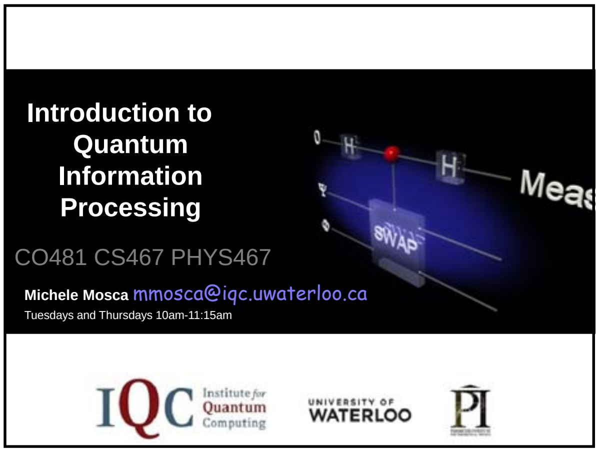


Introduction to Quantum Information Processing

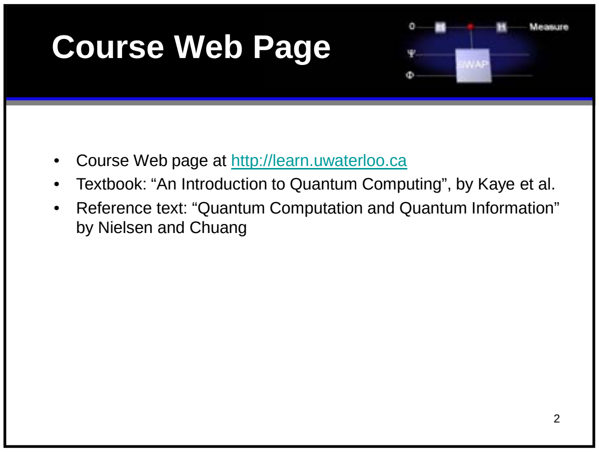
CO481 CS467 PHYS467

Michele Mosca mmosca@iqc.uwaterloo.ca

Tuesdays and Thursdays 10am-11:15am

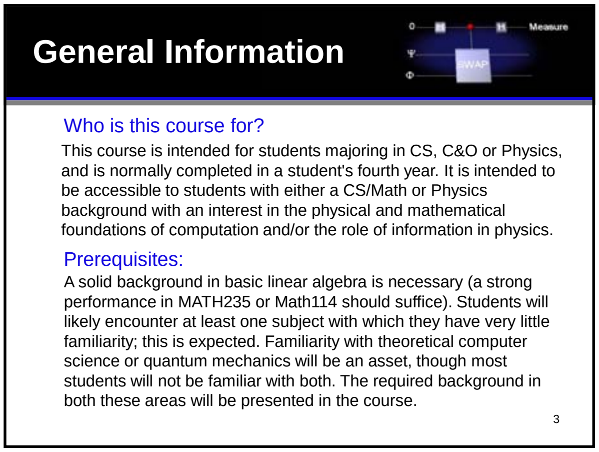
0
H
H
Meas
Ψ
Φ
SWAP

IQC Institute for Quantum Computing   UNIVERSITY OF WATERLOO   PI



Course Web Page

- Course Web page at http://learn.uwaterloo.ca
- Textbook: “An Introduction to Quantum Computing”, by Kaye et al.
- Reference text: “Quantum Computation and Quantum Information” by Nielsen and Chuang



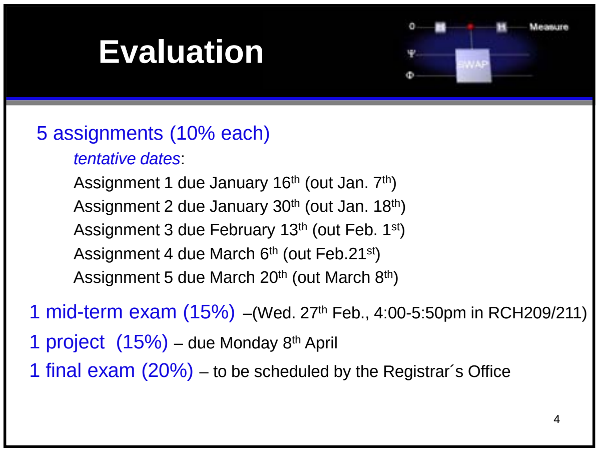
General Information

Who is this course for?

