LECTURE 1

INTRODUCTION TO QUANTUM COMPUTING

CS 4268

COURSE EVALUATION:

DIAGNOSTIC TEST (Week 2 tutorial) : 10%

QUIZ 1 (Week 7 tutorial) : 20%

QUIZ 2 (Week 13 tutorial) : 20%

MIDTERM : SATURDAY, MARCH 28, 10AM - 1PM 30%

SCRIBE NOTES (1 lecture) : 20%

DIAGNOSTIC TEST

- Linear algebra
- Number theory
- Complex Numbers
- Very basic analysis of algorithms

- Weekly tutorial questions may be submitted for feedback.
- They will be graded promptly with detailed feedback
- No weightage for these submissions.
- Solutions will be discussed in tutorials

SCRIBE NOTES :

- Skeleton will be given
- Prepare well organised notes Completing any missing details from lecture
- Every student scribes one lecture
- We edit and share a final version within one week from lecture.

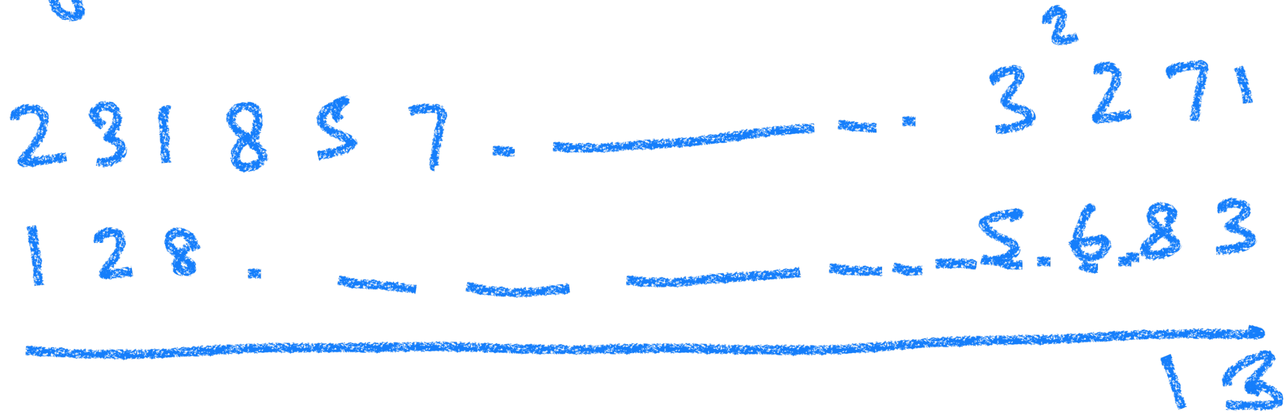
REFERENCE MATERIAL

- Lecture notes by Ronald De Wolf.
- Lecture notes by Ryan O Donnell
- Lecture notes by John Watrous.

- Quantum computing is at the intersection of computer science, math, physics.
- In this course, we will take quantum mechanics laws for granted.
- We will focus on looking at computational tasks that quantum computers are more powerful at.

Computational task : Multiply two large numbers

- given A, B 500 digits each
- Standard algorithm



- Complexity of above algorithm = $O(N^2)$

- Are there faster algorithms

Karatsuba : $n^{\log_2 3}$

$$T(n) = 3T(n/2) + O(1)$$

FFT: $O(n \log n)$

What about factoring.

