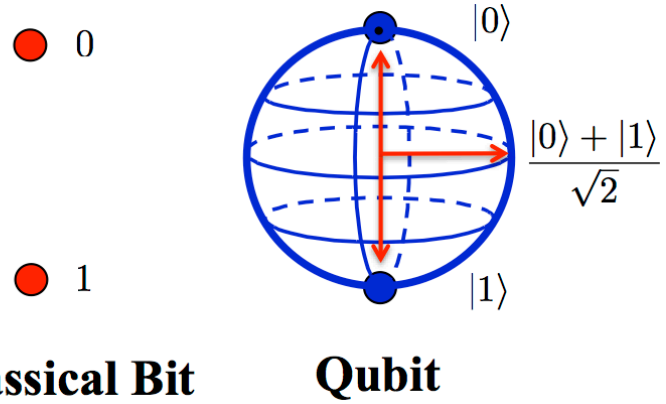
Introduction to Quantum Computing and its Applications to Cyber Security



Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

These slides and audio/video recordings of this class lecture are at:
http://www.cse.wustl.edu/~jain/cse570-23/

Student Questions

Overview

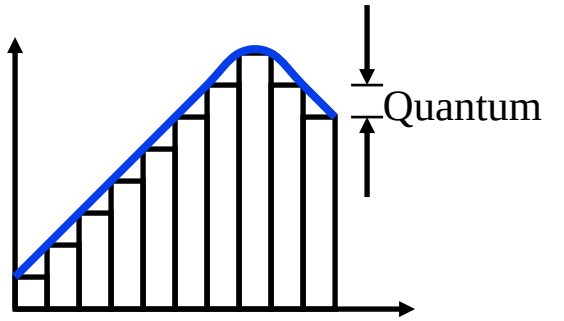
1. What is a Quantum and Quantum Bit?
2. Matrix Algebra Review
3. Quantum Gates: Not, And, or, Nand
4. Applications of Quantum Computing
5. Quantum Hardware and Programming

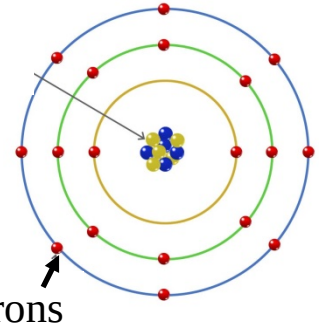
Student Questions

- Do we need to go to the final exam if we plan to use the first two exams as the final exam grade?
- This course was terrific. I enjoyed it immensely! I have gained much valuable knowledge to help me in my future research! Thank you very much, professor!

What is a Quantum?

- Quantization: Analog to digital conversion
- Quantum = Smallest discrete unit
- **Wave Theory**: Light is a wave. It has a frequency, phase, amplitude
- **Quantum Mechanics**: Light behaves like discrete packets of energy that can be absorbed and released
- **Photon** = One quantum of light energy
- Photons can move an electron from one energy level to the next higher level
- Photons are released when an electron moves from one level to a lower energy level

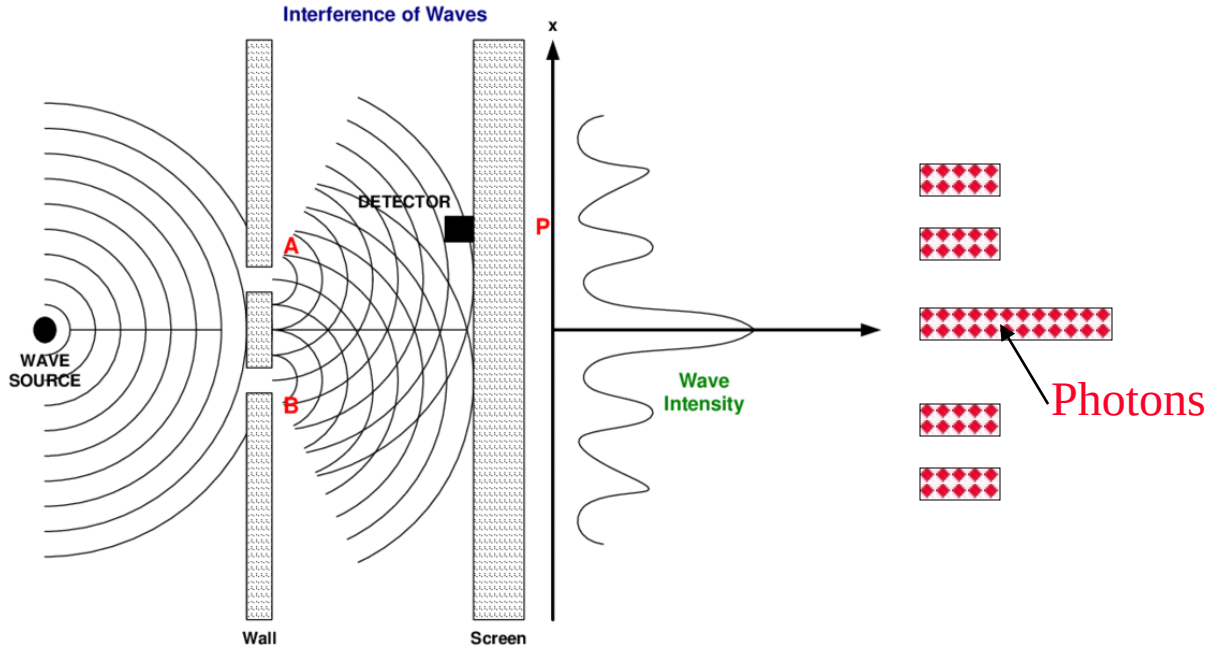




Student Questions

Probabilistic Behavior

- Young's Double-Slit Experiment 1801



- The two waves exiting the slits interfere.
- Interference is constructive in some spots and destructive in others ⇒ Probabilistic

