

Quantum Computation: A Review

By

Nidhi Jain¹, Dr. Mahesh Kumar Porwal²

¹M. Tech. Student, ² Professor

Department of Electronics and Communication Engineering
Shrinathji Institute of Technology & Engineering, Nathdwara (Rajasthan)
nidhijain745@gmail.com, porwal5@yahoo.com

Abstract - In the classical model, the fundamental building block is represented by bits exists in two states a 0 or a 1. Computations are done by logic gates on the bits to produce other bits. By increasing the number of bits, the complexity of problem and the time of computation increases. A quantum algorithm is a sequence of operations on a register to transform it into a state which when measured yields the desired result. This paper provides introduction to quantum computation by developing qubit, quantum gate and quantum circuits.

I. Introduction

In classical computing there are a number of problems that cannot be solved with efficient algorithms. For example, the best classical algorithm for factorization a large integer N increases exponentially with the size of the integer. In searching problem, the best classical algorithm increases directly as the size of the database. Quantum computation is a new computational model that utilizes the principle of quantum physics. It solves the problems more efficiently in comparison with classical

computation and solves that problems also which cannot be solved by classical computation.

Qubit is the fundamental unit in quantum computing. It is similar to a bit, either valued 0 or 1. A qubit can exist in any superposition of the 0 or 1 state simultaneously. When a qubit in such state is measured the superposition will be destroyed. A quantum algorithm consists of sequence operations on a register to transform it into a state which when measured yields the desired result with high probability. An n -bit quantum register can store an exponential amount of information. The register as a whole can be in an arbitrary superposition of the 2^n base states which it can be measured to be in while this superposition. When a qubit is in this state, it can be thought of as existing in two universes: as a 0 in one universe and as a 1 in the other. An operation on such a qubit effectively acts on both values at the same time. The significant point being that by performing the single operation on the qubit, we have performed the operation on two different values.

A quantum computer would consist of many qubit gates with entangled states. These gates could be addressed in parallel by unitary transformations, which must be carried out reversibly, implying no loss of energy in a gate operation. Quantum computers are “wired” so that they can do many calculations at the same time. This is known as “quantum parallelism” and represents the power of a quantum computer.

Several systems have been proposed for quantum computing including photons in nonlinear optical systems, trapped ions, electron and nuclear spins, quantum dots, and Josephson junctions. There are advantages and disadvantages to all these approaches. Some, such as those employing light or trapped ions, have demonstrated that they can provide individual qubits of excellent quality. But, it is not yet known if they can be scaled up to produce systems with many qubits and many possible quantum gate operations. There is nothing a quantum computer can do that cannot also be done by an ordinary computer. However, for some problems, a quantum computer may be many orders of magnitude faster. There are presently two important problems involving commerce and security for which a quantum computer is believed to be superior. These are finding the factors of a large number and searching an unstructured database.

The spectacular promise of quantum computers is to enable new algorithms which render feasible

problems requiring exorbitant resources for their solution on a classical computer. At the time of writing, two broad classes of quantum algorithms are known which fulfill this promise. The first class of algorithms is based upon Shor’s quantum Fourier transform, and includes remarkable algorithms for solving the factoring and discrete logarithm problems, providing a striking exponential speedup over the best known classical algorithms. The second class of algorithms is based upon Grover’s algorithm for performing quantum searching. These provide a less striking but still remarkable quadratic speedup over the best possible classical algorithms. The quantum searching algorithm derives its importance from the widespread use of search-based techniques in classical algorithms, which in many instances allows a straightforward adaptation of the classical algorithm to give a faster quantum algorithm.

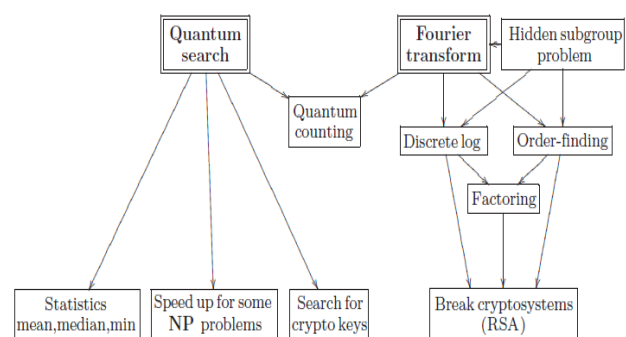


Fig. 1 The main quantum algorithms and their relationships, including some notable applications.

Figure 1 sketches the state of knowledge about quantum algorithms at the time of writing,

including some sample applications of those algorithms. Naturally, at the core of the diagram are the quantum Fourier transform and the quantum searching algorithm. Of particular interest in the figure is the quantum counting algorithm. This algorithm is a clever combination of the quantum searching and Fourier transform algorithms, which can be used to estimate the number of solutions to a search problem more quickly than is possible on a classical computer.