This course is intended for students majoring in CS, C&O or Physics, and is normally completed in a student's fourth year. It is intended to be accessible to students with either a CS/Math or Physics background with an interest in the physical and mathematical foundations of computation and/or the role of information in physics.

Prerequisites:

A solid background in basic linear algebra is necessary (a strong performance in MATH235 or Math114 should suffice). Students will likely encounter at least one subject with which they have very little familiarity; this is expected. Familiarity with theoretical computer science or quantum mechanics will be an asset, though most students will not be familiar with both. The required background in both these areas will be presented in the course.



Evaluation

5 assignments (10% each)

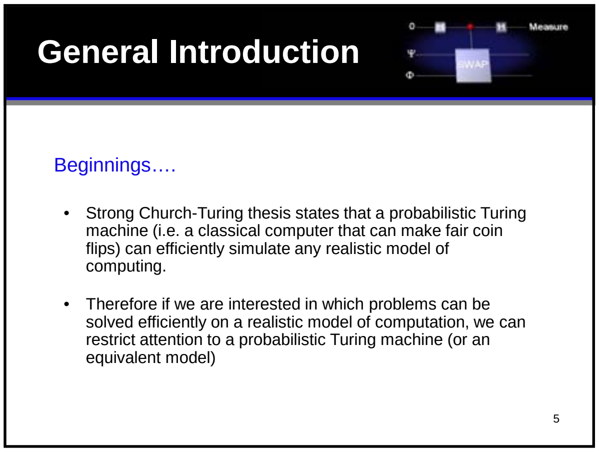
tentative dates:

Assignment 1 due January 16th (out Jan. 7th)
Assignment 2 due January 30th (out Jan. 18th)
Assignment 3 due February 13th (out Feb. 1st)
Assignment 4 due March 6th (out Feb.21st)
Assignment 5 due March 20th (out March 8th)

1 mid-term exam (15%) –(Wed. 27th Feb., 4:00-5:50pm in RCH209/211)

1 project (15%) – due Monday 8th April

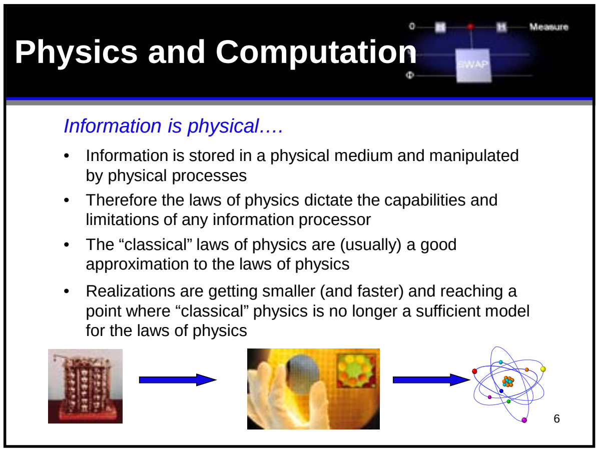
1 final exam (20%) – to be scheduled by the Registrar´s Office



General Introduction

Beginnings….

- Strong Church-Turing thesis states that a probabilistic Turing machine (i.e. a classical computer that can make fair coin flips) can efficiently simulate any realistic model of computing.
- Therefore if we are interested in which problems can be solved efficiently on a realistic model of computation, we can restrict attention to a probabilistic Turing machine (or an equivalent model)



Physics and Computation

Information is physical….