Student Questions

Quantum Bits

1. Computing bit is a binary scalar: 0 or 1
2. Quantum bit (**Qubit**) is a 2×1 **vector**, e.g., $\begin{bmatrix}1\\0\end{bmatrix}$ or $\begin{bmatrix}0\\1\end{bmatrix}$
3. Vector elements of Qubits are **complex numbers** $x+iy$
4. **Modulus** of a complex Number $|x+iy| = \sqrt{(x+iy)(x-iy)} = \sqrt{x^2+y^2}$

   ($x-iy$: Conjugate)

   Example: $|(1+2i)| = \sqrt{(1+2i)(1-2i)} = \sqrt{1+4} = \sqrt{5}$
5. Probability of each element in a qubit vector is proportional to its modulus squared

$$\begin{bmatrix}a_0\\a_1\end{bmatrix} \Rightarrow \begin{matrix}P = |a_0|^2/(|a_0|^2+|a_1|^2)\\ P = |a_1|^2/(|a_0|^2+|a_1|^2)\end{matrix}$$

$$\sqrt{\frac{1}{7}}\begin{bmatrix}1+2i\\1-i\end{bmatrix} \Rightarrow \begin{matrix}\frac{1}{\sqrt{7}}|1+2i|\\ \frac{1}{\sqrt{7}}|1-i|\end{matrix} = \begin{matrix}\sqrt{\frac{1}{7}(1+2i)(1-2i)}\\ \sqrt{\frac{1}{7}(1-i)(1+i)}\end{matrix} = \begin{matrix}\sqrt{\frac{5}{7}}\\ \sqrt{\frac{2}{7}}\end{matrix} \Rightarrow P = \begin{matrix}\frac{5}{7}\\ \frac{2}{7}\end{matrix}$$

Student Questions

- You use the examples of [1,0] and [0,1] for qubits, but they exist in a superposition and will collapse to one of these values?

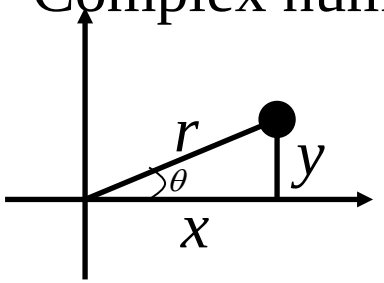
These are just exceptional cases of complex numbers. We need to start with simple real numbers before getting too complex.

- Can you explain how we would run into the probability example in a real quantum scenario?

See the example on the bottom line.

Polar Representation

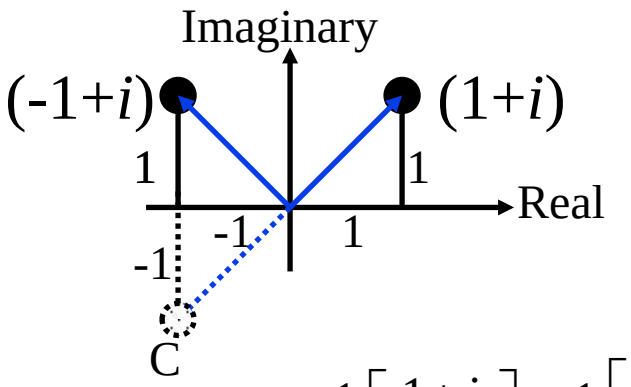
- Complex numbers in polar coordinates:



$$(x+iy) = re^{i\theta} = r\left(cos(\theta)+isin(\theta)\right)$$

$$r = \sqrt{x^2+y^2}$$

$$\theta = tan^{-1}(y/x)$$



$2\pi = 360^o$

$\pi/4 = 45^o$

$$\cos(\pi/4) = \frac{1}{\sqrt{2}} \qquad \sin(\pi/4) = 1$$

$$\frac{1}{2}\begin{bmatrix} 1+i \\ -1+i \end{bmatrix} = \frac{1}{2}\begin{bmatrix} \sqrt{2}e^{i\pi/4} \\ \sqrt{2}e^{3\pi/4} \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{1}{2}}\left(\cos(\pi/4)+i\sin(\pi/4)\right) \\ \sqrt{\frac{1}{2}}\left(\cos(3\pi/4)+i\sin(3\pi/4)\right) \end{bmatrix}$$

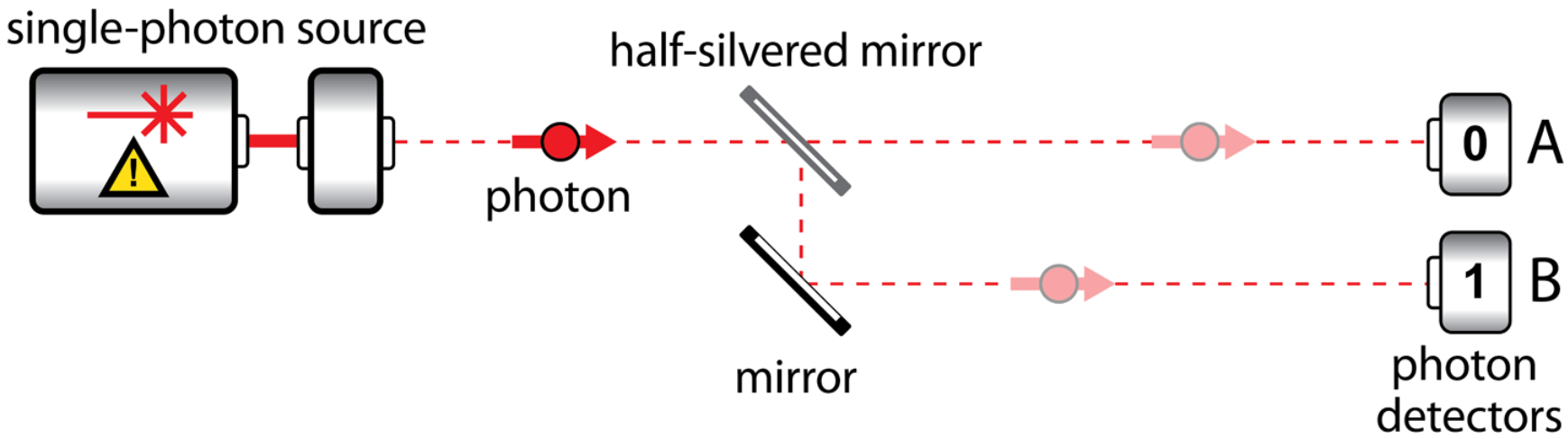
- **Exercise**: Find the complex and polar representation of C

Student Questions

- Could you explain the complex row vectors? I don't know where the minus sign in front of *i* comes from.

