

# Quantum Computation (CO484)

## Quantum Physics and Concepts

Herbert Wiklicky

herbert@doc.ic.ac.uk  
Autumn 2018

Slide 1 of 29

## Overview

Topics we will cover in this course will include:

1. Basic Quantum Physics
2. Mathematical Structure
3. Quantum Cryptography
4. Quantum Circuit Model
5. [MBQC, TQC, etc.]
6. Quantum Teleportation
7. Grover's Search Algorithm
8. Shor's Quantum Factorisation
9. [Quantum Error Correction]

Slide 2 of 29

# Practicalities

Two Lecturers

**Herbert Wiklicky** ~[herbert/teaching.html](http://herbert/teaching.html)

[h.wiklicky@imperial.ac.uk](mailto:h.wiklicky@imperial.ac.uk)

Teaching  $3\frac{1}{2}$  weeks until 30 October

Open-book coursework test **30 October** (or 26?)

**Mario Berta**

[m.bera@imperial.ac.uk](mailto:m.bera@imperial.ac.uk)

Teaching  $3\frac{1}{2}$  weeks from 2 November

Open-book coursework test **27 November**

Exam: Week 11, **10 December 2018**, 2 hours (3 out of 4).

Different classes, different background, different applications.

Slide 3 of 29

## External Students – Registration for DoC Courses

1. Apply at <https://dbc.doc.ic.ac.uk/externalreg/>
2. Then,
  - ▶ Your department's endorser will approve/reject application
3. If approved,
  - ▶ DoC's External Student Liaison will approve/reject your application
4. If approved (again!),
  - ▶ Students will get access to DoC resources (DoC account, CATE, ...)
  - ▶ No access after a few days? Check status of approval and contact relevant person(s)

### Key Dates

- ▶ Exams for DoC 3<sup>rd</sup>/4<sup>th</sup> yr. courses take place at the end of the Term in which the course is taught
- ▶ Registration for exams opens in November for Autumn courses and end January for Spring term courses

If in doubt, read the guidelines available at the link above ☺

Slide 4 of 29

## Text Books

- ▶ Noson S. Yanofsky, Mirco A. Mannucci: Quantum Computing for Computer Scientists, Cambridge, 2008
- ▶ Michael A. Nielsen, Issac L. Chuang: Quantum Computation and Quantum Information, Cambridge, 2000
- ▶ Phillip Kaye, Raymond Laflamme, Michael Mosca: An Introduction to Quantum Computing, Oxford 2007
- ▶ N. David Mermin: Quantum Computer Science, Cambridge University Press, 2007
- ▶ A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi: Classical and Quantum Computation, AMS, 2002
- ▶ Eleanor Rieffel, Wolfgang Polak: Quantum Computing, A Gentle Introduction. MIT Press, 2014
- ▶ Richard J. Lipton, Kenneth W. Regan: Quantum Algorithms via Linear Algebra. MIT Press, 2014

Slide 5 of 29

## Electronic Resources

### Introductory Texts

- ▶ E.Rieffel, W.Polak: An introduction to quantum computing for non-physicists. ACM Computing Surveys, 2000  
[doi:10.1145/367701.367709](https://doi.org/10.1145/367701.367709)
- ▶ N.S.Yanofsky: An Introduction to Quantum Computing  
<http://arxiv.org/abs/0708.0261>

Preprint Repository <http://arxiv.org>

### Physics Background

- ▶ Chris J. Isham: Quantum Theory – Mathematical and Structural Foundations, Imperial College Press 1995
- ▶ Richard P. Feynman, Robert B. Leighton, Matthew Sands: The Feynman Lectures on Physics, Addison-Wesley 1965

Slide 6 of 29

## Quantum Money (Stephen Wiesner 1960s)

Quantum Postulates: (i) It is **impossible to clone** a quantum states, (ii) in general, an inspection of a quantum state is **irreversible and destructive**.