- Information is stored in a physical medium and manipulated by physical processes
- Therefore the laws of physics dictate the capabilities and limitations of any information processor
- The “classical” laws of physics are (usually) a good approximation to the laws of physics
- Realizations are getting smaller (and faster) and reaching a point where “classical” physics is no longer a sufficient model for the laws of physics

Physics and Computation

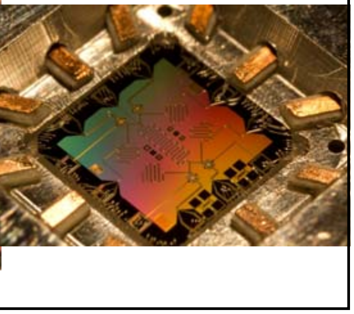
Quantum vs Classical

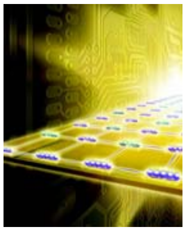
- The theory of quantum physics is a much better approximation to the laws of physics
- The probabilistic Turing machine is implicitly a “classical” device and it is not known in general how to use it to efficiently simulate quantum mechanical systems [Feynman82]
- A computer designed to exploit the quantum features of Nature (a *quantum computer*) seems to violate the Strong Church-Turing thesis

Physics and Computation

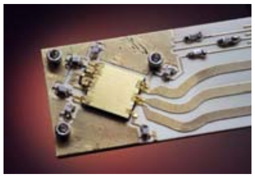
Quantum vs Classical

- Is a quantum computer realistic? Answer seems to be YES (chapter 10)

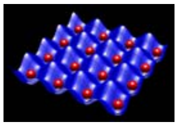




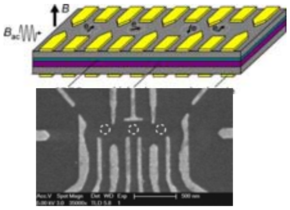
This picture illustrates our vision of a future quantum computer. Strings of ions are held as separate strings above an “ion trap chip”. Through the antennae-effect, quantum information can be exchanged between neighbouring ion strings. *Graphics: Harald Ritsch. Copyright statement: The picture may be freely used provided that the source is correctly stated.*
http://heart-c704.uibk.ac.at/



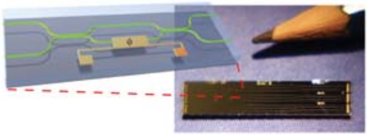
NIST's gold ion trap on an aluminium-nitride backing. (Courtesy: Y Colombe/NIST)
PhysicsWorld



Optical lattices use lasers to separate rubidium atoms (red) for use as information “bits” in neutral-atom quantum processors—prototype devices that designers are trying to develop into full-fledged quantum computers. NIST scientists have managed to isolate and control pairs of the rubidium atoms with polarized light, an advance that may bring quantum computing a step closer to reality.
Credit: NIST



http://www.tnw.tudelft.nl/index.php?id=36313&L=1



From the following article:
Quantum computers
T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe & J. L. O'Brien
Nature 464, 45-53(4 March 2010)
doi:10.1038/nature08812

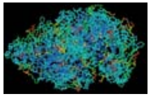
Physics and Computation

Quantum vs Classical

- If the quantum computers are a reasonable model of computation, and classical devices cannot efficiently simulate them, then the strong Church-Turing thesis needs to be modified to state that a quantum Turing machine can efficiently simulate any realistic model of computation

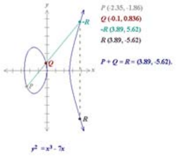
Quantum-enhanced computation

commons.wikimedia.org/wiki/Image:ProteinStructure.jpg



Simulating quantum mechanical systems

http://certicom.com/



Computational number theory and algebra

General searching, counting, and optimizing

Quantum Algorithms

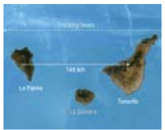
http://math.nist.gov/quantum/zoo/ *(maintained by S. Jordan)*

Quantum Communication and Cryptography

- By exploiting the quantum mechanical behaviour of the communication medium, we can detect eavesdroppers (leading to quantum cryptography, section 12.6 of N&C) and solve distributed computation tasks more efficiently.

