Introduction to
Quantum Information Processing
CS667 C&O681 PHYS767
CS467 C&O481 PHYS467

Michele Mosca (C&O) mmosca@iqc.ca
Richard Cleve (CS) cleve@iqc.ca
Raymond Laflamme (Physics) laflamme@iqc.ca

Tuesdays and Thursdays 10am-11:15am

Introduction to Quantum Information Processing

Lecture 1

Michele Mosca

- Course Web page http://www.iqc.ca/~qipcours/
- Recommended text: "Quantum Computation and Quantum Information" by Nielsen and Chuang (available at the UW Bookstore)
- Supplementary notes will be posted later this month

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 (a strong performance in MATH235 or Phys364&365 should suffice) is necessary. 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

3 assignments (15% each)
1 mid-term exam (20%) –probably Nov. 4th
1 project (35%)

Reading for General Introduction

- Chapter 1 of Text. Sections 1.1-1.5
- Introduction(s) posted on web page

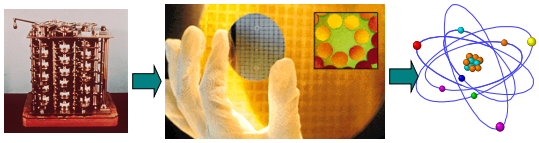
General Introduction

- Strong Church-Turing thesis states that a probabilistic Turing machine (ie 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 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

Physics and Computation



Realizations are getting smaller (and faster) and reaching a point where "classical" physics is not longer a sufficient model for the laws of physics

Physics and Computation

- 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 simulate efficiently quantum mechanical systems [Fey82]
- A computer designed to exploit the quantum features of Nature (a *quantum computer*) seems to violate the Strong Church-Turing thesis

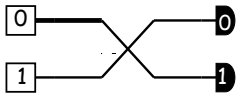
Physics and Computation

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

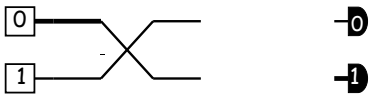
Quantum Communication and Cryptography

- By exploiting the quantum mechanical behaviour of the communication medium, we can detect eavesdroppers (leading to quantum cryptography, section 12.6) and solve distributed computation tasks more efficiently. Unfortunately, we probably won't be covering this much in this course, but we will lay the foundation for further reading in quantum information theory.

A beam-splitter



More experimental data



Quantum Operations

The operations are induced by the apparatus *linearly*, that is, if $|0\rangle \to \frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

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

then

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

Quantum Operations

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

$|0\rangle$ 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

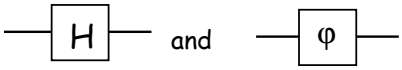
corresponds to $\begin{pmatrix} \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \end{pmatrix}$

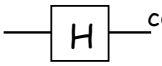
corresponds to

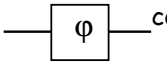
Abstraction

The two position states of a photon in a Mach-Zehnder apparatus is just one example of a quantum bit or *qubit*

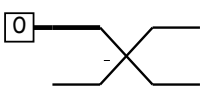
Except when addressing a particular physical implementation, we will simply talk about "basis" states $|0\rangle$ and $|1\rangle$ unitary operations like



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

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

An arrangement like



More than one qubit

If we concatenate two qubits

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)\ (\beta_0|0\rangle + \beta_1|1\rangle)$$

we have a 2-qubit system with 4 basis states

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

and we can also 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

In general we can have arbitrary superpositions

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

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

where there is no factorization into the tensor product of two independent qubits. 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 $|\alpha_{xy}|^2$