Week by week

(1) Introduction to quantum computing
(2) Single qubit representation and operations
(3) Multi-qubit systems
(4) Simple quantum algorithms
(5) Quantum search (Grover's algorithm)
(6) Quantum factorization (Shor's algorithm)
(7) Quantum supremacy and noise
(8) Programming real quantum computers (IBM Q)
(9) Quantum error correction (QEC)
(10) QUBO problems and Adiabatic Quantum Computation (AQC)
(11) Variational/hybrid quantum algorithms (QAOA and VQE)
(12) Solving linear equations, QC computing hardware

Week 3

Lecture 5

3.1 Two qubit systems and operations

3.2 Entanglement

Lecture 6

4.1 Dense coding

4.2 Teleportation

Lab 3

Two qubit operations, entanglement, dense coding, teleportation

Recap: A zoo of one-qubit gates

$$\left.\begin{array}{l} X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ \\ Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ \\ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{array}\right\}$$

π rotation about the x-, y- and z- axes.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

“Hadamard” gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$\pi/2$ rotation about the z- axis.

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

$\pi/4$ rotation about the z- axis.

Recap: General qubit rotation

A rotation by angle θ around a (unit vector) axis $\hat{n}$, is given by:

$$R_n(\theta) = \exp\left(-i\frac{\theta}{2}\hat{n}\cdot\sigma\right)$$

You can write this exponential using this identity:

$$\exp(i\,\theta\,\hat{\mathbf{n}}\cdot\boldsymbol{\sigma}\,) = I\cos\theta + i\,\hat{\mathbf{n}}\cdot\boldsymbol{\sigma}\,\sin\theta$$

General rotation matrix:

$$R_{\hat{\mathbf{n}}}(\theta_R) = e^{i\theta_g}\left(I\cos\frac{\theta_R}{2} - i\,\hat{\mathbf{n}}\cdot\boldsymbol{\sigma}\,\sin\frac{\theta_R}{2}\right)$$

5.1 Multi-qubit systems and operations

MULT90063

Lecture 5

Lecture overview

In this lecture:

5.1 Two qubit systems and operations

- Mulitple qubits and binary numbers
- Linear algebra of two-qubit systems
- Two-qubit logic gates
- Universality

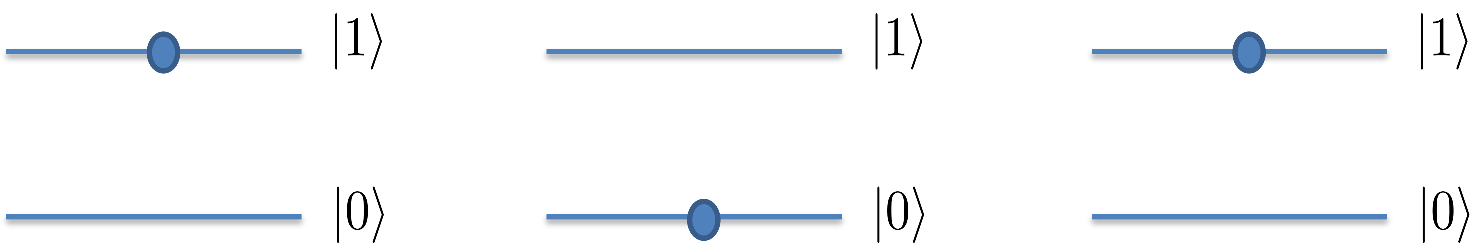
5.2 Entanglement

- Separable states
- Entangled states
- Entropy of entanglement
- Entanglement in the QUI

- Reiffel, Chapter 3
- Kaye, 2.6
- Mike and Ike, 1.3.2-1.3.4

Recap: qubits and binary numbers

Computers represent integers as binary numbers. Similarly, we can think as the state of several qubits as a binary digits.

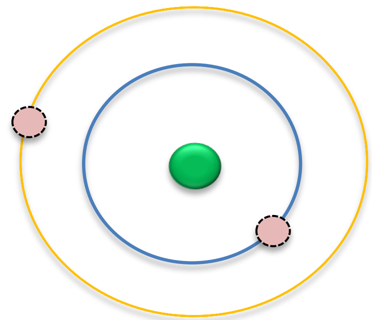


For example, the number 5 can be represented in binary as *101*, and this can be encoded directly in the state of three individual atoms.

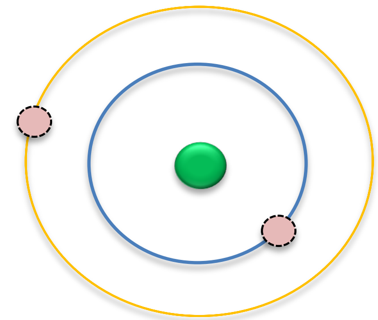
This lecture we will talk about multi-qubit systems (i.e. 2-qubit systems).

