Solution corresponding to

$[1,0,0]$ is $35 \times 2 = 70$

$[0,1,0]$ is 21

$[0,0,1]$ is 15

∴ The general solution

$x = (70 \times 1 + 21 \times 2 + 15 \times 3) \bmod (3 \times 5 \times 7)$

$= (70 + 42 + 45) \bmod 105$

$= 52$

∴ In general, $x = 52 + m \cdot 105$

Note that, for sol^n to exist, the inverse must exist. For this to be possible, ~~A~~ the numbers must be mutually prime

LECTURE - XV

LECTURE - XVI

PUZZLE

Assuming each character is a ~~digit~~ distinct digit, solve :-

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

~~d+e~~

$$1000(s+m) + 100(e+o) + 10(n+r)e + d+e = 10^4 m + 1000 o + 100 n + 10 e + y$$

$$(d+e) \bmod 10 = y ;$$

```
  9999
+ 9999
------
```

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

de + e ≡ y mod 10

Note that

$m = 1$

$\Rightarrow s = 9$ or 8

$\therefore o = 0$ or 1 (1 not possible as $m = 1$)

$\Rightarrow o = 0 \Rightarrow s = 9$

Also, $n \neq 0$

```
  SEND
+ 10RE
-------
 10NEY
```

```
  SEND
  9END
+ 10RE
-------
 10NEY
```

Now, $N = E + 1$

$10 + R = E + 1 + R + C$

$9 = R + C$

Since $R \neq 9$, $C = 0$ or 1,

$C = 1$ and $R = 8$

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

$D + E \geq 12$ ($y \geq 2$)

```
  9567
+ 108S
-------
 1065 2
```

$D = 7, E = 5 \Rightarrow N = 6, y = 2$

★ → END-SEM PROBLEM :- SOLVE

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

→ each character is a distinct digit.

31

32

GO
× GO
COME

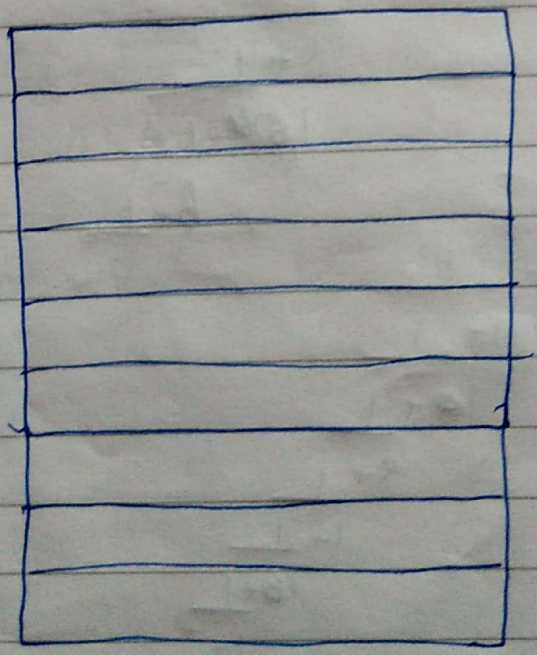
GO
× GO
COME

$(10g+0)(10g+0) = 100g^2 + 20g0 + 0^2$
$= 10^2c + 10^2o + 10m + e$

$c = o^2$
$\therefore e = 1, 4 \text{ or } 9$
$o = 0, 1, 2 \text{ or } 3$

$(g^2 \bmod 10) = e$
$20go = 10o + 10m$
$2go = 10o + m$
$20(g-5) = m$
$\therefore o \neq 0, g \geq 5$
$g = 5, 6, 7, 8, 9$

↳ Given a chessboard with LR and UL cell removed. Prove whether it is impossible to cover this with exactly 31 1×2 blocks.



$a=0$

$a, -a, a>0$

$x^2 - ax - b = 0$

$x^2 = +ax + b$

$x^2 = b$ $\quad x = +a + \frac{b}{x} = +\left(a + \frac{b}{x}\right)$

→ CONTINUED FRACTIONS

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \dots}}}$$

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

$$x^2 - x - 1 = 0$$

$$\Rightarrow x = \frac{1 \pm \sqrt{1+4}}{2} \quad \text{as } x > 0$$

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

~~FANO~~

1.) $e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + 1}}}}}}$ → 9

$$e_n = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + 1}}}}}}$$

$e_n 2$

$e_n 2 x$

$x = +\left(a + \cfrac{b}{a+\cfrac{b}{a+\cfrac{b}{\ddots}}}\right)$ ⇒ given a number as root of a quadratic we can form it's continued fraction (if it converges)

2) $\tan x = \cfrac{x}{1-\cfrac{x^2}{3-\cfrac{x^2}{5-\cfrac{x^2}{7-\ddots}}}}$

$\cfrac{x}{\tan x} = 1 - \cfrac{x^2}{3-\cfrac{x^2}{5-\cfrac{x^2}{7-\ddots}}}$

$1 - \cfrac{x}{\tan x} = \cfrac{x^2}{3-\cfrac{x^2}{5-\cfrac{x^2}{7-\ddots}}}$

3) ~~$\sqrt{x}$ ~~ ~~Let $\sqrt{2}$ be a non~~

We wish to generate fraction for $\sqrt{2}$.