**Bank of Quantum** issue bank notes with a unique quantum code.

**Quantum Forger** tries to make a copy of quantum money, however

- ▶ she can't copy/clone a banknote directly, and
- ▶ when she inspects it, she destroys the code.

**Bank of Quantum** can inspect the quantum code on a banknote

- ▶ to confirm it is authentic, and then
- ▶ issue a replacement quantum banknote.

Simon Singh: *Code Book*, Forth Estate, 1999.

Slide 7 of 29

## Quantum History

Quantum Mechanics was 'born' or, better, proposed by M.Plank on

**14 December 1900, 5:15pm (Berlin)**

**1900** Max Plank: Black Body Radiation

**1905** Albert Einstein: Photoelectric Effect

**1925** Werner Heisenberg: Matrix Mechanics

**1926** Erwin Schrödinger: Wave Mechanics

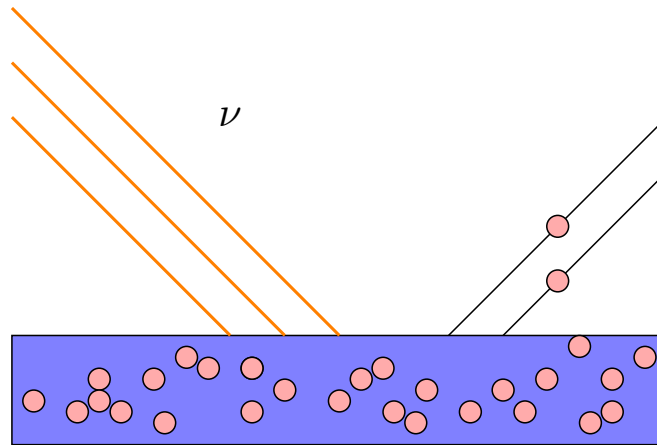
**1932** John von Neumann: Quantum Mechanics

Manjit Kumar: *Quantum – Einstein, Bohr and Their Great Debate about the Nature of Reality*, Icon Books 2009

Slide 8 of 29

# Photoelectric Effect – Millikan Experiment

Experimental Setup:



Observed: The velocity, and thus kinetic energy, of the emitted electrons depends not on the intensity of the incoming light but **only** on its “colour”, i.e. frequency  $\nu$ .

Slide 9 of 29

## Radiation Law

Observed relationship:

$$W_k = h\nu - W_e$$

$W_k$  ... Kinetic Energy of Electron

$W_e$  ... Escape Energy of Material

$\nu$  ... Frequency of Light

$h$  ... Planck's Constant

$$h = 6.62559 \cdot 10^{-34} \text{ Js}$$

$$\hbar = \frac{h}{2\pi} = 1.05449 \cdot 10^{-34} \text{ Js}$$

Slide 10 of 29

# Quantum Physical Problems

Around 1900 there were a number of experiments and observations which could not be explained using classical physics/mechanics, among them:

## Spectra of Elements

Emission/absorption only at particular “colours”.

## Stern-Gerlach Experiment

Interference in double slit experiment.

## Black Body Radiation

Radiation law involves “quantised” energy levels.

## Photo-Electric Effect

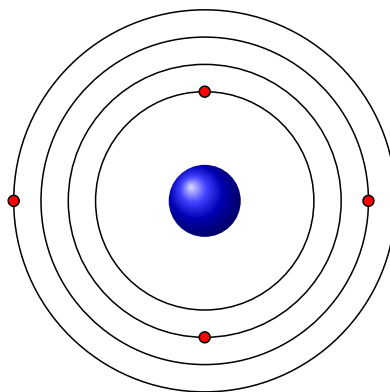
Einstein’s explanation got him the Nobel prize.

These were the perhaps most exciting years in the history of theoretical physics, at the same time there were also breakthroughs in special and general relativity, etc.

Slide 11 of 29

# Einstein’s Explanation

Albert Einstein 1905: Not all **energy levels** are possible, they only come in **quantised** portions. In Bohr’s (incomplete) “model” of the atom this corresponds to allowing only particular “orbits”.



