# "Quantum algorithms and Foundations: A general introduction"

Carlos Tavares

High-Assurance Software Laboratory/INESC TEC

*ctavares@inesctec.pt*

January 27, 2016

# Overview

1. Quantum Physics

2. Quantum Computation

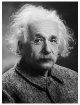
3. Algorithmics

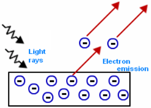
# Quantum Theory

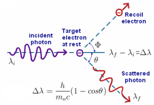
# Old Quantum Theory

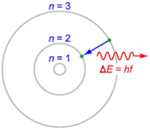
- In the beggining, there were only a set of radical ideas to solve several issues in classical physics
- Black-body radiation, Compton and Photoelectric effects, Atomic structure

$$u(\nu,T) = \frac{8\pi\hbar}{c^3}\frac{\nu^3}{e^{\hbar\nu/kT}-1}$$









- It was then necessary to unify these ideas into coherent foundations and thus was born quantum mechanics.

# Wave Mechanics - Erwin Shrödinger

- Erwin Shrödinger formulated quantum physics as waves

$$\psi(x,t) = Ae^{i(kx-wt)} + Be^{-i(kx-wt)}; k = p/\hbar; \omega = E/\hbar \qquad (1)$$

- He also managed to derive an important equation: the Shrödinger's equation

$$i\hbar\frac{\partial\psi(x,t)}{\partial t} = -\frac{\hbar}{2m}\frac{\partial^2\psi(x,t)}{\partial x^2} \qquad (2)$$

  which, can also be rewritten in the Operator form: $H\psi(x,t) = E\psi(x,t)$, where $H$ is the Hamiltonian operator

- It is a higher-order differential equation, with several possible solutions, which constitute the eigenfunctions of the equation. This has important implications in the theory!

# Quantum mechanics

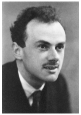
- What means the a "wave equation"?
  - Born interpretation - The wave gives the probability of a certain value of an observable to happen;
  - Possible values of an observable are given by the eigenvalues given by the observable equations, e.g. see the Hamiltonian case
  - Born rule - probability of a certain event to happen $= |\langle\psi|\psi\rangle|^2$
- Werner Heisenberg - Matrix mechanics
  - Alternative, yet equivalent, formulation of quantum mechanics;
  - Observables are Hermitian operators;
  - Heisenberg uncertainty principle - Well known for the *position* and *momentum* (velocity). Appliable to all Hermitian operators that do not commute.

$$AB - BA \neq 0$$

# Quantum mechanics

- Quantum mechanics is counter-intuitive!
- Quantum Entanglement
    - It is a classical *no-go theorem*. Very important for quantum information and quantum computation.
    - Two particles can "share" a state. The observables of each one of the particles are highly correlated.
    - The action happens regardless the distance of the particles. Einstein-Podolsky-Rosen (EPR) paradox.
    - Bell experiments apparently ruled out local hidden variable theories
- What is a measurement? What causes the collapse of the wave function?
    - Copenhagen interpretation
    - Hidden variable theories
    - Multiverse interpretation

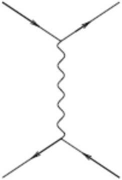
# Foundations and Postulates of Quantum mechanics



- Several possible foundations for quantum mechanics with contributions of many: Born, Shrödinger, Heinsenberg, Dirac, Von Neumman, Feynman
- Hilbert spaces equiped with inner products are proper structures to support quantum physics
  - Any linear superposition of possible states is also a possible state of the system. Supported for the *tensor product* of spaces
- Dirac braket notation: $\langle\Psi| \, , |\Psi\rangle \, , \langle\Psi|\Psi\rangle$, Refers to vectors in Hilbert spaces and inner products
- Observables are linear Hermitian operators, base vectors are the eigenvalues of such operators: $O^{\dagger} = O$
- Unitary evolution: $U^{-1}U = I$

# New Foundations for Quantum Mechanics

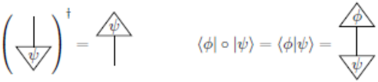
- There are several other foundations for quantum mechanics
  - C*-Algebras, W*-Algebras, Operator algebras, Effect algebras, Probabilistic theories, among several others
- Categorical Quantum Mechanics
  - Semantics: processes that handle quantum information. Intuition: *Feynman diagrams*.



