18-819F: Introduction to Quantum Computing 47-779/785: Quantum Integer Programming & Quantum Machine Learning

Introduction to Quantum Gates and Circuits

Lecture 10

2021.10.05.

Electrical & Computer
ENGINEERING

TEPPER

USRA Universities Space Research Association

Agenda

- Review of classical gates and circuits
  - The "not", "and", and "or" operators (gates)
  - Reversible CNOT gate

- Qubit representation on the complex polar coordinate system
  - Qubit as a 3D vector on the Bloch sphere
  - Qubit evolution and transformations as rotations on the unit Bloch sphere
  - Gate representation of qubit operations
  - Gate based circuits for qubit transformations

- No Cloning theorem

Logic

- George Boole introduced the notion that certain aspects of logic could be represented algebraically.

- The most common logical operators that connect logical statements are *not*, *and* and *or*.

- When used to join statements, the operators can help establish the combined truth or falseness of a compound statement.

- For example: if "$P = i + 1 = even,$ for $i = 1, 2, 3 \ldots n$" and "$Q = 2i = even,$ for $i = 1,2,3 \ldots n$" one realizes that each of the statements can either be true (T) or false (F) and nothing else. A truth table specifying the joint truthfulness of "$P \ and \ Q$" and "$P \ or \ Q$" can be created as indicated on the right; the "or" here is inclusive "or."

P	Q	P and Q
T	T	T
F	T	F
T	T	T
⋮	⋮	⋮

P	Q	P or Q
T	T	T
F	T	T
T	T	T
⋮	⋮	⋮

Electrical & Computer ENGINEERING

TEPPER

USRA Universities Space Research Association

General Logical Statements and Operators

- The logical operator "or" usually has two definitions: one is inclusive and the other exclusive, meaning that in the former case if both P and Q are true, then "P or Q" is true; in the later, if P is true and Q is true, then "P or Q" is false. The exclusive "or" is symbolized as "P⊕Q".

- For P and Q, the "not" operator signifies falseness of P as ¬P and that of Q as ¬Q.

- Statements P and Q can be general statements where each is either true or false on its own right. Any of the two "joining" logical operators "and" and "or" can be used to combine them after or before application of the "not" operator. The combined statement can then be written in Boolean algebraic form.

- The symbols for the logical operators are "not ≔ ¬", "and ≔∩", "or ≔∪", and "xor ≔⊕".

Boolean Algebra

P	Q	$P \cup Q$	$P \oplus Q$	$\neg P$	$\neg Q$	$\neg P \cap \neg Q$	$\neg(\neg P \cap \neg Q)$
F	F	F	F	T	T	T	F
F	T	T	T	T	F	F	T
T	F	T	T	F	T	F	T
T	T	T	F	F	F	F	T

- A consequence of joining logical statements with logical operators is Boolean algebraic statements. The example above shows how the two general statements P and Q can be joined with any of the logical operators and then re-expressed in Boolean algebraic form.

- The third and last columns of the Table above are logically equivalent, allowing one to write

$$P \cup Q = \neg(\neg P \cap \neg Q) \quad \text{Eqn. (10.1)}.$$

- One also deduces that the 4th column in the Table is equivalent to column combinations (1, 2, 5, &6):

  - $P \oplus Q = (P \cap \neg Q) \cup (\neg P \cap Q)$ Eqn. (10.2).
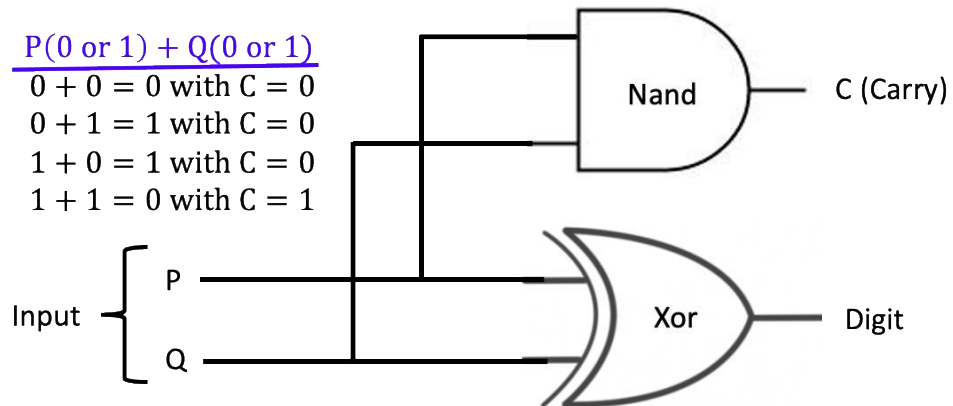
Nand Operator (and Gate)

- We have shown that logical statements that are either true or false have a binary character to them that is easily represented by either 1 or 0.

- With 1 and 0 standing in for T and F, the truth table for our general P and Q statements using only the "and" and "not" operators is illustrated on the right.

- Notice that $\neg Q \equiv \neg(Q \cap Q)$, which indicates that the "not-and" operator or "Nand" can replace other operators; the Nand is therefore a universal operator (gate).

P	Q	$P \cap Q$	$\neg(P \cap Q)$	$Q \cap Q$	$\neg(Q \cap Q)$
0	0	0	1	0	1
0	1	0	1	1	0
1	0	0	1	0	1
1	1	1	0	1	0

Electrical & Computer ENGINEERING

TEPPER

USRA Universities Space Research Association

(Classical) Gates

- It was realized early and demonstrated by Claude Shannon (of information theory fame) that since logic could be expressed in algebraic terms, then switches could be built that could emulate the 1's and 0's of the logical algebraic expressions.

