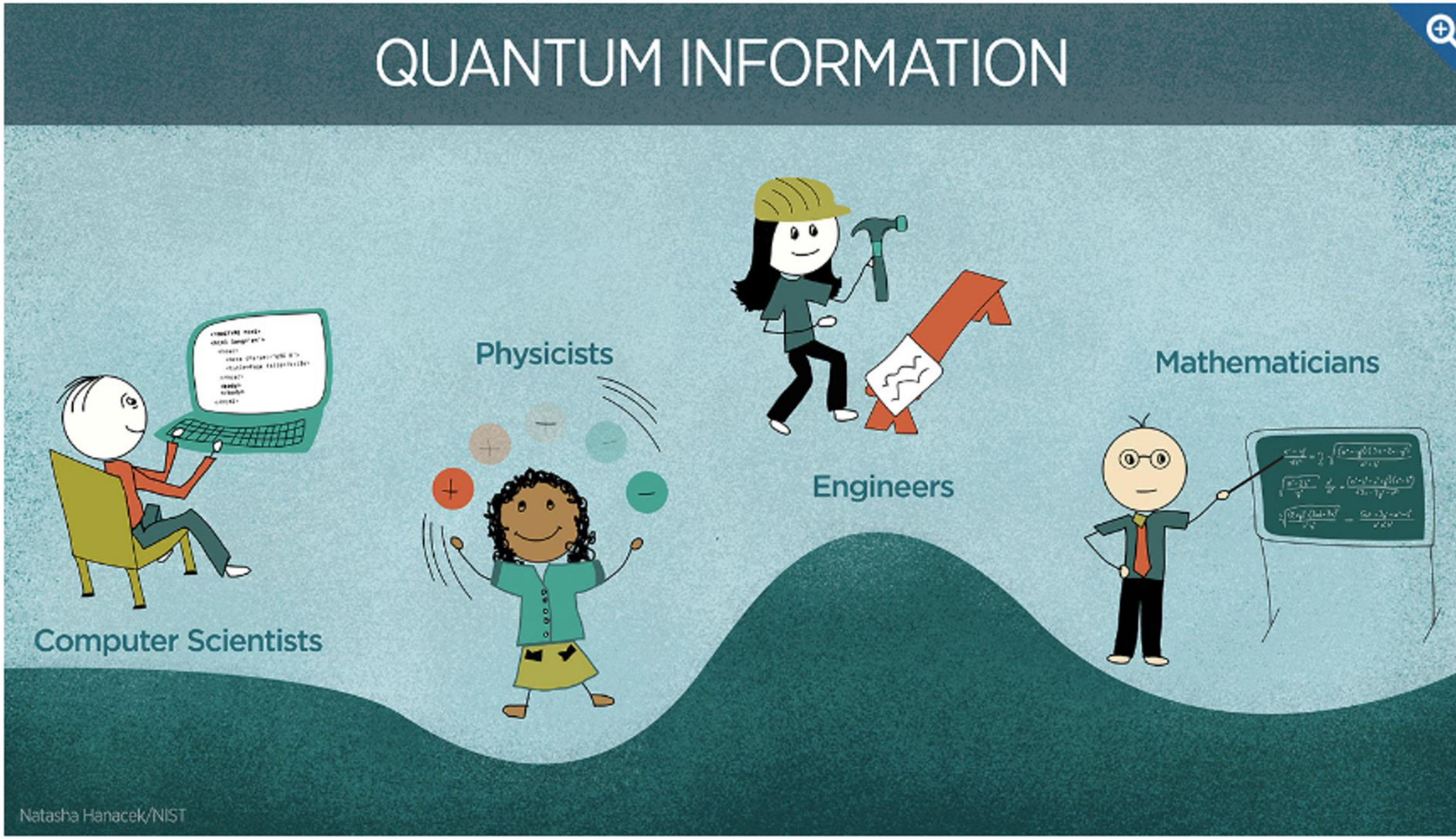
Introduction to Quantum Gate

Dr. Upendra Kumar
Assistant Professor
Advanced Functional Materials Laboratory
Department of Applied Science
IIIT Allahabad
Prayagraj-211015, Uttar Pradesh

August 19 2025



The emerging field of quantum information requires professionals from many disciplines, including computer scientists, physicists, engineers, and mathematicians.

Credit: N. Hanacek/NIST

Motivation: Factorization

- An important problem in computing is finding the prime factorization of an integer.
- Using classical algorithms, a number *N* of size $n = \log_2(N)$ takes super-polynomial time. $2^{\sqrt{n}}$ time is about the best we can get.

