Lecture II : Rotate, Compute, Rotate

25/07/19

- Quantum Mechanics
  ↳ probability with negative signs :)
- Probabilistic Computing ← parable for QC
  ↳ Deterministic + coin flip

Q Is probabilistic computing >> classical?
Ans : Yes, by definition eg. generate random bits.
Ans : Maybe not, when just computing functions
eg. multiply, factorize, find MST etc.

- Probabilisting computation trades errors for efficiency
eg : primality testing. (polynomial speedup, not exp)

Primality Testing :

naive : $O(\sqrt{2^n}) = O(2^{n/2})$ steps

G. Miller '76 : Assuming Extended Riemann Hypothesis
↳ $O(n^4)$ steps ≡ in "P" time

Solovay - Strassen '77 : $\approx O(n^3)$ steps
Rabin '80 : prob. riff on Miller
↳ $O(n^2)$ steps

AKS '02 : Deterministic alg. Provable

↳ $O(n^{12})$ steps

Lenstra - Pomeance : $O(n^6)$ steps

deterministic

Strongly believed :

* Every algorithm that's "in P" probabilistically, is also "in P" deterministically

Probabilistic Computation :

- Deterministic + one extra power
- Quintessential use : simulate random phenomenon
- Speedups over deterministic for many problems
- Doesn't give exponential speed ups (strongly believed)

{shor, grover, SAT, Subset Sum}

<u>Quantum Computation</u> :

- Classical + one extra power
- Simulate quantum phenomenon
- gives speedups over deterministic & probabilistic
- QC gives exponential speeds over classical

  eg : factoring
- Strongly believed that QC doesn't give exp speedups for many problems, eg : SAT and other NP complete problems

Probabilistic Code

- Initialize A[ ] of length 1000
- for $0 \leq i < 100$
  $A[i] := \text{CoinFlip}(0/1)$
- followed by deterministic code
- state is defined by 2^{1000} #s

QC code

- Initialize 1000 photons
- run through obstacle course (mirrors, prism, lasers)
- state is defined by 2^{1000} #s ("amplitudes")

QC's one extra power:

ELI4: Finding patterns in a list of #s

ELI8: Getting clues about " very long list of #s (eg. 10^{500} length)

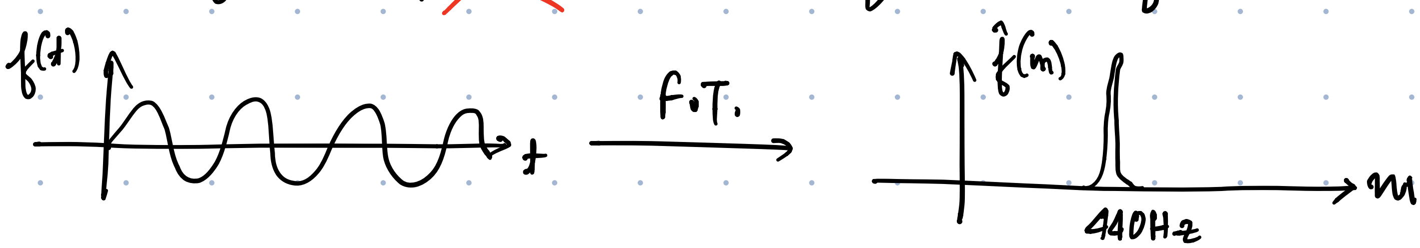
ELI highschooler: implicitly represented list

20	18	-42	3	41	....	f(x)	$\longrightarrow 2^{1000}$
0	1	2	3			x	

x ↑ 1000 bits

$$f : \{0, 1, 2 \ldots 2^{1000} - 1\} \longrightarrow \mathbb{C}$$

ELI undergrad: ~~patterns~~ → discrete fourier transform



$f : \{\text{domain}\} \to \mathbb{C}$ $\qquad$ $\hat{f} : \{\text{domain}\} \to \mathbb{C}$

① $\mathbb{R}$ on $[0,1]$ $\qquad$ freqs : sin/cos

② $\{0, 1, 2 \ldots N-1\}$ $\qquad$ freqs : discretized sin/cos

integers mod N

↳ $N = 2^n$

$n \leftarrow$ no. of particles involved

③ $\{0,1\}^n \to \mathbb{C}$ $\qquad$ freqs : XOR function

"Boolean cube" $\qquad$ "Hadamard F.T."

"Simon's algorithm"

Discrete Fourier Transform:

$$\underbrace{\left.\begin{bmatrix} W_N \\ (\text{DFT}) \end{bmatrix}\right\}N}_{N} \times \begin{bmatrix} f(0) \\ f(1) \\ \vdots \\ f(N-1) \end{bmatrix} = \begin{bmatrix} \hat{f}(0) \\ \hat{f}(1) \\ \vdots \\ \hat{f}(N-1) \end{bmatrix}$$

↳ this is a rotation/reflection operator it preserves the lengths

Naive algorithm

↳ $O(N^2)$

FFT (divide and conquer)

↳ $O(N \log N)$

Quantum algorithm

↳ $O(\log N)$

2^{1000} combined state : "Measure", QM. You "detect" some $y^* \in \{0,1\}^n$ with probability $|\hat{f}(y^*)|^2$

$$\hat{f}(y) = \mathbb{1}_{y = y^*}$$

↳ once a measurement is done states collapse