In this way one can also explain the spectral emissions (and absorption) of various elements, e.g. to analyse the material composition of stars (and to make great fireworks).

Slide 12 of 29

# Quantum Paradoxes and Myths

There are a number of physical problems which require quantum mechanical explanations. Unfortunately, QM is not 'really intuitive'. This leads to various *Gedanken* experiments which point to a contradiction with so-called *common sense*.

- ▶ Black Body Radiation
- ▶ Double Slit Experiment
- ▶ Spectral Emissions
- ▶ Schrödinger's Cat
- ▶ Einstein-Podolsky-Rosen
- ▶ Quantum Teleportation

7. Whereof one cannot speak, thereof one must be silent.  
Ludwig Wittgenstein: *Tractatus Logico-Philosophicus*, 1921

Slide 13 of 29

## From Quantum Physics to Computation

There are a number of disciplines which play an important role in trying to understand *quantum mechanics* and in particular **quantum computation**.

**Philosophy:** What is the nature and meaning reality?

**Logic:** How can one reason about events, objects etc.?

**Mathematics:** How does the formal model look like?

**Physics:** Why does it work and what does it imply?

**Computation:** What can be computed and how?

**Engineering:** How can it all be implemented?

Each area has its own language which however often applies only to classical entities – for the quantum world we often have simply the wrong vocabulary.

Slide 14 of 29

# Natural Philosophy

Arguably, **physics** is ultimately about explaining experiments and forecasting measurement results.

**Observable:** Entities which are (actually) measured when an experiment is conducted on a system.

**State:** Entities which completely describe (or model) the system we are interested in.

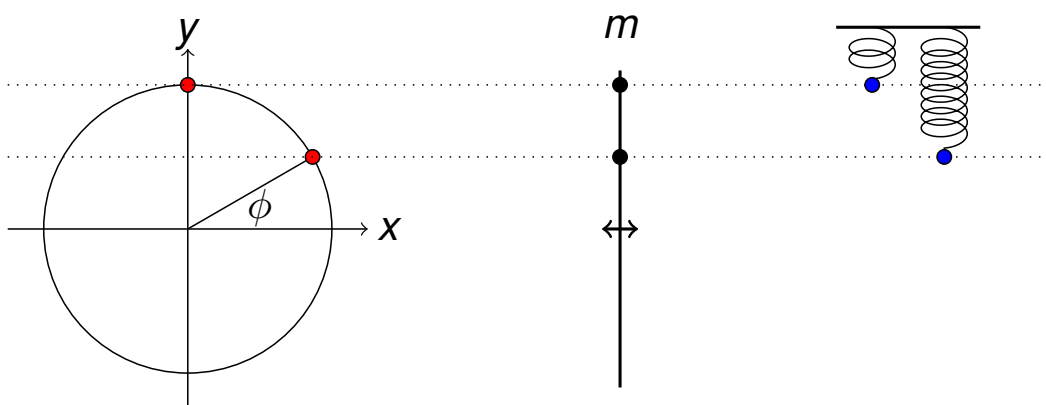
**Measurement** brings together/establishes a relation between states and observables of a given system. **Dynamics** describes how observables and/or the state changes over time.

**Related Questions:** What is our knowledge of what? How do we obtain this information? What is a description on how the system changes?

Slide 15 of 29

## Harmonic Oscillator or just a “Shadow”

One can observe the same “behaviour” of the shadow of a rotating object or an object on a spring.