Quantum Communication and Cryptography

- Quantum communication can provide a new kind of cryptography that is "information theoretically" secure.
- Most famous example is quantum key establishment (QKD) invented by Bennett and Brassard in 1984



Canary Islands:
Longest Free Space distance for QKD

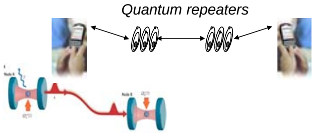
JGN2
Fig. 1 Network Layout of the Tokyo QKD Network

Towards a quantum internet

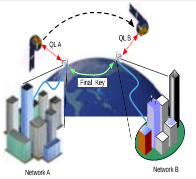
New technologies will achieve reliable quantum communication on global distances, well the beyond current range of about 100 km.

Quantum repeaters, quantum teleportation, and satellites, can someday be used to span the globe.

Quantum repeaters



Reviews on Quantum Repeaters: Sangouard et al, Rev. Mod. Phys. 83, 33 (2011); Kimble, NATURE, 453 (2008).



A quantum satellite in LEO can interconnect ground networks located anywhere on Earth.

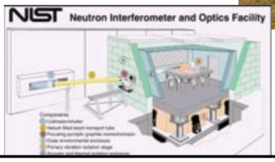
Active research in Canada (QEYSSAT), USA, Europe (Space-QUEST), Japan, China, Singapore.

Quantum-Enhanced Sensing

- Quantum devices also provide a degree of sensitivity that can improve the quality of measurements and sensing beyond what is achievable with classical methods

http://www.iaea.org/newscenter/images/landmines_300x200.jpg

http://www.nist.gov/public_affairs/releases/images/04PHY011_ChipScaleClock2.jpg



http://www.diabetescare.net/

IQC's Vision: harnessing quantum mechanics will lead to transformational technologies that will benefit society and become a new engine of economic development in the 21st century.

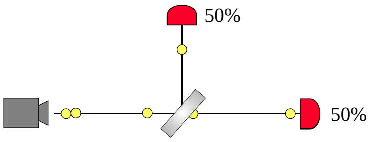
http://iqc.uwaterloo.ca/resources/reports/iqcannualreport2012.pdf

This course

The aim of this course is:

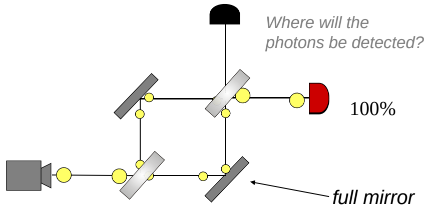
- to provide an introduction to quantum information processing, with a focus on the foundations and basic applications (we have another introductory course focusing on the implementations)
- to lay the foundations for future study and/or research in quantum information processing or related subjects

A beam-splitter



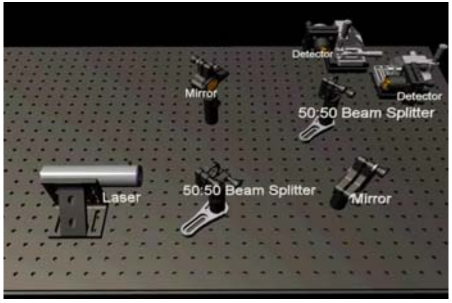
The simplest explanation is that the beam-splitter acts as a classical coin-flip, randomly sending each photon one way or the other.

Quantum Interference

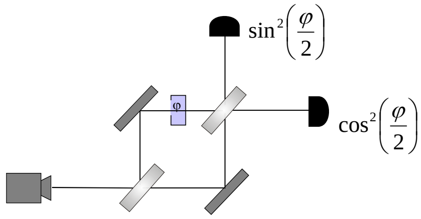


The simplest explanation must be wrong, since it would predict a 50-50 distribution.