~~Take $\sqrt{2}$, $\sqrt{2}-2$~~

$\therefore x^2 \neq$ 2 ~~rational~~

$\sqrt{2} = \lceil \alpha + \frac{\beta}{\sqrt{2}}$

$\Rightarrow \sqrt{2} - \alpha = \frac{\beta}{\sqrt{2}}$

$\Rightarrow \beta = 2 - \alpha\sqrt{2}$

Taking $\beta = 1$, $\alpha\sqrt{2} = 1 \Rightarrow \alpha = \frac{1}{\sqrt{2}}$

$\therefore$ ~~$\sqrt{2}$~~ C.F for $\sqrt{2}$ is

$\cfrac{1}{\sqrt{2}} + \cfrac{1}{1+\cfrac{1}{\sqrt{2}+\cfrac{1}{\sqrt{2}+\cdots}}}$

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

$$x = 1 + \cfrac{\sqrt{2}-2}{1+\cfrac{\sqrt{2}-2}{1+\sqrt{2}-2}}$$

In general to find continued fraction of $\sqrt{\alpha}$ form quadratic with roots $1+\sqrt{\alpha}$, $1-\sqrt{\alpha}$.

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

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

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

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

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

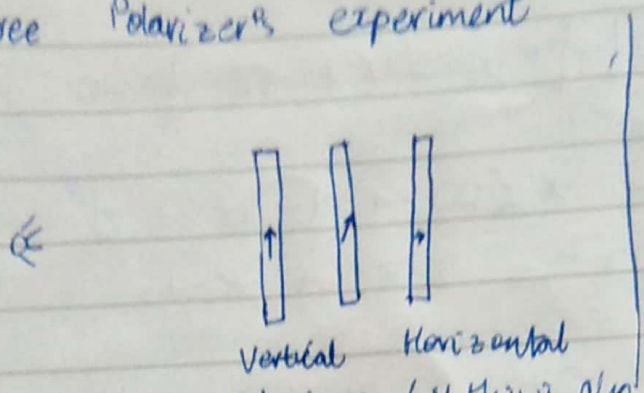
$$\Rightarrow \sqrt{\alpha} = 1 + \cfrac{\alpha-1}{2+\cfrac{\alpha-1}{2+\cfrac{\alpha-1}{2+\cfrac{\alpha-1}{2+\ddots}}}}$$

END-SEM QUESTION:- Find general continued fraction for $\sqrt{\alpha}$.

LECTURE - XVII

Intro. To Quantum Algorithms

→ Three Polarizers experiment



(due to this alone, only 50% of the photons pass through). (If this is also added, 0% of photons pass through)

Vertical ⇒ 50% photons pass through

V+H ⇒ only 0% photons pass through

V + ↗ + H ⇒ $\frac{1}{8}$ of the photons pass through.

→ Qubits :- Models simplest non-trivial quantum systems.

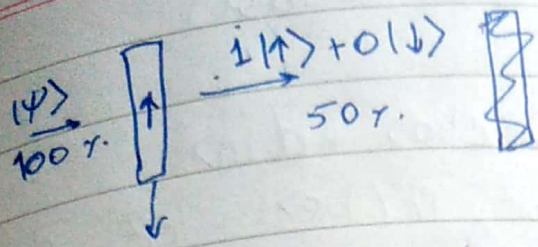
Simplified postulates for 1 qubit systems :-

1.) For each system, ∃ a vector in $\mathbb{C}^2$ s.t it's norm is 1.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$\therefore |\psi\rangle = a|\uparrow\rangle + \beta|\downarrow\rangle \quad , \quad |a^2| + |b^2| = 1$$
$$|\psi\rangle = a|\nearrow\rangle + b|\swarrow\rangle$$

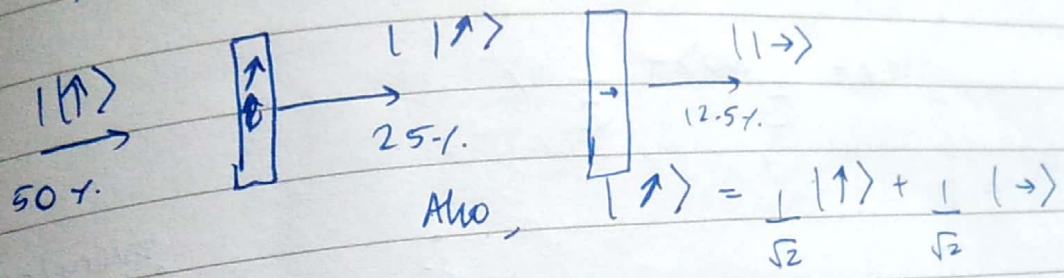
2.) On measuring, probability of measuring $|0\rangle$ is $|a|^2$, probability of measuring $|1\rangle$ is $|b|^2$

3.) After measurement, system collapses to either $|0\rangle$ or $|1\rangle$.



only allows vertical photons to pass (after measurement).

These are 50% in number.



∴ only 50% of the photons pass.