**Observable:** **Shadow**  $m$

**State:** **Position**  $(x, y)$  or: **Phase**  $\phi$

**Measurement:**  $m((x, y)) = y$ , or:  $m(\phi) = \sin(\phi)$

**Dynamics:**  $(x, y)(t) = (\cos(t), \sin(t))$  or also:  $\phi(t) = t$

Slide 16 of 29



## Postulates for Quantum Mechanics [\*]

- ▶ **Observables** and **states** of a system are represented by *hermitian* (i.e. self-adjoint) elements  $a$  of a  $C^*$ -algebra  $\mathcal{A}$  and by *states*  $w$  (i.e. normalised linear functionals) over this algebra.
- ▶ Possible results of **measurements** of an observable  $a$  are given by the *spectrum*  $Sp(a)$  of an observable. Their probability distribution in a certain state  $w$  is given by the probability measure  $\mu(w)$  induced by the state  $w$  on  $Sp(a)$ .

Walter Thirring: *Quantum Mathematical Physics*, Springer 2002

Key Notions: A quantum systems is (may be) in a certain **state**, but physicists have to decide which properties they want to **observe** before a **measurement** is made (which instrument?).

Slide 17 of 29

## Postulates for Quantum Mechanics (ca. 1950) [\*]

- ▶ The quantum **state** of a (free) particle is described by a (normalised) complex valued [wave] function:

$$\vec{\psi} \in L^2 \text{ i.e. } \int |\vec{\psi}(x)|^2 dx = 1$$

- ▶ Two quantum states can be **superimposed**, i.e.

$$\psi = \alpha_1 \vec{\psi}_1 + \alpha_2 \vec{\psi}_2 \text{ with } |\alpha_1|^2 + |\alpha_2|^2 = 1$$

- ▶ Any **observable**  $A$  is represented by a linear, self-adjoint operator  $\mathbf{A}$  on  $L^2$ .
- ▶ **Possible measurement** results are (only) the eigen-values  $\lambda_j$  of  $\mathbf{A}$  corresponding to eigen-vectors/states  $\vec{\phi}_j \in L^2$  with

$$\mathbf{A}\vec{\phi}_j = \lambda_j \vec{\phi}_j$$

- ▶ **Probability** to **measure** (the possible eigenvalue)  $\lambda_n$  if the system is in the state  $\vec{\psi} = \sum_i \psi_i \vec{\phi}_i$  is

$$Pr(A = \lambda_n | \vec{\psi}) = |\psi_n|^2$$

Slide 18 of 29

# Mathematical Framework

Quantum mechanics has a well-established and precise mathematical formulation (though its ‘common sense’ interpretation might be non-intuitive, probabilistic, etc.).

The (standard) mathematical model of quantum system uses:

- ▶ Complex Numbers  $\mathbb{C}$ ,
- ▶ Vector Spaces, e.g.  $\mathbb{C}^n$ ,
- ▶ Hilbert Spaces, i.e. inner products  $\langle \cdot | \cdot \rangle$ ,
- ▶ Unitary and Self-Adjoint Matrices/Operators,
- ▶ **Tensor Products**  $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$ .

There are additional mathematical details in order to deal with “real” quantum physics, e.g. systems an infinite degree of freedom; for quantum computation it is however enough to study finite-dimensional Hilbert spaces.

Slide 19 of 29

## Quantum Postulates I – States and Observables

The standard mathematical model of (closed) quantum systems is relatively simple and just requires some basic notions in **(complex) linear algebra**.

- ▶ The information describing the **state** of an (isolated) quantum mechanical system is represented mathematically by a (normalised) vector in a complex Hilbert space  $\mathcal{H}$ .
- ▶ An **observable** is represented mathematically by a self-adjoint matrix (operator)  $\mathbf{A}$  acting on the Hilbert space  $\mathcal{H}$ .

Two states can be combined to form a new state  $\alpha |x\rangle + \beta |y\rangle$  as long as  $|\alpha|^2 + |\beta|^2 = 1$ , by **superposition**.

**Consequence:** We can compute with many inputs in parallel.

Slide 20 of 29

## Quantum States and Notation

The state of a quantum mechanical system is usually denoted by  $|x\rangle \in \mathcal{H}$  (rather than maybe  $\vec{x} \in \mathcal{H}$ ). This notation is ‘inherited’ from the **inner product**  $\langle x|y\rangle$  of vectors  $x$  and  $y$  in a Hilbert space – which can be seen as describing the “*geometric angle*” between the two vectors in  $\mathcal{H}$ .

