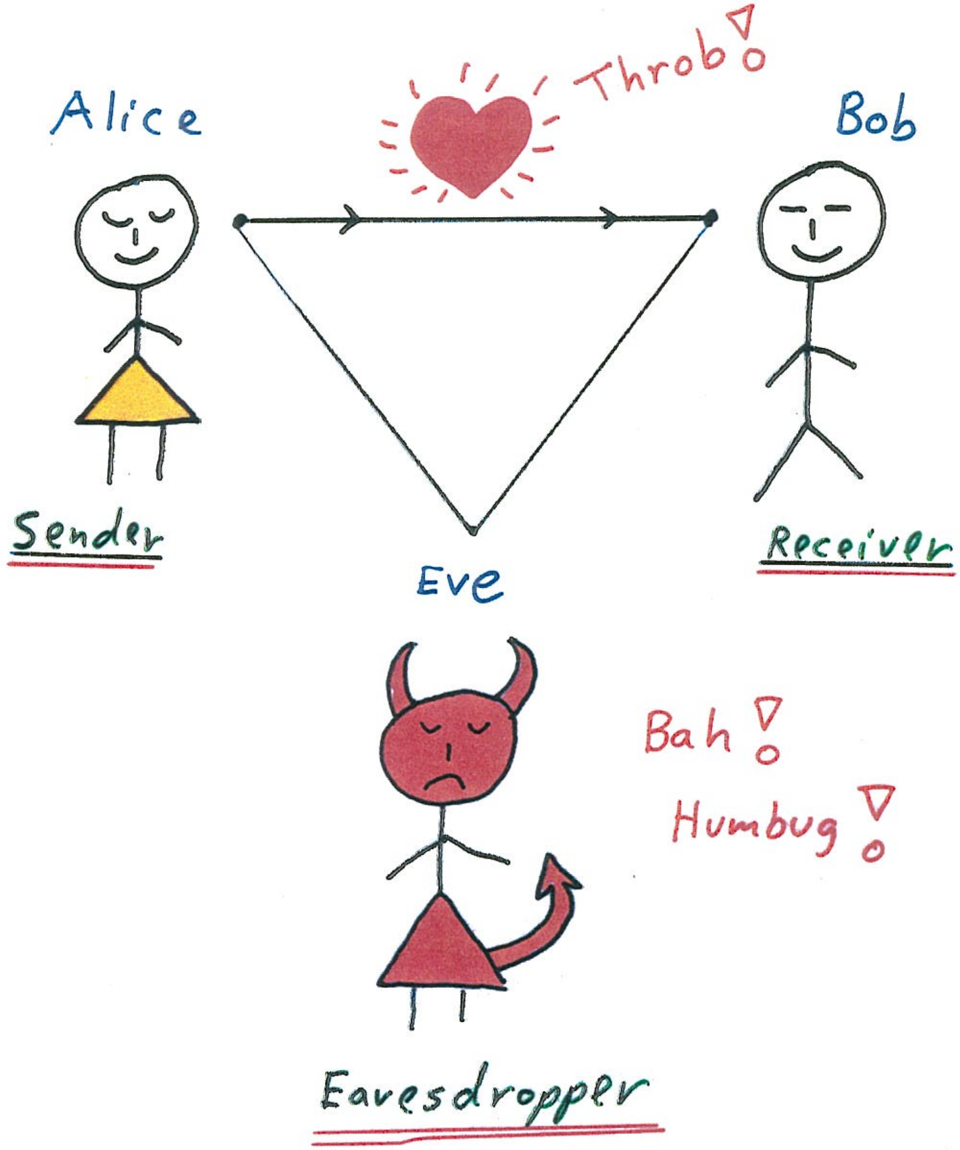
# Short Course

# Quantum Information Science

Samuel J. Lomonaco, Jr.



# Short Course Schedule

## Quantum Information Science

## Prof. Samuel J. Lomonaco, Jr., PhD

**Tuesday**, March 20, 2001 (Hilton Garden Inn, Cleveland Airport)

| | |
|---|---|
| 8:30AM – 9:45AM | A Rosetta Stone for Quantum Mechanics: Part 1 |
| 9:45AM – 10:30AM | BREAK |
| 10:30AM – 11:45AM | A Rosetta Stone for Quantum Mechanics: Part 2 |
| 11:45AM – 1:00PM | LUNCH |
| 1:00PM – 2:15PM | Quantum Entanglement & Applications |
| 2:15PM – 2:45PM | BREAK |
| 2:45PM – 4:00PM | Discussion/Problem Session |

