# Short Course in Quantum Information Lecture 4 

Qubits and
Quantum Circuits

I. H. Deutsch, University of New Mexico Short Course in Quantum Information

## Course Info

- All materials downloadable @ website http://info.phys.unm.edu/~deutschgroup/DeutschClasses.html
- Syllabus

Lecture 1: Intro
Lecture 2: Formal Structure of Quantum Mechanics
Lecture 3: Entanglement
Lecture 4: Qubits and Quantum Circuits
Lecture 5: Algorithms
Lecture 6: Error Correction
Lecture 7: Physical Implementations
Lecture 8: Quantum Cryptography

## Course Info

- All materials downloadable @ website http://info.phys.unm.edu/~deutschgroup/DeutschClasses.html
- Syllabus

Lecture 1: Intro
Lecture 2: Formal Structure of Quantum Mechanics
Lecture 3: Entanglement
Lecture 4: Qubits and Quantum Circuits
Lecture 5: Algorithms
Lecture 6: Error Correction
Lecture 7: Physical Implementations
Lecture 8: Quantum Cryptography

## Qubits: The binary quantum system

## Quantum object in a two-dimensional Hilbert Space, $\mathbb{C}_{2}$

Logical Basis: Two chosen orthogonal states: $\{|0\rangle,|1\rangle\}$ General (pure) state: $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle=\left[\begin{array}{l}\alpha \\ \beta\end{array}\right] \quad|\alpha|^{2}+|\beta|^{2}=1$

Physical example: Photon Polarization

$$
\begin{aligned}
& |0\rangle=|H\rangle,|1\rangle=|V\rangle \quad|\psi\rangle \Rightarrow \text { Generally Elliptical } \\
& \left|D_{+}\right\rangle=\frac{1}{\sqrt{2}}\left[\begin{array}{l}
1 \\
1
\end{array}\right] \quad\left|D_{-}\right\rangle=\frac{1}{\sqrt{2}}\left[\begin{array}{c}
1 \\
-1
\end{array}\right] \\
& |R\rangle=\frac{1}{\sqrt{2}}\left[\begin{array}{l}
1 \\
i
\end{array}\right] \quad|L\rangle=\frac{1}{\sqrt{2}}\left[\begin{array}{c}
1 \\
-i
\end{array}\right]
\end{aligned}
$$

## Spin 1/2

Intrinsic Magnetic Moment of Particles (e.g. proton)


Like spin ball of charge


Stern Gerlach: Measurement of spin along z-axis (two possible outcomes)

## Spin 1/2: Repeated Measurement



Isomorphic to photon polarization measurement: HV followed by $\mathrm{D}_{+} \mathrm{D}_{\text {. }}$

General State: $\quad \alpha\left|\uparrow_{z}\right\rangle+\beta\left|\downarrow_{z}\right\rangle \quad$ Spin-up/down along some axis

## Bloch Sphere Representation

General (pure) state: $\quad|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$
Two parameters needed to specify state: relative probability and phase
Let $\quad \alpha=\cos (\theta / 2), \beta=e^{i \phi} \sin (\theta / 2) ; 0 \leq \theta<\pi, 0 \leq \phi<2 \pi$

$$
0 \leq|\alpha|^{2} \leq 1 \quad 0 \leq|\beta|^{2} \leq 1 \quad|\alpha|^{2}+|\beta|^{2}=1
$$

2D Hilbert space is the surface of a sphere


## Bloch Sphere Representation

General (pure) state: $\quad|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$
Two parameters needed to specify state: relative probability and phase
Let $\quad \alpha=\cos (\theta / 2), \beta=e^{i \phi} \sin (\theta / 2) ; 0 \leq \theta<\pi, 0 \leq \phi<2 \pi$

$$
0 \leq|\alpha|^{2} \leq 1 \quad 0 \leq|\beta|^{2} \leq 1 \quad|\alpha|^{2}+|\beta|^{2}=1
$$

