Introduction to Quantum Computing

by

Jens Hee
http://jenshee.dk

February 2020

Change log

6. February 2020

1. Document started.

Contents

Chapter 1

Background

The interest in quantum computing started in the 1970's, where it was suggested that quantum states could be used as an alternative to classical bits in order to construct a computer being more efficient than a classical computer solving certain problems . It was shown in the 1990's that this was possible although the physical implementation was not available. Several algorithms of this kind has been developed, but it still remains to build a quantum computer having control over the quantum states. One may say that the software for quantum computers are ready, but the hardware is not. This paper is mainly about the logical part of the quantum computer, but the last chapter gives some insight into the physical implementation.
In classical computers the central elements are the physical gates with low and high voltage inputs and outputs. The gates and the inputs and outputs can be mapped into an abstract description whereby the physical implementation (the hardware) is separated from the abstraction (the software). The inputs and outputs to the gates are mapped into logical states (the bits) being "0" or "1" and the physical gates are mapped into logical gates (boolean algebra).
A similar separation is possible talking about quantum computers, but due to the different nature of physical implementation the abstract description is also somewhat different. The logical states are called qubits and the logical gates are called quantum gates. This is covered by the next chapter.

Chapter 2

States and gates

2.1 States

An abstract state is called a qubit. It is a superposition of the two states called $|0\rangle$ and $|1\rangle$.

$$\langle\Psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \qquad |a|^2 + |b|^2 = 1$$

Where $|a|^2$ and $|b|^2$ are the probabilities of finding the qubit (the superposition) in state $|0\rangle$ and $|1\rangle$. Finding, means here measure the state. When a quantum gate is acting on a qubit (see below), the qubit is not measured, the gate acts on the superposition. The quebits are only measured when a result is required. The a and b are in general complex numbers. When having two qubits the superposition becomes:

$$\langle\Psi\rangle = (a\,|0\rangle + b\,|1\rangle)(c\,|0\rangle + d\,|1\rangle) = a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|10\rangle + a_{11}\,|11\rangle$$

Similar when more qubits are considered.

2.2 Gates

An abstract gate is called a quantum gate. It is a unitary matrix H with an output superposition given by:

$$|\Psi_2\rangle = H\,|\Psi_1\rangle$$

For a single quantum gate this should be interpreted as:

$$|\Psi_1\rangle = a_1\,|0\rangle + b_1\,|1\rangle$$

$$|\Psi_2\rangle = a_2\,|0\rangle + b_2\,|1\rangle$$

where:

$$\begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} h_{00} & h_{01} \\ h_{10} & h_{11} \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$$

Similar for a multi quantum gate with two qubit inputs:

$$|\Psi_1\rangle = a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|10\rangle + a_{11}\,|11\rangle$$

$$|\Psi_2\rangle = b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$$

where:

$$\begin{pmatrix} b_{00} \\ b_{01} \\ b_{10} \\ b_{11} \end{pmatrix} = \begin{pmatrix} h_{00} & h_{01} & h_{02} & h_{03} \\ h_{10} & h_{11} & h_{12} & h_{13} \\ h_{20} & h_{21} & h_{22} & h_{23} \\ h_{30} & h_{31} & h_{32} & h_{33} \end{pmatrix} \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$$

A unitary matrix is a quadratic matrix and has the property $H^*H^T = I$, where I is an identity matrix. Since the matrix is quadratic, a quantum gate always has the same number of inputs and outputs. Later the reason for the matrix being unitary is given.

2.2.1 Single quantum gates

A single quantum gate has a single qubit as input. Some important gates are:

The NOT gate

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The Z gate

$$H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

2.2.2 Multi quantum gates

The CNOT gate

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

It can be shown that any multi quantum can be made from a set of single quantum gates and CNOT gates.

The Toffoli gate

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

A Toffoli gate can be made form single quantum gates and CNOT gates as follows see Nielsen p 183

Chapter 3

Comparison with classical bits and gates

3.1 Toffoli gate

A Toffoli gate can be used to make a NAND gate by setting the lower input to $|1\rangle$ and since a similar Toffoli gate can be made in a classical circuit, a quantum computer can simulate any clasical computer. Since all clasical circuits can be made from NABD gates alone.

3.2 Entanglement

It is important to notice that the CNOT gate requires the physical implementation to implement entanglement since Hadamard followed by CNOT gives bell states. Entanglement means for example that the two physical quantum states are the same such that if one is measured to be 1 so is the other and vice versa.

3.3 Parallelism

Several algorithms exists taht can be parallel and super fast examples start with a simple one quantum chryptation

Chapter 4

Hardware

some examples

Bibliography

[1]