Negative i means the imaginary part is negative, which is the mirror image of the vector on the vertical axis. A negative real part means a mirror image on the horizontal axis.

Qubit Interpretation



[Source: Johnston, et al. 2019]

- If a single photon is emitted from the source, the photon reaches position A or B with some probability
  ⇒ Photon has a *superposition* (rather than a position)
- Each position has a different path length and, therefore, different amplitude and phase

Ref: E. R. Johnston, N. Harrigan, and M. Gimeno-Segovia, "Programming Quantum Computers," O'reilly, 2019, ISBN:9781492039686, 320 pp.

Student Questions

Bra-Ket Notation

- The vector ψ is denoted in bra-kets $|\psi>$
- Brackets: { }, [ ], < >
- Bra <a|
- Ket |a>
- Example: Ket-zero and ket-one

$$\begin{bmatrix}1\\0\end{bmatrix} = |0> \quad \begin{bmatrix}0\\1\end{bmatrix} = |1>$$

- Bra is the transpose of the complex conjugate of a Ket.
  Example: Bra-zero and Bra-one

$$\begin{bmatrix}1 & 0\end{bmatrix} = <0| \quad \begin{bmatrix}0 & 1\end{bmatrix} = <1|$$

Student Questions

- In quantum computing, Ket |a>, a could only be 0 or 1?

No. There are no deterministic numbers in quantum computing. Everything is probabilistic and complex. The examples in this slide are simple examples. Throughout this lecture, we use non-complex numbers for simplicity.

Matrix Multiplication

- **Matrix multiplication ×:**

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \end{bmatrix} \times \begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \\ b_{20} & b_{21} \end{bmatrix}$$

$$= \begin{bmatrix} a_{00}b_{00} + a_{01}b_{10} + a_{02}b_{20} & a_{00}b_{01} + a_{01}b_{11} + a_{02}b_{21} \\ a_{10}b_{00} + a_{11}b_{10} + a_{12}b_{20} & a_{10}b_{01} + a_{11}b_{11} + a_{12}b_{21} \end{bmatrix}$$

- Example:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 0 & 0 & 0 \end{bmatrix}$$

3×2 **2×3** **3×3**

Student Questions

Tensor Product

- **Tensor Product $\otimes$:** $m\times n \otimes k\times l$ results in $mk\times nl$ matrix

$$A=\begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} B=\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix}$$

$$A\otimes B=\begin{bmatrix} a_{00}\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix} & a_{01}\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix} \\ a_{10}\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix} & a_{11}\begin{bmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{bmatrix} \end{bmatrix}$$

$$=\begin{bmatrix} a_{00}b_{00} & a_{00}b_{01} & a_{00}b_{02} & a_{01}b_{00} & a_{01}b_{01} & a_{01}b_{02} \\ a_{00}b_{10} & a_{00}b_{11} & a_{00}b_{12} & a_{01}b_{10} & a_{01}b_{11} & a_{01}b_{12} \\ a_{00}b_{20} & a_{00}b_{21} & a_{00}b_{22} & a_{01}b_{20} & a_{01}b_{21} & a_{01}b_{22} \\ a_{10}b_{00} & a_{10}b_{01} & a_{10}b_{02} & a_{11}b_{00} & a_{11}b_{01} & a_{11}b_{02} \\ a_{10}b_{10} & a_{10}b_{11} & a_{10}b_{12} & a_{11}b_{10} & a_{11}b_{11} & a_{11}b_{12} \\ a_{10}b_{20} & a_{10}b_{21} & a_{10}b_{22} & a_{11}b_{20} & a_{11}b_{21} & a_{11}b_{22} \end{bmatrix}$$

Student Questions

Tensor Product (Cont)

- Example 1:

$$\begin{bmatrix} a_{00} \\ a_{10} \\ a_{20} \end{bmatrix} \otimes \begin{bmatrix} b_{00} \\ b_{10} \end{bmatrix} = \begin{bmatrix} a_{00}\begin{bmatrix} b_{00} \\ b_{10} \end{bmatrix} \\ a_{10}\begin{bmatrix} b_{00} \\ b_{10} \end{bmatrix} \\ a_{20}\begin{bmatrix} b_{00} \\ b_{10} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_{00}b_{00} \\ a_{00}b_{10} \\ a_{10}b_{00} \\ a_{10}b_{10} \\ a_{20}b_{00} \\ a_{20}b_{10} \end{bmatrix}$$

3×1 **2×1** **6×1**

- Example 2:

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

2×2 **1×3** **2×6**

Student Questions

Multiple Qubits and QuBytes

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

Two Qbits: $|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$ $|01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$ $|10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$ $|11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$

Tensor Product

Three Qbits:

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

$|000\rangle$ $|001\rangle$ $|010\rangle$ $|011\rangle$ $|100\rangle$ $|101\rangle$ $|110\rangle$ $|111\rangle$

- In a k-qubit register, each of the 2^k positions can be any complex number
- QuByte=8-Qubits = 256-element vector

Student Questions

- Can you please explain two Qubits again?