- The combination of switches corresponding to the *binary operators* are called *gates.* Common gates include the "or", "nor", "and", and "nand" gates. The "nand" gate is said to be *functionally complete* which means it is *universal;* it can replace any other logical gate.

- Gates are the building blocks of modern computers and are the basis for implementing computation. We have already established (in slide 6, when you replace T with 1 and F with 0) that the "exclusive or" operator has the following properties:
$$0 \oplus 0 = 0, \qquad 0 \oplus 1 = 1, \qquad 1 \oplus 0 = 1, \qquad 1 \oplus 1 = 0.$$

- The "exclusive or" operator and the "and" operator can be used to build a half-adder for computing.

Electrical & Computer ENGINEERING

TEPPER

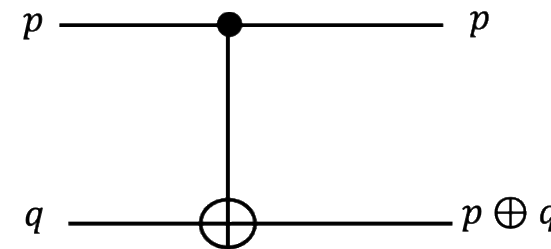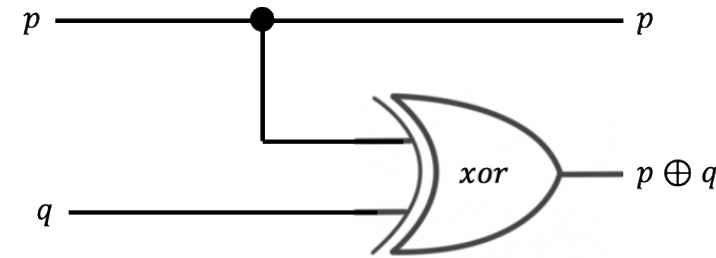USRA Universities Space Research Association

(Classical) Gates and Circuits

- Classical computing circuits are created by connecting gates that represent certain logical operations derived from algebraic simplification of Boolean functions. The gates are connected using wires; whenever necessary, one can *fan-out* signals to share with other gates (as long as there is sufficient signal to drive the sharing inputs) .

- The half-adder circuit described in the previous slide can be implemented using an "exclusive or" gate and an "and" gate. A full adder circuit can be implemented with just the universal "nand" gate.

- Observe that the "copying" of information as indicated in the sharing of signals by the "xor" and the "and " gates, while allowed for classical circuits such as the half-adder example here, is prohibited in quantum gate circuits .

P(0 or 1) + Q(0 or 1)
0 + 0 = 0 with C = 0
0 + 1 = 1 with C = 0
1 + 0 = 1 with C = 0
1 + 1 = 0 with C = 1

Input
P
Q

Nand — C (Carry)

Xor — Digit

Electrical & Computer ENGINEERING

TEPPER

USRA Universities Space Research Association

Reversible Classical Operators (Gates)

- Sometimes it is of interest to determine the input of a gate given the output. This is generally not possible for most classical gates since most gates have two inputs and one output.

- If a gate can perform a function that provides an output from which one can determine the input, then such a gate is called reversible.

- The only known classical gate that is reversible is the Controlled Not Gate or CNOT gate. The CNOT function is defined as $f(p, q) = (p, p \oplus q)$. The circuit diagram, symbol, and the truth table for the CNOT gate are shown on the right.

- For each pair of output, there is only one pair of input that correspond to it.

Input		Output	
p	q	p	$p \oplus q$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Electrical & Computer
ENGINEERING

TEPPER

USRA Universities Space Research Association

9

The Qubit in Complex Number Polar Representation

- In a previous Lecture, we defined the qubit as an object in complex two-dimensional space, $\mathbb{C}^2$. The definition is repeated below in three variations.

$$\begin{aligned}
|\psi> \quad &= \alpha|0> +\beta|1> \\
&= \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} \\
&= \begin{pmatrix}\alpha\\\beta\end{pmatrix}
\end{aligned}\right\} \quad \text{where } |\alpha|^2 + |\beta|^2 = 1, \text{ Eqn. (10.3).}$$

- The amplitude coefficients α and β are complex numbers, which permits us to rewrite the first version of the qubit definition in Eqn. (10.3) using the polar form of complex numbers; thus

$$|\psi\rangle = r_\alpha e^{j\vartheta_\alpha}|0\rangle + r_\beta e^{j\vartheta_\beta}|1\rangle \quad \text{Eqn. (10.4).}$$

- To simplify (10.4), we invoke the fact that phase factors in state vectors have no physical significance in measurable quantities; we can therefore multiply (10.4) by a phase $e^{-j\vartheta_\alpha}$ without changing the physics;

$$\begin{aligned}
|\tilde\psi\rangle \quad &= e^{-j\vartheta_\alpha}\left(r_\alpha e^{j\vartheta_\alpha}|0\rangle + r_\beta e^{j\vartheta_\beta}|1\rangle\right) \\
&= r_\alpha|0\rangle + r_\beta e^{j(\vartheta_\beta-\vartheta_\alpha)}|1\rangle \\
&= r_\alpha|0\rangle + r_\beta e^{j\vartheta}|1\rangle
\end{aligned}\right\} \quad \text{Eqn. (10.5)}$$

Electrical & Computer ENGINEERING

TEPPER

USRA Universities Space Research Association

The Qubit in Spherical Coordinates

- Our new state vector from (10.5) inherits the constraint on the original state vector (10.3), thus

$$|\tilde{\psi}\rangle = r_\alpha|0\rangle + r_\beta e^{j\vartheta}|1\rangle \text{ with constraint } |r_\alpha|^2 + \left|r_\beta e^{j\vartheta}\right|^2 = 1 \text{ Eqn. (10.5).}$$

- The constraint on (10.5) is rewritten as $|\alpha|^2 + |\beta|^2 = 1 = |r_\alpha|^2 + |x + jy|^2 = r_\alpha^2 + x^2 + y^2$ Eqn. (10.6).

