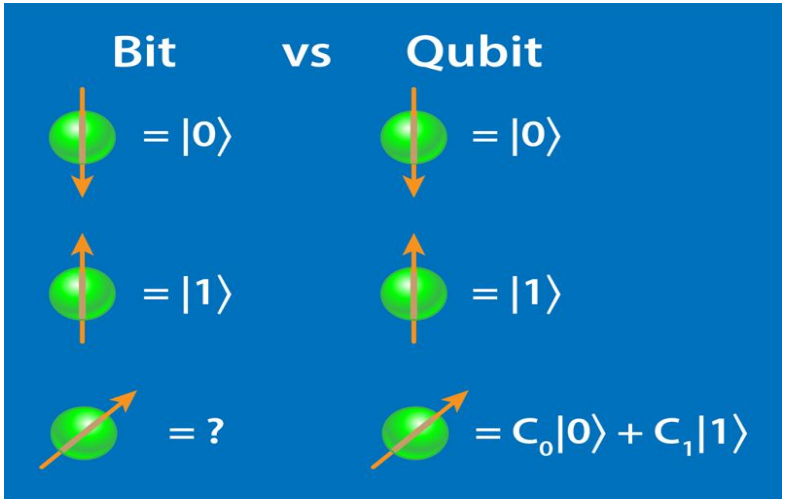
Demystifying Quantum Computing



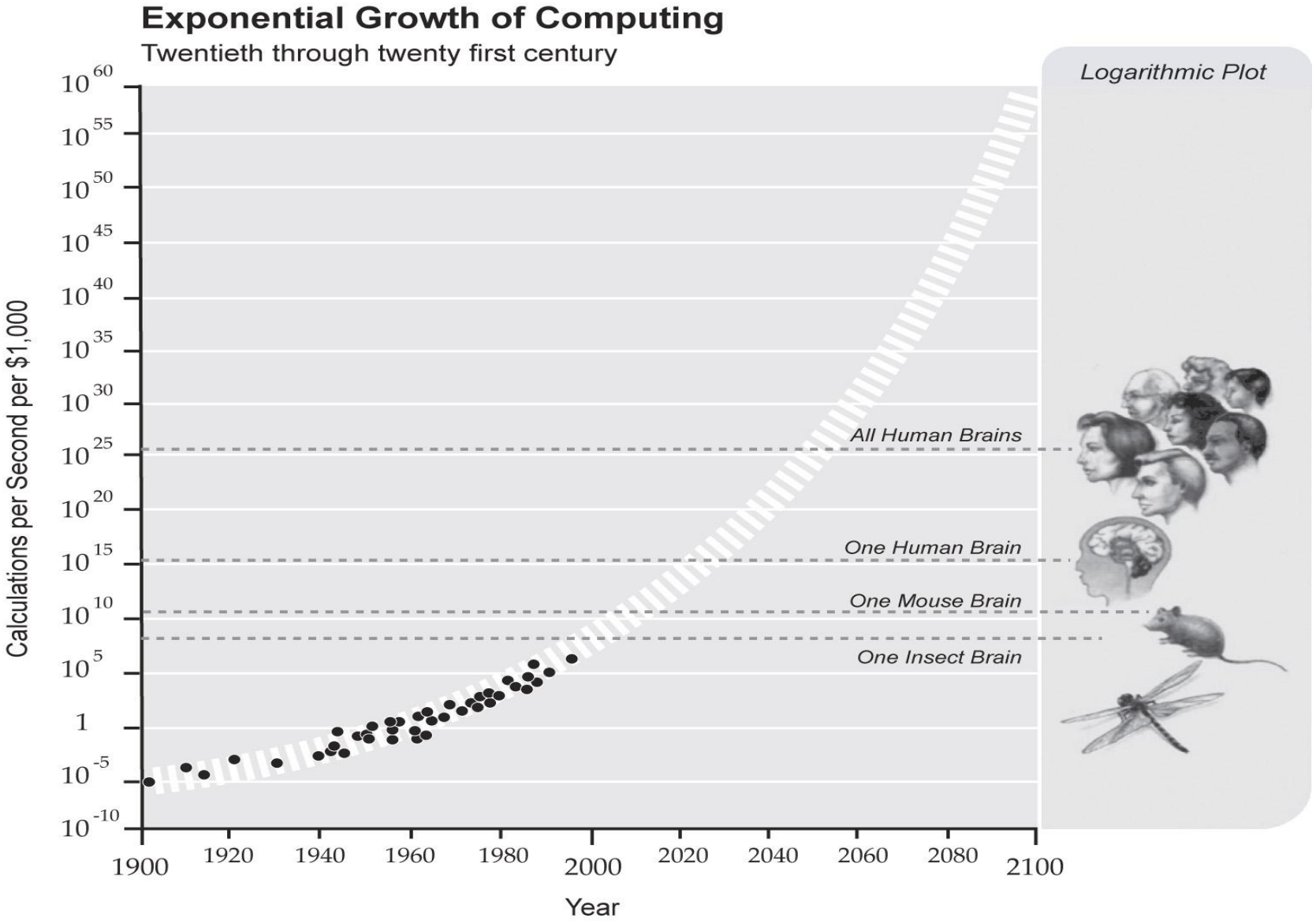
Dr. Aswani Kumar. Cherukuri
Professor
School of Information Technology and Engineering

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Sessions Includes

- Need for Quantum Computing
- Quantum Computing - Principles
- Quantum Computing Blocks - Qubits & Gates
- Applications – Quantum Key Distribution
- Challenges in Quantum Computing

Prologue


Exponential Growth of Computing
Twentieth through twenty first century
Logarithmic Plot
Calculations per Second per $1,000
10^{60}
10^{55}
10^{50}
10^{45}
10^{40}
10^{35}
10^{30}
10^{25}
10^{20}
10^{15}
10^{10}
10^{5}
1
10^{-5}
10^{-10}
All Human Brains
One Human Brain
One Mouse Brain
One Insect Brain
1900
1920
1940
1960
1980
2000
2020
2040
2060
2080
2100
Year

Quantum Computing

- Classical computing devices increased computing performance by many orders of magnitude by making the operations faster (increasing the clock frequency) and increasing the number of operations completed during each clock cycle.

