**RESEARCH ASSIGNMENT 1**

**Team members:**

**Sri Mahathi Gayathri Kolli - 916503606  
Sundari Rakesh - 916504450**

**1. Answer**

Quantum computing is an innovative method of calculation founded on the principles of quantum mechanics for processing data. Quantum computers uses quantum bits or qubits, which can, due to superposition and entanglement, exist in more than one state at the same time, unlike the classical computers, which utilize bits as the smallest unit of information (0 or 1). This makes quantum computers exponentially better at carrying out more than one calculation at a time. The quantum state of a system will, with relatively few qubits be capable of encoding an exponentially large amount of information. Quantum gates, unlike the ordinary logic gates, operate on wavefunctions and probabilities, which allows them to carry out complex transformations of states in qubits. There are profound implications for its applications, even though quantum computing is in its primary level of development. It is already able of calculating issues that are effectively impossible with the use of conventional machines. It is a combination of physics, mathematics, and computer science that shatters the limitations on processing, storage, and problem-solving.

**Computational Power**

Quantum computers have quadratic or exponential speedup over some problems. The beauty of quantum computers is the method by which they handle information:

* Superposition makes qubits capable of holding many values at once, thus quantum computers can hold much more computation space than classical computers with an equal number of bits.
* Entanglement gives quantum computers the enormous correlations between qubits, making extremely parallel calculation possible without copying memory.
* Interference gets sharper to take the right decisions on correct solutions by eliminating wrong ways and enhancing correct ones.

**Advantages**

* Speed - Shor's-factoring-algorithm and Grover's-search-algorithm exhibit theoretical and actual speedups.
* Accuracy – Quantum-simulations of atoms and molecules get accurate beyond classical computers' range.
* Handling of Complexity - Quantum computers fix combinatorial explosion issues, i.e., huge optimizations and simulations.
* Memory Density - Several hundred qubits contain as much information as would a million billion classical exabytes.

But only problems involving quantum-accelerable gain advantage from this capability, not all of them.

**Potential Applications**

Quantum-computing is in its primary level but has the promise of transformative impacts on a wide range of endeavors

**Cryptography** - Shor's algorithm makes the RSA encryption susceptible to being broken, forcing a transition to post-quantum cryptography.

**Drug & Material Discovery** - Quantum models to simulate molecules, proteins, or emergent materials more realistically than classical chemistry models.

**Optimization Problems** - Variational methods and quantum annealing are applied to logistics, financial portfolio, and machine learning model optimization.

**Machine Learning & AI** - Quantum kernels and quantum neural networks enable faster classification, clustering, and model training.

**Climate & Physics Simulations** - Simulate complex weather systems, quantum gravity, or nuclear interactions.

Quantum search is orders of magnitude improved in large, unsorted databases. Scaling hardware, future progress is envisioned by using hybrid classical-quantum designs with Noisy Intermediate-Scale Quantum (NISQ) devices.

**2. Answer**

Quantum computation is based upon quantum mechanics and specifically upon entanglement, superposition, and interference between quantum systems. Classical switching theory is based upon binary values (0,1) and AND, OR and NOT gate logic for dealing with information, and quantum computation is a generalization of these in quantum gate and qubit language.

**Classical Switching Theory**

* Boolean logic regulates digital circuits within classical digital systems.
* A switch (e.g., transistor) can be ON (1) or OFF (0).
* Logic gates control these binary values deterministically.
* Circuits perform through a sequence of binary switches.

**Quantum Computing**

* A qubit is a 0 and 1 superposition
* |ψ⟩=α|0⟩+β|1⟩, where α and β are complex amplitudes.
* Instead of simple “Switches”, we have quantum states, which are created during unitary transforms (like logic gates, but probabilistic and reversible).
* Quantum gates (Hadamard gate, Pauli-X gate, CNOT gate) are linear algebra operations on qubits, operating on state vectors.

**Classical vs Quantum**  
1. Information units  
Classical: It employs 0 and 1 as its digits.  
Quantum: We have qubits here, which are both 0 and 1 at once (i.e., ∣ψ⟩ = α∣0⟩ + β∣1  
2. Logic and Operations  
It is Boolean algebra based and employs deterministic digital gates that include OR, AND, and NOT.  
Quantum: Uses reversible quantum gate implementations (Hadamard, CNOT) based on linear algebra and probability amplitudes.  
3. System Behavior and Control  
Classical: Computation is based upon a truth table with binary switching by switches (transistors).  
Quantum: Evolution of state vector under transformation, controlled by quantum systems like photons, ions, or superconducting circuits.  
  
