UT AUSTIN PORTUGAL 2019 ANNUAL CONFERENCE

MASTERCLASS I
QUANTUM COMPUTING: PRINCIPLES, ALGORITHMS AND APPLICATIONS

Lecture 1: “Grover’s algorithm: an example of the use of quantum superposition and interference principles”

Mikhail Vasilevskiy (UMinho & INL)

One of the main ideas behind Quantum Computing is the superposition principle that states the possibility of a quantum bit (qubit) be in a linear combination of base state, with arbitrary complex coefficients which only must obey the normalization condition. In principle, it means that such a qubit can contain an infinite amount of information.

However, a single measurement made on a qubit returns only one bit of “classical” information, so the use of this potentially huge benefit can only be indirect and requires intelligent algorithms. One such algorithm was proposed by L. Grover in 1996. This algorithm permits a faster search through an unstructured database by using the superposition principle and the phenomenon of quantum interference. An example is the search of a person in an alphabetically ordered telephone book by his or her phone number.

Mathematically, it corresponds to a binary function which is equal to 1 for a single value of the argument which can be interpreted as a label (phone number in the above example) of the desired state (person’s name). One needs to design a device that compares the labels (an “oracle”) and a set of n qubits, which can be used to store 2n different vectors.

By preparing this set of qubits in an appropriate superposition state of all possible vectors one can “write” the whole database at once but the problem is to extract the desired vector. Here the quantum interference comes to help and one can gradually increase the amplitude of the state of interest in the superposition by repeatedly applying a certain unitary operator together with the oracle. Grover’s algorithm provides a quadratic speed up in the number of attempts necessary in a straightforward “classical” search.