- Note that we have replaced $e^{j(\vartheta_\beta - \vartheta_\alpha)}$ with $e^{j\vartheta}$ in (10.4) and $r_\beta e^{j\vartheta}$ with $x + jy$ in (10.5); In Eqn. (10.6) is the first clue that tells us that the complex amplitudes can be thought of as living in 3D space, with $r_\alpha \equiv z$.

- In geometry, the spherical coordinate system and the Cartesian coordinate system are related through the expressions:

$$x = r \sin\vartheta \cos\varphi, \quad y = r \sin\vartheta \, \sin\varphi, \quad z = r \cos\vartheta \quad \text{for } 0 \leq \vartheta < \pi \text{ and } 0 \leq \varphi < 2\pi \text{ Eqn. (10.7).}$$

- We can therefore rewrite (10.5) using the relationships in (10.7), with $r = 1$, to get:

$$\left.\begin{array}{rcl} |\tilde{\psi}\rangle & = & z|0\rangle + (x + jy)|1\rangle \\ |\tilde{\psi}\rangle & = & \cos\vartheta|0\rangle + \sin\vartheta(\cos\varphi + j\sin\varphi)|1\rangle \\ |\tilde{\psi}\rangle & = & \cos\vartheta|0\rangle + e^{j\varphi}\sin\vartheta|1\rangle \end{array}\right\} \text{ Eqn. (10.8).}$$

The Quantum Bit as a 3D Unit Vector

- To properly embed the complex amplitudes into 3D space, we must recognize that ϑ is restricted between 0 and π; for the sphere we are interested in, it must be extended to 2π, or we must use a definition that is half the angle ϑ in (10.8).

- We rewrite e(10.8) to take account of this fact, thus

$$|\tilde{\psi}\rangle = \cos\frac{\vartheta}{2}|0\rangle + e^{j\varphi}\sin\frac{\vartheta}{2}|1\rangle \quad \text{Eqn. (10.9).}$$

- We now note that our original qubit (10.4) only differs from (10.9) by a phase factor, i.e., $|\tilde{\psi}\rangle = e^{-j\vartheta_\alpha}|\psi\rangle$. According to one of the Axioms of Quantum Mechanics, the average value of any real physical quantity represented by a Hermitian operator, $\hat{H}$, is given by $\langle\psi|\hat{H}|\psi\rangle = \langle\tilde{\psi}|\hat{H}|\tilde{\psi}\rangle$, independent of any phase factor. We can therefore invoke the equality of $|\psi\rangle$ to $|\tilde{\psi}\rangle$; thus

$$|\psi\rangle = |\tilde{\psi}\rangle = \cos\frac{\vartheta}{2}|0\rangle + e^{j\varphi}\sin\frac{\vartheta}{2}|1\rangle = \begin{pmatrix} \cos\frac{\vartheta}{2} \\ e^{j\varphi}\sin\frac{\vartheta}{2} \end{pmatrix} \quad \text{Eqn. (10.10).}$$

- The last equality of Eqn. (10.10) is equivalent to out original vector version of the qubit in Eqn. (10.3).

Electrical & Computer ENGINEERING

TEPPER

USRA Universities Space Research Association

12

The Qubit on the Bloch Unit Sphere

- The last expression of Eqn. (10.10) indicates how the qubit is a point on a circle with unit radius on a 2D plane. This is illustrated on the right. However, according to (10.8), the qubit can also be considered as a 3D vector that lives on a sphere of unit radius, shown alongside the circle. Both interpretations are valid.
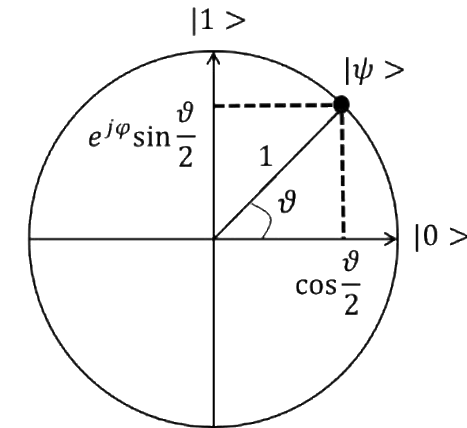

- To determine the location of the quantum state of $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, we simply equate this to the last expression of (10.10) and find the relevant angles:

- $\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \cos\frac{\vartheta}{2} \\ e^{j\varphi}\sin\frac{\vartheta}{2} \end{pmatrix} \implies \vartheta = \pi$ and $\varphi = 0$. This is pointing in the negative z-axis.

- For the state $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\vartheta}{2} \\ e^{j\varphi}\sin\frac{\vartheta}{2} \end{pmatrix} \implies \vartheta = 0$ and $\varphi = 0$.

- The $|0\rangle$ state is pointing in the positive z-axis while the state $|1\rangle$ states is pointing in the negative z-direction. These states are shown on the spherical graphic. Single-qubit state vectors correspond to points on the Bloch sphere.