  - Symmetric Monoidal categories, use FHilb or FRel as base categories.
  - Further inclusion of a dagger Functor, making them †-Symmetric monoidal categories.
  - This allows the construction of orthogonal basis, complementarity, phases, measurements, and of all features of quantum mechanics.

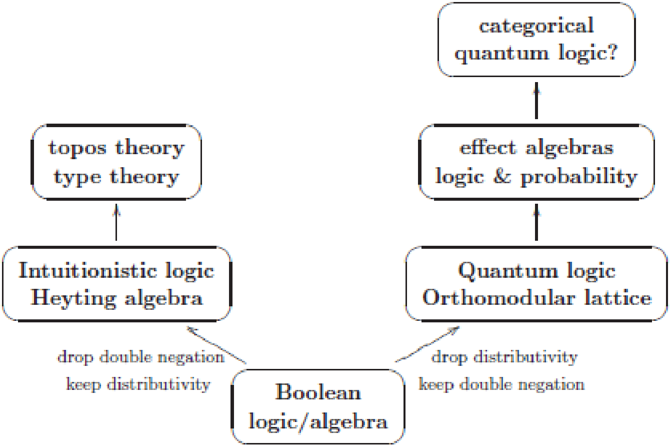
# Foundations for Quantum mechanics

- Symmetric monoidal categories have a natural diagrammatic interpretation. It is possible to use a visual language to reason about quantum physics.



- A lot of work has been developed in the field of logics for model quantum phenomenons
  - Quantum logics, Dynamic logics, Temporal logic with institutions

# Foundations for Quantum mechanics



categorical quantum logic?

topos theory type theory

effect algebras logic & probability

Intuitionistic logic Heyting algebra

Quantum logic Orthomodular lattice

drop double negation keep distributivity

drop distributivity keep double negation

Boolean logic/algebra

# Quantum Computation

# Quantum Computation

- Created in the eighties by Richard Feynman (Quantum simulation) and David Deutsch (Universal Quantum Computer);

- "Memory"
  - Qubit is the fundamental unit of information (as similarly to bit)

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,;|\alpha|^2 + |\beta|^2 = 1$$

    $|0\rangle, |1\rangle$ are an orthogonal basis. However the possible states are provided by all superpositions of the system.
  - Due to entanglement it is also possible to build sets of qubits.

$$H^n = H_1 \otimes H_2 \otimes H_3 \ldots \otimes H_n$$

# Quantum Computation

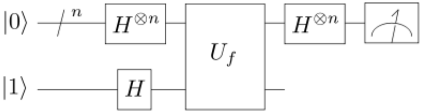
- "Memory" (cont.)
  - The possible states for two qubits is

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \lambda\,|11\rangle\,;\, |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\lambda|^2 = 1$$

  - The information that can be maintained in memory grows exponentially!
- Processing
  - It is possible to perform operations over all the computational basis, in an exponential time improvement. Such phenomenon is denominated *quantum parallelism*.
  - Algorithms must be adapted to this setting, which has revealed as a hard task
  - In particular due to a few restrictions:
    - No cloning theorem (there can be no copies of information while processing);
    - Measurements destroy the status of the system (so as decoherence);
    - Transitions are unitary, e.g. they must be revertible;

# Quantum Computation: the Circuit Model

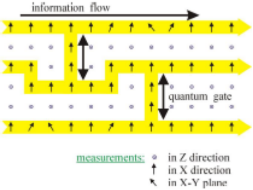
- There are several models to quantum computers: quantum circuits, measurement based, adiabatic, topological. All of them are computationally complete!
- Quantum circuit model:



- Quantum circuits are built out of sets of quantum gates
- Quantum gates are unitary transformations, which actually do the actions over states
    - *CNOT*, *Toffoli*, *Phase*, *Z gate*, ...

# Quantum Computation: Measurement based model

- Measurement based model
  - Measurements are made over qubits, computational change according outcomes (classical processing is necessary)
  - More robustness to decoherence
  - Two ways of doing it: *one-way* and *teleportation based*
  - In the one way computer the problem is set up as a tree search tree problem. After each measurement a branch of the tree is excluded from the search space.