- Bernstein et al. showed in 1993 that quantum computers could violate the extended Church-Turing thesis, and in 1994 Peter Shor showed a practical example of this power in factoring a large number: a quantum computer could solve this problem exponentially faster than a classical computer.

- But at that time no one knew how to build even the most basic element of a quantum computer, a quantum bit, or “qubit.

Quantum Computing

- These results catalyzed interest among researchers in developing other quantum algorithms with exponentially better performance than classical algorithms, and trying to create the basic quantum building blocks from which a quantum computer could be built.

- During the past few decades, this research has progressed to the point where very simple quantum computers have been built, and a positive outlook is emerging based upon the assumption that the complexity of these machines will grow exponentially with time, analogous to the growth that has been achieved in performance of classical computers.

Quantum Computing

- Quantum computing, which harnesses quantum mechanical phenomena to greatly enhance the way in which information is stored and processed, has been an area of ongoing research for more than 30 years.

- Although physicists and mathematicians were able to theorize three decades ago how a quantum computer could work, scientists and engineers had difficulty building one.

- In the last five years, we have seen the hardware and software capability move out of university labs and into tangible business products; however, the technology still needs to mature in order for it to become fully enterprise-ready and deliver meaningful, cost-effective business results.

Quantum Computing - Principles

- According to the theory, a quantum object does not generally exist in a completely determined and knowable state.
- In fact, each time one observes a quantum object it looks like a particle, but when it is not being observed it behaves like a wave.
- This so-called wave-particle duality leads to many interesting physical phenomena.

Quantum Computing

- There are many hyped statements being made about the capabilities of quantum computing to do tasks such as breaking modern encryption methods in seconds and solving intractable problems in minutes.

- While in theory this is possible, the reality today is that quantum computers have yet to achieve these types of results.

- As such, it is unlikely classical computing will be replaced any time soon by quantum computing.

- The more likely future scenario is that quantum computing will augment subroutines of classical algorithms that can be efficiently run on quantum computers, such as sampling, to tackle specific business problems.

- However, problems that cannot be solved on classical computers but can potentially be solved on quantum computers are likely worth the expense in the near term.

Quantum Computing

- A bit can either be 0 or 1, while a qubit can represent the values 0 or 1, or some combination of both at the same time (known as a "superposition").

- While the state of a classical computer is determined by the binary values of a collection of bits, at any single point in time the state of a quantum computer with the same number of quantum bits can span all possible states of the corresponding classical computer, and thus works in an exponentially larger problem space.

- However, the ability to make use of this space requires that all of the qubits be intrinsically interconnected ("entangled"), well isolated from the outside environment, and very precisely controlled.

Quantum Computing - Principles

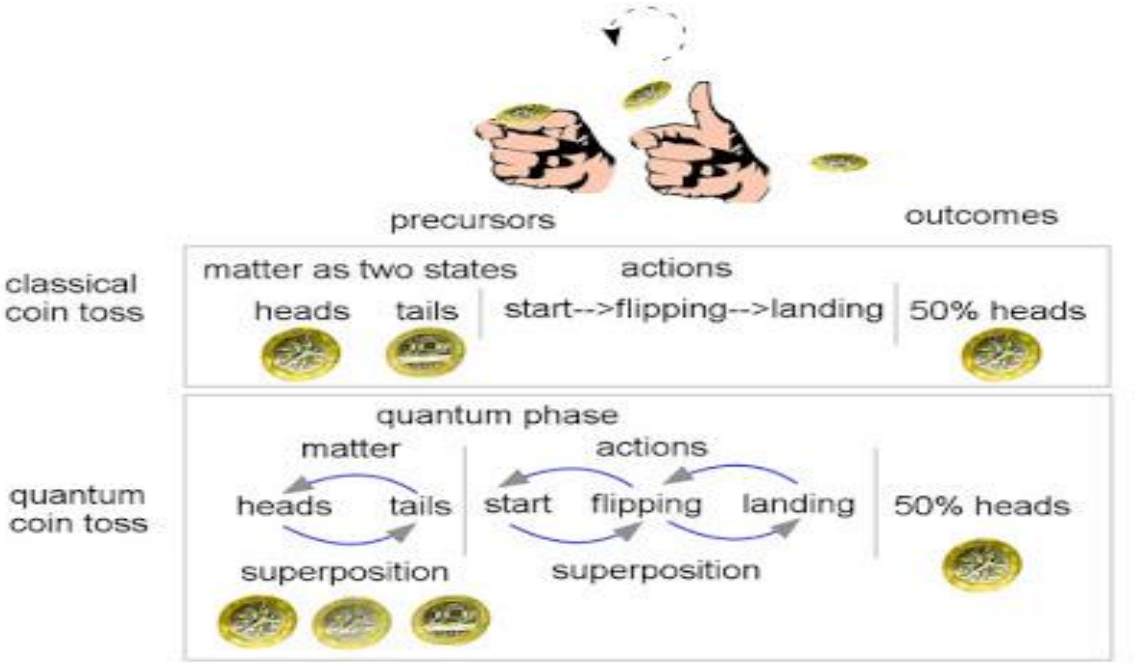
- Quantum objects can exist in multiple states all at once, with each of the states adding together and interfering like waves to define the overall quantum state.
- In general, the state of any quantum system is described in terms of "wave functions."
- The state of a system can be expressed mathematically as a sum of the possible contributing states, each scaled by a complex number coefficient that reflects the relative weight of the state.
- Such states are said to be "coherent," because the contributing states can interfere with each other constructively and destructively, much like wavefronts.