Motivation: Factorization

- For example, on a particular personal computer, it may take four hours to factor a number with 78 digits ($n = 256$).
- On the same computer, a 174 digit number ($n = 576$, which is the record) would take 43 days.
- A 617 digit number ($n = 2048$, current size recommended for RSA encryption), would take 300,000 years.

Motivation: Factorization

- Such superpolynomial growth is characteristic of many algorithms in classical computing.
- However: Quantum Computing could provide a miraculous decrease in time.
- A quantum algorithm reduces the integer factorization problem to polynomial time (n^3).
- Then, if n = 256 number takes four hours, n = 2048 will take 85 days.

Outline

- Review of Classical Computing
- Qubits and Quantum Operations
- Quantum Algorithms
- Physical Implementations
- Future Developments

Outline

- **Review of Classical Computing**
  - Data Representation
  - Operations
- Qubits and Quantum Operations
- Quantum Algorithms
- Physical Implementations
- Future Developments

Classical Data Representation

- The basic unit in classical data is a binary digit, called a bit, that can take on the value 0 or 1.
- In classical computing, we represent a datum by a string of bits.
- The letter ‘A’ may be written 0100 0001
- The number 137 can be written 1000 1001

Classical Operations

- All operations in classical computing are based on logic gates.
- For example, the logical AND gate takes in two bits and returns 1 if and only if both inputs are 1.

AND		
Input 1	Input B	Output
0	0	0
0	1	0
1	0	0
1	1	1

OR		
Input 1	Input B	Output
0	0	0
0	1	1
1	0	1
1	1	1

Classical Algorithm

- We define a Classical Algorithm to be any sequence of such classical operations (usually to do something useful).
- A classical computer is any device that can implement a classical algorithm.

Classical Computing

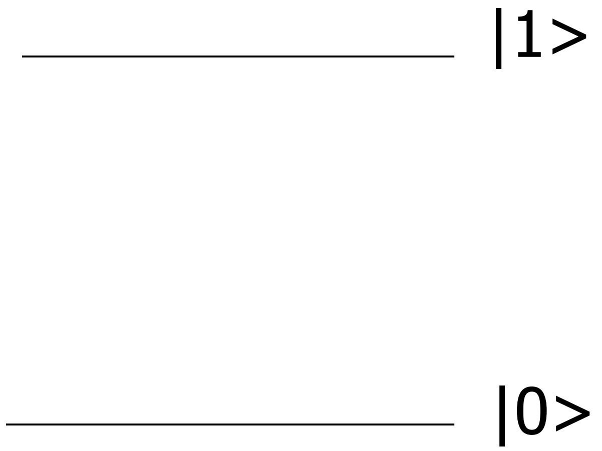
- Although modern classical computers depend on quantum mechanics, the algorithms that they implement do not.
- We could, in principle, design a classical computer that does not depend on quantum mechanics.

Outline

- Review of Classical Computing
- **Qubits and Quantum Operations**
  - Qubits as Two-State Systems
  - Quantum Gates
  - Quantum Registers
  - Entanglement
- Quantum Algorithms
- Physical Implementations
- Future Developments

Qubits

- A Quantum Bit (Qubit) is a two-level quantum system.
- We can label the states |0> and |1>.
- In principle, this could be any two-level system.



Qubits

- Unlike a classical bit, which is definitely in either state, the state of a Qubit is in general a mix of |0> and |1>.

$$\left|\psi\right\rangle = c_0\left|0\right\rangle + c_1\left|1\right\rangle$$

- We assume a normalized state:

$$\left|c_0\right|^2 + \left|c_1\right|^2 = 1$$

Qubits

- For convenience, we will use the matrix representation

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

Quantum Gate

- A Quantum Logic Gate is an operation that we perform on one or more Qubits that yields another set of Qubits.
- We can represent them as linear operators in the Hilbert space of the system.

Quantum NOT Gate

- As in classical computing, the NOT gate returns a 0 if the input is 1 and a 1 if the input is 0.
- The matrix representation is

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

Other Quantum Gates

- Other gates include the Hadamard-Walsh matrix:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- And Phase Flip operation:

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

Multiple Qubits

- Any useful classical computer has more than one bit. Likewise, a Quantum Computer will probably consist of multiple qubits.
- A system of *n* Qubits is called a Quantum Register of length *n*.
- To represent that Qubit 1 has value b_1, Qubit 2 has value b_2, etc., we will use the notation:

$$\left|b_1\right\rangle_1 \left|b_2\right\rangle_2 \cdots \left|b_n\right\rangle_n$$

Multiple Qubits

- For *n* Qubits, the vector representing the state is a *2n* column vector.
- The operations are then *2n* x *2n* matrices.
- For *n* = 2, we use the representations

$$|0\rangle_1|0\rangle_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |0\rangle_1|1\rangle_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |1\rangle_1|0\rangle_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |1\rangle_1|1\rangle_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

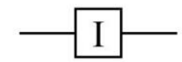
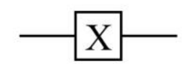
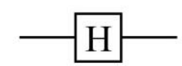
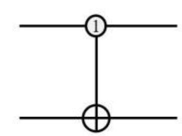
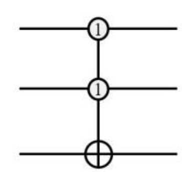
Quantum CNOT Gate

- An important Quantum Gate for $n = 2$ is the conditional not gate.
- The conditional not gate flips the second bit if and only if the first bit is on.