# Quantum Computation: Adiabatic and Topological model

- Adiabatic Computation
  - Works on the base the *Adiabatic theorem*. Every Hamiltonian converges to the *ground state*. It goes through all the possible Hamiltonians in the system. If the transition was slow enought then the transition was *adiabatic*
  - It is a dynamic technique, e.g. involves the time variable
  - Can simulate any circuit model
  - Can be understood as a actual *simulated annealing*, in which the ground state holds the proper solution
- Topological model
  - Lies upon Topological Field theory (a topological phrasing of quantum field theory)
  - Works based on *anyons*, the topological version of a qubit
  - It is a natural fit for topological problems, e.g. *Jones Polynomial*

# Algorithmics

# *Deutsch-Jozsa* Algorithm

- Created in 1992, by *David Deutsh* and *Richard Jozsa*.
- Was also the first algorithm that took advantage of "quantum parallelism" and here lies its main interest.
- Verifies if a function is *constant* or *balanced*. Works only for $f : 0, 1 \rightarrow 0, 1$, altough there are several adaptations for $n + m$ qubits.
- Rationale:
    - Evaluate both images of the function in a single step using an oracle
    - Apply the *Hadamard* operator. It will provide a distribution of the original function.
    - After measurement it is possible to take immediate conclusions about the *balance* of the function. It is a deterministic algorithm.

# *Deutsch-Jozsa* Algorithm

- The algorithm:
  - Prepare the system in the initial state:

$$|\Psi\rangle = \frac{1}{2}(\sum_{x=0}^{1} |x\rangle) \otimes (|0\rangle - |1\rangle)$$

  - Apply the oracle over the state and it will read as follows:

$$|\varphi\rangle = \frac{1}{\sqrt{2}}((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle)$$

  - Apply the Hadamard Gate and the final state will read as follows:

$$H|\varphi\rangle = \frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)$$
$$= \frac{1}{2}(((-1)^{f(0)} + (-1)^{f(1)})(|0\rangle) + ((-1)^{f(0)} - (-1)^{f(1)})(|1\rangle)$$

# Grover algorithm

- Formulated by L.K. Grover in 1996. Applies to the search of *unsorted databases*, e.g. it is a general search algorithm
- It has a quadratic speedup, e.g. the solution of the search problem can be found in $\sqrt{N}$
- Intuition
  - Mark the correct solution, from all the solution space.
  - Isolate the solution (by augmentation of its amplitude) through the application of several operators.
  - In the measurement, the solution shall be the most probable outcome.

# Grover algorithm

- Prepare the system

$$|\Psi\rangle = H^{\otimes n} |0^{\otimes n}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \tag{3}$$

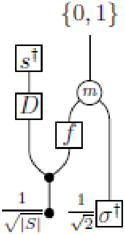
- The algorithm consists in the repetition of the following steps $\sqrt{(}N)$ times
  - Apply the *oracle* over all possible solutions, marking the correct solution.

$$O|x\rangle = (-1)^{f(x)} |x\rangle \tag{4}$$

  - Apply a selective rotation gate: $H^{\otimes n} X H^{\otimes n}$

# Grover algorithm, Amplitude amplification and estimation

- Grover algorithm is a optimal search algorithm
- It is a specific case of a more general technique: Amplitude amplification.
- May be complemented by another technique: Amplitude estimation
- There are many derivations of this algorithm, such as one-shot Grover algorithm
- Foundations (Jamie Vicary):



Single-shot Grover

# Shor algorithms

- Shor algorithm is the most relevant algorithm of quantum computation as it could potentially break RSA cryptography.
- Shor was inspired in Simon algorithm for the calculation of discrete logarithms.
- Intuition:
  - Prepare the system with entangled pairs from a domain correspondent co-domain elements
  - Reading the co-domain register will isolate the correspondent elements of the domain
  - Fourier transform will provide generators (e.g. the period) for the group generated in previous step
- The algorithm
  - System preparedness

$$|\Phi\rangle = \frac{1}{2^{n/2}} \left( \sum_{x=0}^{2^n-1} |x\rangle \right) \otimes |0\dots0\rangle \tag{5}$$