2D Hilbert space is the surface of a sphere


Bloch Sphere


## Bloch Sphere Representation

General (pure) state: $\quad|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$
Two parameters needed to specify state: relative probability and phase

$$
\text { Let } \quad \alpha=\cos (\theta / 2), \beta=e^{i \phi} \sin (\theta / 2) ; 0 \leq \theta<\pi, 0 \leq \phi<2 \pi
$$

$$
0 \leq|\alpha|^{2} \leq 1 \quad 0 \leq|\beta|^{2} \leq 1 \quad|\alpha|^{2}+|\beta|^{2}=1
$$

2D Hilbert space is the surface of a sphere


## Poincaré Sphere



## Pauli Matrices

$$
X=\sigma_{x}=\left[\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right], \quad Y=\sigma_{y}=\left[\begin{array}{cc}
0 & -i \\
i & 0
\end{array}\right], Z=\sigma_{z}=\left[\begin{array}{cc}
1 & 0 \\
0 & -1
\end{array}\right]
$$

For spin-1/2, these correspond to observables that can be measured in a Stern-Gerlach analysis along $x, y, o r z$ axis respectively.

Eigenvalues, $\pm 1$. Eigenvectors, $\left\{\left|\uparrow_{x, y, z}\right\rangle,\left|\downarrow_{x, y ; z}\right\rangle\right\}$
Incompatible Measurements. Commutator: $\left[\sigma_{i}, \sigma_{j}\right]=2 i \varepsilon_{i j k} \sigma_{k}$

$$
\text { e.g. } \quad X Y-Y X=2 i Z
$$

Other useful properties:

- Anticommute: $X Y=-Y X, X Z=-Z X, Y Z=-Z Y$
- Hermitian and Unitary: $X^{2}=Y^{2}=Z^{2}=I$


## General Pauli Observable

$$
\sigma_{\mathrm{n}}=\cos \theta Z+\sin \theta(\cos \phi X+\sin \phi Y)
$$

Eigenvalues: $\pm 1$. Eigenvectors


Quantum Dynamics (closed system): Unitary Matrix
Rotation on the Bloch Sphere (axis/angle)

$$
\begin{aligned}
& R_{\mathbf{n}}(\Theta)=\exp \left\{-i \Theta \sigma_{\mathbf{n}} / 2\right\} \\
&=\cos (\Theta / 2) I-i \sin (\Theta / 2) \sigma_{\mathbf{n}} \\
& \mathrm{U}(2): \quad e^{i \alpha} R_{\mathbf{n}}(\Theta)
\end{aligned}
$$



## Example: Hadamard Matrix

$H=i R_{\frac{\mathbf{e}_{x}+\mathbf{e}_{y}}{\sqrt{2}}}(\pi)=i\left(\cos \frac{\pi}{2} I-i \sin \frac{\pi}{2}\left(\frac{X+Z}{\sqrt{2}}\right)\right)=\frac{X+Z}{\sqrt{2}}=\frac{1}{\sqrt{2}}\left[\begin{array}{cc}1 & 1 \\ 1 & -1\end{array}\right]$
Rotation about $\frac{\mathbf{e}_{x}+\mathbf{e}_{z}}{\sqrt{2}}$ by $180^{\circ}$

Change of basis X-->Z

$$
\begin{array}{lr}
H Z H^{\dagger}=X & H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)=\left|\uparrow_{x}\right\rangle \equiv|+\rangle \\
H X H^{\dagger}=Z & H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)=\left|\downarrow_{x}\right\rangle \equiv|-\rangle
\end{array}
$$

## Example: Pauli Operations as Unitaries

$$
\begin{gathered}
X=i R_{x}(\pi)=i \exp (-i \pi X / 2)=\left[\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right] \\
X|0\rangle=|1\rangle \quad X|1\rangle=|0\rangle \quad \text { Bit Flip ("NOT") } \\
Z=i R_{z}(\pi)=i \exp (-i \pi Z / 2)=\left[\begin{array}{cc}
1 & 0 \\
0 & -1
\end{array}\right]
\end{gathered}
$$

$$
Z|0\rangle=|0\rangle \quad Z|1\rangle=-|1\rangle \quad \text { Sign Change, Phase Flip }
$$

