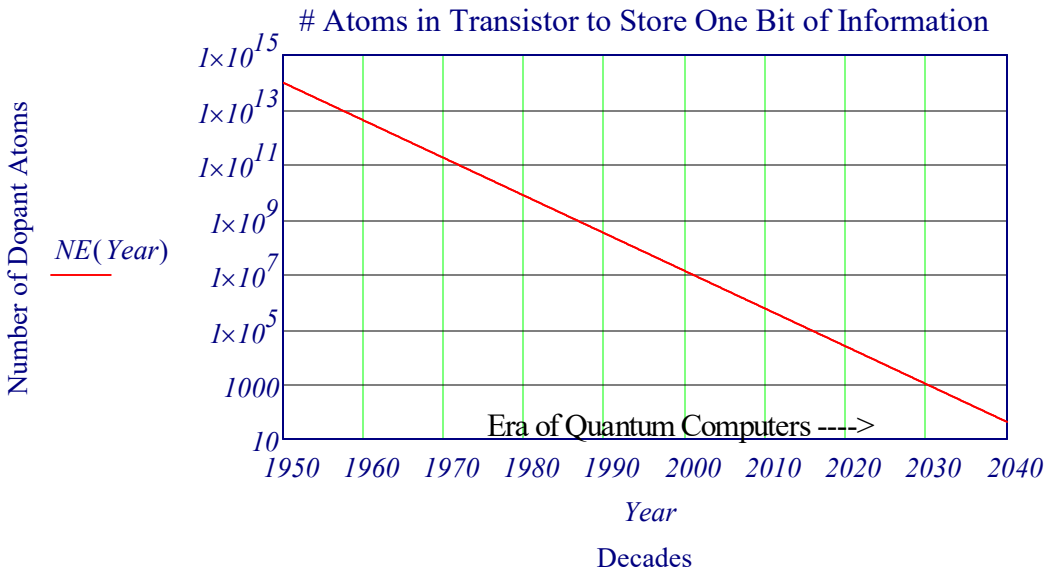
I. Introduction

With the development of science and technology, leading to the advancement of civilization, new ways were discovered exploiting various physical resources such as materials, forces and energies. The history of computer development represents the culmination of years of technological advancements beginning with the early ideas of Charles Babbage and eventual creation of the first computer by German engineer Konard Zeise in 1941.

The number of atoms needed to represent a bit of memory has been decreasing exponentially since 1950. An observation by Gordon Moore in 1965 laid the foundations for what came to be known as "Moore's Law" – that computer processing power doubles every eighteen months. If Moore's Law is extrapolated naively to the future, it is learnt that sooner or later, each bit of information should be encoded by a physical system of subatomic size. The plot below shows the number of electrons required to store a single bit of information. An extrapolation of the plot suggests that we might be within the reach of atomic scale computations with in a decade or so at the atomic scale however. This is the point at which Moore's Law for a transistor (not the architecture of the integrated circuit system) and the **exponential growth** of classical computers comes to an end.

Decrease in the Number of Electrons Needed Per Bit Versus Years (TWK Estimate)

$$NE(Y) := 10^{\left(14-11\cdot\frac{Y-1950}{80}\right)}$$



Dimensions of 3 nm Node Transistor: 4nm x 42 nm x 5nm

Volume of Transistor, V_{xtr}

$$V_{xtr} := 4nm\cdot 42nm\cdot 5nm$$

Density of Silicon atoms per m^3:

$$\rho_{Si} := 5\cdot 10^{28}\cdot\frac{1}{m^3}$$

$$NumAtoms := V_{xtr}\cdot\rho_{Si}$$

$$NumAtoms = 42000$$

How does Quantum Computing Work? An interview with Peter Shor, discoverer of the *Shor Algorithm*.

Peter Shor: "The key to factoring is identifying prime numbers, which are whole numbers divisible only by one and by themselves. (Five is prime. Six, which is divisible by two and by three, is not.) There are twenty-five prime numbers between one and a hundred, but as you count higher they become increasingly rare." Shor, drawing a series of compact formulas on the chalkboard, explained that certain sequences of numbers repeat periodically along the number line. The distances between these repetitions grow exponentially, however, making them difficult to calculate with a conventional computer.