Quantum Interference



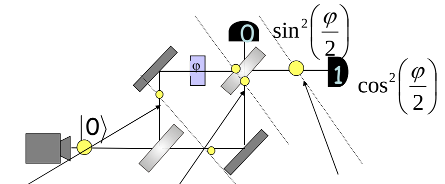
More Experimental Data


$\sin^2\left(\frac{\varphi}{2}\right)$
φ
$\cos^2\left(\frac{\varphi}{2}\right)$

Adding a phase shift in one arm (unbalancing the interferometer) produces even more interesting data.

A new theory…

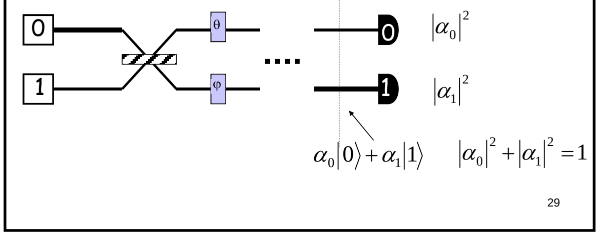
The particle can exist in a linear combination or *superposition* of the two paths


0
$\sin^2\left(\frac{\varphi}{2}\right)$
φ
1
$\cos^2\left(\frac{\varphi}{2}\right)$
$|0\rangle$

$\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$ $\frac{1}{\sqrt{2}}|0\rangle + \frac{ie^{i\varphi}}{\sqrt{2}}|1\rangle$ $\frac{e^{i\varphi}-1}{2}|0\rangle + \frac{i(e^{i\varphi}+1)}{2}|1\rangle$

Probability Amplitude and Measurement

If the photon is measured (with some external apparatus) when it is in the state $\alpha_0|0\rangle + \alpha_1|1\rangle$ then we get $|0\rangle$ with probability $|\alpha_0|^2$


0
1
θ
φ
....
0
1
$|\alpha_0|^2$
$|\alpha_1|^2$
$\alpha_0|0\rangle + \alpha_1|1\rangle$
$|\alpha_0|^2 + |\alpha_1|^2 = 1$

Quantum Operations I

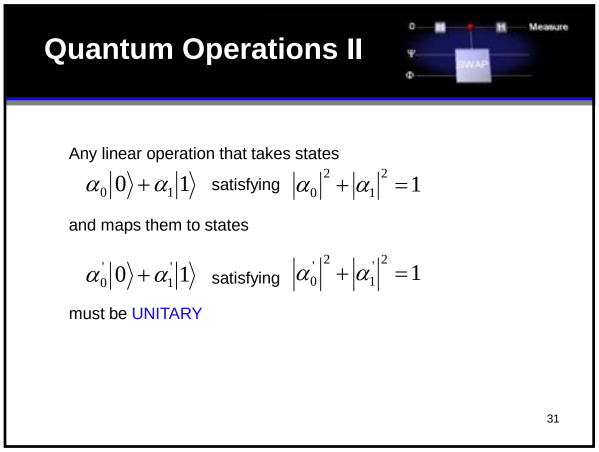
The operations are induced by the apparatus *linearly*, that is, if

$|0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$ and $|1\rangle \mapsto \frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

then

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle\right) + \alpha_1\left(\frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$= \left(\alpha_0\frac{1}{\sqrt{2}} + \alpha_1\frac{i}{\sqrt{2}}\right)|0\rangle + \left(\alpha_0\frac{i}{\sqrt{2}} + \alpha_1\frac{1}{\sqrt{2}}\right)|1\rangle$$