Quantum Computing - Principles

- However, when one attempts to observe a quantum system, only one of its components is observed, with a probability proportional to the square of the absolute value of its coefficient.
- To an observer, the system will always look classical when measured.
- Observation of a quantum object, formally called "measurement," occurs when the object interacts with some larger physical system that extracts information from it.
- Measurement fundamentally disrupts a quantum state: it "collapses" the aspect of wave function that was measured into a single observable state, resulting in a loss of information.
- After the measurement, the quantum object's wave function is that of the state that was detected, rather than that of its premeasurement state.

Quantum Computing - Principles

- Consider a coin toss. Its state is either heads-up (U) or heads-down (D).
- A quantum version of a coin would exist in a combination, or "superposition," of both states at the same time.
- The wave function of a quantum coin could be written as a weighted sum of both states, scaled by coefficients C_U and C_D.

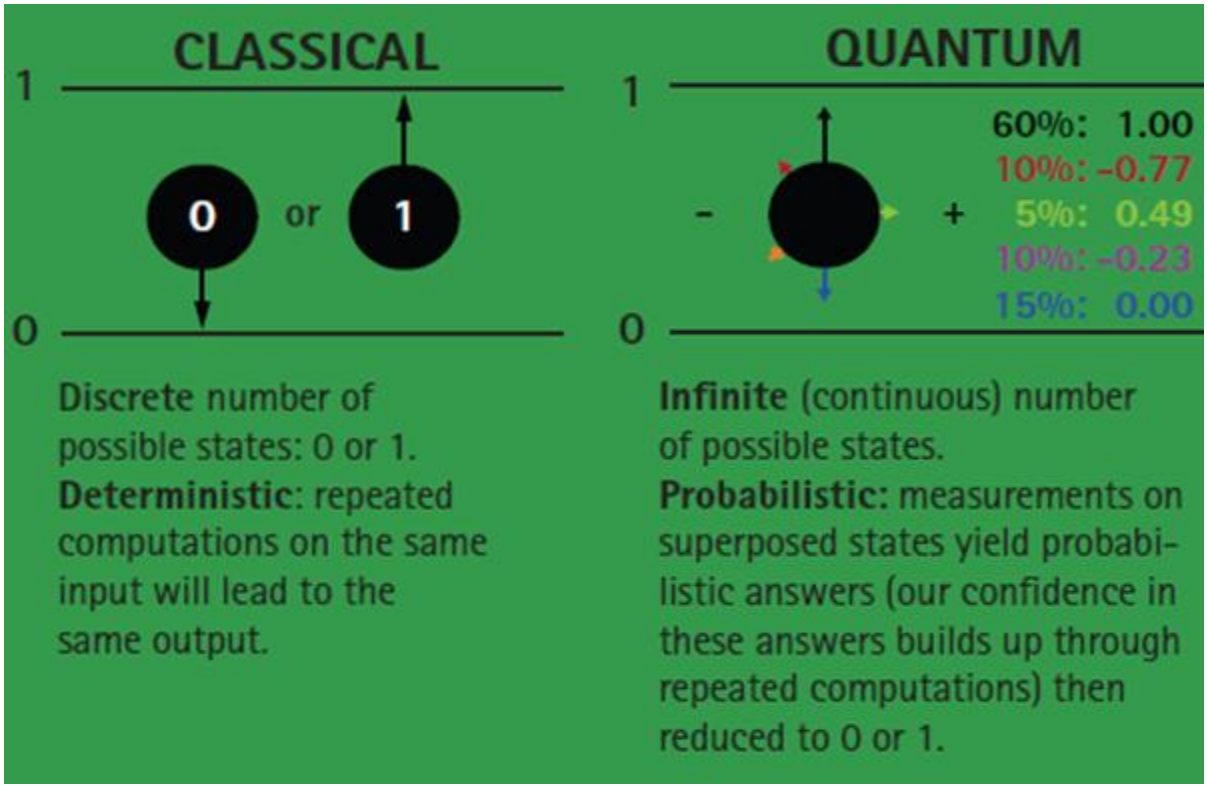


Quantum Computing

Information representation—In classical computing, a computer runs on bits that have a value of either 0 or 1.

- Quantum bits or “qubits” are similar in that for practical purposes we read them as a value of 0 or 1, but they can also hold much more complex information, or even be negative values.

- Before we read their value they are in an indeterminate state called superposition and can be influenced by other qubits (entanglement).



Quantum Computing

Information processing—In a classical computer, at the fundamental level, bits are processed sequentially, which is similar to the way a person would solve a math problem by hand, one step at a time.

- In quantum computation, superposition qubits are entangled together so changing the state of one qubit influences the state of others regardless of their physical distance. This allows quantum computers to intrinsically converge on the right answer to a problem very quickly.

- As a result, qubits working together to find the optimal solution are more efficient than certain classical approaches.

Interpreting results—In classical computing, only specifically defined results are available, inherently limited by an algorithm's design.

- Quantum answers (which are in quantity called amplitudes) are probabilistic, meaning that because of superposition and entanglement multiple possible answers are considered in a given computation.

- Problems are run multiple times, giving a sample of possible answers and increasing confidence in the best answer provided. Statistics are used to rank from 0 to 100 percent the likelihood an answer is the correct one.

- This confidence threshold is balanced to provide the optimal speed and accuracy.

Quantum Computing

- These factors allow quantum computers to solve certain classes of complex problems much more efficiently than classical computers.

- While classical computers would take more and more time for each variable added (e.g., exponential time), quantum computers can harness the properties mentioned above to solve complex problems in a way that increasing the problem size causes a far smaller increase in the time required to solve the problem.