Sure.

Homework 19A

- Given two matrices:

$$A = \begin{bmatrix} 1+i & 1 \\ 1-i & i \end{bmatrix} B = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

- Compute: $A \times B,\ A \otimes B$

- Compute the probabilities of each element of $A \times B$

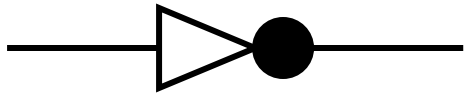
Student Questions

Quantum Gates

1. Quantum NOT Gate
2. Quantum AND Gate
3. Quantum OR Gate
4. Quantum NAND Gate
5. Quantum √NOT Gate

Student Questions

Quantum NOT Gate

- **NOT:** 

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

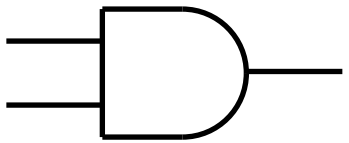
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} ? \\ ? \end{bmatrix}$$

$$NOT\,|1> \;=\; |0> \qquad NOT\,|0> \;=\; |?>$$

- **Exercise:** Fill in the ?'s

Student Questions

AND Gate

- **AND:** 

$$\text{AND} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} ? \\ ? \end{bmatrix}$$

$$\text{AND} \quad |00> \quad |01> \quad |10> \quad |11> = \quad |0> \quad |0> \quad |0> \quad |?>$$

2×4 **4×1** **2×1**

- **Exercise:** Fill in the ?'s

Student Questions

- Why is the AND gate matrix like that?

In binary computing,
0 AND 0 = 0
0 AND 1 = 0
1 AND 0 = 0
1 AND 1 = 1
This is a matrix multiplication

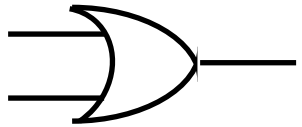
$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 0 \end{bmatrix} = 0$$

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

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

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

OR Gate

- **OR:** 

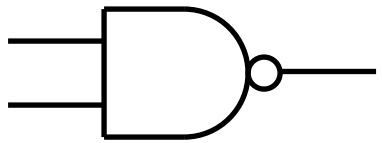
$$OR = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

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

$$\text{OR} \quad |00> \quad |01> \quad |10> \quad |11> = \quad |0> \quad |1> \quad |1> \quad |1>$$

Student Questions

NAND Gate

- **NAND:** 

$$\text{NAND} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\text{NAND} \quad |00> \quad |01> \quad |10> \quad |11> = \quad |1> \quad |1> \quad |1> \quad |0>$$

Student Questions

Quantum √NOT Gate

- **√NOT:** √NOT ×√NOT = NOT

$$\sqrt{\text{NOT}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}\times\begin{bmatrix}0\\ 1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}-1\\ 1\end{bmatrix}$$

$|1\rangle$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}\times\begin{bmatrix}1\\ 0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}$$

$|0\rangle$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}\times\frac{1}{\sqrt{2}}\begin{bmatrix}-1\\ 1\end{bmatrix}=\begin{bmatrix}-1\\ 0\end{bmatrix}$$

$|0\rangle$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}\times\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}=\begin{bmatrix}0\\ 1\end{bmatrix}$$

$|1\rangle$

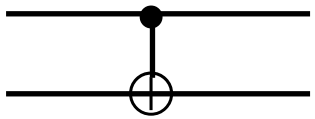
Student Questions

- Could you explain the √ NOT Gate?

Sure.

Controlled NOT Gate

- **CNOT:** If the control bit is 0, no change to the 2nd bit
  If control bit is 1, the 2nd bit is complemented



$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

CNOT $|00\rangle$ $|01\rangle$ $|10\rangle$ $|11\rangle$ = $|00\rangle$ $|01\rangle$ $|11\rangle$ $|10\rangle$

- A controlled-NOT gate can be used to produce two bits that are **entangled** ⇒ Two bits behave similarly even if far apart
  ⇒ Can be used for teleportation of information.

Student Questions

- Can you present more details about how entanglement is used to teleport information? Suppose A sends B, one of the two entangled qubits. How is the qubit interpreted? *I am not sure.*
- Could you explain the CNOT multiply example of the slide?

Note that the third and fourth vectors on the right are interchanged.
The first bit in ket is the control bit.

- Can you point out which is the control bit?

The upper wire is the control bit.
In the matrix example, the first bit in the ket is the control bit.

Gates: Summary

$$\text{NOT}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \qquad \text{AND}=\begin{bmatrix}1 & 1 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

$$\text{OR}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 1 & 1\end{bmatrix} \qquad \text{NAND}=\begin{bmatrix}0 & 0 & 0 & 1\\ 1 & 1 & 1 & 0\end{bmatrix}$$

} Classical

$$\sqrt{\text{NOT}}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix} \qquad \text{CNOT}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

} Non-Classical Quantum

- The first four gates above are the classical gates. The last two are non-classical/quantum gates.
- There are many other non-classical/quantum gates, e.g., Read/Measurement, Pauli Gates, Controlled Pauli Gates, …
- Using such gates, one can design **quantum circuits**

Ref: Summary of Quantum Operations, https://qiskit.org/documentation/tutorials/circuits/3_summary_of_quantum_operations.html#Pauli-gates

Student Questions

Quantum Applications

- It has been shown that quantum computation makes several problems hard currently. Including:
  - **Fourier Transforms**
  - **Factoring large numbers**
  - Error correction
  - Searching an extensive unordered list
- There are some new methods:
  - Quantum Key Exchange
  - Quantum Teleportation (transfer states from one location to another)

Quantum-Safe Cryptography is being standardized

Student Questions

- Does quantum have the ability to deal with factoring numbers?