Note: Action of $X$ and $Z$ reversed in "Hadmard Basis"

$$
\begin{aligned}
& X|+\rangle=X(|0\rangle+|1\rangle)=X|0\rangle+X|1\rangle=|1\rangle+|0\rangle=|+\rangle \\
& X|-\rangle=X(|0\rangle-|1\rangle)=X|0\rangle-X|1\rangle=|1\rangle-|0\rangle=-|-\rangle \\
& Z|+\rangle=X(|0\rangle+|1\rangle)=Z|0\rangle+Z|1\rangle=|0\rangle-|1\rangle=|-\rangle \\
& Z|-\rangle=Z(|0\rangle-|1\rangle)=Z|0\rangle-Z|1\rangle=|0\rangle+|1\rangle=|+\rangle
\end{aligned}
$$

## Multiple Qubits

n qubits $=\mathrm{n}$ two-level quantum systems (e.g. n spin-1/2 particles)
Tensor product Hilbert space: $\left(\mathbb{C}_{2}\right)^{\otimes n}=\mathbb{C}_{2^{n}}$
Dimension $N=2^{n}$ orthogonal states
Logical Basis: $\left\{|x\rangle \mid x=0,1, \ldots, 2^{n}-1\right\} \quad x$ in binary.

$$
\begin{array}{cl}
\text { E.g. } & |0\rangle \equiv|0\rangle|0\rangle\langle 0\rangle,|1\rangle \equiv|0\rangle|0\rangle|1\rangle,|2\rangle \equiv|0\rangle|1\rangle|0\rangle,|3\rangle \equiv|0\rangle|1\rangle|1\rangle \\
n=3, N=8 & |4\rangle \equiv|1\rangle|0\rangle|0\rangle,|5\rangle \equiv|1\rangle|0\rangle|1\rangle,|6\rangle \equiv|1\rangle|1\rangle|0\rangle,|7\rangle \equiv|1\rangle|1\rangle|1\rangle
\end{array}
$$

Photon polarization: $|4\rangle=|V\rangle|H\rangle|H\rangle$
General State: $|\psi\rangle=\sum_{x=0}^{2^{n}-1} c_{x}|x\rangle \quad$ Can be entangled

## Bell Basis

Bipartite (two qubits) Logical Basis: $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$
Simulate Eigenvectors of: $Z \otimes I, I \otimes Z \quad$ Two bits specify state

Bell Basis

$$
\begin{array}{ll}
\left|\Phi^{(+)}\right\rangle=\frac{1}{\sqrt{2}}(|0,0\rangle+|1,1\rangle), & \left|\Phi^{(-)}\right\rangle=\frac{1}{\sqrt{2}}(|0,0\rangle-|1,1\rangle) \\
\left|\Psi^{(+)}\right\rangle=\frac{1}{\sqrt{2}}(|0,1\rangle+|1,0\rangle), & \left|\Psi^{(-)}\right\rangle=\frac{1}{\sqrt{2}}(|0,1\rangle-|1,0\rangle)
\end{array}
$$

Eigenvectors of $X \otimes X$
$Z \otimes Z$

Eigenvalues $\pm 1$
(phase bit)

Eigenvalues $\pm 1$
(parity bit)