Quantum Computing

Comparison	Classical Supercomputing	Quantum Computing
Information Storage	Bit based on voltage or charge	Quantum bit based on the direction of an electron spin
Information Processing	Achieved by logic gates e.g. NOT, AND, OR etc.	Achieved by Quantum logic gates
Circuit Behavior	It is governed by classical physics	It is governed explicitly by quantum mechanics
Representing Information	Utilize binary codes i.e. bits 0 or 1 to represent information	Utilize Qubits i.e. 0, 1 and both of them simultaneously to run machines quicker.
Operations Definition	Represented by Boolean Algebra	Represented by linear algebra over Hilbert Space
Advantages	- There are no limitations on copying or measuring signals. - Circuits are easily integrated in quick, scalable and macroscopic technologies such as CMOS.	- Faster than classical computation - Quantum computer can tackle classes of problems that choke conventional machines - The use of quantum computing is very green in nature. It can save enormous heat consumption in datacenters
Disadvantages	- Slower than Quantum computation	- Severe restrictions occur on measuring and copying signals - Circuits should utilize microscopic technologies which are not scalable, slow and fragile e.g. Nuclear magnetic resonance - High Q Error rates - Qubits live very short - Physical size of the machines is too huge to be of practical use to everyday society

Abdelsamea, A., Nassar, S. M., & Eldeeb, H. (2020). The past, present and future of scalable computing technologies trends and paradigms: A survey. *International Journal of Innovation and Applied Studies*, *30*(1), 199-214.

Quantum Computing - Qubits

- When creating conventional ICs, designers take great pains to minimize the effect of quantum phenomena, which typically manifest as noise or other errors that affect transistor performance, especially as devices get smaller and smaller.

- Quantum computing in all its forms takes a very different approach by embracing rather than trying to minimize quantum phenomena, using quantum rather than classical bits.

Quantum Computing - Qubits

- A quantum bit, or qubit, has two quantum states. While the qubit can be in either state, it can also exist in a “superposition” of the two.

- These states are often represented in so-called Dirac notation, where the state’s label is written between a | and a ⟩.

- Thus, a qubit’s two component, or “basis,” states are generally written as |0⟩ and |1⟩.

- Any given qubit wave function may be written as a linear combination of the two states, each with its own complex coefficient a_i:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Quantum Computing - Qubits

Quantum Computing - Qubits

- Any given qubit wave function may be written as a linear combination of the two states, each with its own complex coefficient a_i:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

- $|a_0|^2$ corresponds to the probability of detecting the state $|0\rangle$, and $|a_1|^2$ to the probability of detecting $|1\rangle$.

- The sum of the probabilities of each possible output state must be 1, mathematically expressed as

$$|a_0|^2 + |a_1|^2 = 1.$$

While a classical bit is entirely specified either as 1 or 0, a qubit is specified by the continuum of the values a_0 and a_1, which are actually analog.

Quantum Computing - GATES

For an operation or logic gate to be reversible, you must be able to determine the set of inputs used, given the output and the name of the operation used.

Identity	f(x) = x	0 → 0 1 → 1
Negation	f(x) = ¬x	0 → 1 1 → 0
Constant-0	f(x) = 0	0 → 0 1 → 0
Constant-1	f(x) = 1	0 → 1 1 → 1

- Identity and Negation operations are reversible, while the constant-1 and 0 operations are not.
- Quantum computers only ever use reversible operations. We will be converting non-reversible gates to reversible ones to make them possible to use in a quantum computer.

Quantum Computing - GATES

- We can represent multiple bits at a time by using the tensor product of each bit together.

$$|00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad |01\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |11\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Quantum Computing - GATES

CNOT, or controlled NOT

CNOT Gate

Input		Output
$\|00\rangle$	$\longrightarrow$	$\|00\rangle$
$\|01\rangle$	$\longrightarrow$	$\|01\rangle$
$\|10\rangle$	$\longrightarrow$	$\|11\rangle$
$\|11\rangle$	$\longrightarrow$	$\|10\rangle$

The first bit is designated the 'control' bit, and the other the 'target' bit. If the control bit is 1, the target bit is flipped, and if the control bit is 0, the target bit is left unchanged.

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathrm{CNOT}|10\rangle = \mathrm{CNOT}\left(\begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = |11\rangle$$

$$\mathrm{CNOT}|11\rangle = \mathrm{CNOT}\left(\begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = |10\rangle$$

https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

Quantum Computing - GATES

More formally, a qbit is represented as a linear combination of both $|0\rangle$ and $|1\rangle$ with the following definition:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle$$

a_0 and a_1 are the amplitudes of $|0\rangle$ and $|1\rangle$ respectively.

$$\begin{aligned} |\psi\rangle &= a_0|0\rangle + a_1|1\rangle \\ &= a_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} a_0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_1 \end{pmatrix} \\ &= \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \end{aligned}$$

the qbit: $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$

has a chance of $|1/\sqrt{2}|^2$, or 1/2 chance of collapsing into a 1, making it a 50/50 chance.

the squares of the absolute values of the amplitudes of $|0\rangle$ and $|1\rangle$ must also add up to 1.

$$|a_0|^2 + |a_1|^2 = 1$$

https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

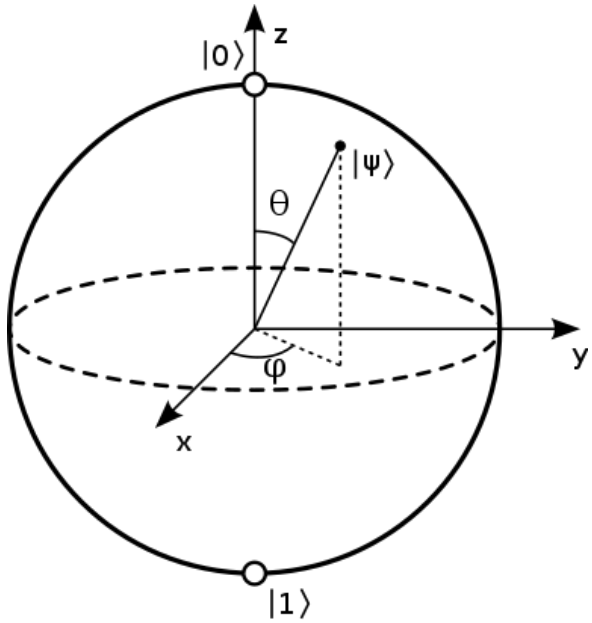
Quantum Computing - GATES

- The matrix operators have the effect of manipulating each of the amplitudes of a qbit without measuring and collapsing it.