Electrical & Computer ENGINEERING

TEPPER

USRA Universities Space Research Association
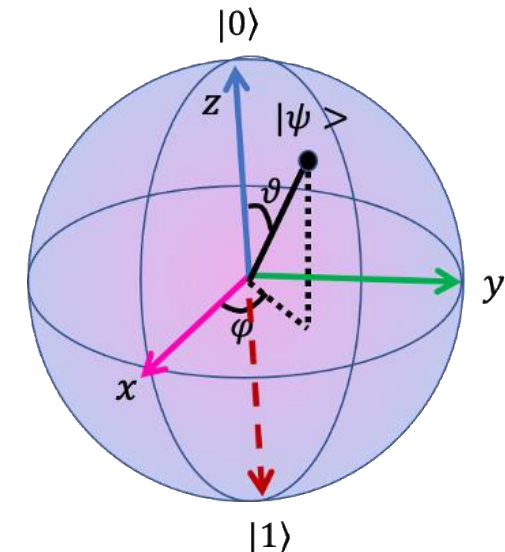
Operations on a Single Qubit

- Now that we know what a qubit is, we would like to know what kind of operations are allowed on it.

- Quantum operations correspond to evolution of the state vector, $|\psi\rangle$, according to the Schrodinger equation,

$$j\hbar \frac{\partial |\psi\rangle}{\partial t} = \hat{H}|\psi\rangle \quad \text{Eqn. (10.11).}$$

- Assuming an initial state $|\psi(t = 0)\rangle$, the solution of (10.11) can be obtained by integration as

$$|\psi(t)\rangle = e^{-j(\hat{H}/\hbar)t}|\psi(t = 0)\rangle = U|\psi(t = 0)\rangle \quad \text{Eqn. (10.12).}$$

- Since a state vector must remain normalized and for the qubit in particular, the length must not change, this means the evolution operator, U, in (10.12) must be unitary.

- Since $U = e^{-j(\hat{H}/\hbar)t}$, the unitarity requirement means

$$UU^\dagger = U^\dagger U = \mathbb{I} \quad \text{Eqn. (10.13).}$$

- From the definition of the qubit in (10.3) as a 2D vector, it must follow that U is a unitary 2×2 matrix operator, $U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$.

Rotations on the Bloch Sphere

- Temporal evolution of the qubit or its manipulations over time are equivalent to rotations of the qubit on the surface of the Bloch Sphere.

- For an arbitrary rotation of the qubit on the Bloch sphere by an angle $\tilde{\theta}$, one can write the unitary operator for carrying out this rotation as

$$U = e^{j\frac{\vartheta}{2}\rho} = \cos\frac{\vartheta}{2}\mathbb{I} + j\sin\frac{\vartheta}{2}\boldsymbol{\rho} \quad \text{Eqn. (10.14),}$$

- To obtain the expression in red, expand the exponential as a series, then collect terms to identify the trigonometric functions. We define $\boldsymbol{\rho} = \hat{n}.\boldsymbol{\rho}_i = xX + yY + zZ$ in Eqn. (10.14), and further provide the unit normal vector on the Bloch sphere as $\hat{n} = \hat{x} + \hat{y} + \hat{z}$ $(x = \sin\vartheta\cos\varphi, y = \sin\vartheta\sin\varphi, z = \cos\vartheta)$; $\boldsymbol{\rho}_i$ is a "vector" comprised of the orthonormal Pauli basis "vectors" on the Bloch sphere. These "vectors" are the Pauli matrices we have discussed before and are listed below.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -j \\ j & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{Eqn. (10.15).}$$

- From (10.14) and (10.15), rotations in various axes are therefore given by

$$R_x(\vartheta) = \begin{pmatrix} \cos\frac{\vartheta}{2} & j\sin\frac{\vartheta}{2} \\ j\sin\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{pmatrix}, \quad R_y(\vartheta) = \begin{pmatrix} \cos\frac{\vartheta}{2} & \sin\frac{\vartheta}{2} \\ -\sin\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{pmatrix}, \quad R_z(\vartheta) = \begin{pmatrix} e^{j(\vartheta/2)} & 0 \\ 0 & e^{-j(\vartheta/2)} \end{pmatrix} \quad \text{Eqn. (10.16).}$$

Electrical & Computer ENGINEERING

TEPPER

USRA Universities Space Research Association

Important Properties of the Pauli Matrices

- It can be easily proved that the Pauli matrices in (10.15) have the following properties

$$X^2 = Y^2 = Z^2 = jXYZ = \mathbb{I} \quad \text{Eqn. (10.17)}.$$

- In addition, they have the anti-commutation relations below.

$XY + YX = 0, \quad XZ + ZX = 0, \quad YZ + ZY = 0, \ ZX = -jY$ (and any permutation of this) Eqn. (10.18).

- Any combinations of the operators above can therefore be applied to the single qubit. Such operations would correspond to rotations of the single qubit on the Bloch sphere.

- A single operation (or rotation) can be therefore be accomplished by two or more rotations on the Bloch sphere.

- Our central result for operations (rotations) on the qubit for an arbitrary angle ϑ is

$$R_{\hat{n}}(\vartheta) = e^{-j\left(\frac{\vartheta}{2}\hat{n}.\rho\right)} = \cos\frac{\vartheta}{2}\,\mathbb{I} - j\sin\frac{\vartheta}{2}\hat{n}.\rho \quad \text{Eqn. (10.18)}.$$

The Hadamard Operator as a Rotation

- The rotation operator can rotate any Bloch vector onto any other Bloch vector, including qubits with global phase (which we have discussed earlier in this lecture).