"O.K., here is the heart of my discovery," he said. "Do you know what a diffraction grating is?" I confessed that I did not, and Shor's eyes grew wide with concern. He began drawing a simple sketch of a light beam hitting a filter and then diffracting into the colors of the rainbow, which he illustrated with colored chalk. "Each color of light has a wavelength," Shor said. "We're doing something similar. This thing is really a computational diffraction grating, so we're sorting out the different periods." Each color on the chalkboard represented a different grouping of numbers. A classical computer, looking at these groupings, would have to analyze them one at a time. *A quantum computer could process the whole rainbow at once*."

What is a Quantum Computer (QC)?

Qubit: A qubit is a **two-dimensional system** that is in a state of 0 or 1 or both. Just as a classical bit has a state – either 0 or 1, a qubit also has a state. Two possible states for a qubit are the states |0> and |1> , which as you might guess correspond to the states 0 and 1 for a classical bit. Notation like ' |> ' is called the *Dirac notation.*

Quantum Computing: A type of computation whose operations can harness the phenomena of quantum mechanics, such as superposition, interference, entanglement, and teleportation. Devices that perform quantum computations are known as quantum computers. Operations are done by gates. **All Operators in QC are reversible.**

The qubit is represented by the superposition of the two spin basis vectors in Hilbert space given by: A linear combination of the two gives what is called the single qubit state $|\Psi = \alpha\,|1\rangle + \beta\,|0\rangle$, where α and β are the probability amplitudes and give the probability that an observation of the spin will result in |1> or a |0> state respectively

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

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

We can model a qubit computationally: **where |0> and |1> are basis vectors**

$|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ where $\alpha^2 + \beta^2 = 1$, α and β are complex numbers.

If a qubit gets measured, it will return a classical bit value of 0 with probability of α^2 or a bit value of 1 with probability β^2.

Potential Applications: Cyber Security, Factorization, Breaking Codes (RSA), Simulate Quantum Phenomena. Rapid Prototyping and Testing of Chemical Reactions, Electronic and Material Properties, Molecular Folding, Calculating Fourier Transforms, Finding Solutions to a system of nonlinear equations, e.g. the Quantum Navier-Stokes Algorithm.

QC Key Concepts: Quantum Behavior, Superposition, Entanglement, Interference, Teleportation, "Oracle" Algorithms, Computational Complexity/Scaling, Born Rule, Reversibility, and of the Physics of states in a quantum system.

Computational Complexity: Computational complexity studies the amount of time and space required to solve a computational problem. Another measure is the number of gates & depth of circuit. Another important computational resource is energy. Energy consumption in computation turns out to be deeply linked to the reversibility of computation.

Reversibility: Consider a gate like the NAND gate, which takes as input two bits, and produces a single bit as output. This gate is intrinsically *irreversible* because, **given the output of the gate, the input is not uniquely determined**. The gate is an example of a reversible logic gate because, given the output of the gate, it is possible to infer what the input must have been. NAND Gate: A Boolean operator which gives the value zero if and only if all the operands have a value of one, and otherwise has a value of one (equivalent to NOT AND).

Erasure: Another way of understanding irreversibility is to think of it in terms of information erasure. If a logic gate is irreversible, then some of the information input to the gate is lost irretrievably when the gate operates – that is, some of the information has been erased by the gate. A computation is reversible if no information is erased during computation. Landauer's principle states that, in order to erase information, it is necessary to dissipate energy. A minimum of kBT ln2.

Entanglement is a different way of encoding information. If we have two particles that are entangled, the information about them is **not encoded locally in each particle**, but rather in correlation of the two. This is the Principle of Non Locality.

Algorithms: Shor's (Factorization), Deutsch–Jozsa., Grover's (Search), Bernstein–Vazirani, Quantum phase estimation.

Measurements: Every measurable physical quantity, o, is described by a corresponding Hermitian operator, O, acting on the state ψ. The eigenvalues of Hermetian operators are always real. Example: $H_{op}\psi = E\psi$ gives the Eigenvalue of Energy for state ψ. For every classically defined Function $F(x,p) \exists F_{op} = F(x, \hbar/i\ d/dx$

The Poisson Bracket Formulation for the momentum operator: $\dot{p}_k = \{p_k, H\}$