In quantum hardware, qubits are realized by physical systems like ions, superconducting devices or photons. Physical systems evolve with time under quantum mechanics and not under classical logic. Applying a quantum gate (such as a Hadamard) is like flipping or chaining out a logic gate's output—probabilistically, wave-like.

**3. Answer**

Quantum computing differs from classical computing primarily based upon how time complexity of certain computation problems is treated. Time complexity refers to how computation time scales with input size. Classical computers perform computation sequentially or bounded parallelism, and hence certain computation problems turn out to be intractable for large input size. Quantum computers, by exploiting quantum effects, perform computation under massive parallelism and enjoy exponential speedup for certain types of problems.

**Main Differences in Efficiency**

1. Quantum Superposition

* A classical computer only handles one input at a time.
* A quantum computer handles several inputs at once through superposition. For example, n qubits have 2n states at once.
* It does not suggest quantum computers have ready solutions to everything but reduces steps required for certain algorithms.

2. Quantum Interferences and Entanglement

* Quantum qubits are linked to pass messages to one another with reduced redundancy during computation.
* Quantum interference can aid correct answers and eliminate incorrect answers to facilitate computing, simplifying output.

3. Quantum Algorithms

* The ideal traditional approach takes exponential time (~O(e^(N^1/3))), whereas the integer factorization methods used by Shor takes polynomial time (~O(log N)³)).
* Grover's-algorithm searches an unsorted database in O(√N) time, and classical searching - O(N) time.

4. Parallelism by Nature

* Classical parallel computation requires additional processors or threads.
* Quantum computing is parallel because of manipulation of qubit states—a set of paths can be computed simultaneously by one processor.

**Limitations**

All problems will not be aided. For instance, simple arithmetic or graphics rendering will not be aided at all. Quantum algorithms are typically faster in theory only, practical efficiency will hinge on error correction and qubit quality.

**Example of Time Complexity Optimization**

1. Integer factorization

Classical - It requires exponential time, and therefore RSA is secure.

Quantum - Shor's algorithm accomplishes this in polynomial time, threatening current cryptography systems.

2. Unstructured Search

Classical - An unsorted database can retrieved in O(N) time.

Quantum - Grover's-algorithm reduces this to O(√N), which is a quadratic speedup.

3. Quantum System Simulation

Classical - Needs exponentially huge resources to simulate quantum behavior.

Quantum - Can simulate these kinds of systems within polynomial time or shorter, thus ideally suited to materials science, chemistry, and physics.

Not only does quantum computing speed things up, but it actually transforms what's computationally feasible. Quantum computing redefines what's efficient as it provides speed-ups that are exponential or quadratic for specific categories of issues, which are impossible or practically impossible to calculate for classical computers. So, while classical systems use Boolean switching to calculate expressions, quantum computing uses quantum operation with probability amplitudes. State is not merely true or false, it is how much of both states it is prior to measurement.

**4. Answer**

Quantum computing originated at a confluence of several domains mainly quantum mechanics, mathematics, computer science, and information theory. Quantum computing is being created as an openly interdisciplinary field through inclusion of concepts of concepts based upon theoretical physics as well as upon concepts based upon computational science.

**1. Quantum Mechanics (Physics) -** Quantum computing is based itself on quantum physics, i.e., the law of superposition, entanglement, and unitary evolution. Physicists, who researched quantum behavior between fields, particles, and atoms, created this. Physicist Richard Feynman outlined, at an early stage in the 1980s, that quantum systems were extremely difficult for classical computers to simulate and estimated that only a second quantum system could actually simulate a second quantum system efficiently. It was thus proposed to use quantum mechanics for computation.

**2. Theoretical CS and Algorithms -** Theoretical models of computation (Turing machines, for instance) and complexity theory have been provided to us by computer science. Quantum Turing machine model, proposed by David Deutsch in 1985, provided computation based on quantum theory. A theory framework, as for classical computation by Turing machines, was thus provided. Quantum algorithms have ensued, e.g., Shor's-algorithm (by Peter-Shor, 1994) and Grover's-algorithm (Lov-Grover, 1996), to show quantum advantage at solving computational problems.

**3. Quantum Information Theory -** Quantum information theory traced the path quantum systems use to process, store, and convey information. Quantum entropy, qubit fidelity, and quantum error correction are integral to it. Quantum mechanics and Shannon's classical theory of information have been integrated by this research to address information at a quantum level.

**4. Mathematics (Linear Algebra and Probability) -** Quantum computing heavily relies upon linear algebra (matrices, vectors, and unitary transformation) and probability theory because qubits evolve in advanced vector space and measurement results are probabilistic. Mathematicians have helped with quantum gate, circuit, and algorithm formalization's mathematical foundation.

**5. Materials Science and Engineering (Follow-on Development) -** While research directed toward building quantum hardware, materials science, electrical engineering, and nanotechnology became crucial to developing and maintaining robust quantum systems (i.e., ion traps, superconducting circuits, and photonic systems).