→ 2-qubit systems

4 possibilities :- |0⟩ ; |0⟩
|0⟩ ; |1⟩
|1⟩ ; |0⟩
|1⟩ ; |1⟩

For such systems, their state can be written as superposition of all the four states.

i.e $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

This shows why classical computers cannot compute quantum systems properly - for n-bit quantum system, 2^n amplitudes needs to be stored.

∴ Exponential increase of storage.

- This also shows why quantum computers can easily solve classical problems. (inverse of above argument)

Scanned by CamScanner

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

→ EPR Paradox (Einstein - Podolski - Rosen Paradox)

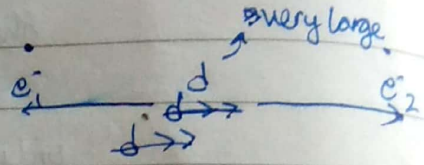
for 2 qubit systems,

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

$\therefore Pr(|00\rangle) = |a|^2$, $Pr(|01\rangle) = |b|^2$, $Pr(|10\rangle) = |c|^2$, $Pr(|11\rangle) = |d|^2$

Consider systems with wavefunction

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



On measurement of one e^-, system collapses to $|00\rangle$ or $|11\rangle$ ⇒ e^-_2 collapses

∴ On measurement of one e^-, second one also collapses instantaneously.

This violates relativity.

Such states are called entangled systems.

Entanglement provides exponential speedups as compared to classical methods.

→ Feynmann's Argument

But, problems arise as we cannot use all the numbers - on measurement, only 1 number remains, rest are lost. Also, the one number we get is random.

→ Shor's intuition :-

Even to choose 1 number out of 2^n numbers, classical computers will be slow. ∴ Quantum methods offer an advantage - sampling from 2^n elements is still slow.

LECTURE-XVIII

Schrodinger equation :- Governs evolution of wavefunction with time
equivalent formulation in matrix mechanics :- If time evolution
is linear and norm-preserving, then time evolution is
given by multiplication with a unitary matrix U.

Unitary matrix :-

$$U \otimes U^{\dagger} = \mathbb{I}$$

$$\therefore U(t) \otimes |\psi(0)\rangle = |\psi(t)\rangle$$

$$\begin{bmatrix} U \end{bmatrix} \begin{bmatrix} v \end{bmatrix} \rightarrow \begin{bmatrix} w \end{bmatrix}$$

Quantum algorithm :- We start with a ~~qubit~~ state, proceed
by multiplication with unitaries, then measure, and gather
consequences or information.

Quantum gates :- Unitary transforms that can approximate
~~Every quantum~~ most other unitary transforms i.e some
sort of universal gates (like NAND and NOR).
but, quantum gates are not optimal - ~~so~~ as opposed to
classical gates, where only a small number of gates can
~~automate~~ help in forming all other transforms.
Simulating a 2n ~~8~~-bit qubit quantum system with n-qubit
systems require an exponential increase in the gates, as opposed
to classical systems, where blowup is atmost polynomial

Universal basis :- the C-NOT gate and all single qubit
unitary matrices form a basis.

Out of all 2×2 unitary matrices, a few are ~~some~~ more important

$T\begin{bmatrix}1\\0\end{bmatrix}$ $T:$ $\begin{bmatrix} | & | & & | \\ T(u_1) & T(u_2) & \cdots & T(u_n) \\ | & | & & | \end{bmatrix}$

$T(u_1)T(u_2)\ldots T(u_n)$

$I = \begin{bmatrix}1&0\\0&1\end{bmatrix}$ $|0\rangle \to |0\rangle$, $|1\rangle \to |1\rangle$ $\quad |0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$

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

$Z = \begin{bmatrix}1&0\\0&-1\end{bmatrix}$ $|0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$

$Y = \begin{bmatrix}0&1\\-1&0\end{bmatrix}$ $|0\rangle \to -|1\rangle$, $|1\rangle \to |0\rangle$

(note that our nomenclature is non-standard)

C-NOT :- A 2-qubit gate i.e 4×4 unitary transform.

$$\text{C-NOT} = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

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

$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$, $|01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$

$|11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$

Hadamard gate H:-

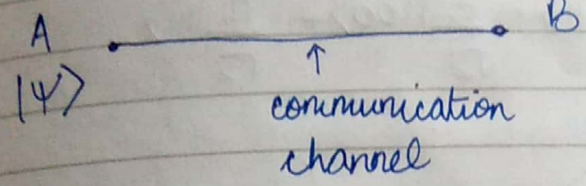
$|0\rangle \to \frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|1\rangle \to \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ $\quad \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$