- A negation operator on a qbit:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{pmatrix}$$

The values of the amplitudes of a_0 and a_1 are really complex numbers, and so the state of a qbit can be more accurately represented as a 3d unit sphere, also known as a bloch sphere:



https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

Quantum Computing - GATES

- The most important operators is the ‘Hadamard gate’. A Hadamard gate takes a bit in a 0 or 1 state, and puts it into an exactly equal superposition, with a 50% chance of collapsing into a 1 or 0 when measured.

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$$

- Hadamard gate is reversible, so it can take a qbit in an exactly equal superposition and transform it into a $|0\rangle$ or $|1\rangle$.

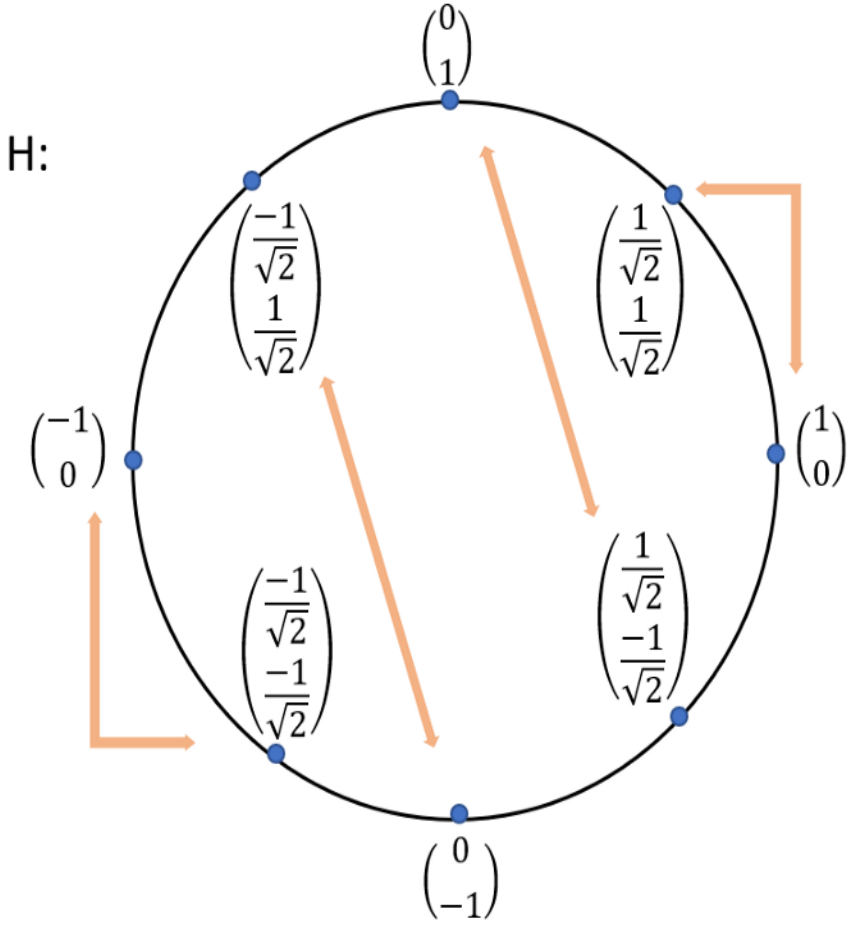
$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

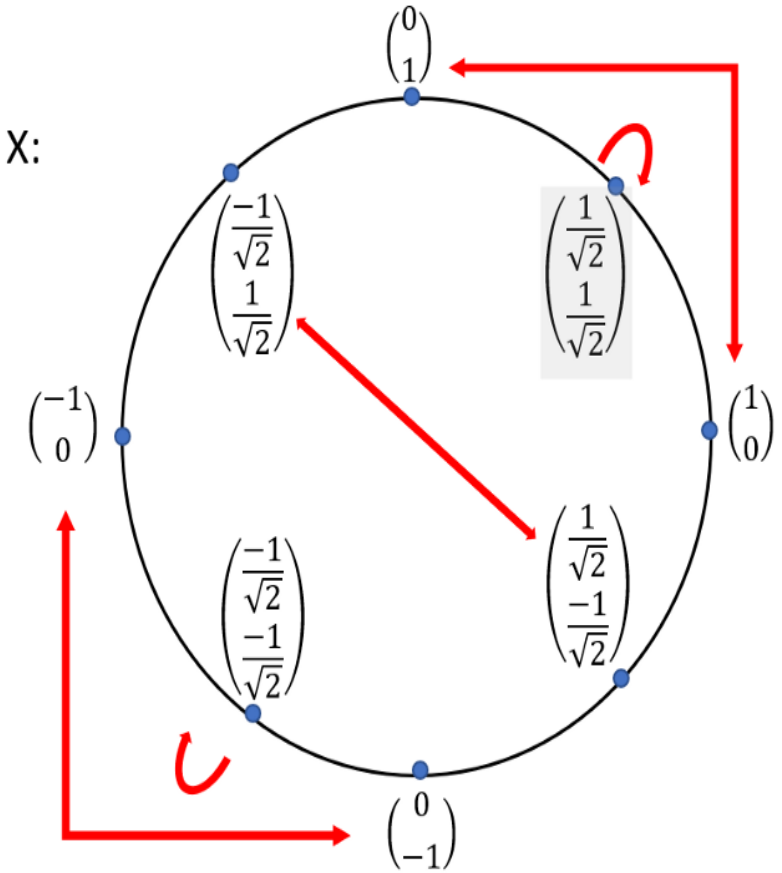
$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