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

Input		**Output**	
Qubit 1	Qubit 2	Qubit 1	Qubit 2
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Brief Overview Gates

Gate	Equation	Matrix	Transform	Notation
Identity ($\boldsymbol{I}$)	$\boldsymbol{I} = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\boldsymbol{I}\|0\rangle = \|0\rangle$ $\boldsymbol{I}\|1\rangle = \|1\rangle$	
Pauli-X ($\boldsymbol{X}$ or **NOT**)	$\boldsymbol{X} = \|0\rangle\langle 1\| + \|1\rangle\langle 0\|$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\boldsymbol{X}\|0\rangle = \|1\rangle$ $\boldsymbol{X}\|1\rangle = \|0\rangle$	
Hadamard ($\boldsymbol{H}$)	$\boldsymbol{H} = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}\langle 0\| + \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\langle 1\|$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\boldsymbol{H}\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $\boldsymbol{H}\|1\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	
Controlled-NOT (**CNOT**)	$\mathbf{CNOT} = \|0\rangle\langle 0\| \otimes \boldsymbol{I} + \|1\rangle\langle 1\| \otimes \boldsymbol{X}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	$\mathbf{CNOT}\|00\rangle = \|00\rangle$ $\mathbf{CNOT}\|01\rangle = \|01\rangle$ $\mathbf{CNOT}\|10\rangle = \|11\rangle$ $\mathbf{CNOT}\|11\rangle = \|10\rangle$	
Toffoli ($\boldsymbol{T}$ or **CCNOT**)	$\mathbf{T} = \|0\rangle\langle 0\| \otimes \boldsymbol{I} \otimes \boldsymbol{I} + \|1\rangle\langle 1\| \otimes \mathbf{CNOT}$	$\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{pmatrix}$	$\mathbf{T}\|000\rangle = \|000\rangle, \mathbf{T}\|001\rangle = \|001\rangle$ $\mathbf{T}\|010\rangle = \|010\rangle, \mathbf{T}\|011\rangle = \|011\rangle$ $\mathbf{T}\|100\rangle = \|100\rangle, \mathbf{T}\|101\rangle = \|101\rangle$ $\mathbf{T}\|110\rangle = \|111\rangle, \mathbf{T}\|111\rangle = \|110\rangle$	

Reversibility and No-Cloning

- In Quantum Computing, we use unitary operations ($U^* U = 1$).
- This ensures that all of the operations that we perform are reversible.
- This fact is important, because there is no way to perfectly copy a state in Quantum Computing (No-Cloning Theorem).

No-Cloning Theorem

- That is, the No-Cloning Theorem says that there is no linear operation that copy an arbitrary state to one of the basis states:

$$|\psi\rangle|e_i\rangle \to |\psi\rangle|\psi\rangle$$

- We can get around this if we are only interested in copying basis vectors, though.

Entanglement

- In Quantum Mechanics, it sometimes occurs that a measurement of one particle will effect the state of another particle, even though classically there is no direct interaction. (This is a controversial interpretation).
- When this happens, the state of the two particles is said to be entangled.

Entanglement: Formalism

- More formally, a two-particle state is entangled if it cannot be written as a product of two one-particle states.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right)$$

- If a state is not entangled, it is decomposable.

$$|\psi\rangle = \frac{1}{2}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2 + |1\rangle_1|1\rangle_2\right)$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle_1 + |1\rangle_1\right)\frac{1}{\sqrt{2}}\left(|0\rangle_2 + |1\rangle_2\right)$$

Entanglement: Example

- The state of two spinors is prepared such that the *z*-component of the spin is zero.
- If we measure $m = +1/2$ for one particle, then the other particle must have $m = -1/2$.
- The measurement performed on one particle resulted in the collapse of the wavefunction of the other particle.

Outline

- Review of Classical Computing
- Qubits and Quantum Operations
- **Quantum Algorithms**
  - Definitions
  - Universal Gate Sets
  - Example: Quantum Teleportation
- Physical Implementations
- Future Developments

Definitions

- A Quantum Algorithm is any algorithm that requires Quantum Mechanics to implement.
- A Quantum Computer is any device that can implement a Quantum Algorithm.