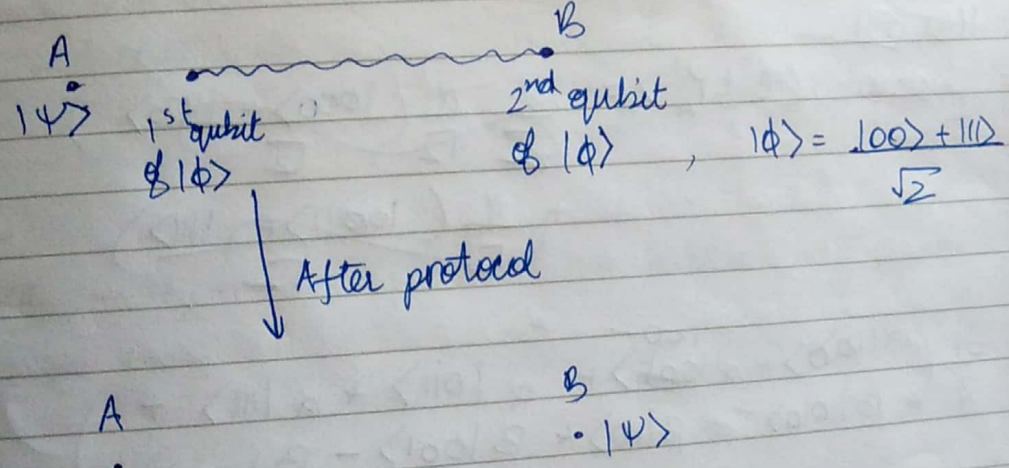
$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix}$$

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

→ Quantum Teleportation Protocol :- ~~we send data~~



We wish to send $|\psi\rangle$ across A, B
For this, we can consider ~~the two~~ to ~~have~~ share an EPR pair (~~quanto~~ entangled pair).



Protocol :- For A

① Apply CNOT to the entangled pair
② Apply H to the first qubit
③ Measure the two qubits and obtain two (classical) bits b_0, b_1. Send these bits to B.

For B :- If $b_0 b_1 = 00$, B applies nothing
$b_0 b_1 = 01$, B applies X-gate
$b_0 b_1 = 10$, B applies Z-gate
$b_0 b_1 = 11$, B applies ~~Z then X gate~~ Y-gate

$A^\dagger A = I \Rightarrow A^\dagger = A^{-1}$ $\quad AB = BA$

$B^\dagger B = I$ $\quad = A^\dagger B$

Proof :-

If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, then initial state for two qubits with A is

$$|\psi_{AB}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

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

$$(\text{C-NOT} \otimes I)\,|\psi_A\rangle = |\psi'_A\rangle$$

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

$$|\psi''_A\rangle = (H \otimes I \otimes I)\,|\psi'_A\rangle = \frac{\alpha}{\sqrt{2}}\left(\frac{|000\rangle + |100\rangle}{\sqrt{2}}\right) + \frac{\alpha}{\sqrt{2}}\left(\frac{|011\rangle + |111\rangle}{\sqrt{2}}\right)$$

$$|\psi''_A\rangle = \frac{1}{2}\left(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle\right)$$

Now, we measure the two qubits with A.

If b_0 = state of qubit after collapse

b_1 = state of 1st entangled qubit after collapse.

$|x\rangle$:- state of qubit with B after measurement

b_0 b_1	$\|x\rangle$
00	$\alpha\|0\rangle + \beta\|1\rangle = \|\psi\rangle$
01	$\alpha\|1\rangle + \beta\|0\rangle = X\|\psi\rangle$
10	$\alpha\|0\rangle - \beta\|1\rangle = Z\|\psi\rangle$
11	$\alpha\|1\rangle - \beta\|0\rangle = XZ\|\psi\rangle$

∴ After end of the protocol, $|\psi\rangle$ is sent across to B without actually sending the physical object.

→ Fourier Transform :- a linear transform from the set of functions to another set itself. If it is linear and norm preserving a unitary matrix, then, if we can represent it as a sum of the universal gates, then we can do the transform very fast.

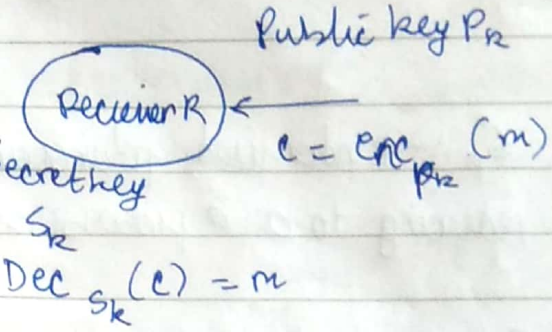
→ RSA Algorithm

Public key P_k

Secret key S_k

enc_{P_k} :- encrypt with P_k

dec_{S_k} :- decrypt with S_k



RSA :-

P_k : N, e :- publish the public key

S_k : p, q

↓

large primes

$N = pq$

e : co-prime to number s.t

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

$$ed \equiv 1 \bmod [(p-1)(q-1)]$$

Encryption algorithm :-

$$c = m^e \bmod N$$

Decryption algorithm :-

$$m = c^d \bmod N$$

Proof :-

$$c^d \bmod N = (m^e \bmod N)^d \bmod N = m^{ed} \bmod N = m^{ed \bmod \phi(n)} \bmod N$$

↳ extended Fermat's theorem

By our choice of e, d,

$$m^{ed} \bmod N = m \bmod N = m$$

$$\therefore c^d \bmod N = m$$

LECTURE - XIX

→ Integer factorization $\leq_p^r$ Non-trivial square roots of unity $\leq_p^r$ order of a random group element $\leq_p^r$ (Quantum) Fourier sampling (Shor's algorithm)

$\leq_p^r$ – randomised polynomial time reduction i.e polynomially reducing to a probabilistic extent.