- given 500 digit number N

$2, 3, 5, 7, \ldots \approx \sqrt{N}$

Complexity = $\tilde{O}(\sqrt{N})$

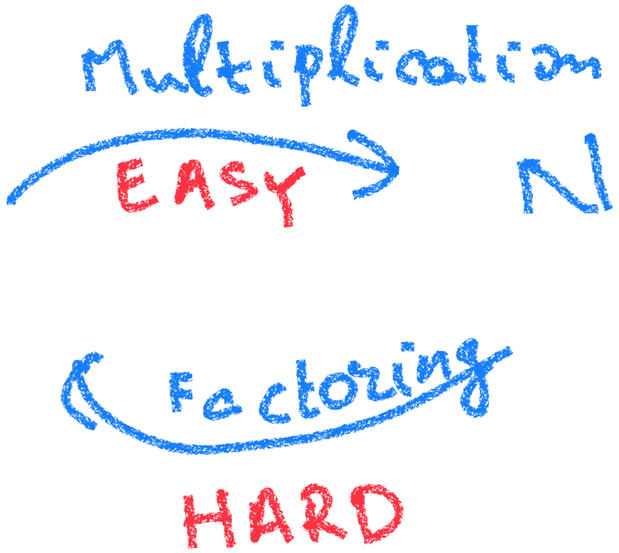
Fastest algorithms:

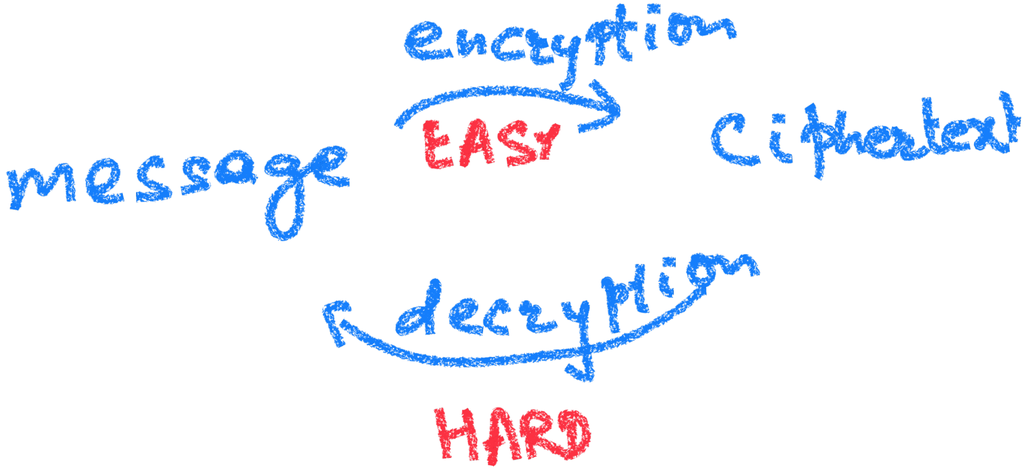
Number Field Sieve: $2^{c(\log N)^{1/3}(\log\log N)^{2/3}}$

For $N = 10^{500}$, time complexity $> 2^{120}$

- No one knows a poly algorithm for factoring

— One of the most useful facts in crypto





Punchline for this course

- There is a polynomial time algorithm for a machine following laws of quantum mechanics (quantum computing)

(Peter Shor 1994)

Problem : given a bitstring $a_1 \ldots\ldots a_N$ with one position 1 and remaining 0's.

Question: Find i s.t. $a_i = 1$.

Deterministic $\Theta(N)$

Randomized $\Theta(N)$

Quantum : $\Theta(\sqrt{N})$ (Grover 1996)

APPLICATION:

Boolean satisfiability (SAT) on n variables can be solved in $\sqrt{N}$ time

where $N = 2^n = 2^{0.5n}$

Quantum mechanics: probability with minus signs.

Quantum computing can be seen as an extension of probabilistic computing

Probabilistic computing

Deterministic algorithm + Coin tosses → 0 w.p. ½, 1 w.p. ½

- Can we do more with probabilistic computing than deterministic computing?

Of course we can do more, by definition.

Does it help with computing functions?

Key idea: Trade efficiency for error

PRIMALITY TESTING

1976 (Miller): ERH implies $O(n^4)$ algo for primality testing.

1977 (Solovay Strassen): n^3 time using randomness

1978 (Rabin): Modified Miller, using randomness

$O(n^2)$ algo

↑

called Miller Rabin test (the algo used in practice)

AKS 02: Deterministic algo n^{12} time

Lenstra Pomerance: " " n^6 time

Strongly believed conjecture:

$$BPP = P$$

(Problems solvable in randomized poly time
can be solved in deterministic poly time

Probabilistic computing

- Classical computing + extra power
- gives speed ups over deterministic computation
  (large poly-time to small poly-time)
- Widely believed : No exponential speed-up for any problem.