II. Quantum Computation model

In the quantum circuit model, we have logical qubits carried along ‘wires’, and quantum gates that act on the qubits. A quantum gate acting on n qubits has the input qubits carried to it by n wires, and n other wires carry the output qubits away from the gate. A quantum circuit is often illustrated schematically by a circuit diagram. The wires are shown as horizontal lines, and we imagine the qubits propagating along the wires from left to right in time. The gates are shown as rectangular blocks. For example, the 4-qubit state $|\psi_i\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle$ enters the circuit at the left. These qubits are processed by the gates U_1 , U_2 , U_3 , and U_4 . At the output of the circuit we have the collective (possibly entangled) 4-qubit state $|\psi_f\rangle$. A measurement is then made of the resulting state. The measurement will often be a simple qubit-by-qubit measurement in the computational basis, but in some cases may be a more general measurement of the joint state. A

measurement of a single qubit in the computational basis is denoted on a circuit diagram by a small triangle.

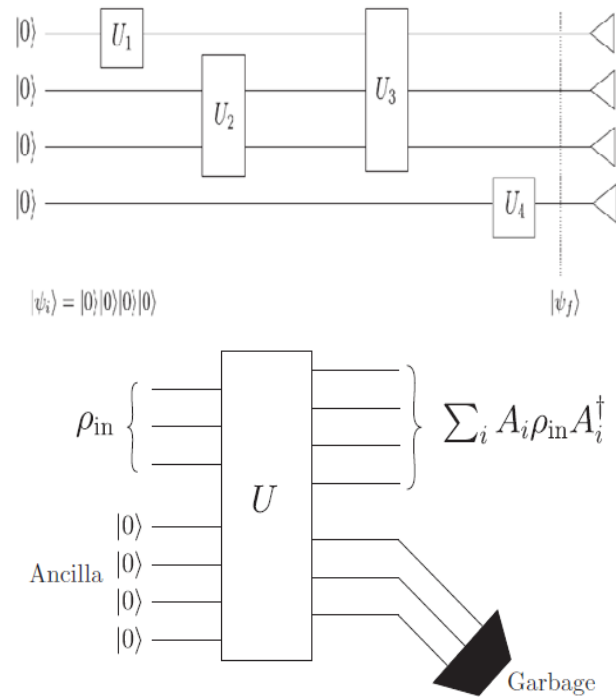


Fig. 2 quantum circuit

Fig. 3 A general quantum operation or super operator can be realized using a unitary operation by adding an ancillary and tracing out part of the output.

The triangle symbol will be modified for cases, in which there is a need to indicate different types of measurements. The measurement postulate stated that a measurement outputs a classical label ‘ i ’ indicating the outcome of the measurement and a quantum state $|\phi_i\rangle$. Thus, we could in general draw our measurement symbol with a ‘quantum’ wire carrying the quantum state resulting from

the measurement, together with a classical wire carrying the classical label.

III. Existing work in Quantum Computation

Quantum Computation can be used to extract statistics, such as the minimal element, from an unordered data set, more quickly than is possible on a classical computer. It can be used to speed up algorithms for some problems in NP – specifically, those problems for which a straightforward search for a solution is the best algorithm known. Finally, it can be used to speed up the search for keys to cryptosystems such as the widely used Data Encryption Standard (DES). In the early 1980's, physicist Richard Feynman observed that no classical computer could simulate quantum mechanical systems without incurring exponential slowdown. At the same time, it seems reasonable that a computer which behaves in a manner consistent with quantum mechanics could, in principle, simulate such systems without exponential slowdown.

For many years the study of quantum computing was primarily an academic curiosity. Shor (1994) developed a polynomial time algorithm for factoring large integers. According to Williams and Clearwater (1998), it is not known if there is a classical algorithm for factoring large integers efficiently, but the best algorithms published thus far are super-polynomial. This algorithm coupled with the prominence of cryptographic systems

based on factoring large integers fueled study of quantum computation, both from an algorithmic and a manufacturing point of view. Grover (1996) provided an $O(\sqrt{n})$ time algorithm for finding a single marked element in an unsorted database of n elements. The best possible classical algorithm would run in $O(n)$ time. This search problem was not the first problem for which a quantum computer was shown to be better than any possible classical computer, but it was the first problem of real utility found where a quantum computer outperforms a classical computer in an asymptotic sense.

While Shor's algorithm may be of more immediate utility, Grover's algorithm seems more interesting in a theoretical sense, as it highlights an area of fundamental superiority in quantum computation.

IV. References

- [1]. Michael A. Nielsen & Isaac L. Chuang, *Quantum Computation and Quantum information*, 10th anniversary edition, Cambridge University press.
- [2]. Phillip Kaye, Raymond Laflamme, Michele Mosca, *An Introduction to Quantum Computing*, Oxford University Press
- [3]. Quantum computation and grover's algorithm, aaron krahn