## Global Properties in Joint Operators

$$
Z \otimes Z\left|\Phi^{( \pm)}\right\rangle=Z|0\rangle \otimes Z|0\rangle \pm Z|1\rangle \otimes Z|1\rangle=|0,0\rangle \pm|1,1\rangle=+\left|\Phi^{( \pm)}\right\rangle
$$

$$
Z \otimes Z\left|\Psi^{( \pm)}\right\rangle=Z|0\rangle \otimes Z|1\rangle \pm Z|0\rangle \otimes Z|1\rangle=-|0,0\rangle \mp|1,1\rangle=-\left|\Psi^{( \pm)}\right\rangle
$$

$$
X \otimes X\left|\Phi^{( \pm)}\right\rangle=X|0\rangle \otimes X|0\rangle \pm X|1\rangle \otimes X|1\rangle=|1,1\rangle \pm|0,0\rangle= \pm\left|\Phi^{( \pm)}\right\rangle
$$

$$
X \otimes X\left|\Psi^{( \pm)}\right\rangle=X|0\rangle \otimes X|1\rangle \pm X|1\rangle \otimes X|0\rangle=|1,0\rangle \pm|0,1\rangle= \pm\left|\Psi^{( \pm)}\right\rangle
$$

Eigenvalue of $Z \otimes Z$. Are you $\Phi$ or $\Psi$ ? (parity bit)
Eigenvalue of $X \otimes X$. Are you + or -? (phase bit)
Alternative notation: $\left\lvert\, \begin{array}{cc} & \begin{array}{l}\text { phase bit } \\ \text { ab }\end{array} \\ \text { parity bit }\end{array} \quad \begin{aligned} X \otimes X\left|\beta_{a b}\right\rangle & =(-1)^{a}\left|\beta_{a b}\right\rangle \\ Z \otimes Z\left|\beta_{a b}\right\rangle & \rangle=(-1)^{b}\left|\beta_{a b}\right\rangle\end{aligned}\right.$

$$
\left|\beta_{00}\right\rangle=\left|\Phi^{(+)}\right\rangle,\left|\beta_{01}\right\rangle=\left|\Psi^{(+)}\right\rangle,\left|\beta_{10}\right\rangle=\left|\Phi^{(-)}\right\rangle,\left|\beta_{11}\right\rangle=\left|\Psi^{(-)}\right\rangle
$$

## Entanglement as a Resource:

Suppose Alice and Bob share prior entanglement.
Can Alice communicate with Bob in ways not possible classically?

## Entanglement as a Resource:

Suppose Alice and Bob share prior entanglement.
Can Alice communicate with Bob in ways not possible classically?


Alice

Yes! But no information transfer faster than speed of light (causality).

## E.g. Superdense Coding

## Superdense Coding

- Alice wants to send Bob two bits of information.
- Message one of four secrets: $\{00=\mathrm{I}, \quad 01=\mathrm{X}, \quad 10=\mathrm{Z}, 11=\mathrm{Y}\}$.
- She has in her possession one qubit. If she manipulates it any way she likes, sends this to Bob, and he measures it, he can learn no more than ONE bit of information.
- If Alice's qubit is entangled with one already in Bob's possession, and he performs a joint measurement, he can extract TWO bits of information.
- Alice thus encodes a two-bit message in her one qubit, correlated with Bob's qubit ---> superdense coding! Like effecting a four sized die while only manipulating a two-sized object.


## Local operation changes global state

$$
\begin{array}{r}
X_{A} \otimes I_{B}\left|\Phi^{(+)}\right\rangle=X_{A}|0\rangle \otimes I_{B}|0\rangle+X_{A}|1\rangle \otimes I_{B}|1\rangle=|1,0\rangle+|0,1\rangle=\left|\Psi^{(+)}\right\rangle \\
Z_{A} \otimes I_{B}\left|\Phi^{(+)}\right\rangle=Z_{A}|0\rangle \otimes I_{B}|0\rangle+Z_{A}|1\rangle \otimes I_{B}|1\rangle=|0,0\rangle-|1,1\rangle=\left|\Phi^{(-)}\right\rangle \\
Y_{A} \otimes I_{B}\left|\Phi^{(+)}\right\rangle=Y_{A}|0\rangle \otimes I_{B}|0\rangle+Y_{A}|1\rangle \otimes I_{B}|1\rangle=i(|0,0\rangle-|1,1\rangle)=\left\langle i \mid \Psi^{(-)}\right\rangle \\
\text {irrelevant overall phase }
\end{array}
$$

- By acting on her qubit locally, Alice can effect the state of the joint state.
- Bob can detect this action with ONLY his qubit. Must measure BOTH qubits.


