Quantum Computation

Antoine Groudiev

Last edited November 15, 2023

One of the most widely used system for secure data transmission is the RSA scheme; its security relies on the assumption that the integer factorization problem is hard. To this day, there is indeed no known efficient algorithm to factor an integer *on a classical computer*.

Nevertheless, this problem can be solved in polynomial time on a quantum computer, using Shor's algorithm. A large enough quantum computer would therefore be able to break the RSA encryption scheme.

We will define the behavior of a quantum computer using two quantum computational models, and delve into quantum complexity theory, the study of complexity classes of problems solved using these quantum models. We will end by describing Shor's algorithm, to understand the gain of a quantum-based model for computing.

Contents

Introduction to Quantum Computers

A classical computer uses the *bit* as a basic unit, a system which can be in exactly one of the two states `0` and `1`. Similarly, a quantum computer uses a basic unit called *qubit*, which can be in a *superposition* of two states. A qubit can be described as a linear combinaison of both states, each coefficient being related to the probability that the qubit is in the given state. This way, a qubit can store more information than a simple bit, by storing information for both states at a time.

1 Quantum Computational Models

To study the complexity of different problems with a quantum point of view, we need a model for a quantum computer. Much like classical computers, two approaches exists: the representation of a quantum computer as a circuit, using quantum logic gates, and an abstract model called quantum Turing machine, by analogy with the classical Turing machine.

1.1 Quantum Logic Gates

A quantum gate takes into input n qubits, and intuitively modifies the probability of each qubit to be in each state. More precisely, it changes the position of the qubit on the surface of the Bloch sphere. Therefore, quantum gates are often represented as unitary matrices of size $2^n \times 2^n$, i.e. elements of $U(2^n, \mathbb{C})$. We will present basic quantum gates.

1.2 Quantum Turing Machine

Another approach to model a quantum computer is to describe it as a generalized Turing machine. The set of states is replaced by a Hilbert space, and the transition function is replaced by a set of unitary matrices, similarly to the logic gates representation.

2 Quantum Complexity Theory

2.1 Relationship between classical and quantum complexity classes

2.1.1 Simulating a quantum computer

2.1.2 Efficiently simulating a classical computer

2.2 The BQP class

2.3 Query complexity

3 An example of Quantum Algorithm: Shor's Algorithm

3.1 Motivation and overview

3.2 Classical part

3.3 Quantum part

3.3.1 Quantum Fourier Transform

Conclusion