- A general way to write the rotation is there to include the global phase, ϕ, (in case it is necessary), then

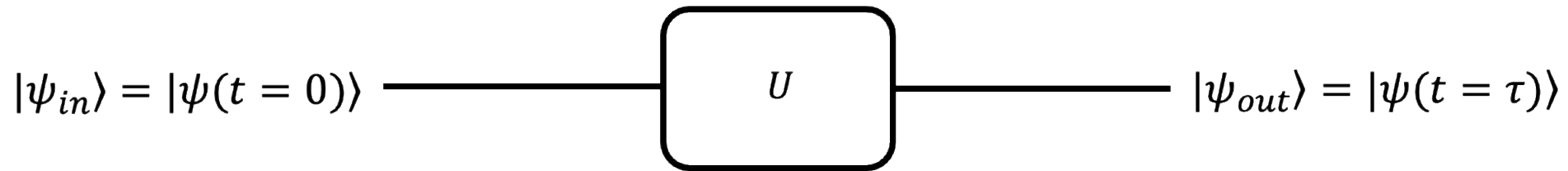$$U = \exp(j\phi)\, R_{\hat{n}}(\vartheta) = \quad \text{Eqn. (10.19).}$$

- As a concrete example, we will insert numerical values into (10.19); take the global phase $\phi = \pi/2$, $\vartheta = \pi$ and $\hat{n} = \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$, so

$$U = \exp(j\phi)\, R_{\hat{n}}(\vartheta) = \exp(j\phi)\left[\cos\frac{\vartheta}{2}\,\mathbb{I} - j\sin\frac{\vartheta}{2}\hat{n}.\rho\right] = \exp\left(\frac{\pi}{2}\right)\left[\cos\frac{\pi}{2}\,\mathbb{I} - j\sin\frac{\pi}{2}\frac{1}{\sqrt{2}}(X+Z)\right]$$

$$\Rightarrow U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \text{H} \quad \text{Eqn. (10.20).}$$

- Eqn. (10.20) is the Hadamard operator we have encountered before, which we now confirm is a rotation.

Electrical & Computer ENGINEERING   TEPPER   USRA Universities Space Research Association

Single Qubit Gates

$$|\psi_{in}\rangle = |\psi(t = 0)\rangle \quad\rule{3cm}{0.4pt}\quad \boxed{U} \quad\rule{3cm}{0.4pt}\quad |\psi_{out}\rangle = |\psi(t = \tau)\rangle$$

- A single qubit gate is defined by a unitary operator. Similar to the case of a classical gate, one can realize a unitary operator by a physical device that performs the action of the gate on a single qubit. One represents the gate symbolically as a box with one input and one output wire.

- In accordance with the Schrodinger equation (discussed in the Axioms of Quantum Mechanics), evolution of a state vector for a qubit starts at some initial time and stops at some predetermined time.

- Action of a quantum gate is therefore to take a qubit state from $|\psi_{in}\rangle$ at $t = 0$ to another state $|\psi_{out}\rangle$ at time $t = \tau$. This is written mathematically as

$$\begin{aligned}|\psi_{in}\rangle &= |\psi(t = 0)\rangle = a_0|0\rangle + a_1|1\rangle \\ |\psi_{out}\rangle &= |\psi(t = \tau)\rangle = b_0|0\rangle + b_1|1\rangle\end{aligned} \Bigg\} \quad \text{Eqn. (10.21).}$$

Reversible Single-qubit Quantum Gates

- Quantum gates are reversible because of the nature of the operator, which we said must obey the unitarity condition

$$UU^\dagger = U^\dagger U = \mathbb{I} \Longrightarrow U = U^{-1} \text{ Eqn. (10.22).}$$

- The input state is available from the output since

$|\psi_{out1}\rangle = U|\psi_{in}\rangle$ Eqn. (10.23); this output can be used as input to a second gate whose action is $U^\dagger = U^{-1}$.

- Thus, $|\psi_{out2}\rangle = U^\dagger|\psi_{out1}\rangle = U^\dagger(U|\psi_{in}\rangle) = (U^\dagger U)\psi_{in}\rangle = 1|\psi_{in}\rangle$ Eqn. (10.24).

- Single-qubit gates are linear in their function; this means several inputs can be operated on by the gate one at a time. The output will be the sum of the individual outputs for each input.

- The Pauli matrices, $X, Y, Z,$ the identity matrix, $I,$ and the Hadamard, $H,$ are all single-qubit operators; we can represent them with gates and design circuits with them.

Phase Gates

- It turns out any complex (2×2) matrix A can be written as an expansion of the form

$$A = \begin{pmatrix} a_0 + a_z & a_x - ja_y \\ a_x + ja_y & a_0 - a_z \end{pmatrix} = a_0 \mathbb{I} + a_x X + a_y Y + a_z Z = a_0 \mathbb{I} + \bar{a}.\bar{\sigma} \quad \text{Eqn. (10.25).}$$

- $\mathbb{I}$ is the identity matrix and a_0, a_x, a_y, a_z are complex numbers; $\bar{a}$ is a complex vector with the complex numbers (a_x, a_y, a_z) and $\bar{\sigma}$ is the Pauli "vector" with matrix components (X, Y, Z).

- From (10.4) and (1018), the unitary matrices for implementing the rotations we have been discussing can also be written in an alternative way as

$$U = u_0 \mathbb{I} + j(u_x X + u_y Y + u_z Z), \quad \text{Eqn. (10.26).}$$

- Note that the u_i can be parameterized in the terms of the polar and azimuthal angles (ϑ, φ) and the unit vector of the Bloch sphere as before. For an operator with a global phase, the most common phase gate derived from (10.26) is

$$P_\vartheta = \begin{pmatrix} 1 & 0 \\ 0 & e^{j\vartheta} \end{pmatrix} \quad \text{Eqn. (10.27).}$$

Electrical & Computer ENGINEERING

TEPPER

USRA Universities Space Research Association

Two-Qubit Gates

- Two-qubit gates have two inputs and two outputs, and like the single-qubit gates are reversible.