Quantum computing is a result of a union between physics and computer science.  
Quantum Mechanics + COMPUTER SCIENCE + Information Theory + Mathematics + ENGINEERING = Quantum Computing

**5. Answer**

**Scientists and Theorists**

1. Richard Feynman explained why classical computers find it difficult to model quantum systems realistically. Feynman proposed that we use quantum concepts to develop a different kind of computer.

2. David Deutsch came up with the quantum computer's theoretical model, essentially creating the basic design of how it could function.

3. Peter Shor created an algorithm demonstrating that quantum computers can factor large numbers, and thus specific math problems, faster than any existing computer.

4. Lov Grover developed a quantum algorithm for searching an unsorted database much more quickly than classical approaches.

**Top Research Institutes**

1. MIT is just one of several locations at which researchers are building quantum computers, employing materials that are superconducting and creating instructions (algorithms) for quantum computers.

2. University of Oxford is where scientists like David Deutsch and Artur Ekert first came up with some of quantum computing's initial concepts, as well as those of secure communication (cryptography) and quantum key distribution.

3. The University of Waterloo's Institute for Quantum Computing (IQC) is known worldwide for its cutting-edge research into quantum information processing and for creating building blocks for quantum computers.

4. The University of Innsbruck is said to have carried out world-first experiments with quantum computers realized with trapped ions and facilitated elementary operations (quantum gate) carried out by the computers.

**Tech giants leading the Quantum Computing revolution**

1. IBM first made quantum computers available with IBM Quantum Experience through the cloud. They have also been investing efforts into harnessing superconducting qubits for hardware development.

2. Google achieved a major milestone as it achieved "quantum supremacy" with its Sycamore processor. It refers to solving a problem faster with a quantum processor than with the world's most advanced classical supercomputers.

3. It's also examining a different type of qubit, known as topological qubits, and it created a programming language, Q#, to encourage programmers to code quantum computers.

4. Rigetti Computing provides quantum computing via the internet and is dedicated to bringing quantum and classical forms of computing together to make quantum computers applicable to actual issues.

**6. Answer**

**Journey of Quantum Computing**

|  |  |  |  |
| --- | --- | --- | --- |
| Year | Contributors | Milestone | Details |
| 1981 | Richard Feynman | Feynman suggests quantum simulation | The Use of Quantum Systems to simulate Quantum Physics Problems is suggested by Richard Feynman at MIT. |
| 1985 | David Deutsch | Quantum Turing Machine | A formalized model of the universal quantum computer is introduced by David of Oxford University. |
| 1994 | Peter Shor | Shor’s Algorithm | Peter-Shor develops a polynomial time quantum algorithm for integer factoring displaying practical capability. |
| 1996 | Lov Grover | Grover’s Algorithm | Using Quantum Physics, Lov Grover creates a method for a faster database search |
| 1998 | IBM & Stanford | 1st 2-Qubit Quantum Computer | 1st practical implementation of quantum gates is a 2-Qubit NMR based quantum computer created by IBM & Stanford. |
| 2001 | IBM & Stanford | Shor’s-Algorithm Demonstrated | A 7-qubit NMR quantum computer was used to successfully complete factor 15. |
| 2007 | D-Wave | D-Wave announces 1st Quantum Computer | D-Wave claims the first commercial quantum computer ‘D-Wave One’ using quantum annealing. |
| 2011 | IBM | IBM launches Quantum Research Initiative | IBM starts open research to create superconducting quantum hardware. |
| 2014 | Microsoft | Microsoft develops Q# language | Q# programming language is developed for quantum simulation and computing applications under Station Q project. |
| 2016 | IBM | IBM Quantum Experience | World’s 1st 5-Qubit Quantum Computer released by IBM. |
| 2017 | Rigetti | Launch of Cloud Quantum Platform | Release of an open access hybrid quantum classical programming platform named ‘Forest’ by Rigetti. |
| 2019 | Google | Achieves Quantum Supremacy | Google’s Sycamore processor computes a random sampling task in ~200 seconds. |
| 2020 | USTC China | Achieved Photon Quantum Advantage | USTC exhibits Quantum Supremacy by using Photonic Quantum Computing. |
| 2021 | IBM | IBM Eagle | IBM introduces Eagle most powerful 127-qubit processor. |
| 2022 | Honeywell | Quantinuum and error correction | Honeywell takes crucial step towards quantum error correction. |
| 2023 | IBM | IBM Osprey | Introduction of IBM Osprey 433-qubit processor. |
| 2024 | IBM | IBM Condor | Introduction of IBM Condor 1,121-qubit processor. |