# Shor algorithms

- Continuation of the Algorithm:
  - Entangle $f(x)$ in co-domain register with the correspondent $x$ in the domain register

$$|\Psi_f\rangle = U_f\,|\Phi\rangle = \frac{1}{2^{n/2}}\left(\sum_{x=0}^{2^n-1}|x\otimes f(x)\rangle\right) \tag{6}$$

  - Measure the counter domain register such that the coset will be identified.

$$|\Psi_0\rangle = \frac{1}{\sqrt{K}}\sum_{k=0}^{K-1}|x_0+kr\rangle \tag{7}$$

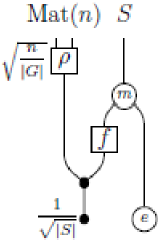
  - Then apply the Fourier transform over the domain register.

$$\frac{1}{2^{n/2}}\frac{1}{\sqrt{K}}\sum_{k=0}^{K-1}e^{2i\pi y(x_0+kr)/2^n} \tag{8}$$

  - When properly measured this state will yield the most probable period for the function.

# Shor algorithms

- The algorithm can be generalized to many other problems, based on groups: *Hidden Subgroup Problem*
- From the foundational perspective the flux of information works as follows:



Hidden subgroup

# Quantum Random Walks

- Quantum walks are analogous to classical random walks. It is becoming one of the most important techniques in quantum computation, and can be used with many algorithms, particularly search algorithms.
- Intuition:
  - They have three main components: a set of connected nodes, a *flipping* coin), an operator that generates the transitions.
  - The successive application of a unitary operator turns highly probable to converge to the node of the graph that contains the solution.
- A very simple example:
  - Given a state

$$|\Psi_{in}\rangle = \alpha^{\uparrow}|\uparrow\rangle + \alpha^{\downarrow}|\downarrow\rangle \otimes |\psi_{x_0}\rangle$$

  - The random walk will progress as follows:

$$U|\Psi_{in}\rangle = \alpha^{\uparrow}|\uparrow\rangle \otimes |\psi_{x_0-1}\rangle + \alpha^{\downarrow}|\downarrow\rangle \otimes |\psi_{x_0+l}\rangle$$

# Applications of Quantum Algorithms

- The number of algorithms is already quite big. Some of them are "hybrid", e.g. use classical and quantum techniques;
- Primitive Techniques
  - Fourier Sampling/Transform, Hadamard transform, Phase estimation;
  - Amplitude amplification and estimation, Random walks;
  - Adiabatic search and optimization;
  - Quantum simulation;
- Applications for quantum algorithms
  - Algebraic and Crytography (Principal Ideal, Pell's equation, Period finding, solving linear equations)
  - Search and Optimization
  - Machine Learning (pattern detection)
  - A good survey can be found in the "Quantum Algorithm Zoo"
- Quantum simulation seems to be the "killer" application.

# Quantum Complexity classes

- There are many quatum computational classes. A good survey is available in "The Complexity Zoo"
- All quantum classes are contained in PSPACE
- *Bounded Quantum Probability*
  - BQP is believed to contain *all* problems that are solvable in polynomial time by quantum computers
  - NP-Complete problems do not seem to be contained in BQP.
  - BQP is contained in classical PP.
- *Quantum Merlin Arthur*
  - It is closely related with *Hamiltonian Complexity*, which, generally, studies the *hardness* of simulating a physical theory. Has a natural relation with *Quantum simulation*.
  - Some problems related with simulation of quantum physical systems are *QMA-Complete*, such as the *Local Hamiltonian Problem*

# References

- Michael A Nielsen and Isaac L Chuang. Quantum computation and quantum information. Cambridge university press, 2010.
- Complexity Zoo
  - `https://complexityzoo.uwaterloo.ca/Complexity_Zoo`
- Quantum algorithm Zoo
  - `http://math.nist.gov/quantum/zoo/`
- Stephen Gasiorowicz. Quantum physics. John Wiley & Sons, 2007.
- Bob Coecke, New Structures for Physics, Springer, 2010
- Carlos Tavares, Foundations for Quantum Algorihms and Complexity, MAPi pre-thesis, 2015. *Available upon request*

# Questions ?