Universal Gate Sets

- It would be convenient if there was a small set of operations from which all other operations could be produced.
- That is, a set of operators $\{U_1,\ldots,U_n\}$ such that any other operator W could be written $W = U_i U_j \ldots U_k$.
- Such a set of operators in the context of computation is called a universal gate set.

Classical NAND Gate

- One universal set for Classical Computation consists of only the NAND gate which returns 0 only if the two inputs are 1.

NAND		
Input 1	Input B	Output
0	0	1
0	1	1
1	0	1
1	1	0

$$NOT(P) = NAND(P, P)$$

$$AND(P, Q) = NAND(NAND(P, Q), NAND(P, Q))$$

$$OR(P, Q) = NAND(NAND(P, P), NAND(Q, Q))$$

Quantum Universal Gate Set

- There are a few universal sets in Quantum Computing.
- Two convenient sets:
  - CNOT and single Qubit Gates
  - CNOT, Hadamard-Walsh, and Phase Flips
- Having such a set could greatly simplify implementation and design of Quantum Algorithms.

Outline

- Review of Classical Computing
- Qubits and Quantum Operations
- Quantum Algorithms
- **Physical Implementations**
  - Requirements
  - NMR Implementation
- Future Developments

Physical Implementation

- Any physical implementation of a quantum computer must have the following properties to be practical(DiVincenzo)
  - The number of Qubits can be increased
  - Qubits can be arbitrarily initialized
  - A Universal Gate Set must exist
  - Qubits can be easily read
  - Decoherence time is relatively small

Other Implementations

- There are other possible ways to produce quantum computers:
  - Quantum dots
  - Superconductors
  - Lasers acting on ion traps
  - Molecular magnetic computers

Outline

- Review of Classical Computing
- Qubits and Quantum Operations
- Quantum Algorithms
- Physical Implementations
- **Future Developments**

Future Prospects

- Currently, research in Quantum Computing is more based on proof-of-principle rather than research into practical applications.
- The infancy of the science is a significant inhibitor. In the future, decoherence may be a serious issue.

Future Prospects

- Although many Quantum Algorithms seem to threaten classical computing (such as RSA-encryption), Classical Computers will be significantly larger than Quantum Computers for the foreseeable future.
- Kurzweil, for example, suggests that practical quantum computing will be achieved at approximately the same time humanity achieves immortality (before 2099).

Concluding Remarks

- Quantum Computing could provide a radical change in the way computation is performed.
- The unit of information in Quantum Computing is the Qubit, which is a two state-system. Basic operations are unitary operators on the Hilbert space of this system.
- The advantages of Quantum Computing lie in the aspects of Quantum Mechanics that are peculiar to it, most notably entanglement.
- Practical Quantum Computers are a significant ways off.

References

General

Hirvensalo, M. (2004) *Quantum Computing*. Springer-Verlag [Good introduction to the material. Much of the material in the presentation in elaborated this text.]

Lo, H., Popescue, S., and Spiller, T., eds. (1998) *Introduction to Quantum Computation and Information*. World Scientific.

Shor's Algorithm

Shor, P. (1994) Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, Santa Fe, NM, Nov. 20-22, 1994. (Available electronically at quant-ph/9508027) [Shor's original paper describing the quantum algorithm used to factor integers].

Physical Implementation

Boschi, D., et al. (1998). Experimental Realization of Teleporting of an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, **80**, 1121-1125.

Bouwmeester, D., et al. (1997). Experimental Quantum Teleportation. *Nature*, **390**, 575-579.

DiVincenzo, D. (2000) The Physical Implementation of Quantum Computation. (Prepared for Fortschritte der Physik special issue, *Experimental Proposals for Quantum Computation*, eds. H.-K. Lo and S. Braunstein. Available electronically at quant-ph/0002077)

Vandersypen, L. M. K., et al. (2001) Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance. *Nature*, **414**, 883-887.

References

Lego Logic Gates

The Goldfish Online, “LEGO Logic Gates” <http://goldfish.ikaruga.co.uk/logic.html>. Accessed April 18, 2005.

Other

Foot, C. J. (2005). *Atomic Physics*. Oxford University Press (Paperback). [Provides a brief perspective on Quantum Computing that is relevant to a student of atomic physics]

Kurzweil, Ray. (2000). *The Age of Spiritual Machines: When Computers Exceed Human Intelligence.* Penguin Books (Paperback) [Very little about Quantum Computing *per se*, but provides an interesting comparison of the future prospects of the field in comparison to other forms of computing].

Thank you

Any Questions

& Suggestions are Welcome