Quantum Computing:

- Classical computing + 1 extra power (Rotation)

- Analyzing requires linear algebra
- gives polynomial speedups over probabilistic computation for many problems (Grover's algo)
- (Seems to) give exponential speedup for some problems

Understanding and measuring 1 qubit

logical bit

0

1

qubit

$|0\rangle$ } Two states

$|1\rangle$ } (Don't worry about $|\cdot\rangle$ notation right now.

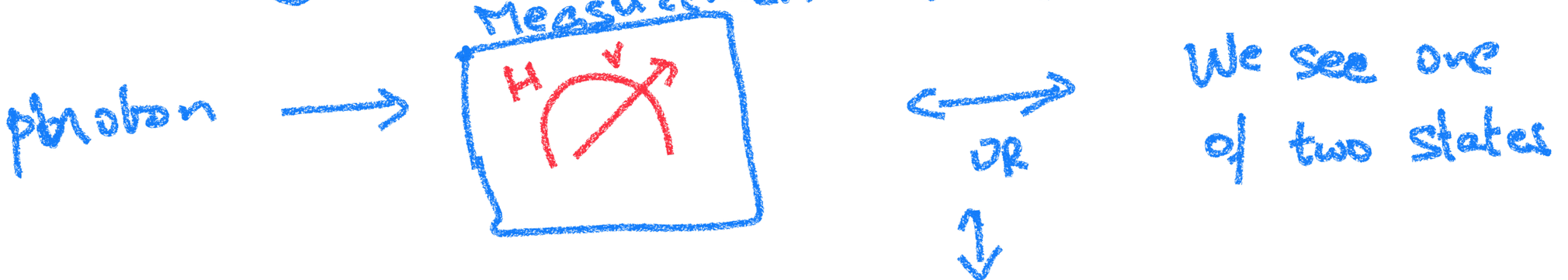
- Quantum objects can be in more than one state at the same time

example: eletron can be in two different levels "0" and "1" at the same time.

photon polarization

horizontal ↔ "0"

vertical ↕ "1"



Quantum Mechanics Law 1 :

If a quantum particle can be in one of the basic states $|0\rangle$ or $|1\rangle$ then it Can also be in superposition state

α "amplitude" on $|0\rangle$

β "amplitude" on $|1\rangle$

where α, β are numbers s.t. $|\alpha|^2 + |\beta|^2 = 1$.

(α, β are complex numbers)

Example: a photon has $\frac{3}{5}$ amplitude on $|0\rangle$

and $\frac{4}{5}$ amplitude on $|1\rangle$

Note: $\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$.

written as $\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$

Other examples $\frac{4}{5}|0\rangle + \left(\frac{-3}{5}\right)|1\rangle$, $\frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$$|a+ib| = \sqrt{a^2+b^2}$$

$$|i| = \sqrt{1^2}$$

$$\frac{|0\rangle}{\sqrt{2}} + \frac{i}{\sqrt{2}}|1\rangle$$

$$|\alpha|^2 = \frac{1}{2} + 0 = \frac{1}{2}$$

$$\alpha = \frac{1}{\sqrt{2}}, \quad \beta = \frac{i}{\sqrt{2}}$$

$$|\beta|^2 = 0 + \frac{1}{2} = \frac{1}{2}$$

Q.M. Law 2:

When we measure $\alpha|0\rangle + \beta|1\rangle$, the following happens

- with probability $|\alpha|^2$, we see $|0\rangle$ and the "state" of the qubit changes to $|0\rangle$.
- with probability $|\beta|^2$, we see $|1\rangle$ and the "state" of the qubit changes to $|1\rangle$

Example:

$0.8|0\rangle + 0.6|1\rangle \rightarrow$ [Measuring Device]

— w.p. 0.64
we get a qubit $|0\rangle$

— w.p. 0.36
we get a qubit $|1\rangle$

So w.p. $|\alpha|^2$, we get $1|0\rangle + 0|1\rangle$

↑ amplitude on $|0\rangle$ ↑ amplitude on $|1\rangle$

– Contrast this with looking at the result of a coin toss.

