Quantum Facts

Miguel Sozinho Ramalho

November, 2018

Table of contents

Introduction

This is an atypical week. Firstly, because it touches on various topics. Secondly, because these topics are *typically* mentioned earlier when learning about quantum, but the author believes it ought to be easier to understand them at this point, some are also prerequisites for the upcoming content.
So, some more considerations will be made on **Quantum Circuits**, namely universal gates, a new example of the consequences of unitary operators.
Entanglement will be explained, at last.
Finally, introductory notes on **Big O notation**.
Thus: Quantum Facts!

Classical Universal Gates

In Classical Computing, any calculation is achievable through some simple sets of gates, for instance the set {AND, NOT} allows to derive any other operator. Moreover, there are singleton sets that also permit this, such as the {NAND} set (as a classical exercise you can try to simulate an OR using only NANDs).

Quantum Universal Gates

After Quantum Computing was initially thought of, and with the development of quantum gates, such simple sets were also procured. And they exist! Although they require some more complex considerations. We will not be proving this, as it is too theoretic and there are plenty of good explanations for it online, yet we will take a glimpse at what gates we would need.

Quantum Universal Gates

Firstly, it is **not** possible to do so using only single qubit operators (some we already know, others are here for completeness purposes):

$$T = \begin{bmatrix} 1 & 0 \\ 0 & \epsilon^{i\pi/4} \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

*Given: $\epsilon^{ix} = \cos(x) + i\sin(x)$

The first way of achieving the Universal Gate set is to take these single qubit gates and including the **CNOT** gate!

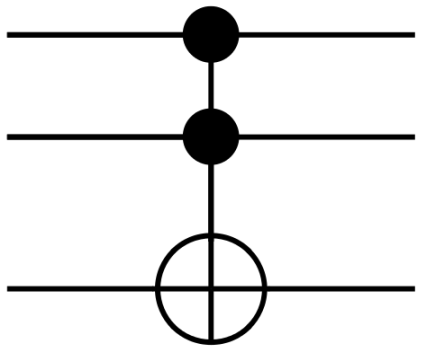
Quantum Universal Gates

The **Toffoli** (CCNOT) gate is one of the most eloquent gates that can perform any **Boolean** operation (universal for Boolean reversible computation). However, alone it is **not enough** for quantum universality. But, if we add to it the ability to **generate superposition**, with the **Hadamard** gate, they form a set of size two that is capable of quantum universal computation $\{Toffoli, H\}$. (There is another such pair $\{U_{qubit}, \sqrt{SWAP}\}$ which are gates you can research on your own).

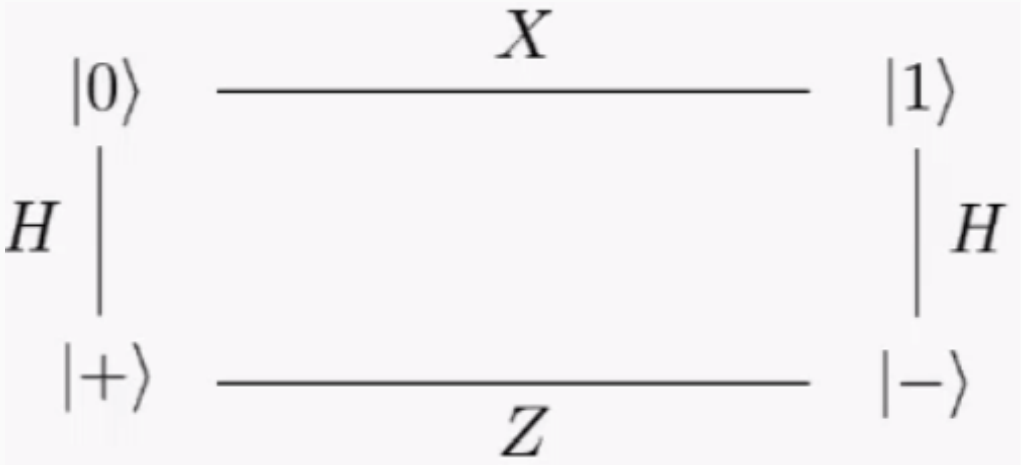
Quantum Universal Gates

The Toffoli gate transformation maps 3 qubits and is therefore of size $2^3 = 8$. It is essentially an identity matrix, except for the intersection of the last two columns and two lines, which matches the X gate: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (Can you understand why?)