Quantum Computing - GATES

- We can represent an operator's effect on a qbit as a transformation around the unit circle as a state machine:

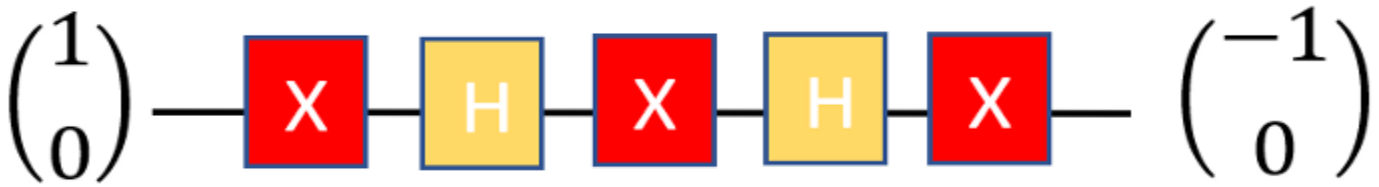


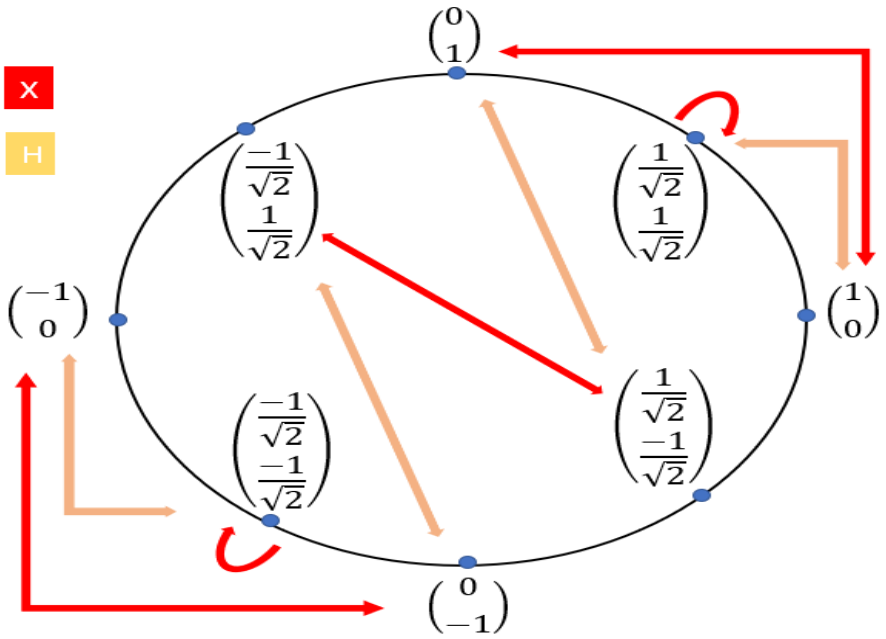


https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

Quantum Computing - GATES

- To perform more complicated operations on qbit, we can chain multiple operators together, or use gates multiple times. We can represent an example of a series of transformations using Quantum circuit notation as follows:





https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

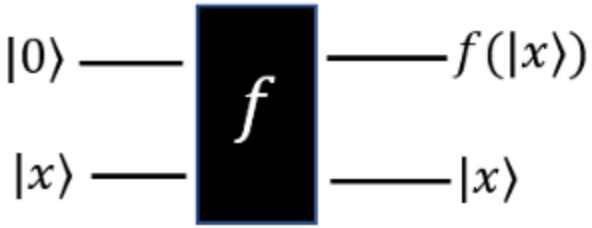
Quantum Computing - GATES

- Constant-1 and 0 functions as they are not reversible.
- How to handle it??

- Add an additional output qbit that returns whatever input was given to the function

Before:

After:



- We can determine the inputs just from knowing the outputs, making the function reversible.
- We also need an additional input bit.
- We will assume that this additional input qbit will always be $|0\rangle$.

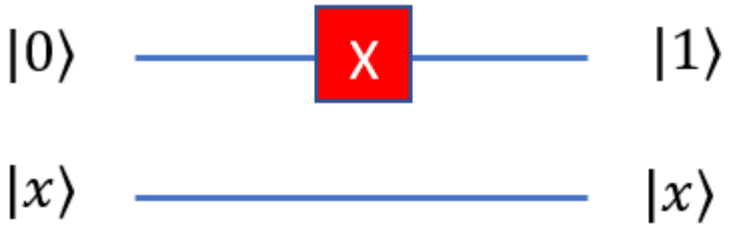
https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

Quantum Computing - GATES

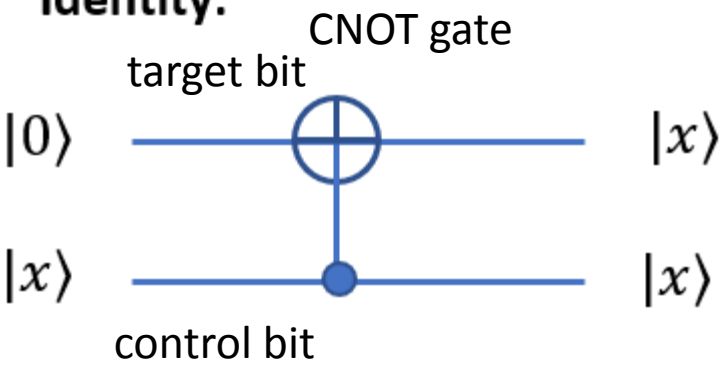
- lets go through how we would design each of the four gates, Reversible.