**Wednesday**, March 21, 2001 (Hilton Garden Inn, Cleveland Airport)

| | |
|---|---|
| 8:30AM – 9:45AM | Quantum Algorithms I: Shor's algorithm |
| 9:45AM – 10:30AM | BREAK |
| 10:30AM – 11:45AM | Quantum Algorithms II: Grover's algorithm |
| 11:45AM – 1:00PM | LUNCH |
| 1:00PM – 2:15PM | Quantum Cryptography<br>Basic concepts, BB84 & B92 protocols |
| 2:15PM – 2:45PM | BREAK |
| 2:45PM – 4:00PM | Discussion/Problem Session |

# Short Course Schedule (Cont.)

## Quantum Information Science

## Prof. Samuel J. Lomonaco, Jr., PhD

**Thursday**, March 22, 2001 (Hilton Garden Inn, Cleveland Airport)

| | |
|---|---|
| 8:30AM – 9:45AM | Quantum Noise & Quantum Decoherence |
| 9:45AM – 10:30AM | BREAK |
| 10:30AM – 11:45AM | Quantum Information Theory |
| 11:45AM – 1:00PM | LUNCH |
| 1:00PM – 2:15PM | A Simple But Illustrative Example of<br>Quantum Error Correcting Codes |
| 2:15PM – 2:45PM | BREAK |
| 2:45PM – 4:00PM | Discussion/Problem Session & closing remarks |

**Friday**, March 23, 2001 (John Glenn Research Center)

Day reserved for **one-on-one informal discussions** on Quantum Information Science

Short Course

on

# Quantum Information Science

Instructor

**Samuel J. Lomonaco, Jr.**

**Dept. of Comp. Sci. & Electr. Engr.**
**University of Maryland Baltimore County**
**Baltimore, MD 21250**

Lomonaco@UMBC.EDU
http://www.csee.umbc.edu/~lomonaco





Adami, Barenco, Benioff, Bennett,
Brassard, Calderbank, Crepeau,
Deutsch, DiVencenzo,
Ekert, Einstein,
Feynman, Grover,
Heisenberg,

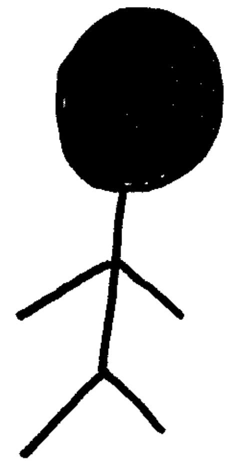
Jozsa, Knill, Laflamme, Lloyd,
Penrose, Peres, Preskill, Podolsky,
Rosen, Schumacher,
Shannon, Shor, Simon
Sloane, Schrödinger,
Towsend, Unruh,
Von Neuman,
wooters,
Yao, Zeh,
Zurek

# The Classical World





# Classical Shannon Bit



Decisive Individual

0 or 1

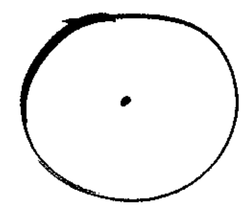
# The Quantum World



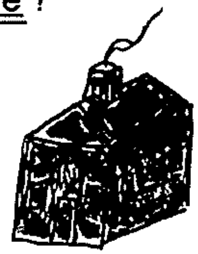


# Introducing the Qubit

???



## Where does a Qubit Live ?

$\mathcal{H}$ =  Home

**Definition.** A **Hilbert space** is a vector space over the complex numbers $\mathbb{C}$ together with an inner product

$$\mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}$$

such that

1) $\langle u_1 + u_2,\ v\rangle = \langle u_1,\ v\rangle + \langle u_2,\ v\rangle$ and
$\langle u,\ v_1 + v_2\rangle = \langle u,\ v_1\rangle + \langle u,\ v_2\rangle$
2) $\langle u,\ \lambda v\rangle = \lambda \langle u,\ v\rangle$
3) $\overline{\langle u,\ v\rangle} = \langle v,\ u\rangle$
4) For ever Cauchy sequence $u_1,\ u_2,\ u_3,\ \ldots$ in $\mathcal{H}$,