This is the Toffoli gate in, you may notice some similarity with the CNOT gate, recall that this is also called CCNOT. The black circles actually represent both the control bits.



Gates and Basis



The above diagram is a useful shorthand for quantum states conversion using quantum gates, and it also depicts the consequences of reversible computation. Literally, you can have a qubit in any of the four states $|0\rangle, |1\rangle, |-\rangle |+\rangle$ and obtain any other from it by performing simple one qubit gates.

Exercise: Start with $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and obtain each of the other states by chaining the respective operations on this cycle.

Entanglement

Entanglement is a curious phenomenon on a quantum level. It describes the state of a system in which the quantum state of two or more particles cannot be considered independently from each other. There is a correlation between their quantum properties. Pragmatically, if two qubits are entangled then measuring one will produce the measurement on the other to be the same, when the experiment is repeated many times, they are entangled.
This property holds over long distances despite the uncertainty over the question we begin to be accustomed to: **Why?**

Entanglement possibilities

This property carries both potential and controversy, as even Albert Einstein contested its possibility. Its existence is, however, unquestionable. We will not get into the paradoxical views and debate over different interpretations for it.

We will make use of it, and we actually already have, with the CNOT gate! Think about it: The state of a qubit **controls** the flipping of the other. In classical computing that would mean they are dependant, but in quantum terms they are entangled, **not just dependant**, because if we apply this gate to qubits in superposition, we get a non-deterministic result that is deterministically correlated.
This week's exercises will help understand entanglement.

Big O notation

Lastly, on this factual menu, there comes a topic that most computer scientists already know, if this is your case, do not skip this slides, as some new concepts are introduced.

Big O notation is used to describe the limiting behaviour of an algorithm (worst-case scenarios), essentially giving an estimate of the complexity (which reflects how the execution time evolves with the size of the input).

Big O notation

The notation is as follows: $O(COMPLEXITY)$.

- Assume you have a classical loop over an array of size N. The complexity of this algorithm in the Big O notation, would be $O(N)$.
- If you were to compute the square values of each cell in an $N \times N$ matrix, its complexity would be $O(N^2)$
- A typical binary search has a complexity of $O(log_2(N))$

Big O notation

Computational problems are described by the most efficient algorithm that can solve them.
P (polynomial) problems are classified as *easy/efficiently solvable/tractable*, since the amount of time it takes to solve increasingly larger instances evolves polynomially.
NP (nondeterministic polynomial time) problems, on the other hand, are not considered *efficiently solvable*. This means that as the size of the problem instances increases linearly, the time (sometimes space) required grows exponentially. Nondeterministic implies not solvable on a deterministic Turing Machine.