## Superdense Coding



Alice
I. H. Deutsch, University of New Mexico Short Course in Quantum Information

## Superdense Coding



Alice
I. H. Deutsch, University of New Mexico Short Course in Quantum Information

## Superdense Coding



Alice
I. H. Deutsch, University of New Mexico Short Course in Quantum Information

## Superdense Coding



Alice

## Quantum Teleportation

Quantum Channel


Alice wants to send Bob a qubit in an unknown (pure) state. The quantum channel connecting them is noisy so the qubit would be corrupted if she transmitted. She cannot measure the qubit and then call Bob to have give make his own copy because her measurement will project it onto an eigenstate.

## Quantum Teleportation



## Quantum Teleporation: The Math

Three qubit joint state of Alice, Bob, and "Victor" who prepared $|\psi\rangle$ :

$$
\begin{gathered}
|\chi\rangle=|\psi\rangle_{V} \otimes\left|\Phi^{(+)}\right\rangle_{A B}=\left(\alpha|0\rangle_{V}+\beta|1\rangle_{V}\right) \otimes\left(|0\rangle_{A} \otimes|0\rangle_{B}+|1\rangle_{A} \otimes|1\rangle_{B}\right) \\
=\frac{1}{2}\left[\left(|0\rangle_{V} \otimes|0\rangle_{A}+|1\rangle_{V} \otimes|1\rangle_{A}\right) \otimes\left(\alpha|0\rangle_{B}+\beta|1\rangle_{B}\right)+\left(|0\rangle_{V} \otimes|0\rangle_{A}-|1\rangle_{V} \otimes|1\rangle_{A}\right) \otimes\left(\alpha|0\rangle_{B}-\beta|1\rangle_{B}\right)\right. \\
\left.+\left(|0\rangle_{V} \otimes|1\rangle_{A}+|1\rangle_{V} \otimes|0\rangle_{A}\right) \otimes\left(\alpha|1\rangle_{B}+\beta|0\rangle_{B}\right)+\left(|0\rangle_{V} \otimes|1\rangle_{A}-|1\rangle_{V} \otimes|0\rangle_{A}\right) \otimes\left(\alpha|1\rangle_{B}-\beta|0\rangle_{B}\right)\right] \\
|\chi\rangle=\frac{1}{2}\left(\left|\Phi^{(+)}\right\rangle_{V A} \otimes|\psi\rangle_{B}+\left|\Phi^{(-)}\right\rangle_{V A} \otimes Z|\psi\rangle_{B}+\left|\Psi^{(+)}\right\rangle_{V A} \otimes X|\psi\rangle_{B}-i\left|\Psi^{(-)}\right\rangle_{V A} \otimes Y|\psi\rangle_{B}\right)
\end{gathered}
$$

A measurement by Alice in Bell-basis leaves Bob's qubit in one of four states:

$$
\left\{|\psi\rangle_{B}, Z|\psi\rangle_{B}, X|\psi\rangle_{B}, Y|\psi\rangle_{B}\right\}
$$

Alice uses the classical channel to tell Bob which Bell state she found. Bob can then put his qubit in the unknown state, through application of a Pauli.

## Digital (Classical) Information Processing

Classical Computing: Function on n-bit string $\quad F\left(\{0,1\}^{N}\right)=\{0,1\}^{M}$
Function constructed from operations on small collections of bits
"Logic Gates"


| in | out |
| :---: | :--- |
| 0 | 1 |
| 1 | 0 |


| in- <br> a | in- <br> $b$ | out |
| :---: | :---: | :---: |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |



| in- <br> a | in- <br> $b$ | out |
| :---: | :---: | :---: |
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Note: Not is reversible. XOR and NAND are not.
Can be made reversible with extra bits.
NAND (plus copy) is UNIVERSAL for computation.