$$\lim_{n\to\infty} u_n \in \mathcal{H}$$

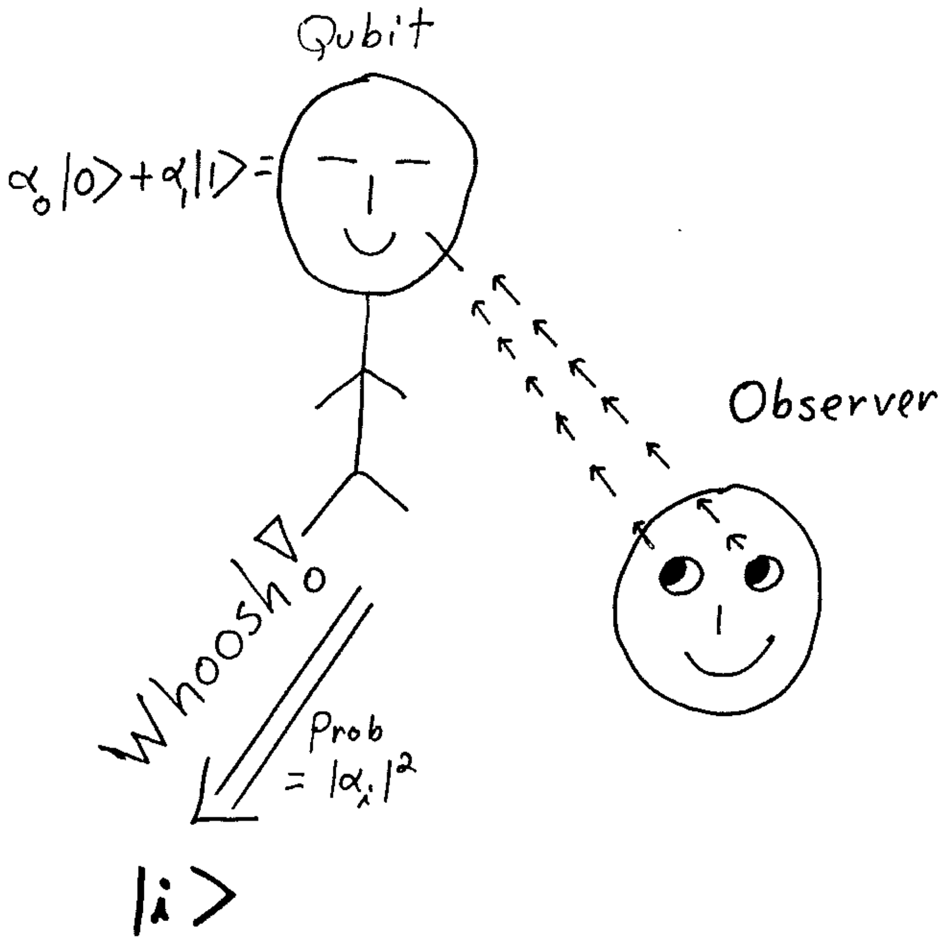
The elements of $\mathcal{H}$ will be called **kets**, and will be denoted by

$$|\ \text{label}\ \rangle$$



# A qubit is a Ket (State) in a 2-D Hilbert Space $\mathcal{H}$

# "Collapse" of the Wave Function








## Tensor Product of Hilbert Spaces

Let $\mathcal{H}$ and $\mathcal{K}$ be Hilbert spaces. The tensor product of $\mathcal{H}$ and $\mathcal{K}$, written

$$\mathcal{H} \otimes \mathcal{K}$$

is the simplest Hilbert space such that the map

$$(h, k) \longmapsto h \otimes k$$

$$\mathcal{H} \times \mathcal{K} \longrightarrow \mathcal{H} \otimes \mathcal{K}$$

is bilinear, i.e., such that

$$\begin{cases} (h_1 + h_2) \otimes k &= h_1 \otimes k + h_2 \otimes k \\ h \otimes (k_1 + k_2) &= h \otimes k_1 + h \otimes k_2 \\ (\lambda h) \otimes k &= h \otimes (\lambda k) \end{cases}$$

Moreover, we define the action of $\mathbb{C}$ on $\mathcal{H} \otimes \mathcal{K}$ as

$$\lambda (h \otimes k) \equiv (\lambda h) \otimes k = h \otimes (\lambda k)$$

for all $\lambda \in \mathbb{C}$.