Two qubits: tensor product

Two atoms, each with one electron in a superposition of the bit states:



$$|\psi\rangle = a|0\rangle + b|1\rangle$$



$$|\phi\rangle = c|0\rangle + d|1\rangle$$

Then the joint state of both atoms is:

$$|\psi\rangle \otimes |\phi\rangle$$

Tensor product!

Ordering of amplitudes in vectors

We want to order the elements of the vector so that they correspond to binary numbers.

One qubit state

$$|\psi\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

Two qubit state

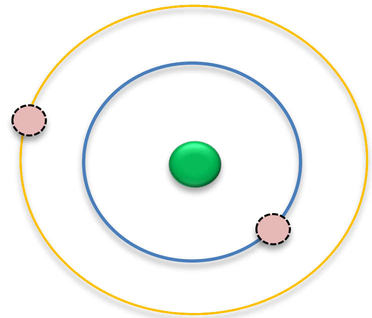
$$|\psi\rangle = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix}$$

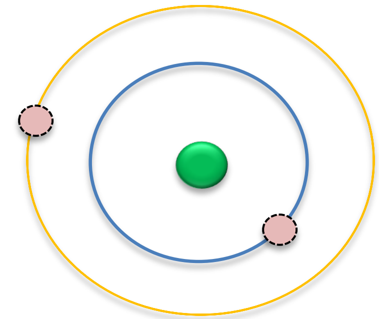
Three qubit state

$$|\psi\rangle = \begin{bmatrix} a_{000} \\ a_{001} \\ a_{010} \\ a_{011} \\ a_{100} \\ a_{101} \\ a_{110} \\ a_{111} \end{bmatrix}$$

Tensor product

Two atoms, each with one electron in a superposition of the bit states:





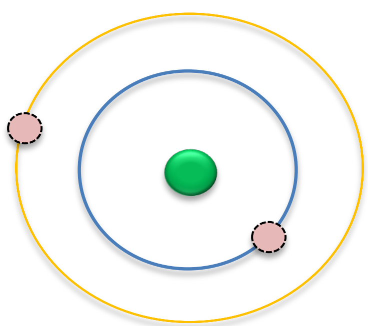
$$|\psi\rangle = a|0\rangle + b|1\rangle \qquad |\phi\rangle = c|0\rangle + d|1\rangle$$

For these two atoms in the states indicated:

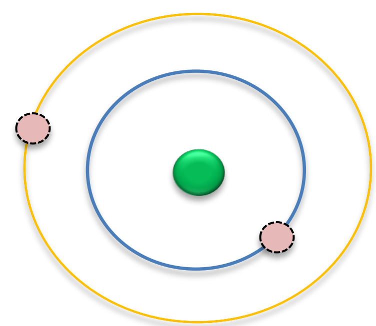
$$\begin{aligned} |\psi\rangle \otimes |\phi\rangle &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac\ |0\rangle \otimes |0\rangle + ad\ |0\rangle \otimes |1\rangle + bc\ |1\rangle \otimes |0\rangle + bd\ |1\rangle \otimes |1\rangle \\ &= ac\ |00\rangle + ad\ |01\rangle + bc\ |10\rangle + bd\ |11\rangle \end{aligned}$$

Tensor product of vectors

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} \begin{array}{l} \text{00 amplitude} \\ \text{01 amplitude} \\ \text{10 amplitude} \\ \text{11 amplitude} \end{array}$$



$$|\psi\rangle = a|0\rangle + b|1\rangle$$



$$|\phi\rangle = c|0\rangle + d|1\rangle$$

Tensor product of operators

Similarly, we can define a Kronecker tensor product of qubit operators:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \otimes \begin{bmatrix} m & n \\ p & q \end{bmatrix} = \begin{bmatrix} am & an & bm & bn \\ ap & aq & bp & bq \\ cm & cn & dm & dn \\ cp & cq & dp & dq \end{bmatrix}$$

Single qubit gates on multi-qubit systems

We can apply single-qubit operators to multi-qubit systems:

$$(X \otimes I)\,|0\rangle \otimes |0\rangle \;\longrightarrow\; X_1\,|00\rangle = |10\rangle$$
$$(I \otimes X)\,|0\rangle \otimes |0\rangle \;\longrightarrow\; X_2\,|00\rangle = |01\rangle$$

Simplest way to think of it: the subscript represents which qubit the operation is applied to.