## Digital Quantum Information Processing

Map on n-qubits is a $2^{n} \times 2^{n}$ unitary matrix - Reversible.
Single qubit logic gates: Rotations on the Bloch sphere.

$$
\begin{aligned}
& \text { E.g. } \quad \mathrm{NOT}=X=i R_{x}(\pi)=\left[\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right] \\
& \sqrt{\mathrm{NOT}}=e^{i \pi / 4} R_{x}(\pi / 2)=\frac{e^{i \pi / 4}}{\sqrt{2}}\left[\begin{array}{cc}
1 & -i \\
-i & 1
\end{array}\right] \\
& \text { Hadamard } \quad H=\left[\begin{array}{cc}
1 & 1 \\
1 & -1
\end{array}\right]
\end{aligned}
$$

## Logic Tables and Quantum Circuits

Action of unitary determined by action on logical basis:

\[

\]

$$
H|x\rangle=|x\rangle+(-1)^{x}|\bar{x}\rangle
$$

| in | out |
| :--- | :---: |
| $\|0\rangle$ | $\|0\rangle+\|1\rangle$ |
| $\|1\rangle$ | $\|0\rangle-\|1\rangle$ |

Quantum Circuit


## Two Qubit Logic

Classical XOR: $\quad(x, y) \rightarrow y \oplus x \quad$ (binary addition)
Classical Reversible XOR: $(x, y) \rightarrow(x, y \oplus x)$

"Control NOT":
Flip the target when Control is 1 .

| $\mathrm{C}_{\text {in }}^{\text {in }}$ | ${ }_{\text {O }}^{\text {out }}$ |
| :---: | :---: |
| 00 | 00 |
| 01 | 01 |
| 10 | 11 |
| 11 | 10 |

Transformation on logical basis states is a unitary matrix!

## Controlled Unitaries: If-Then in QC



Apply $U$ to the second qubit when the first qubit is logical-1.

$$
\begin{aligned}
& \text { Matrix in logical basis: } \\
& \{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}
\end{aligned} \quad C_{U}=\left[\begin{array}{cccc}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & U \\
0 & 0 & U
\end{array}\right]
$$

CNOT=C ${ }_{x}$


CPhase $=\mathrm{C}_{z}$

$$
C N O T=\left[\begin{array}{llll}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{array}\right]
$$

$$
\text { CPhase }=\left[\begin{array}{cccc}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1
\end{array}\right]
$$

## CNOT is Entangling

Consider the following circuit


$$
\begin{aligned}
& \left|\psi_{\text {in }}\right\rangle=|0\rangle|0\rangle \\
& \left|\psi_{1}\right\rangle=(|0\rangle+|1\rangle)|0\rangle=|0\rangle|0\rangle+|1\rangle|0\rangle \\
& \left|\psi_{\text {out }}\right\rangle=|0\rangle|0\rangle+|1\rangle|1\rangle=\left|\Phi^{(+)}\right\rangle \quad \text { Entangled State }
\end{aligned}
$$

By putting the control in a quantum super position, the circuit undergoes a superposition of classical computations.

## Quantum Parallelism

## Universal Quantum Logic

An arbitrary unitary matrix on $n$-qubits can be constructed from a sequence of unitaries on subsets of qubits.

## Universal set.

All single qubit rotations + one entangling two-qubit unitary (e.g. CNOT) acting between pairs on a connected graph.

Note: Any single qubit unitary can be constructed from discrete set. E.g. $\left\{H, T \equiv R_{z}(\pi / 4)\right\}$

Note: Arbitrary unitary will require exponential number of gates. Quantum algorithm = Efficiently implementable useful unitary that scales like a polynomial in $n$, for which the answer can be found by measuring in logical basis with high probability.