Constant-0:

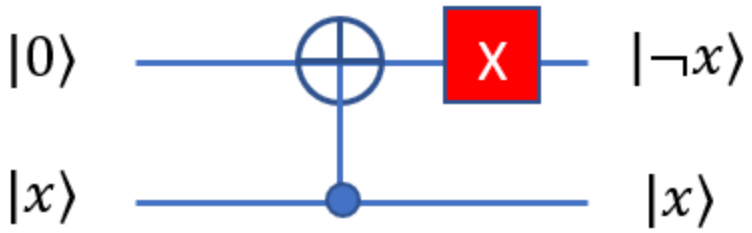
Constant-1:



Identity:



Negation:



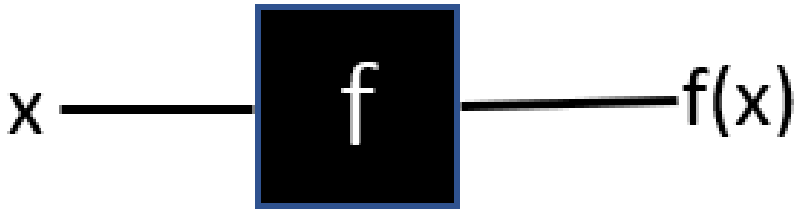
https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

Quantum Computing - GATES

- How a QC can clearly outperform a classical computer?

- Consider Deutsch-Jozsa algorithm, a deterministic & unlike other probabilistic Q. algos.

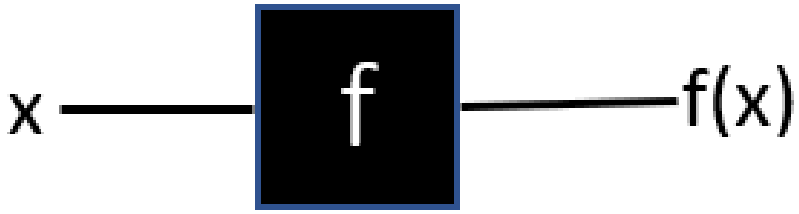
Imagine that you were given a black box that contains a function on one bit. You don't know which function is inside the box.



How many inputs and outputs would you have to run through the black box to figure out which function is being used? (Constant-1/0, identity & negation)

https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

Quantum Computing - GATES



How many inputs and outputs would you have to run through the black box to figure out which function is being used? (Constant-1/0, identity & negation)

- On a classical computer, it will take two queries to figure out which function is being applied.
- if an input of ‘1’ gets ‘0’, it’s either a constant-0 , or a negation function, and so we run an input of ‘0’ as well to see if the output changes.

- On a quantum computer, this will also take two queries to determine.
- We still need two different outputs to determine precisely which function is being applied to the input.

BUT

https://whiteheadsoftware.dev/quantum-computings-internals-demystified/

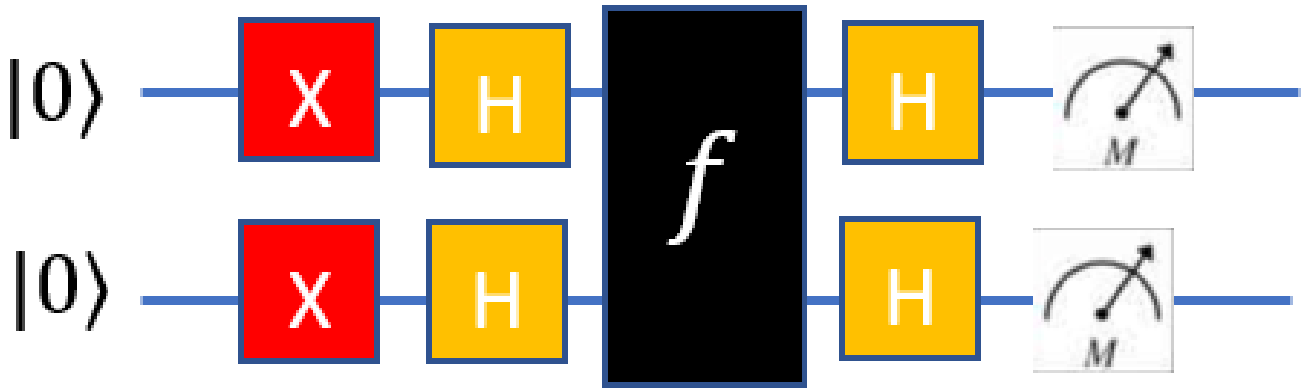
Quantum Computing - GATES

If we only want to know whether the function is constant or variable

The function in the box is variable if different inputs produce different outputs (i.e, Identity and bit-flip), and it is constant if the output is fixed, regardless of the input (i.e, Constant-1 and Constant-0).

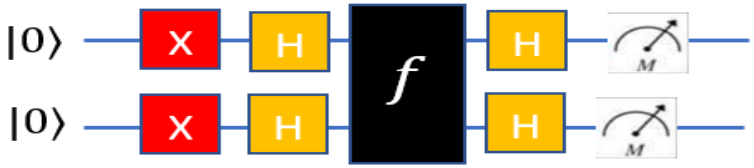
By using a quantum algorithm, we can figure out whether the function in the black box is constant or variable by only using one query.