So ...

$$
\begin{aligned}
|01\rangle &= |0\rangle\,|1\rangle = |0\rangle \otimes |1\rangle \\
&= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}
\end{aligned}
$$



## *Representing Integers in Quantum Mechanics*

Let $\mathcal{H}_2$ be a 2-D Hilbert space with orthonormal basis

$$|0\rangle, |1\rangle$$

Then $\mathcal{H} = \bigotimes_0^{n-1} \mathcal{H}_2$ is a $2^n$-D Hilbert space with induced orthonormal basis

$$|0\cdots 00\rangle,\ |0\cdots 01\rangle,\ |0\cdots 10\rangle,\ |0\cdots 11\rangle,\ \ldots\ ,|1\cdots 11\rangle\ ,$$

where

$$|b_{n-1}b_{n-2}\cdots b_1 b_0\rangle = |b_{n-1}\rangle \otimes |b_{n-2}\rangle \otimes \cdots \otimes |b_1\rangle \otimes |b_0\rangle$$

In $\mathcal{H}$, we represent the integer $m$ with binary expansion

$$m = \sum_{j=0}^{n-1} m_j 2^j \qquad \left(m_j = 0 \text{ or } 1 \text{ for all } j\right)$$

as the ket

$$|m\rangle = |m_{n-1}m_{n-2}\cdots m_1 m_0\rangle$$

For example,

$$|23\rangle = |010111\rangle$$

# $\underline{n}$-Qubit Register

| | | | |
|---|---|---|---|
| $\lvert\Psi_1\rangle$ | $\lvert\Psi_2\rangle$ | $\cdots$ | $\lvert\Psi_n\rangle$ |

where each Qubit lies in $\mathcal{H}$.

The contents of the $n$-Qubit register is

$$\bigotimes_{j=1}^{n} |\Psi_j\rangle = |\Psi_1\rangle\,|\Psi_2\rangle\,\ldots\,|\Psi_n\rangle = |\Psi_1\Psi_2\,\cdots\,\Psi_n\rangle \in \bigotimes_{j=1}^{n}\mathcal{H}$$



# Massive Parallelism

**Example.** For $j = 1,\ 2,\ \ldots\ ,\ n$, let

$$|\Psi_j\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Then

$$\begin{aligned}
|\Psi_1\Psi_2\,\cdots\,\Psi_n\rangle &= \bigotimes_{j=1}^{n}\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\\
&= \left(\tfrac{1}{\sqrt{2}}\right)^n (|0\rangle + |1\rangle)\,(|0\rangle + |1\rangle)\,\cdots\,(|0\rangle + |1\rangle)\\
&= \left(\tfrac{1}{\sqrt{2}}\right)^n (|00\,\ldots\,0\rangle + |00\,\ldots\,1\rangle\\
&\qquad + \ldots\,|11\,\ldots\,1\rangle)\\
&= \left(\tfrac{1}{\sqrt{2}}\right)^n \sum_{a=0}^{2^n-1} |a\rangle
\end{aligned}$$

Therefore, the $n$-qubit register contains all $n$-bit binary numbers **simultaneously!**

# Observables

What does our observer observe ?

Observables = Hermitian Operators

$$\mathcal{H} \xrightarrow{\mathcal{O}_A} \mathcal{H}$$

where

$$\overline{\mathcal{O}_A}^T = \mathcal{O}_A$$



# Observables (Cont.)

Let $|\varphi_i\rangle$ be the eigenkets of $\mathcal{O}_A$ , and let $a_i$ denote the corresponding eigenvalue , i. e.,

$$\mathcal{O}_A |\varphi_i\rangle = a_i |\varphi_i\rangle$$

In the cases we shall consider, the eigenkets form an orthonormal basis of $\mathcal{H}$

## Measurement Example

Consider a 2-D quantum system in state

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \qquad \text{where } |a|^2 + |b|^2 = 1$$

What happens when the observable $\sigma_1$ is measured?

To answer our question, we begin by expressing $|\psi\rangle$ in terms of the eigenket basis of $\sigma_1$

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \frac{a+b}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \frac{a-b}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Now if $\sigma_1$ is observed, one of two possible events will occur

| $EVENT_0$ | | $EVENT_1$ |
|---|---|---|
| $Prob = \left\|\frac{a+b}{\sqrt{2}}\right\|^2$ | OR | $Prob = \left\|\frac{a-b}{\sqrt{2}}\right\|^2$ |
| Eigenvalue $\lambda_0 = +1$ is meas. | | Eigenvalue $\lambda_1 = -1$ is meas. |
| $\|\psi\rangle \searrow \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$ | | $\|\psi\rangle \searrow \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$ |





## Important Feature of Quantum Mechanics

It is important to mention that:

**We cannot completely control the outcome of a quantum measurement**

Let $\mathcal{H}^* = Hom(\mathcal{H}, \mathbb{C})$ (Hilbert space of morphisms from $\mathcal{H}$ to $\mathbb{C}$)

We call the elements of $\mathcal{H}^*$ Bra's, and denote them as

$$\langle \text{label} |$$

There is a dual correspondence (D.C.) between $\mathcal{H}$ and $\mathcal{H}^*$, i.e.,

$$\overset{\text{Ket}}{|\psi\rangle} \overset{\text{D.C.}}{\longleftrightarrow} \overset{\text{Bra}}{\langle\psi|}$$