- Nothing special about two possible states

- Qutrit : particle with 3 possible states

$|0\rangle$, $|1\rangle$, $|2\rangle$

- Qudit with dimension $d = 4$

$|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$

Equivalently $\leftrightarrow\leftrightarrow$, $\leftrightarrow\updownarrow$, $\updownarrow\leftrightarrow$, $\updownarrow\updownarrow$

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

Don't worry, we will get used to this

Quantum Mechanics Law 1 :

General state $\alpha_0 |0\rangle + \dots + \alpha_{d-1} |d-1\rangle$

s.t. $|\alpha_0|^2 + \dots + |\alpha_{d-1}|^2 = 1.$

Quantum mechanics Law 2 :

Measuring $\alpha_0 |0\rangle + \dots + \alpha_{d-1} |d-1\rangle$

Changes state to $|i\rangle$ with probability $|\alpha_i|^2$.

$|1\rangle$, $|1\rangle$

- So far we didn't say what $|0\rangle$, $|1\rangle$, ... mean.

- Time to explain the math properly

- A quantum state $\alpha_0 |0\rangle + \cdots + \alpha_{d-1} |d-1\rangle$

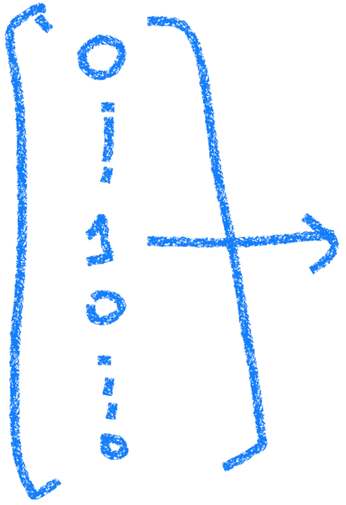
is just the vector

- $\begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{bmatrix} \in \mathbb{C}^d$

If is a d-dimensional vector

$|\alpha_0|^2 + \cdots + |\alpha_{d-1}|^2 = 1$

Same as $\alpha_0 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \alpha_{d-1} \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$

$|i\rangle$ is just  1 in i-th position.

We are used to calling this e_i.

NOTE : $|i\rangle$ makes sense if the dimension d is clear from the context.

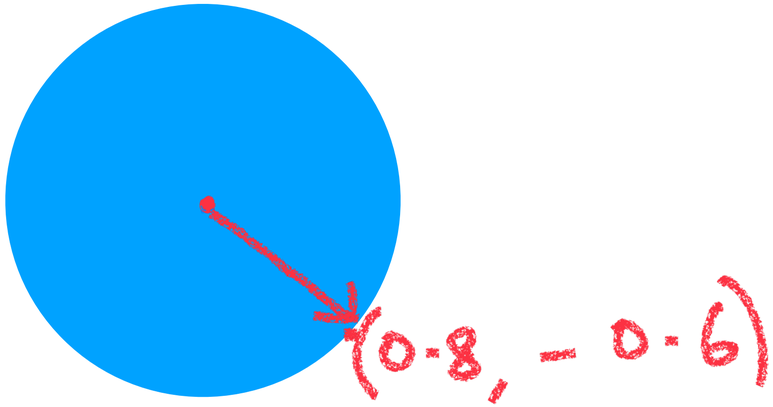
$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

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

2 dimensions, qubit.

Example: $d=2$

$$0.8|0\rangle - 0.6|1\rangle = \begin{bmatrix} 0.8 \\ -0.6 \end{bmatrix}$$



- We can only draw such a picture for real amplitude
- Mostly we focus on real amplitudes.

In general: qubit is given by 2 complex numbers
ie. 4 real numbers.

- But for real amplitudes, we will often draw in 2 dimensional plane.