- Inputs to two-qubit gates can take a single qubit per input or a superposition of qubits; for example, the inputs to the two-qubit gate illustrated on the right can be written as

$$|A_i\rangle = |0\rangle, \text{ and}$$

$$|B_i\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) \text{ Eqn. (10.27).}$$

- Two-qubit gates are also linear like the single-qubit gates we have already discussed.

$$|A_i\rangle \quad\quad\quad\quad\quad |A_o\rangle$$

$$U$$

$$|B_i\rangle \quad\quad\quad\quad\quad |B_o\rangle$$
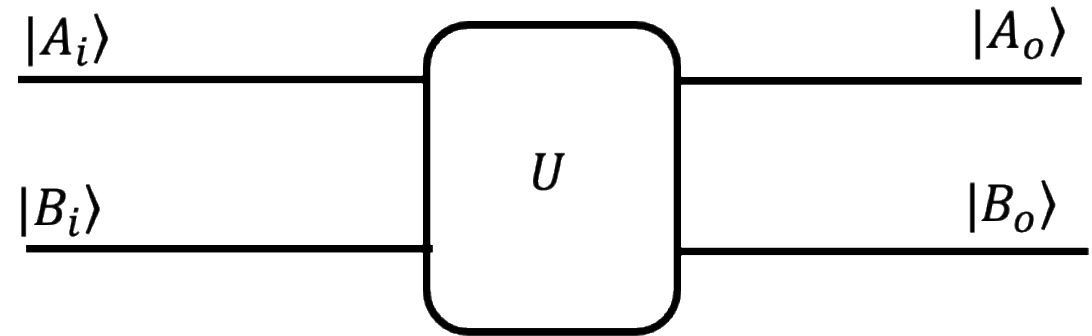
Two-Qubit Control-X (CNOT) Gate

- The quantum control-X gate is represented by the Pauli X operator (matrix); we saw that its action on $|0\rangle$ and $|1\rangle$ was, respectively, as follows:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle; \quad \text{and}$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \quad \text{Eqn. (10.28)}.$$

- In a control-X (CNOT) gate with inputs $|A_i\rangle$ and $|B_i\rangle$, and outputs $|A_o\rangle$ and $|B_o\rangle$ whenever the input $|A_i\rangle = |1\rangle$, whatever the corresponding $|B_i\rangle$ input is, its output is flipped. The value of $|A_i\rangle = |1\rangle$ acts as control for flipping $|B_i\rangle$ at the output. This is shown in the truth Table for the CNOT gate.

- The CNOT gate is linear; this means for an input comprised of a superposition of qubits, the output can be determined by summing the outputs for each individual input

Input		Output	
$|A_i\rangle$	$|B_i\rangle$	$|A_o\rangle$	$|B_o\rangle$
$|0_A\rangle$	$|0_B\rangle$	$|0_A\rangle$	$|0_B\rangle$
$|0_A\rangle$	$|1_B\rangle$	$|0_A\rangle$	$|1_B\rangle$
$|1_A\rangle$	$|0_B\rangle$	$|1_A\rangle$	$|1_B\rangle$
$|1_A\rangle$	$|1_B\rangle$	$|1_A\rangle$	$|0_B\rangle$

Hadamard and the CNOT Gates as an Entangling (Bell) Circuit

- By combining the Hadamard and the CNOT gate as shown in the graphic on the left, one can entangle qubits. The inputs to the CNOT gate after the Hadamard are:

$$|H_{Ai}\rangle = H|0_A\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle), \text{ Eqn. (10.29) and}$$

$$|B_i\rangle = |0_B\rangle \text{ Eqn. (10.30).}$$

- For the input (10.29) and (10.30) to the CNOT gate are acted to produce the entangled output given by
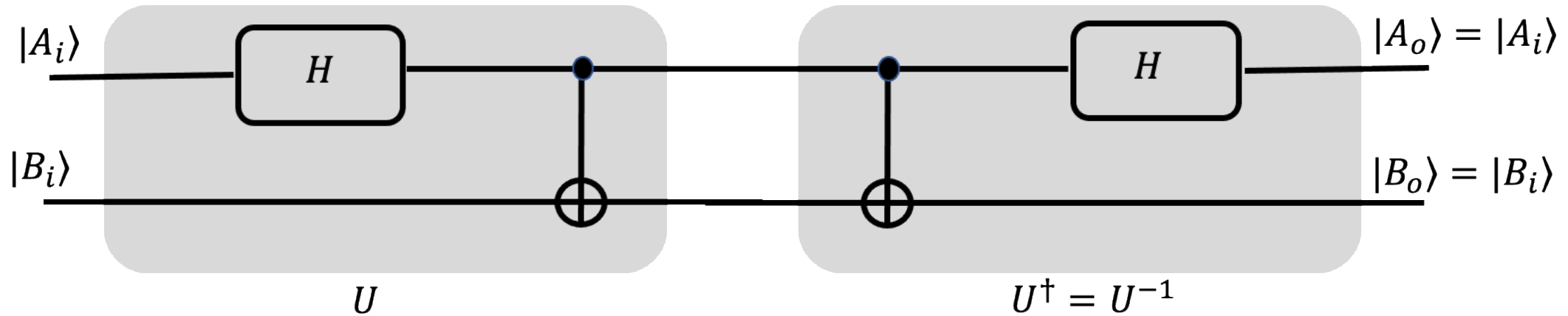
$$|AB_o\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle) \quad \text{Eqn. (10.30).}$$