Yes. That was the first invention that woke up the computer/security scientists.

- Does implementing quantum-safe cryptography assume that users use quantum devices to encrypt? Or doing encryption on standard devices, but quantum computers are used to launch the attack?

No. Quantum computers can easily break encryption on standard devices.

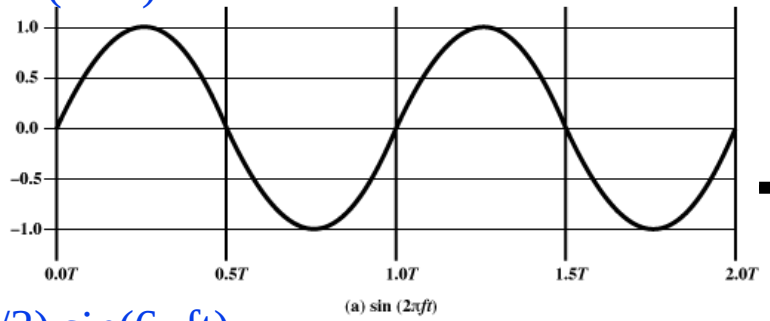
- When using quantum computing to deal with some problems without using an exhaustive method, is the computing speed the same or even worse than traditional computing?

It is expected to be much faster than standard computing for some problems. Currently, quantum computers are rugged to make.

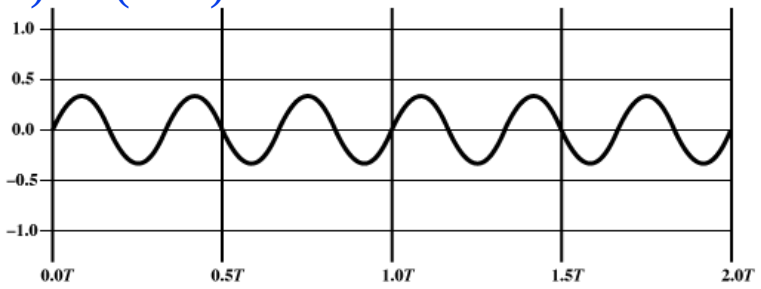
Fourier Transforms

Time Domain

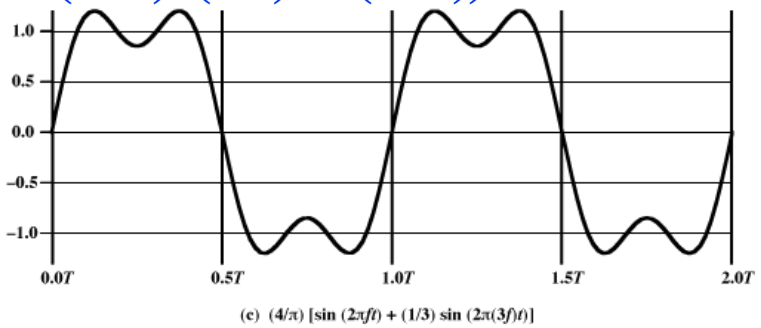
A sin(2πft)



(A/3) sin(6πft)

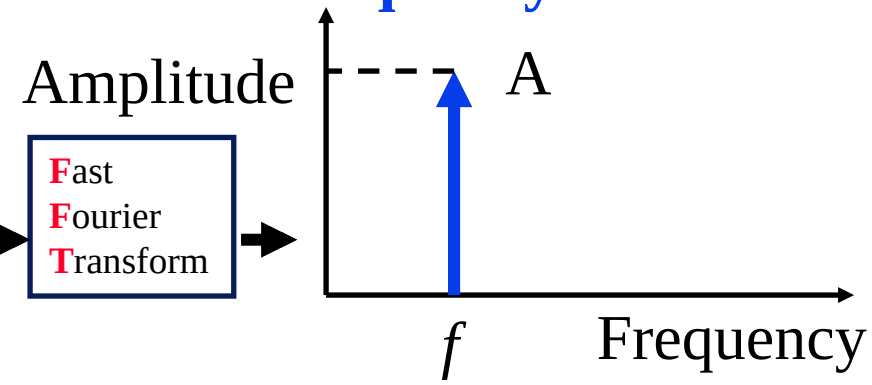


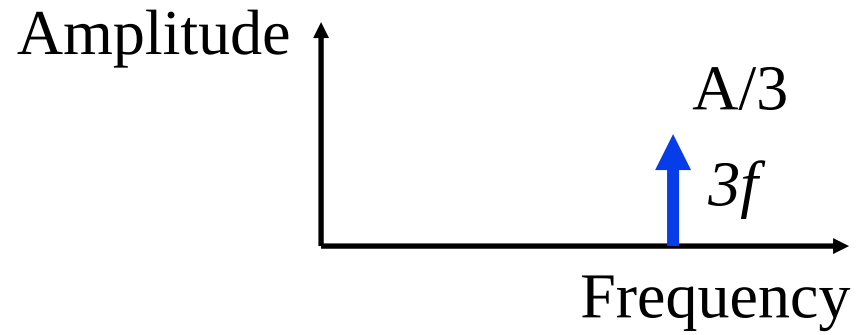
A(Sin(2πft)+(1/3) sin(6πft))

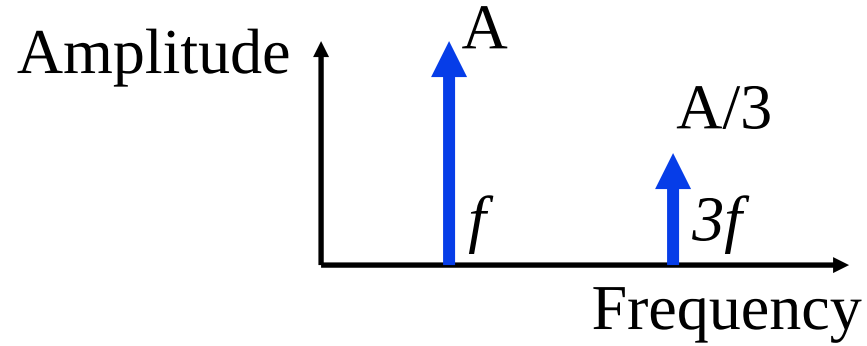


Fast Fourier Transform

Frequency Domain







Student Questions

Quantum Fourier Transform (QFT)