Transform the input qbits to a superposition through H gate:



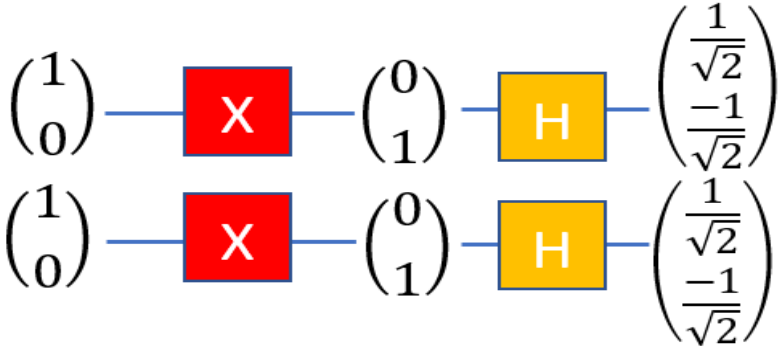
H gate at outputs of the function to take the qbits out of superposition. Deterministic o/p

Quantum Computing - GATES



initialise the system with state |00⟩

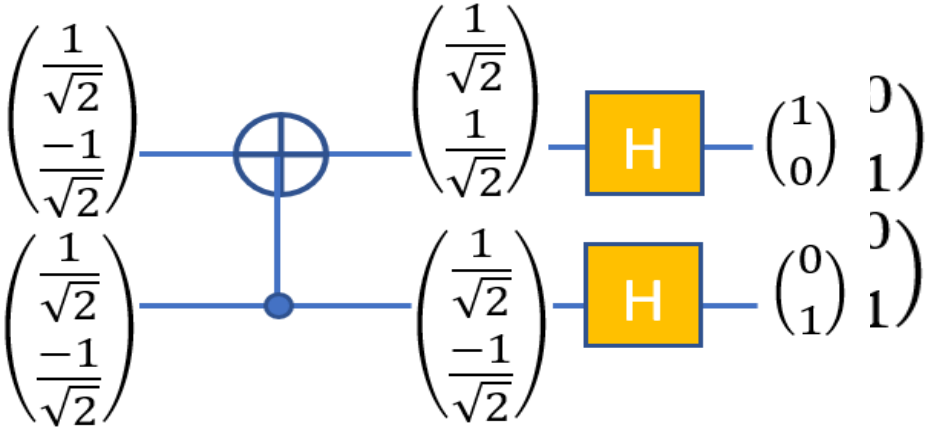
By applying a bit-flip operator & a Hadamard gate to both inputs of |0⟩, they both transformed into an equal superposition of |0⟩ &|1⟩ :



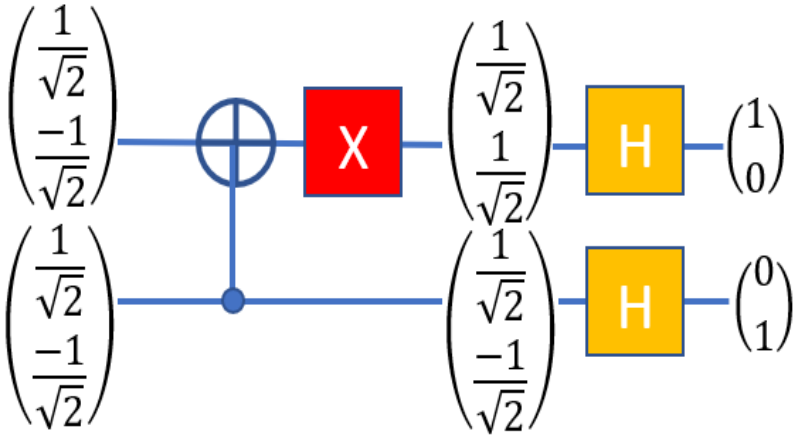
If this goes as input to a Constant 0 /1 function, it will return |11⟩:

If it is a Variable function (identity/negation) it will return |01⟩:

Identity:



Negation:



Quantum Computing

Types of quantum computers: There are several approaches to building quantum computers.

- The most business-relevant types today are the adiabatic quantum computer and the gate model quantum computer.

- These two methods have been explored using various hardware implementations and both have strengths and weaknesses.

Quantum Computing

- Quantum technology is still maturing and there are some hurdles left to overcome in order to build fully scalable quantum computers.

- As just one example, quantum systems are much more sensitive than classical computers to noise (i.e., factors that the system adjusts for on a regular basis). Noise causes a quantum system to decohere and lose its quantum properties.

- There is a lot of room for progress in devising quantum error correction schemes (also known as fault-tolerant quantum computing), as well as engineering advancements toward suppressing noise effects.

Quantum Computing: Applications

- At this point in time, quantum computing is best suited to solving problems using three types of algorithms: optimization, sampling and machine learning.

- These are non-linear polynomial optimization problems with discrete variables.

Challenges & Risks

- Qubits Cannot Intrinsically Reject Noise:

Since a qubit can be any combination of one and zero, qubits and quantum gates cannot readily reject small errors (noise) that occur in physical circuits.

- Error-Free QC Requires Quantum Error Correction:

it is possible to run a quantum error correction (QEC) algorithm on a physical quantum computer to emulate a noise-free QC.

- Large Data Inputs Cannot Be Loaded into a QC Efficiently:

Challenges & Risks

- Quantum Algorithm Design Is Challenging:

achieving quantum speedup requires totally new kinds of algorithm design principles and very clever algorithm design.

- Quantum Computers Will Need a New Software Stack:

- The Intermediate State of a Quantum Computer Cannot Be Measured Directly

Conclusions

- The first major constraint is that the number of coefficients required to describe a state of a quantum computer increases exponentially with the number of qubits only when the qubits all become entangled with each other.
- A second constraint comes from the fact that it is impossible to make a copy of a quantum system, because of the so-called no-cloning principle.

- The third main constraint comes from the lack of noise immunity of quantum operations.

- The final constraint is the inability to actually observe the full state of the machine after it has completed its operation.

References

- Hidary, J. D. (2019). *Quantum Computing: An Applied Approach*. Springer International Publishing.
- National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum computing: progress and prospects*. National Academies Press.
- Trabesinger, A. (2017). Quantum computing: towards reality. *Nature*, *543*(7646), S1-S1.
- Yanofsky, N. S., & Mannucci, M. A. (2008). *Quantum computing for computer scientists*. Cambridge University Press.

cherukuri@acm.org