Quantum Operations II

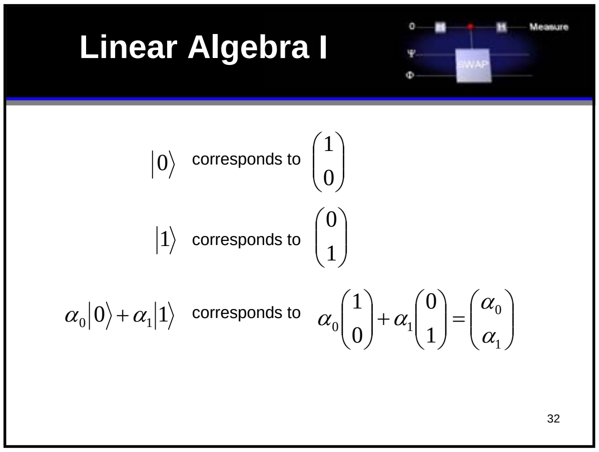
Any linear operation that takes states

$\alpha_0|0\rangle + \alpha_1|1\rangle$ satisfying $|\alpha_0|^2 + |\alpha_1|^2 = 1$

and maps them to states

$\alpha_0^{'}|0\rangle + \alpha_1^{'}|1\rangle$ satisfying $|\alpha_0^{'}|^2 + |\alpha_1^{'}|^2 = 1$

must be UNITARY

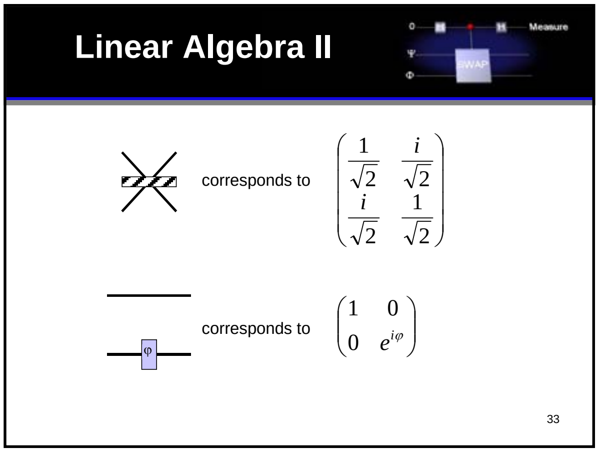


Linear Algebra I

$|0\rangle$ corresponds to $\begin{pmatrix}1\\0\end{pmatrix}$

$|1\rangle$ corresponds to $\begin{pmatrix}0\\1\end{pmatrix}$

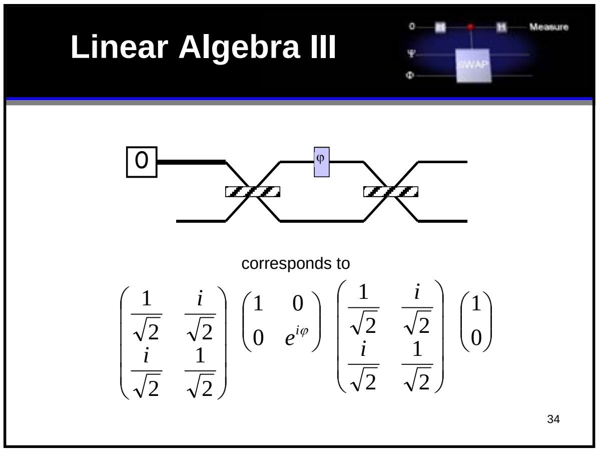
$\alpha_0|0\rangle + \alpha_1|1\rangle$ corresponds to $\alpha_0\begin{pmatrix}1\\0\end{pmatrix} + \alpha_1\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha_0\\\alpha_1\end{pmatrix}$



Linear Algebra II

corresponds to $\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}}\\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}$