(I) Integer factorization
Input – A composite integer n
Output – $p \geq 2$ s.t $p \mid n$
(Recursively applying this can help us get the prime factorization)

(II) Non-trivial square roots of unit
Input – N (composite)
Output – $x \neq \pm 1$ s.t $x^2 \equiv 1 \bmod N$

(III) Order of a random group element.
Input – $x \in G$, G is a group
Output – Smallest integer r s.t
$x^r = 1$, $1 \in G$ is the identity element
$(r = O(x))$

(II) (Quantum) Fourier sampling

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

output :- $[\beta_0\ \beta_1 \ldots \beta_{N-1}] = DFT(\vec{\alpha})$, where DFT is the Discrete Fourier transform

(normalised)

The output is the index i with probability $|\beta_i|^2$.

~~(note that that index will be more probab~~

① $\Rightarrow$ (I) $\leq_p^r$ (II)

$x^2 \equiv 1 \bmod N \Rightarrow x^2 - 1 \equiv 0 \bmod N$, $x \neq \pm 1$

$\Rightarrow (x-1)(x+1) \equiv 0 \bmod N$, $x \neq \pm 1$

$\Rightarrow N \mid (x-1)(x+1)$, $x \neq \pm 1$

Note that, $x < N$

Take $p = \gcd(x+1, N)$. Then $p \mid N$

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

If $p \in$ Prime, $p \mid N$, then $p \mid (x-1)(x+1)$??

W.L.O.G, ~~take~~ we can take

$p = \gcd(x+1, N)$

e.g.

$N = 187$

We wish to find p s.t $p \geq 2$, $p \mid N$.

We find x s.t $x^2 \equiv 1 \bmod 187$, and then, $p = \gcd(x+1, 187)$ is a $p \geq 2$ s.t $p \mid N$.

Such an x is $x = 67$, as $187 \mid (67^2 - 1)$

$\therefore p = \gcd(68, 187) = 17$

$\therefore 17$ is a prime factor of 187.

$$a + a^2 + \dots + a^{d-1} = \frac{a^d - 1}{a - 1}$$

① (II) $\leq_p^r$ (III)

$x \in G_1$

$r = \text{Order}(x)$ i.e. r is smallest number s.t. $x^r = 1$

Taking $G_1 = Z_N^*$, then $Z_N^* = \{ x \in Z \mid n \text{ is coprime with } N \}$

group operation is product modulo N

$x^r \equiv 1 \bmod N$

Now, if $r = 2n$, $n \in Z$, then

$(x^{r/2})^2 \equiv 1 \bmod N$

$\Rightarrow$ $x^{r/2}$ is a non-trivial square root of unity.

~~If $r = 2n+1$, then we find r for some x~~

~~$x^{2n} \cdot x \equiv 1 \bmod N$~~

If $r = 2n+1$, then we take some other random number y, and proceed.

e.g.

$N = 15$, $x = 7$ (picked randomly)

Now $7^4 \equiv 1 \bmod 15$

$\Rightarrow r = 4$,

$\therefore (7^2)^2 \equiv 1 \bmod 15$

$\therefore$ Non-trivial square root of unity is $7^{4/2} = 4$

③ ~~DFT~~ (III) $\leq_p^r$ (IV)

DFT :-

$$[M]_{N \times N} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} = \begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{bmatrix}, \text{ where}$$

$M_{ij} = \omega^{ij}$, ω is N^{th} root of unity.

2401

Suppose α_i's are periodic i.e

$$\vec{\alpha} = \begin{bmatrix} \alpha_0 \\ 0 \\ 0 \\ \vdots \\ \alpha_k \\ 0 \\ \vdots \\ \alpha_{2k} \\ \vdots \\ \alpha_{3k} \\ \vdots \end{bmatrix} \begin{matrix} \} k \\ \} k \\ \} k \end{matrix}$$

i.e k - fixed zeros

Then, $\vec{B} = M\vec{\alpha}$ is also periodic, with period $\frac{N}{k}$

~~$M\vec{\alpha} = 0$~~

Proof :-

$B_j = M_j \cdot \vec{\alpha}$, where M_j is j^{th} row of M

$$\Rightarrow B_j = \sum_{l=0}^{N-1} \alpha_l \omega^{jl}$$

Now $\alpha_l = 0$ if $k \nmid l$, ~~$k \in l$~~ $\alpha_l = 1$ if $k \mid l$

i.e $\alpha_l = \begin{cases} 0 & \text{if } k \nmid l \\ \neq 0 & \text{if } k \mid l \Rightarrow l = jk \end{cases}$

$$\therefore B_j = \sum_{l=0}^{\frac{N}{k}-1} \omega^{jkl} \alpha_{kl}$$

If α_{kl} are all equal ~~to~~ to α, then

$$B_j = \alpha \sum_{l=0}^{\frac{N-1}{k}} \omega^{jkl}$$ (where, in quantum case, α is normalisation factor)