**P.A.M. Dirac** “invented” the **bra-ket** notation (most likely inspired by the limitations of old mechanical type-writers); Simply “take the inner product apart” to denote vectors in  $\mathcal{H}$ :

$$\text{inner product } \langle x|y\rangle = \text{product } \langle x| \cdot |y\rangle$$

For indexed sets of vectors  $\{\mathbf{x}_i\}$  (maybe because typographic “typing” was problematic) different notations are used:

$$\mathbf{x}_i = \vec{x}_i = \mathbf{x}_i = |i\rangle$$

Slide 21 of 29

## Quantum States and Vectors

Finite quantum **states** can be described by vectors in  $\mathbb{C}^n$ , e.g.

$$\vec{\psi} = |\psi\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ or } \langle\phi| = (1 \ 0)$$

**Observables** are defined by matrices  $\mathbf{A}$  in  $\mathcal{M}(\mathbb{C}^n) = \mathbb{C}^{n \times n}$ .

$$\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \text{ with eigenvalues } \lambda_0 = 1, \lambda_1 = 2$$

Note: There are sometimes two types of indices

- ▶ for enumerating, for example, all eigenvectors of an operator like  $\mathbf{A}$  with  $|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  and  $|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- ▶ to enumerate coordinates of one vector, e.g.  $\vec{\psi}_1 = 1/\sqrt{2}$ , or better perhaps:  $|0\rangle_1 = 0$ .

Slide 22 of 29

## Quantum Postulates II – Measurement

- ▶ The **expected result** (average) when measuring observable  $\mathbf{A}$  of a system in state  $|x\rangle \in \mathcal{H}$  is given by:

$$\langle \mathbf{A} \rangle_x = \langle x | \mathbf{A} | x \rangle = \langle x | \mathbf{A} x \rangle$$

- ▶ The only **possible** results are eigen-values  $\lambda_i$  of  $\mathbf{A}$ .
- ▶ The **probability** of measuring  $\lambda_n$  in state  $|x\rangle$  is

$$Pr(A = \lambda_n | x) = \langle x | \mathbf{P}_n | x \rangle$$

with  $\mathbf{P}_n$  the orthogonal projection onto the  $n$ -th eigenspace of  $\mathbf{A}$  generated by eigen-vector  $|\lambda_n\rangle$

$$\mathbf{P}_n = |\lambda_n\rangle \langle \lambda_n|$$

then we have:  $\mathbf{A} = \sum_i \lambda_i \mathbf{P}_i$  (Spectral Theorem).

Slide 23 of 29

## Heisenberg's Uncertainty Relation

### Theorem

For two observables  $\mathbf{A}_1$  and  $\mathbf{A}_2$  we have:

$$(\Delta_{|x\rangle} \mathbf{A}_1)(\Delta_{|x\rangle} \mathbf{A}_2) \geq \frac{1}{2} |(\langle x | [\mathbf{A}_1, \mathbf{A}_2] | x \rangle)|$$

where the **uncertainty** (classically: variance) is defined by

$$(\Delta_{|x\rangle} \mathbf{A})^2 = \langle x | \mathbf{A}^2 | x \rangle - \langle x | \mathbf{A} | x \rangle^2$$

and the commutator is defined as:

$$[\mathbf{A}_1, \mathbf{A}_2] = \mathbf{A}_1 \mathbf{A}_2 - \mathbf{A}_2 \mathbf{A}_1$$

see e.g. Isham: *Quantum Theory*, ICP 1995, Section 7.3.3.