- Fourier transform is used to find periodic components of signals
- QFT is faster than classical FT for large *inputs*

Student Questions

GCD

- Greatest Common Divisor of any two numbers
  - Divide the larger number with the smaller number and get the remainder less than the divisor
  - Divide the previous divisor with the remainder
  - Continue this until the remainder is zero.
    The last divisor is the GCD.

```
15) 35  (2
    30
    05) 15  (3
        15
        0
```

gcd ↗

Student Questions

Shor's Factoring Algorithm

- Peter Shor used QFT and showed that Quantum Computers could find prime factors of large numbers exponentially faster than conventional computers
- **Step 1:** Find the period of the a^i mod N sequence.
  Here, a is co-prime to $N \Rightarrow a$ is a prime such that gcd(a, N) = 1 $\Rightarrow a$ and N have no common factors.
  - Example: N=15, a=2;
    2^i mod 15 for i=0, 1, 2, …
    = 1, 2, 4, 8, 1, … $\Rightarrow p$=4
  - If p is odd, select another number.
    If mod($a^{p/2}$, N)=-1, select another number.
  - This is the classical method for finding periods.
    QFT makes it fast.
- **Step 2:** Prime factors of N might be $gcd(N, a^{p/2}+1)$ *and* $gcd(N, a^{p/2}-1)$
  - Example: $gcd(15, 2^2-1) = 3$; $gcd(15, 2^2+1) = 5$;

Student Questions

- Could you explain Shor's Factoring Algorithm again?

Sure.

- Is it given to us in advance, or do we have to find one number a co-prime to N?

You should be able to find co-prime for small numbers.

- In the example, N=15, could I take seven since 7 is co-prime to N?

Yes.

- Is it possible that p is odd? If so, $a^{(p/2)-1}$ might not be an integer. How to calculate the GCD?

See the Correction on the left.

- Could you explain this algorithm and homework 19B again? *Sure.*
- So, Shor's algorithm outputs only two numbers? What if we need more than two? E.g., 30 = 2 × 3 × 5?

It can be used repeatedly. In security, the keys are related to two large primes, and so two factors are what we are generally looking for.

Shor's Factoring Algorithm

- Peter Shor used QFT and showed that Quantum Computers could find prime factors of large numbers exponentially faster than conventional computers
- **Step 1:** Find the period of the a^i mod N sequence.
  Here, a is co-prime to $N \Rightarrow a$ is a prime such that gcd(a, N) = 1 $\Rightarrow a$ and N have no common factors.
  - Example: N=15, a=2;
    2^i mod 15 for i=0, 1, 2, …
    = 1, 2, 4, 8, 1, … $\Rightarrow p$=4
  - If p is odd, select another number.
    If mod($a^{p/2}$, N)=-1, select another number.
  - This is the classical method for finding periods.
    QFT makes it fast.
- **Step 2:** Prime factors of N might be $gcd(N, a^{p/2}+1)$ *and* $gcd(N, a^{p/2}-1)$
  - Example: $gcd(15, 2^2-1) = 3$; $gcd(15, 2^2+1) = 5$;

Student Questions

- Is there any intuition or method for selecting the co-prime of the number we are trying to factor so that the period will be shorter?

I am not aware. That doesn't mean there aren't any.

Homework 19B

- Find factors of 35 using Shor's algorithm. Show all steps.
- Optional: Try factoring 407 (Answer: 11×37)

Student Questions

- I have already solved this homework with "a=2", but I was curious about what if I take a=11, which is co-prime to 35. 11^i will be: 1, 11, 121, 1331, 14641..... 11^i mod 35: 1, 11, 16, 1, 11, 16..... in this case, p=3, what should I do when p is odd? Does that mean we must only use the smallest co-prime number to "N" as "a"?

Odd p ⇒ select another number.

- For example, a should be prime. But from other materials, I found that a could be any number that has no common factors with N and is smaller than N. Is it right?

You are right. However, if a is not prime, its factors would lead to answers more quickly.

Quantum Machine Learning (QML)

- Quantum for solving systems of linear equation
- Quantum Principal Component Analysis
- Quantum Support Vector Machines (QSVM)
  - Classical SVM has runtime of O(poly(m,n)), m data points, n features
  - QSVM has runtime of O(log(mn))
    - Currently limited to data that can be represented with a small number of qubits
- QML can process data directly from Quantum sensors with the full range of quantum information

Student Questions

Ref: E. R. Johnston, N. Harrigan, and M. Gimeno-Segovia, "Programming Quantum Computers," O'reilly, 2019, ISBN:9781492039686, 320 pp.

Building Quantum Computers

1. **Neural Atom**: A group of cesium or rubidium atoms are cooled down to a few degrees Kelvin and controlled using lasers
2. **Nuclear Magnetic Resonance** (NMR)
3. **Nitrogen-Vacancy Center-in-Diamond**: Some carbon atoms in diamond lattice are replaced by nitrogen atoms
4. **Photonics**: Mirrors, beam splitters, and phase shifters are used to control photons
5. **Spin Qubits**: Using semiconductor materials
6. **Topological Quantum Computing**: Uses Anyon, which are quasi-particles different from photons or electrons
7. **Superconducting Qubits**: Requires cooling down to 10mK

Student Questions

- It seems impossible for quantum computers to be used for home use. Because it needs nuclear power.