To work out the operator we are applying in matrix representation, we use the Kronecker (tensor) product with the identity:

$$X \otimes I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Identity is applied to second qubit where there's no operation

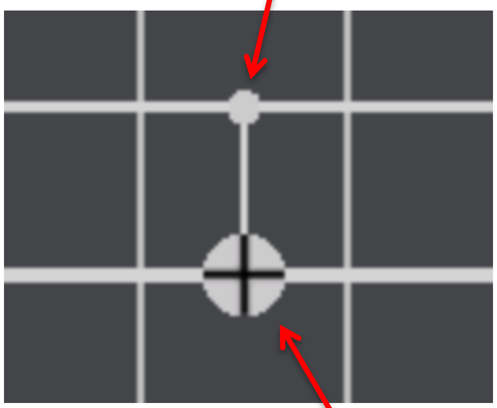
Two qubit logic gate: CNOT

Two qubit gates can be constructed using an interaction between the two systems. Most important is the Controlled-NOT (CNOT) gate.

Symbol for “control”

Control qubit

Target qubit



Symbol for binary addition (flip)

How states transform: CNOT truth table

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |11\rangle$$
$$|11\rangle \rightarrow |10\rangle$$

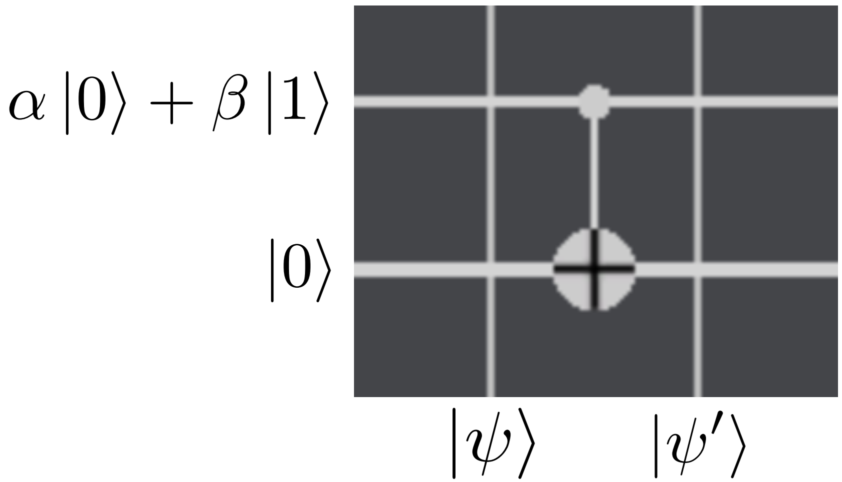
Rule: The target is flipped iff the control qubit is “1”.

As a matrix:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$a|00\rangle + b|01\rangle + \boxed{c|10\rangle + d|11\rangle}$$
$$\rightarrow a|00\rangle + b|01\rangle \boxed{+ d|10\rangle + c|11\rangle}$$

Example: CNOT on superposition



Before the CNOT, the state is:

$$|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha|00\rangle + \beta|10\rangle$$

After the CNOT, the state is:

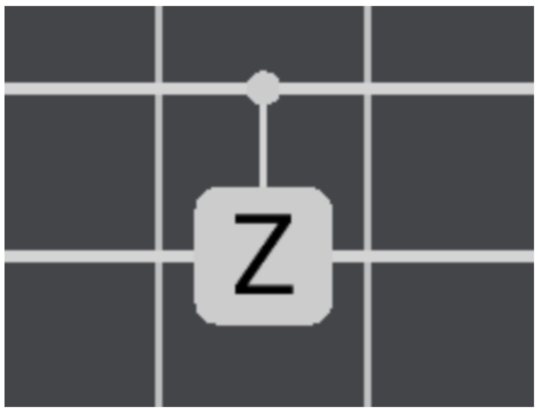
$$|\psi'\rangle = \alpha|00\rangle + \beta|11\rangle$$

Control Phase Gate

Two qubit gates can be constructed using an interaction between the two systems.

Control qubit

Target qubit



How states transform:

$$
\begin{aligned}
|00\rangle &\to |00\rangle \\
|01\rangle &\to |01\rangle \\
|10\rangle &\to |10\rangle \\
|11\rangle &\to -|11\rangle
\end{aligned}
$$

$$a\,|00\rangle + b\,|01\rangle + c\,|10\rangle \boxed{+\, d\,|11\rangle}$$

$$\to a\,|00\rangle + b\,|01\rangle + c\,|10\rangle \boxed{-\, d\,|11\rangle}$$

Rule: the **phase** of the target flipped iff the control qubit is "1".

As a matrix:

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Fun fact: CZ doesn't matter which one you think of as control/target.

Swap gate

A swap operation can be implemented using an interaction between the two qubits – the states of the two qubits are swapped (not the physics qubits).

