Quantum computing basics

P.B. Vijay Kumar

August 4, 2023

1 Small story about Quantum Computing

These days for storing data we are using electronic chips for the easy retrieval and addition of data. For example if we look inside a 2GB pendrive, we can find LEDs, integrated circuits etc., and if we calculate how much memory it can store in bits, it would be roughly

$$1\text{GB} = 8 \times 10^9\text{Bits}$$
$$2\text{GB} = 16 \times 10^9\text{Bits}$$

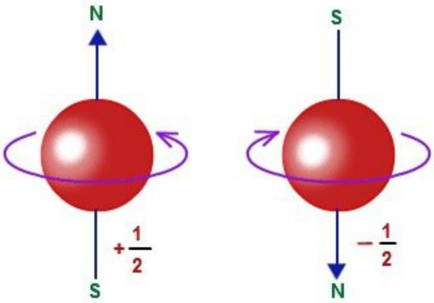
And if we take a pendrive and calculate how many atoms are there inside,can we guess atleast? No right !

So in today modern world we can store 1 Bit of information in one atom, that doesn't mean that we really storing the data in one atom. Infact an atom is used to represent 1 bit of information.

2 Classical Bit

Classical Bits are physical entities that can be implemented using various technologies like ICs where the voltage levels correspond to the logical values of 0 and 1. Typically 10^{10} atoms are used to store 1 bit of information.

Imagine an $e^{(-)}$ (electron), which is a fundamental particle with spin 1/2. The spin of an electron can be either "up" or "down", and these two states can form the basis of the **Qubit**.



We can now associate the "up" state with binary value "0" and "down" state with binary value "1".

3 Shor's Algorithm

Shor's algorithm was discovered by Peter Shor (1959), he was from MIT, and is very famous for his work in the field of "Quantum Computing", for discovering shor's algorithm that has potential to factorize numbers exponentially faster than existing algorithms !

Any number has a unique decomposition into a product of 'primes', and finding prime factors is believed to be a very hard problem.

In fact, security of our online transactions rests on assumption of factoring integers with a 1000 or more digits, which is practically impossible.

here comes the Shor's algo

4 THE ALGORITHM

1. Pick $'a'$ which is a coprime of N, where $N = p \times q$, such that GCD$(a, N) = 1$, where $'p'$ and $'q'$ are the primes we need to find. If unsure, check whether it is a coprime immediately.
2. Find Period or Order $'r'$ of the function $a^r(modN)$ and select the smallest $'r'$ such that $(a^r) = 1(modN)$.
3. If $'r'$ is even, $x = a^r/2(modN)$.
4. if $(x + 1)$ not equals $0(modN)$ then
5. $p, q = GCD(X + 1, N), GCD(X - 1, N)$
6. else find another $'a'$

But the above algorithm is just a classical algorithm which just shows the mathematical explanation. But the finding of order in real requires a Quantum computer where we use "Quantum Fourier Transform" which really sounds very complicated but in fact the math is simple if demystified properly !