Today, it is not possible. This was the case for standard computing in the 1970s. But it may be possible in your lifetime.

Ref: J. D. Hidary, "Quantum Computing: An Applied Approach," Springer, 2019, 380 pp.

Quantum Hardware

- IBM Q Experience: 5-Qubit quantum processor
  Open to the public for experiments using their cloud,

Ref: https://www.ibm.com/blogs/research/2018/04/ibm-startups-accelerate-quantum/

Student Questions

Quantum Hardware (Cont)

- Google's Quantum computer in Santa Barbara Lab

Ref: https://www.nbcnews.com/mach/science/google-claims-quantum-computing-breakthrough-ibm-pushes-back-ncna1070461

Student Questions

Quantum Simulators

- QCEngine: https://oreilly-qc.github.io/
- Qiskit, https://qiskit.org/
- Q# (Qsharp), https://docs.microsoft.com/en-gb/quantum/?view=qsharp-preview
- Cirq, https://github.com/quantumlib/Cirq
- Forest, https://pyquil-docs.rigetti.com/en/v2.7.2/
- List of QC Simulators, https://quantiki.org/wiki/list-qc-simulators
- See the complete list at: https://en.wikipedia.org/wiki/Quantum_programming

Student Questions

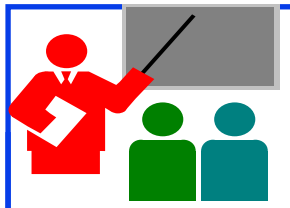
Ref: E. R. Johnston, N. Harrigan, and M. Gimeno-Segovia, "Programming Quantum Computers," O'reilly, 2019, ISBN:9781492039686, 320 pp.

Quantum Supremacy

- Quantum Supremacy: Solve a problem on a quantum computer that can not be solved on a classical computer
- Google announced it had achieved Quantum Supremacy on October 23, 2019
  - Google built a 54-qubit quantum computer using a programmable superconducting processor
- Vendors: IBM, Microsoft, Google, Alibaba Cloud, D-Wave Systems, 1QBit, QC Ware, QinetiQ, Rigetti Computing, Zapata Computing
- Global Competition: China, Japan, the USA, EU are also competing

Student Questions

Ref: F. Arute, K. Arya, R. Babbush, *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature* **574,** 505–510 (Oct. 23, 2019), https://www.nature.com/articles/s41586-019-1666-5



Summary

1. Qubits are two-element vectors. Each element is a complex number that indicates the probability of that level
2. Multi-qubits are represented by tensor products of single-qubits
3. Qbit operations are mostly matrix operations. The number of possible operations is much larger than in classic computing.
4. Shor's factorization algorithm is an example of an algorithm that can be done in significantly less time than in classic computing
5. Quantum computing is here. IBM, Microsoft, and Google all offer platforms that can be used to write simple quantum computing programs and familiarize yourself.
6. Quantum-Safe Crypto is in standardization

Student Questions

Reading List

- J. D. Hidary, “Quantum Computing: An Applied Approach,” Springer, 2019, 380 pp.
- Mercedes Gimeno-Segovia, Nic Harrigan, Eric R. Johnston, "Programming Quantum Computers," O'Reilly Media, Inc., July 2019, ISBN:9781492039686 (Safari Book). **Recommended.**
- N. S. Yanofsky and M. A. Mannucci, “Quantum Computing for Computer Scientists,” Cambridge, 2008, 380 pp.
- N. D. Mermin, “Quantum Computer Science: An Introduction,” Cambridge, 2007, 220 pp.

Student Questions

References

- Gerd Leuchs, Dagmar Bruss, "Quantum Information," 2 Volume Set, 2nd Edition, Wiley-VCH, June 2019, ISBN:9783527413539 (Safari Book).
- Vladimir Silva, "Practical Quantum Computing for Developers: Programming Quantum Rigs in the Cloud using Python, Quantum Assembly Language and IBM QExperience," Apress, December 2018, ISBN:9781484242186 (Safari Book).
- Mingsheng Ying, "Foundations of Quantum Programming," Morgan Kaufmann, March 2016, ISBN:9780128025468 (Safari Book).
- F.J. Duarte, "Quantum Optics for Engineers," CRC Press, November 2017, ISBN:9781351832618 (Safari Book).
- Quantum Algorithm Zoo (Compiled list of Quantum algorithms), http://quantumalgorithmzoo.org/

Student Questions

Wikipedia Links

- https://en.wikipedia.org/?title=Inner-product&redirect=no
- https://en.wikipedia.org/wiki/Bra%E2%80%93ket_notation
- https://en.wikipedia.org/wiki/Complex_number
- https://en.wikipedia.org/wiki/Controlled_NOT_gate
- https://en.wikipedia.org/wiki/Dot_product
- https://en.wikipedia.org/wiki/Fourier_transform
- https://en.wikipedia.org/wiki/Greatest_common_divisor
- https://en.wikipedia.org/wiki/List_of_quantum_processors
- https://en.wikipedia.org/wiki/Matrix_multiplication
- https://en.wikipedia.org/wiki/Polar_coordinate_system
- https://en.wikipedia.org/wiki/Quantum
- https://en.wikipedia.org/wiki/Quantum_algorithm
- https://en.wikipedia.org/wiki/Quantum_computing
- https://en.wikipedia.org/wiki/Quantum_entanglement
- https://en.wikipedia.org/wiki/Quantum_error_correction
- https://en.wikipedia.org/wiki/Quantum_Fourier_transform

Student Questions

Wikipedia Links (Cont)