- Four possible input combinations are possible, resulting in four maximally entangled Bell states.
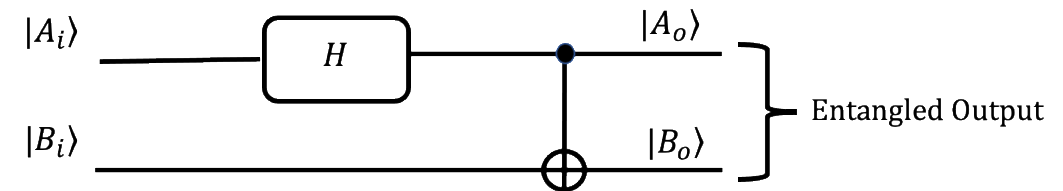
| Input $|AB\rangle$	Output $|AB_{Ent}\rangle$
$|0_A0_B\rangle$	$\frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle)$
$|0_A1_B\rangle$	$\frac{1}{\sqrt{2}}(|0_A1_B\rangle + |1_A0_B\rangle)$
$|1_A0_B\rangle$	$\frac{1}{\sqrt{2}}(|0_A0_B\rangle - |1_A1_B\rangle)$
$|1_A1_B\rangle$	$\frac{1}{\sqrt{2}}(|0_A1_B\rangle - |1_A0_B\rangle)$

Disentangling Bell Circuit

$$|A_i\rangle \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad |A_o\rangle = |A_i\rangle$$

$$H \qquad \qquad \qquad \qquad \qquad \qquad H$$

$$|B_i\rangle \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad |B_o\rangle = |B_i\rangle$$

$$U \qquad \qquad \qquad \qquad \qquad \qquad U^\dagger = U^{-1}$$

- In the previous slide, we determined that a Hadamard and a CNOT gate can be combined to form a circuit that entangles qubits; since two-qubit gates are reversible, it should be possible to disentangle qubits by joining two such circuits together, where the second circuit is connect in reverse to perform the $U^\dagger = U^{-1}$. Such a circuit is shown above.

- Any combination of the following inputs: $|0_A 0_B\rangle, |0_A 1_B\rangle, |1_A 0_B\rangle, |1_A 1_B\rangle$ will first lead to entanglement by the first circuit, and then disentanglement by the second circuit.

Other Two-qubit Controlled Gates

- The single-qubit Pauli X operator become the two-qubit controlled-X gate by adding a controlling input. One can construct other two-qubit controlled gates from the other Pauli operators. For example, it is possible to create a controlled-Y and controlled-Z gates simply by adding a control input. The circuit diagram for a controlled-Y or a controlled-Z gate is shown on the right.

$|A_i\rangle$ ———●——— $|A_o\rangle$

$|B_i\rangle$ ———[Y or Z]——— $|B_o\rangle$

- The standard way of writing the possible inputs into the control-X, control-Y, and control-Z for the two-qubit inputs is $|0_A 0_B\rangle$, $|0_A 1_B\rangle$, $|1_A 0_B\rangle$, $|1_A 1_B\rangle$. This is not the way;
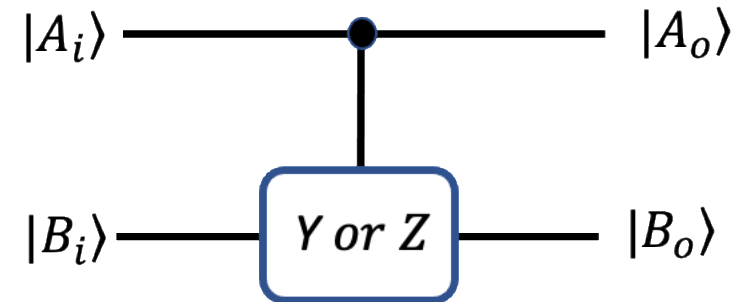
Matrix Representation of Controlled Gates

- One can change how one represents the two-qubit basis by writing out the tensor product as column vector; thus

$$|0_A 0_B\rangle \Longleftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ |0_A 1_B\rangle \Longleftrightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \ |1_A 0_B\rangle \Longleftrightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \ |1_A 1_B\rangle \Longleftrightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad \text{Eqn. (10.31)}$$

- These can be arranged into orthogonal matrices that represent the controlled gates as follows:

- $\text{Controlled} - X = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ \text{Controlled} - Y = \begin{pmatrix} 0 & -j & 0 & 0 \\ j & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ \text{Controlled} - Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Swap Gate

- A swap gate merely exchanges the inputs of a two-qubit gate with the output as illustrated in the graphic. The truth table for the swap operation also provided.

- One can form the 4×4 matrix representation of the swap gate by rearranging the 4 column vectors representation of the input basis in (10.31) as

