f(a)$

Offset will be close to N/r

$gcd(i_1, i_2, i_3 \ldots i_s)$ [i_j is multiple of N/r]
$= N/r$

if r is even, done
else repeat

$|\psi\rangle = \sum \alpha_i |i\rangle$

$\downarrow$ QFT

$\sum \beta_i |i\rangle$

Shor's algo:

$O(\log^2 N)$ instead of $O(n \log N)$

α_i's as input is divided into 2 parts in normal FFT.

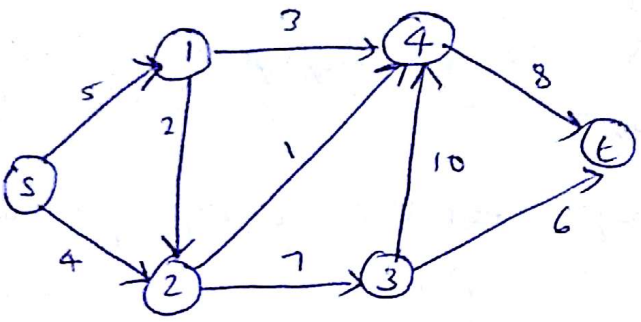
Instead take a superposition and do phase shift.

Take LSB and apply Hadamar transform

To rest of bits apply QFT once.

To the answer, do a phase shift by every power of 2

MAXIMUM NETWORK FLOWS



$f : V \times V \longrightarrow \mathbb{R}$

$$\max \sum_{(s,u) \in E} f(s,u)$$

subject to

$$\forall u, v \in E,\ f(u,v) \leq c(u,v)$$

$$\forall u \in V,\ \sum_{(v,w) \in E} f(v,w) = \sum_{(u,w) \in E} f(u,w)$$

max flow ↔ min cut theorem

max. flow cannot exceed min. cut

~~Min.~~

Residual graph G^f

$V^{(f)} = V$

$E^f = \begin{cases} (u,v) \text{ with capacity } c(u,v) - f(u,v) & \text{if } (u,v) \in E \\ (v,u) \text{ with capacity } f(u,v) & \text{if } (u,v) \in E \text{ with capacity } c(u,v) \end{cases}$

Consider any flow f, get residual graph, if there is any path from s to t, add it and create residual graph for f'

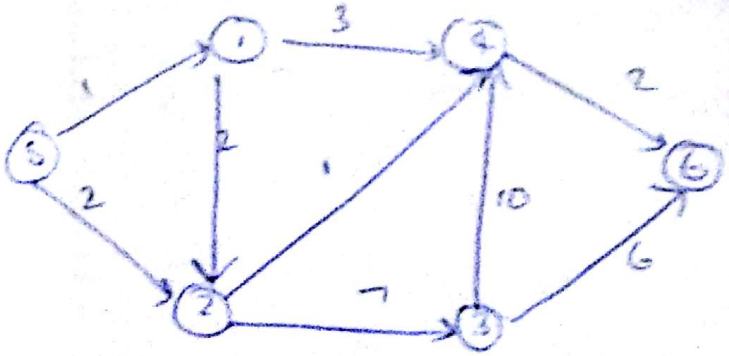
[while ∃ (s-t) path in G_f
$f \leftarrow f + (s-t)$ path]

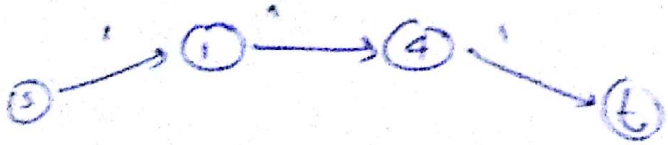
Define two partitions $A, \bar{A}$ in G_f, one which contains s and all nodes reachable from s and other with t and all nodes not reachable from s

All edges from first partition to second will have zero capacity (they would have been reachable otherwise)

In the original graph, in the cut forward would be max full flow and backward with zero

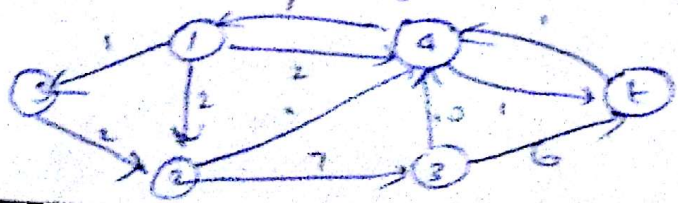
max flow is min. of all cuts





[when initial flow 4 will satisfy the given]

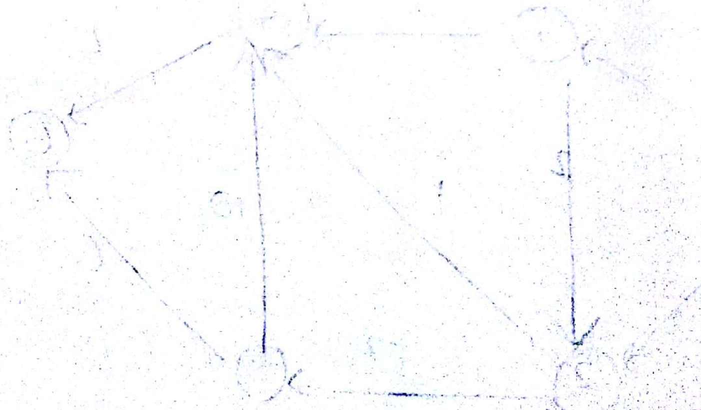
now residual graph becomes



and so on

Ford Fulkerson

Imp (Q) Give an eg. of a graph where this algorithm takes exponential time (graph size and log of capacities)



Q) Writ... perfor... form.