Slide 24 of 29

# Classical vs Quantum Mechanics

The usual interpretation of Heisenberg's uncertainty relation is this: When one tries to measure two observables  $\mathbf{A}_1$  and  $\mathbf{A}_2$  then – if the commutator  $[\mathbf{A}_1, \mathbf{A}_2]$  is non-zero – a small  $\Delta_{|x\rangle} \mathbf{A}_1$  implies a large  $\Delta_{|x\rangle} \mathbf{A}_2$ , and vice versa.

A standard example of so-called *incommensurable* observables are **position**  $\mathbf{A}_1 = x$  and **momentum**  $\mathbf{A}_2 = p$  (on an infinite-dimensional Hilbert Space  $\mathcal{H}$ ) for which  $[x, p] = i\hbar$  and thus:

$$\Delta x \Delta p \geq \hbar/2.$$

In **classical** physics observables always **commute**, are *commensurable*, i.e.  $[\mathbf{A}_1, \mathbf{A}_2] = 0$ . In **quantum** physics for most observables  $[\mathbf{A}_1, \mathbf{A}_2] \neq 0$ , i.e. the observable algebra is typically **non-commutative** or **non-abelian** (cf. multiplication of (complex) numbers vs multiplication of matrices).

Slide 25 of 29

## Quantum Dynamics

- ▶ The **dynamics** of a (closed) system is described by the **Schrödinger Equation**:

$$i\hbar \frac{d|x\rangle}{dt} = \mathbf{H}|x\rangle$$

for the (self-adjoint) Hamiltonian operator  $\mathbf{H}$  (energy).

- ▶ The **solution** is a unitary operator  $\mathbf{U}_t$  (e.g. Isham 6.4)

$$\mathbf{U}_t = \exp\left(-\frac{i}{\hbar} t\mathbf{H}\right)$$

### Theorem

For any self-adjoint operator  $\mathbf{A}$  the operator

$$\exp(i\mathbf{A}) = e^{i\mathbf{A}} = \sum_{n=0}^{\infty} \frac{(i\mathbf{A})^n}{n!}$$

is a **unitary** operator.

Slide 26 of 29

## Irreversible vs Reversible

There are a number of immediate consequences of the postulates.

1. The state develops reversibly, i.e.  $|x_t\rangle = \mathbf{U}_t |x_0\rangle$  for some unitary matrix (operator).  
**Consequence:** No cloning theorem, i.e. no duplication of information.
2. Measurement is partial (Heisenberg Uncertainty Relation).  
**Consequence:** The full state of a quantum computer is not observable.
3. Measurement is irreversible.  
**Consequence:** The state of a quantum system is irrevocably destroyed if we inspect it.

The mathematical structure has also consequences for any **Quantum Logic**, e.g. De Morgan fails, 'Tertium non datur' is not guaranteed, etc.

Slide 27 of 29

## Quantum Physics vs Quantum Computation

### Quantum Physics

Given a quantum system (device).

What is its dynamics?

- ▶ Heisenberg Picture:

$$\mathbf{A} \mapsto \mathbf{A}_t = \mathbf{A}(t) = e^{it\mathbf{H}} \mathbf{A} e^{-it\mathbf{H}}$$

- ▶ Schrödinger Picture:

$$|x\rangle \mapsto |x\rangle_t = |x(t)\rangle = e^{-it\mathbf{H}} |x\rangle$$

### Quantum Computation

Given a desired computation (dynamics).

What quantum device (e.g. circuit) is needed to obtain this?

Slide 28 of 29

# Quantum Computation

Quantum computation tries to utilise quantum systems/devices in order to perform computational tasks or to implement (secure) quantum communication protocols.

1973 C. Bennett: Reversible Computation

1980 P.A. Benioff: Quantum Turing Machine

1982 R. Feynman: Quantum Simulation

1985 D. Deutsch: Universal QTM

1994 P. Shor: Factorisations

1996 L. Grover: Database Search

2008 Harrow, Hassidim, Lloyd: Linear Equations

When will (cheap) quantum computers be available? What will be a **killer application** for quantum computation? When will we reach **quantum supremacy**?