$$\text{Swap} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

| Input $|AB\rangle$	Output $|AB\rangle$
$|0_A 0_B\rangle$	$|0_A 0_B\rangle$
$|0_A 1_B\rangle$	$|1_A 0_B\rangle$
$|1_A 0_B\rangle$	$|0_A 1_B\rangle$
$|1_A 1_B\rangle$	$|1_A 1_B\rangle$
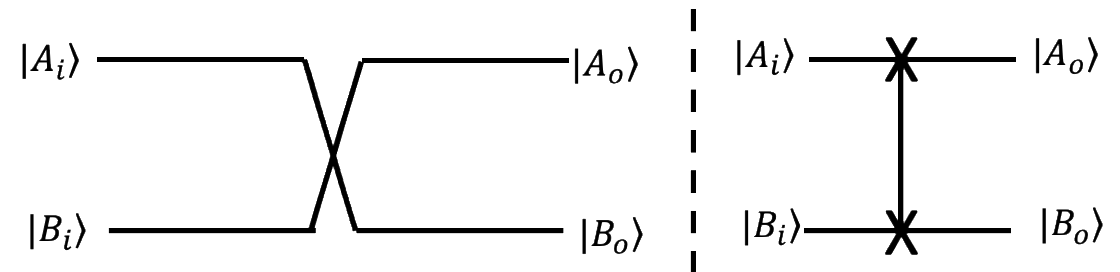
Quantum Gate Circuits
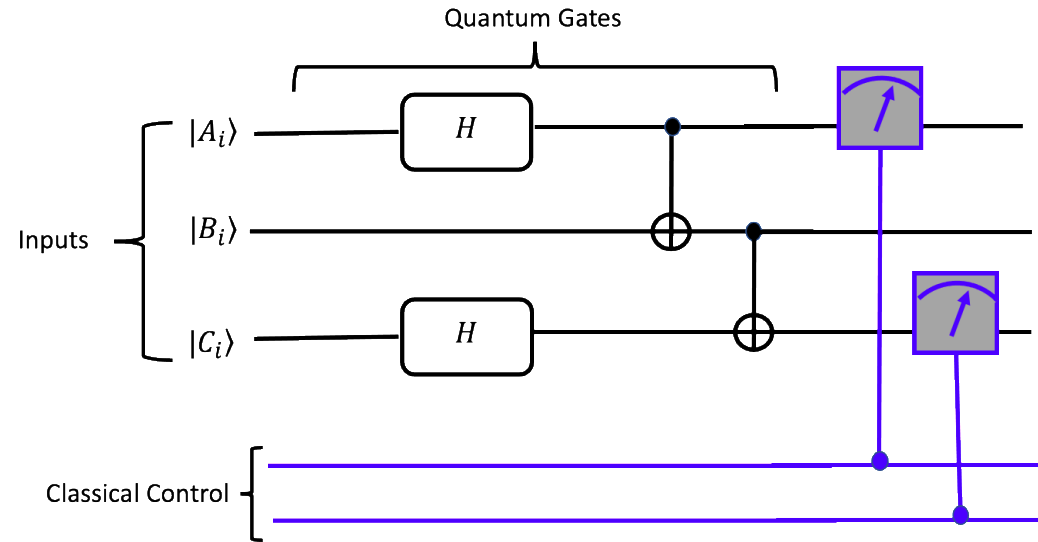
- Gate circuits are a combination of quantum gates interconnected in certain manner to perform a particular desired computation. The circuit operates under classical control and outputs its results as classical bits even though the computation is quantum mechanical. The number of gates and hence the size of a circuit depends on the computation being performed.

- As in classical circuits, a quantum circuit begins and ends its operation according to a timed clock cycle.

Does a Gate (or a Process) for Copying Qubits Exist?
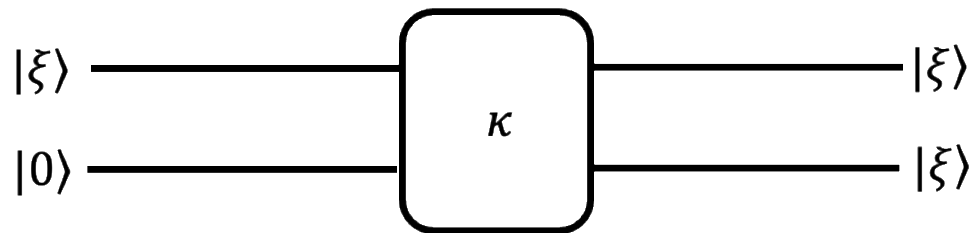
- In discussing classical gates and circuits (such as the half-adder), we discovered that we could make copies of input bits so that they could be used elsewhere in a circuit; this is called the fan-out. Does such a process exist for qubits?

- Assume it is possible to make copies of qubits; we must then prove that it is either possible or impossible to copy (clone) qubits.

- If we can clone qubits, there must be gate that accomplishes this task. Such a gate is illustrated on the right. It is a two-qubit gate with 2 inputs and 2 outputs. The lower input of the gate is permanently the state $|0\rangle$; this is called the ancilla bit. The gate takes the top input, reproduces it at the top output and makes another copy (clone) of it at the bottom output.

$|\xi\rangle$ ——————[κ]—————— $|\xi\rangle$

$|0\rangle$ ——————[ ]—————— $|\xi\rangle$

Electrical & Computer ENGINEERING

TEPPER

USRA Universities Space Research Association

No Cloning Theorem of Qubits

- Given that the copying gate, $|\kappa\rangle$, makes copies of the top input at the bottom, and reproduces the input at the top output, it must have the following properties:

(i) $\kappa(|00\rangle) = |00\rangle$, (ii) $\kappa(|10\rangle) = |11\rangle$, (iii) $\kappa\big((\alpha|0\rangle + \beta|1\rangle)|0\rangle\big) = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$. Eqn. (10.32).

- The third property in (10.32) can be expanded to

$$\kappa(\alpha|00\rangle + \beta|10\rangle) = |\alpha|^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + |\beta|^2|11\rangle \quad \text{Eqn. (10.33).}$$

- Using linearity and property (i) and (ii) on the right-hand side of (10.33), we obtain

$$\alpha|00\rangle + \beta|11\rangle \neq |\alpha|^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + |\beta|^2|11\rangle \quad \text{Eqn. (10.34).}$$

- The inequality of the two sides of (10.34) show that out initial assumption of the existence of a cloning gate is false.

- It is therefore NOT possible to clone qubits: this is the no cloning theorem of quantum mechanics.

Summary

- Reviewed classical gates and circuits
  - Discussed concept of a universal gate

- Detailed discussion of the qubit on the complex plane
  - Derived the Bloch sphere
  - Discussed operations on single qubit as rotations on the Bloch sphere
  - Qubit operations as gates
  - Gate based circuits