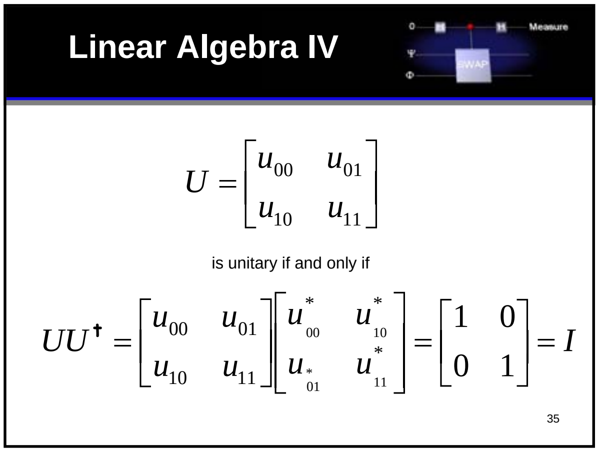
corresponds to $\begin{pmatrix}1 & 0\\ 0 & e^{i\varphi}\end{pmatrix}$



Linear Algebra III

corresponds to

$$\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}}\\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & e^{i\varphi}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}}\\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}$$

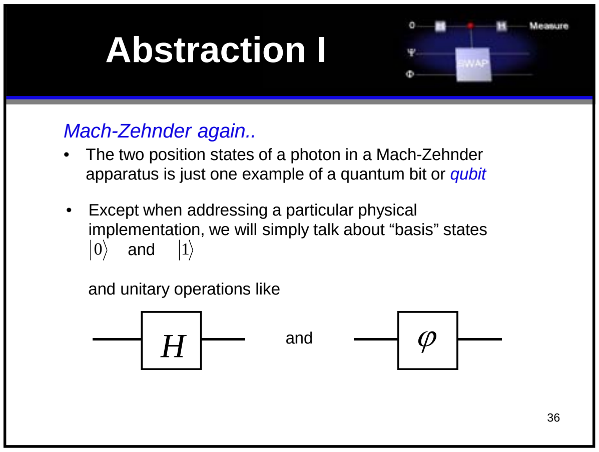


Linear Algebra IV

$$U = \begin{bmatrix}u_{00} & u_{01}\\ u_{10} & u_{11}\end{bmatrix}$$

is unitary if and only if

$$UU^{\dagger} = \begin{bmatrix}u_{00} & u_{01}\\ u_{10} & u_{11}\end{bmatrix}\begin{bmatrix}u^{*}_{00} & u^{*}_{10}\\ u_{*_{01}} & u^{*}_{11}\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = I$$



Abstraction I

Mach-Zehnder again..

- The two position states of a photon in a Mach-Zehnder apparatus is just one example of a quantum bit or *qubit*
- Except when addressing a particular physical implementation, we will simply talk about "basis" states $|0\rangle$ and $|1\rangle$

and unitary operations like

and

Abstraction II

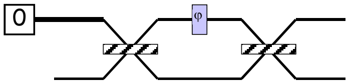
where $-\boxed{H}-$ corresponds to $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}$

, $-\boxed{\varphi}-$ corresponds to $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$

and $-\boxed{X}-$ corresponds to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ - NOT

Abstraction III

An arrangement like



is represented by the circuit

$$|0\rangle - \boxed{\sqrt{X}} - \boxed{\varphi} - \boxed{\sqrt{X}} -$$

More than one qubit I

If we concatenate two qubits $(\alpha_0|0\rangle + \alpha_1|1\rangle)$, and $(\beta_0|0\rangle + \beta_1|1\rangle)$

we have a two qubit system with four basis states

$|0\rangle|0\rangle = |00\rangle$, $|0\rangle|1\rangle = |01\rangle$, $|1\rangle|0\rangle = |10\rangle$, and $|1\rangle|1\rangle = |11\rangle$

We can describe the state as

$$\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

or by the vector $\begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$

More than one qubit II

In general, we can have arbitrary superpositions, for example

$$\alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$$

where

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

If there is no factorization into the tensor product of two independent qubits, then these states are called *entangled*.

Measuring multi-qubit systems

If we measure both bits of

$$\alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$$

we get $|x\rangle|y\rangle$ with probability $|\alpha_{xy}|^2$

Text references

- 1.1 Overview
- 1.2 Computers and the Strong Church-Turing Thesis
- 1.6 A Preview of Quantum Physics
- See also chapter 1 of Nielsen and Chuang