Ans) The ... facto...

$A = \frac{1}{\sqrt{N}}$

~~The ...~~

w_n^k

cos

The ... is

A^+

8) write down the matrix that performs discrete Fourier transform. Show that it is unitary

Sol) The matrix and scalar factor is

$$A = \frac{1}{\sqrt{N}} \begin{vmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & W^1 & W^2 & W^3 & \cdots & W^{N-1} \\ 1 & W^2 & & & & \\ \vdots & & & & & \\ 1 & W^{N-1} & W^{2(N-1)} & & & W^{(N-1)(N-1)} \end{vmatrix}$$

~~The conjugate of W_n^k~~ =

$$W_n^k = e^{\frac{+i2\pi k}{N}} \quad (k \in [0, N))$$

$$\cos\theta - i\sin\theta = \cos(-\theta) + i\sin(-\theta)$$

$$= e^{-i\theta}$$

conjugate

Therefore, conjugate transpose is

$$A^+ = \frac{1}{\sqrt{N}} \begin{vmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 1 & W^{-1} & W^{-2} & & \vdots \\ \cdot & W^{-2} & & & \vdots \\ \vdots & & & & \vdots \\ \cdot & \cdots & \cdots & \cdots & \cdot \end{vmatrix}$$

$AA^T = ?$

Let the resultant matrix be R

The diagonal will consist of N (i.e., $R_{xy} = N$ where $x = y$)

The remaining elements will be equal to 0 since

$$R_{xy} = \sum_{k=0}^{n-1} \underbrace{e^{j(x-y)k}}_{w_0} \qquad (x \neq y)$$

$$= \sum_{k=0}^{n-1} w_0^k \quad \text{(geometric series)}$$

$$= \frac{1 - w_0^N}{1 - w_0}$$

$$= \frac{1-1}{1-w_0} \quad \text{(since } w_0 \text{ is root of unity, } w_0^N = 1\text{)}$$

$\therefore R$ is

$$R = \frac{1}{\sqrt{N}} \frac{1}{\sqrt{N}} A A^T$$

$$= \frac{1}{N} A A^T$$

$$= I$$

Hence, unitary matrix

Q) In genera
fraction
$1+\sqrt{\alpha}$, $1-\sqrt{\alpha}$

Ans) $(x-(1+$

$\Rightarrow x^2 -$

$\Rightarrow x^2 -$

$x = 2$

$1+\sqrt{\alpha}$

$\Rightarrow \sqrt{\alpha} =$

Q) In general, find a continued fraction of $\sqrt{\alpha}$ with roots $1+\sqrt{\alpha}$, $1-\sqrt{\alpha}$

sol) $\left[x-(1+\sqrt{\alpha})\right]\left[x-(1-\sqrt{\alpha})\right]=0$

$\Rightarrow x^2 - x(2) + 1-\alpha = 0$

$\Rightarrow x^2 - 2x + \alpha - 1$

$$x = 2 + \frac{\alpha-1}{x}$$

$$1+\sqrt{\alpha} = 2 + \cfrac{\alpha-1}{2+\cfrac{\alpha-1}{2+\cfrac{\alpha-1}{2+\cfrac{\alpha-1}{2+\ddots}}}}$$

$$\Rightarrow \sqrt{\alpha} = 1 + \cfrac{\alpha-1}{2+\cfrac{\alpha-1}{2+\cfrac{\alpha-1}{2+\cfrac{\alpha-1}{2+\ddots}}}}$$

Q) Show that if we can find order of $A \in Z_m^*$ (random group element), we can factorize a number M.

Ans) We need to find the nontrivial square root of 1 mod M i.e., a no. x such that

$x^2 \equiv 1 \bmod M$ and $x \not\equiv \pm 1 \bmod M$

$\Rightarrow (x+1)(x-1) \equiv 0 \bmod M$

$x+1$ and $x-1$ are non zero and are factors of some multiple of M.

GCD $(M, x-1)$ would give non trivial factor of M, say C.

If C and $\frac{M}{C}$ are not prime, recursively factor them and if they become prime store them as prime factors. The no. of recursive calls are logarithmic in M since there are atmost $\log M$ prime factors of M.

Take a random $A \in Z_m^1$ and find order s.

If s is even, then we could set $x = A^{s/2} \bmod M$ (then $x^2 \equiv A^s \bmod m \equiv 1 \bmod M$). Also, $x \not\equiv -1 \bmod m$

Lemma: Suppose m has ≥ 2 distinct odd prime factors. If we pick $A \in Z_m^*$ uniformly at random, probability that order of s is even and $A^{\frac{s}{2}} \not\equiv 1$ is atleast $1/2$

Randomly pick elements A, compute $GCD(M, A)$ until we find an A for which $GCD = 1$.

If we can't find such an A, then m is an odd prime power in which case we factorize it by binary searching k-th root of m where $k \in [1, \log m]$