↳ GP

$$\Rightarrow B_j = \left(\frac{\omega^{jk\left(\frac{N}{k}\right)} - 1}{\omega^{jk} - 1} \right) \alpha = \alpha \left[\frac{1 - \omega^{j(N)}}{1 - \omega^{jk}} \right], \text{ if } \omega^{jk} \neq 1$$

$$1 + \omega^{jk} + \omega^{2jk} + \dots + \omega^{(N-1)jk}$$

$$B_j = \alpha \left[1 - \omega^{jk} \right]$$

$$B_j = \alpha \sum_{l=0}^{\frac{N-1}{k}} \omega^{jkl}$$

$$= \alpha \left[\frac{1 - \omega^{j\left(\frac{Nk}{k}\right)}}{1 - \omega^{jk}} \right], \text{ if } \omega^{jk} \neq 1 \quad (\omega^N = 1)$$

Now if $K = \frac{N-1}{k}$, then

$$B_j = \alpha \left[\frac{1 - \omega^{jkk}}{1 - \omega^{jk}} \right]$$

If Note that

$$B_j = \begin{cases} 0, & \text{if } jk \neq 0 \bmod N \\ \neq 0, & \text{if } jk \equiv 0 \bmod N \end{cases}$$

∴ The period for the output is

$$j \quad \frac{N}{k}$$

∴ Frequency of $\vec{\alpha}$ → period of $\vec{\beta}$
Period of $\vec{\alpha}$ → ~~period of~~ frequency of $\vec{\beta}$.

This is true even when offset is not zero.

Now, to find period of the elements in the following function

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

$$\therefore f(a+r) = x^a \bmod N, \quad f(a+2r) = x^a \bmod N, \ldots$$

$\therefore$ f is periodic with period r.

Now, if

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

↳ basis state of N qubit system.

If we measure $f(a)$, we get, after the collapse, ↳ on the second term.

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

Now, if

i.e. $\sum \beta_i |i\rangle |f(a)\rangle$ is Fourier Transformed, then, ↳ possible as Fourier transform is a unitary operation

only at multiples of $\frac{N}{r}$, will our β_i be non-zero.

$\therefore$ If we pick i with probability $|\beta_i|^2$, then we will get only those i indices which are close to multiples of $\frac{N}{r}$,

i.e as all others will have probability 0.

$$\ldots i_1, i_2, i_3, \ldots i_5 \simeq \text{Multiple of } \frac{N}{r}$$

If we take gcd of $i_1, i_2, i_3, \ldots i_5$, then, with very high probability, we get $\frac{N}{r}$ as the answer.

$|x_m - x_n| < \epsilon \quad \forall\ m,n > N$

$\forall L > 0\ \exists \epsilon > 0$ s.t $\forall$ terms N

$n > N \Rightarrow |x_n - L| < \epsilon$

Now, we prove that a Quantum Fourier Transform is a polynomial sized ie we can do QFT using polylog no. of gates.

$|\psi\rangle = \sum \alpha_i |i\rangle \Rightarrow F|\psi\rangle = \sum \beta_j |j\rangle$, where $\vec{\beta} = N\vec{\alpha}$

~~Shor's Algorithm :-~~

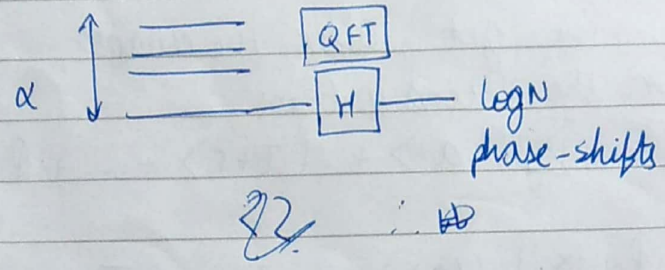
$$FFT(\vec{\alpha}) = FFT(\vec{\alpha}_{odd}) + FFT(\vec{\alpha}_{even})$$

Merge, phase-shift, add.

Instead, we can superpose both the systems.

So, we do the following :-

(I) Apply H (Hadamard) to the LSB.



$\therefore$ We can merge in $O(\log N)$

Hence,

$QFT(\vec{\alpha}) = QFT(\vec{\alpha'}) + O(\log N)$ gates

To $\vec{\alpha'} = \vec{\alpha}$ without LSB.

$\therefore QFT(n) = QFT(n-1) + O(\log N)$, where n is no. of qubits

i.e $n = \log N$

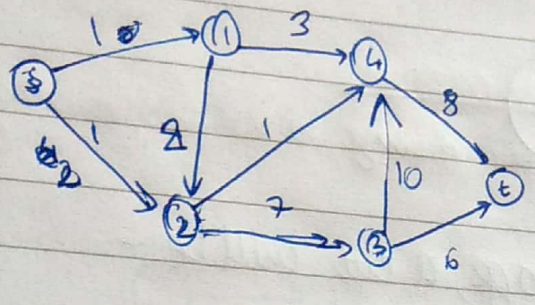
$\therefore QFT(\log n) = QFT(n-1) + O(n)$

$\vdots$

$QFT(n) = O(n^2 \log^2 n) = O(\log^2 N)$

LECTURE - XX

→ MAXIMUM NETWORK FLOWS



Modelling of a network can be done via an undirected graph from source to sink. The weights represent in some way the maximum quantity of flow possible.

Problem :- What is the maximum rate at which capacities can flow ?