$\exists$ a bilinear map $\mathcal{H}^* \times \mathcal{H} \longrightarrow \mathbb{C}$ defined by

$$(\langle\psi_1|)\,(|\psi_2\rangle) \in \mathbb{C}$$

which we more simply denote by

$$\langle\psi_1|\psi_2\rangle \in \mathbb{C}$$

Bra-c-Ket



# Bras as Row Vectors over $\mathbb{C}$

Let $\mathcal{H}$ be a 2-D Hilbert space with orthonormal basis

$$\boxed{|0\rangle, |1\rangle},$$

and let

$$\boxed{\mathcal{H}^* = Hom(\mathcal{H}, \mathbb{C})}$$

be the corresponding dual Hilbert space with corresponding dual orthonormal basis

$$\boxed{\langle 0|, \langle 1|}$$

Then with respect to this basis we have

| |
|---|
| $\langle 0| = (1,0)$ and $\langle 1| = (1,0)$ |
| $\langle 0|\,a + \langle 1|\,b = (a,b)$ |

The dual correspondence

$$\boxed{\mathcal{H} \overset{\dagger}{\longleftrightarrow} \mathcal{H}^*}$$

is given by

$$\boxed{\begin{pmatrix} a \\ b \end{pmatrix} = a\,|0\rangle + b\,|1\rangle \overset{\dagger}{\longleftrightarrow} \langle 0|\,\overline{a} + \langle 1|\,\overline{b} = (\overline{a}, \overline{b})}$$

is called the "adjoint."

If

$$\left\{ \begin{array}{l} |\psi_1\rangle = a\,|0\rangle + b\,|1\rangle \\ |\psi_2\rangle = c\,|0\rangle + d\,|1\rangle \end{array} \right. ,$$

the linear transformation

$$\begin{array}{c} \mathcal{H} \overset{|\psi_1\rangle\langle\psi_2|}{\longrightarrow} \mathcal{H} \\ |\psi\rangle \longmapsto |\psi_1\rangle \langle \psi_2 \mid \psi\rangle \end{array}$$

written in matrix notation becomes the matrix outer-product

$$|\psi_1\rangle \langle\psi_2| = \begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} a\bar{c} & a\bar{d} \\ b\bar{c} & b\bar{d} \end{pmatrix}$$



Let $\mathcal{H}$ be an $N$-D Hilbert space with orthonormal basis

$$|0\rangle,\ |1\rangle,\ \ldots\ ,|N-1\rangle$$

If follow the index scheme mentioned earlier, then the matrix of the linear transformation

$$|m\rangle \langle k|$$

is an $N \times N$ matrix consisting of all zeroes with the exception of entry $(m, k)$ whivh contains a one.

For example, if $N = 4$, then

$$|2\rangle \langle 3| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which has a 1 in entry $(2, 3)$, and 0's everywhere else.

# Unitary Transfs. As Basis Changers

Let $\mathcal{H}$ be a Hilbert space with orthonormal basis

$$\boxed{|e_0\rangle, |e_1\rangle, \ldots, |e_{n-1}\rangle}\ .$$

Then for every unitary transformation

$$\boxed{U : \mathcal{H} \longrightarrow \mathcal{H}}\ ,$$

it follows that

$$\boxed{U|e_0\rangle, U|e_1\rangle, \ldots, U|e_{n-1}\rangle}$$

is also an orthonomal basis.

**Summary:** Unitary operators transform orthonormal bases into orthonormal bases.



## Spectral Decomposition Theorem<br>Matrix Perspective: Diagonalization

Let $\mathcal{H}$ be a Hilbert space with orthonormal basis

$$\boxed{|e_0\rangle, |e_1\rangle, \ldots, |e_{n-1}\rangle}\ ,$$

and let

$$\mathcal{O} : \mathcal{H} \longrightarrow \mathcal{H}$$

be an observable, which in terms of the above basis can be represented as the complex matrix

$$\mathcal{O} = \left(\mathcal{O}_{ij}\right)_{n\times n}$$

Then there exists a unitary transformation

$$U : \mathcal{H} \longrightarrow \mathcal{H}$$

for which the operator $\mathcal{O}$ when representd in this new basis is a diagonal matrix, i.e.,

$$U\mathcal{O}U^{\dagger} = \begin{pmatrix} \lambda_0 & 0 & \cdots & 0 \\ 0 & \lambda_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{n-1} \end{pmatrix}$$