- https://en.wikipedia.org/wiki/Quantum_logic_gate
- https://en.wikipedia.org/wiki/Quantum_machine_learning
- https://en.wikipedia.org/wiki/Quantum_mechanics
- https://en.wikipedia.org/wiki/Quantum_simulator
- https://en.wikipedia.org/wiki/Quantum_supremacy
- https://en.wikipedia.org/wiki/Quantum_technology
- https://en.wikipedia.org/wiki/Quantum_teleportation
- https://en.wikipedia.org/wiki/Qubit
- https://en.wikipedia.org/wiki/Shor%27s_algorithm
- https://en.wikipedia.org/wiki/Superconducting_quantum_computing
- https://en.wikipedia.org/wiki/Sycamore_processor
- https://en.wikipedia.org/wiki/Tensor_product
- https://en.wikipedia.org/wiki/Timeline_of_quantum_computing
- https://en.wikipedia.org/wiki/Category:Quantum_gates

Student Questions

Classic Papers on Quantum Computing

- R. P. Feynman, "Simulating Physics with Computers," *International journal of Theoretical Physics* 21.6 (1982): 467-488, https://www.cs.princeton.edu/courses/archive/fall05/frs119/papers/feynman82/feynman82.html
- D. E. Deutsch, "Quantum theory, the Church-Turing principle, and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985): 97-117, https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1985.0070
- D. E. Deutsch, "Quantum Computational Networks," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 425.1868 (1989), 73-90. , https://royalsocietypublishing.org/doi/pdf/10.1098/rspa.1989.0099 (subscribers only)
- P. W. Shor, "Algorithms for Quantum Computation: Discrete Log and Factoring," Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, IEEE, 1994, p. 124
- A. Barenco et al., "Elementary gates for quantum computation," Physical Review A, March 22, 1995, https://arxiv.org/pdf/quant-ph/9503016

Student Questions

Classic Papers (Cont)

- L. K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings, STOC 1996, Philadelphia PA, USA, pp. 212-219, https://arxiv.org/pdf/quant-ph/9605043
- G. Brassard et al., "Quantum Counting," 1998, https://arxiv.org/pdf/quant-ph/9805082
- G. Brassard et al., "Quantum Amplitude Amplification and Estimation," 2000, https://arxiv.org/pdf/quant-ph/0005055
- S. Lloyd, "Quantum Algorithm for Solving Linear Systems of Equations," American Physical Society, APS March Meeting 2010, March 15-19,2010

Student Questions

Scan This to Download These Slides

Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse570-23/m_18qnt.htm

Student Questions

Related Modules

CSE567M: Computer Systems Analysis (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),

https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw

Wireless and Mobile Networking (Spring 2016),
https://www.youtube.com/playlist?list=PLjGG94etKypKeb0nzyN9tSs_HCd5c4wXF

CSE571S: Network Security (Fall 2011),

https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw

Student Questions

Entanglement

- 2-Qubits: $\begin{bmatrix}00\\01\\10\\11\end{bmatrix}$ $\begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{bmatrix}$ ⇒P= {00} or {11} each 50% {01} or {10} each 0% $\begin{bmatrix}0\\\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\\0\end{bmatrix}$ ⇒P= {00} or {11} each 0% {01} or {10} Each 50%
- Two qubits can be entangled => Their states are correlated
  - Momentum, spin, and polarization could be correlated
  - even when they are far apart
  - One qubit cannot be fully described independently of the other
  - Any change of one qubit affects the other
- 1935: Einstein called it a paradox since change happens at a speed faster than light
- 2022: Physics Nobel prize for experiments with entangled photons

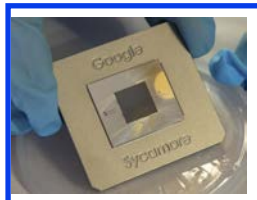
Student Questions

Challenges for Quantum

- Decoherence: Qubits lose their state over time. In nanoseconds to seconds, depending upon the temperature.
  - Need near zero-kelvin (10mK) temperature ⇒ Large cooling equipment.
  - Need redundant qubits for quantum error correction to overcome decoherence
- Errors in quantum computers accumulate fast and require a significant number of qubits to take care of errors
- Most of the research is theoretical. Practical experiments are limited to a minimal number of qubits

Student Questions

Ref: M. Dyaknov, "The case against Quantum Computing," IEEE Spectrum, Nov 15, 2018, https://spectrum.ieee.org/the-case-against-quantum-computing#toggle-gdpr
D. Monroe, "Quantum Computers and the Universe," Communications of the ACM, December 2022, p10-11, https://dl.acm.org/doi/pdf/10.1145/3565977



Challenges for Quantum(Cont)

- The most promising method of quantum computing consists of interconnecting Josephson junctions cooled to 10 milli-Kelvins.
  - Developed initially by D-Wave systems. Now used widely.
  - 49-qubit (Intel), 127-qubit (IBM), 256-qubit (QuEra), and 72-qubit (Google) chips announced but few details
  - November 9, 2022: IBM announced the world's largest quantum computer, Osprey, with 433 qubits
- Need 1000-100,000 qubit quantum computers to do interesting problems
  - 1000 qubits require $2^{1000} \sim 10^{300}$ parameters to describe its state
  - This number is larger than the number of subatomic particles in the observable universe.
  - One potential way is to reduce connectivity between qubits

Student Questions

Status of Shor's Algorithm?

- 2001: IBM could factor 15 with a seven qubits computer.
- 2012: the factorization of 15 was performed with solid-state qubits
- 2012: the factorization of 21 was achieved
- 2019: an attempt to factor 35 on an IBM Q System One failed because of accumulating errors.
- Quantum circuit for Shor's algorithm needs to be custom-designed for each choice of N and each choice of a
- Needs two q-qubit registers, where $q \approx \log_2 N$

Student Questions

Ref: https://en.wikipedia.org/wiki/Shor%27s_algorithm
https://www.newscientist.com/article/2346074-ibm-unveils-worlds-largest-quantum-computer-at-433-qubits/