Flow :- A function $f : V \times V \to \mathbb{R}$

We wish to find f s.t Max $\sum_{(s,u) \in E} f(s,u)$ subject to the following constraints on f :-

1.) $\forall (u, v) \in E, \quad f(u,v) \leq C(u,v)$

2.) $\forall u \in V$

$$\sum_{(u,v) \in E} f(u,v) = \sum_{(v,u) \in E} f(v,u)$$ i.e no storage or blockage on any node (??)

This is also a linear programming problem.

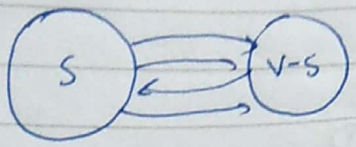
We use the Ford - Fulkerson (??) algorithm.

Theorem:-

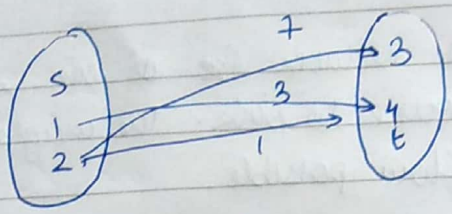
Max flow → Minimum Cut Theorem

~~Max flow~~

Cut of a graph of G:-



e.g. for graph on previous page, a cut will be :-



Capacity of the cut :- Sum of edges connect two parts.

e.g. for above case, it is $7+3+1 = 11$

Maximum flow ≤ minimum capacity of cut

Residual graph of G^f of a flow f :-

If $G = (V, E)$, $G^f = (V^f, E^f)$, then

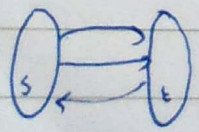
$V^f = V$ and $E^f = \begin{cases} (u,v) \text{ with capacity } c(u,v) - f(u,v) & \forall (u,v) \in E \\ (v,u) \text{ with capacity } f(u,v), & \forall (u,v) \in E \text{ if } f(u,v) \neq 0 \end{cases}$

Algorithm :-

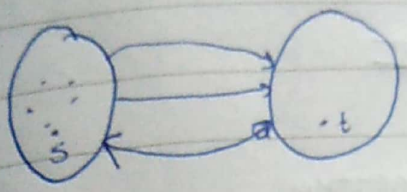
while ∃ path from s to t in G^f,

$f \leftarrow f +$ (s-t) path (add the s-t path to the flow)

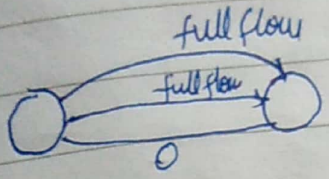
Proof :- Partition G^f into two partitions - all nodes reachable from s, and all nodes not reachable from s.



In the final stage, ∄ path from s to t.
∴ the cut would be of the form



∴ The G would have the form

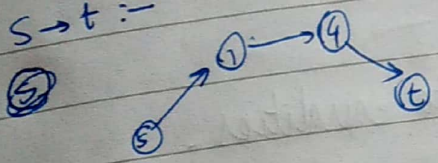


full flow :- ∀ f(u,v) = C(u,v)

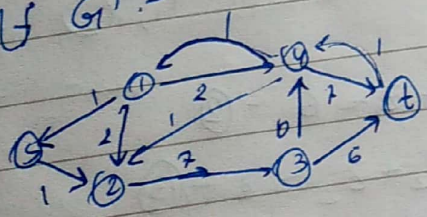
e.g. On our example graph let initially f(u,v) = 0 ∀ (u,v)

∴ G_f = G

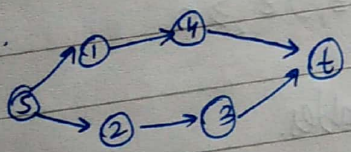
∃ Path from s → t :-



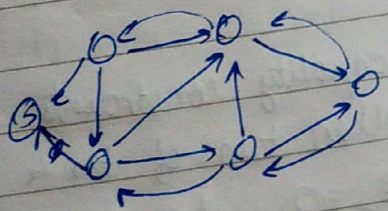
∴ f(u,v) = 0 ∀ G_f :-



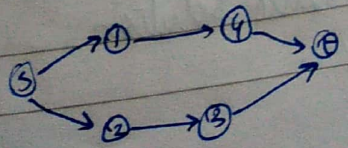
∃ path s → t :-



∴ G_f :-



No path from s → t ⇒ the final flow is



→ QUESTION:- Given an example of a graph where the given algorithm takes exponential time.

LECTURE-XXI

SIMPLEX ALGORITHM

(for solving linear programming problems)

Example

Maximise $x_1 + x_2$

subject to

$$x_1 + 2x_2 \leq 6$$
$$x_1 - x_2 \leq 3$$
$$x_1, x_2 \geq 0$$

We convert inequalities into equalities.

∴ Maximise $x_1 + x_2 = f(x_1, x_2)$ — ①

subject to

$$x_1 + 2x_2 + z_1 = 6 \quad -②$$
$$x_1 - x_2 + z_2 = 3 \quad -③$$
$$x_1, x_2, z_1, z_2 \geq 0$$

$z_1, z_2 \rightarrow$ slack variables.

4 variables, 2 equality constraints.

Basic solution :- when two of the 4 variables are zero.

e.g. $z_1 = 0$, $z_2 = 0$, solve for x_1, x_2, we get

$$x_1 = 4, \quad x_2 = 1$$

∴ $(4, 1, 0, 0)$ is a basic solution.