Big O notation - Quantum impact

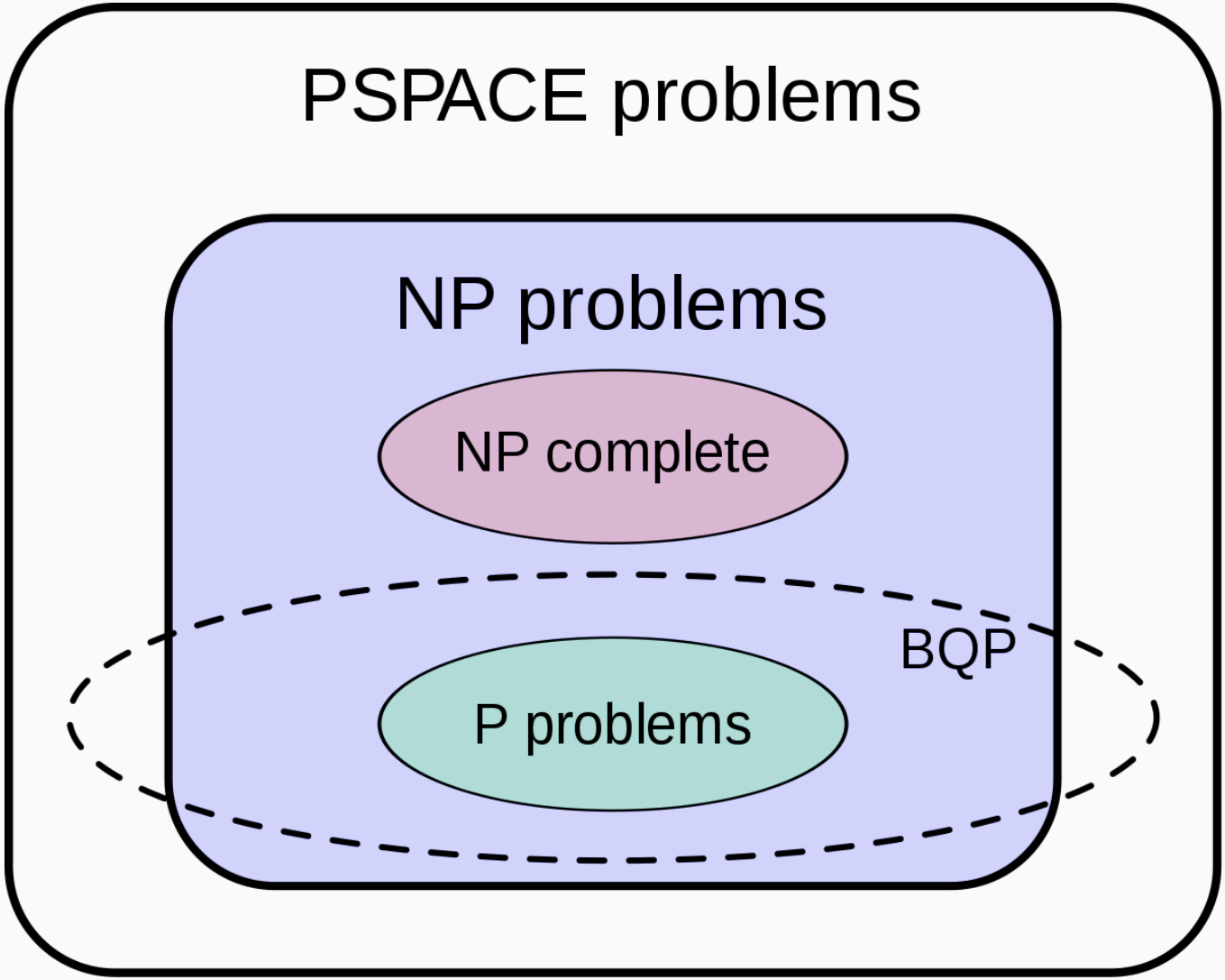
BQP

When we enter the Quantum World, and according to some advances we will study over this course, a new class of problems has emerged: **BQP**- bounded-error quantum polynomial time. This is a class of problems that is solvable in polynomial time in a **quantum computer** (with an error probability $\leq \frac{1}{3}$).

NP vs BQP

The problem with this class is that it reflects the power of quantum computing, as some classical problems that belong to the **NP** class can be solved in **BQP**. What is unclear is how far can quantum computers go, is **BQP** a subset of **NP** or the other way around? do they match? Answering such questions would put a definite stamp on the power of Quantum Computing when compared with Classical Computing.

Big O notation - Quantum impact



Exercises

When you are ready, you can head over to the exercises, where the aforementioned concepts will be revised and where you will also learn some new concepts, such as **bell state**. Once you have finished, the solutions contain detailed detailed explanation of what you should understand about the code you are developing!

Where to learn more?

- The original Einstein–Podolsky–Rosen (EPR) paper
- Medium article: Einstein and entanglement
- Common computational complexities with examples
- P=NP? major unsolved mathematical problem