Basic feasible solution :- A basic solution where all constraints are met e.g. ie $x_1, x_2, z_1, z_2 \geq 0$

For example, $(4, 1, 0, 0)$ is a basic feasible solution.

Basis :- set of variables which are non zero in the basic feasible solution e.g. $\langle x_1, x_2 \rangle$.

Now, we try to get a basic feasible solution s.t the objective function does not contain elements of the basis.

$\therefore$ If $x_1 = x_2 = 0$, $\Rightarrow$ basis $= \langle z_1, z_2 \rangle$

$\therefore z_1 = 6, z_2 = 3$

$(0, 0, 4, 3)$:- basic feasible solution.

The objective function does not contain any basic variables.

Now, it is easy to check whether f is optimum here.

We can observe that it is not optimum as we can increase value of x_1 ~~or x_2~~ (x_1 has coefficient of x_1 is +ve in ~~equality constraint~~).

Choose a variable to ENTER the bases, and another to EXIT

e.g. make $x_1 = 3$, $z_2 = 0$, $z_1 = 3$, $x_2 = 0$

Now, the basis is $\langle x_1, z_1 \rangle$.

Now we check if this is optimum.

x_2, z_2 are non-basic elements, so we try to express f in terms of x_2, z_2.

$f(x_1, x_2) = x_1 + x_2 = 2x_2 - z_2 + 3$ - (3)

(1) - (2) $\Rightarrow 3x_2 + z_1 - z_2 = 3$ - (1) (has exactly one basis variable)

$x_1 - x_2 + z_2 = 3$ - (2) (, , ,)

Now, it is easy to check whether the solution is optimum.
Note that we can increase x_2 by atmost 1 to increase f.
∴ We move to next basis, where $x_2 \uparrow 1$, $z_1 \downarrow 3$, $x_1 \uparrow 1$

$x_1 = 4$, $x_2 = 1$, $z_2 = 0$, $z_1 = 0$

Basis :- (x_1, x_2)

Objective function in terms of non-basis elements :-

$③' = ③ - \frac{2}{3} ①'$

$$f(z_1, z_2) = -z_2 - \frac{2}{3} z_1 + \frac{2}{3} z_2 + 5 \quad — ③''$$

$$f(z_1, z_2) = -\frac{1}{3} z_2 - \frac{2}{3} z_1 + 5$$

①', ②'' must contain exactly one basis element.

$$3x_2 + z_1 - z_2 = 3 \quad — ①''$$

$② = ② + \frac{1}{3} ①'$

$$\therefore x_1 + \frac{1}{3} z_1 + \frac{2}{3} z_2 = 4 \quad — ②''$$

Now, note that we cannot increase z_1, z_2 to increase optimum solution, as coeff. of z_1, z_2 is -ve in ③''.
∴ For optimum solution, $z_1 = z_2 = 0$, and $x_1 = 4$, $x_2 = 1$

$$\therefore \max_{\text{constraint}} \{f(x_1, x_2)\} = 5$$

SIMPLEX ALGORITHM:-

- start with a basic feasible solution
- check whether it is optimum or not (by transforming f in terms of non-basic elements)
  - If yes, output it
  - If no move to the next b.f.s.

e.g.

Maximise $c^T x$

subject to $Ax \leq b$, $x_i \geq 0$

$x \leq y$ means each $x_i \leq y_i$

Subject to

$$Ax = b, \quad x_i \geq 0$$

e.g. $x_1 + x_2$, subject to

$$\begin{bmatrix} 1 & 2 & 1 & 0 \\ 1 & -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} 6 \\ 3 \end{bmatrix}$$

Simplex :- Write constraints as

	x_1	x_2	z_1	z_2	b
z_1	1	2	1	0	6
z_2	1	-1	0	1	3
Objective fn	1	1	0	0	0 → current value. (finally, it gives $-f$)

Step 1:- & Check if ~~sol~~ current solution is feasible.
Step 2:- Choose a variable to ENTER the bases (choose variable non-ve in the objective fn).

OR

Step 1:- Choose some column j such that, in the last row, the value is +ve in that column.
[If no such is found, we have reached the answer and we can output -ve of bottom-right value.]
In our example, we chose column 1 (i.e x_1)

Step 2 :- ~~Find an i~~ Choose the row i s.t among all i ∈ {i} value at $\langle i,j \rangle$ a_{ij} is maximised., and pivot at a_{ij}.

e.g. in our example, after pivot,

	x_1	x_2	z_1	z_2	b
z_1	0	3	1	-1	3
x_1	1	-1	0	1	3
Obj.	0	2	0	-1	-3

Pivot :- In one constraint, only one basis element should be present and, in the other, the other basis element should be present. Also, in obj. function, only non-basis elements must exist.

Now Step 3 :- Repeat.

e.g. now, x_1, x_2 is basis.

	x_1	x_2	z_1	z_2	b
x_2	0	1	1/3	-1/3	1
x_1	1	0	1/3	2/3	4
Obj.	0	0	-2/3	-1/3	-5

Now, in last row, all columns are non -ve. ⇒ $-(-5) = 5$

is the optimum answer.