Qubit 1

Qubit 2

How states transform:

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |10\rangle$$
$$|10\rangle \rightarrow |01\rangle$$
$$|11\rangle \rightarrow |11\rangle$$

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$
$$\rightarrow a|00\rangle + c|01\rangle + b|10\rangle + d|11\rangle$$

Rule: the two qubits are swapped.

As a matrix:

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

NB. Unlike CNOT, swap gates do not generate entanglement (but sqrt SWAP does!) .

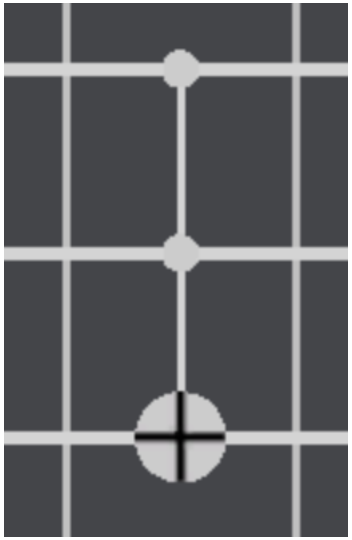
Toffoli gate

Toffoli gate plus NOT is universal for classical computation. It was used in the proof that classical computation can be made reversible!

Control qubit

Control qubit

Target qubit



How states transform:

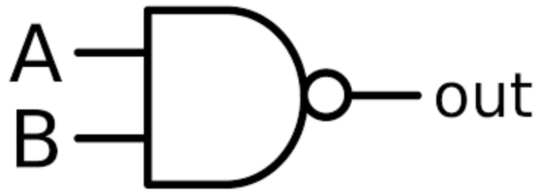
$$
\begin{aligned}
|000\rangle &\to |000\rangle \\
|001\rangle &\to |001\rangle \\
|010\rangle &\to |010\rangle \\
|011\rangle &\to |011\rangle \\
|100\rangle &\to |100\rangle \\
|101\rangle &\to |101\rangle \\
|110\rangle &\to |111\rangle \\
|111\rangle &\to |110\rangle
\end{aligned}
$$

Rule: the target is flipped iff **both** the control qubits are in “1” state.

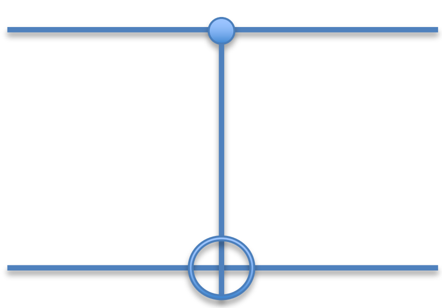
$$
\begin{aligned}
&a\,|000\rangle + b\,|001\rangle + c\,|010\rangle + d\,|011\rangle \\
&e\,|100\rangle + f\,|101\rangle + \boxed{g\,|110\rangle + h\,|111\rangle} \\
&\to a\,|000\rangle + b\,|001\rangle + c\,|010\rangle + d\,|011\rangle \\
&\quad e\,|100\rangle + f\,|101\rangle + \boxed{h\,|110\rangle + g\,|111\rangle}
\end{aligned}
$$

Universality

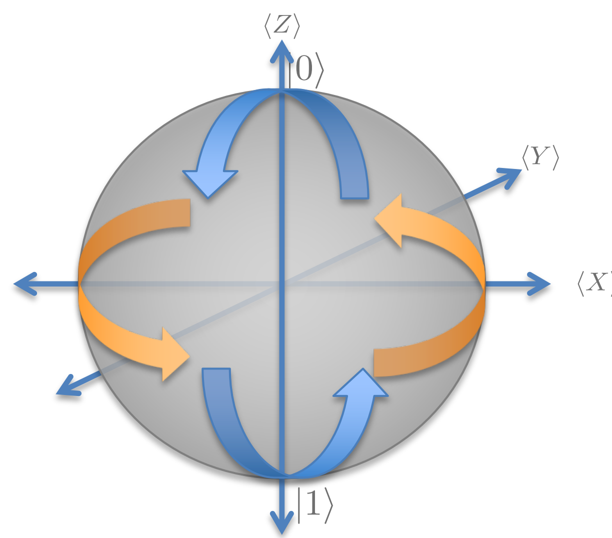
In classical computing the NAND gate is universal, i.e. every Boolean function can be implemented as a sequence of NAND (NOT AND) gates:



In quantum computing every quantum circuit can be expressed as a sequence of:



+

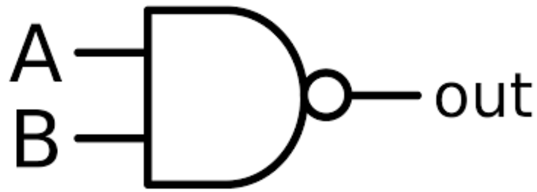


CNOT

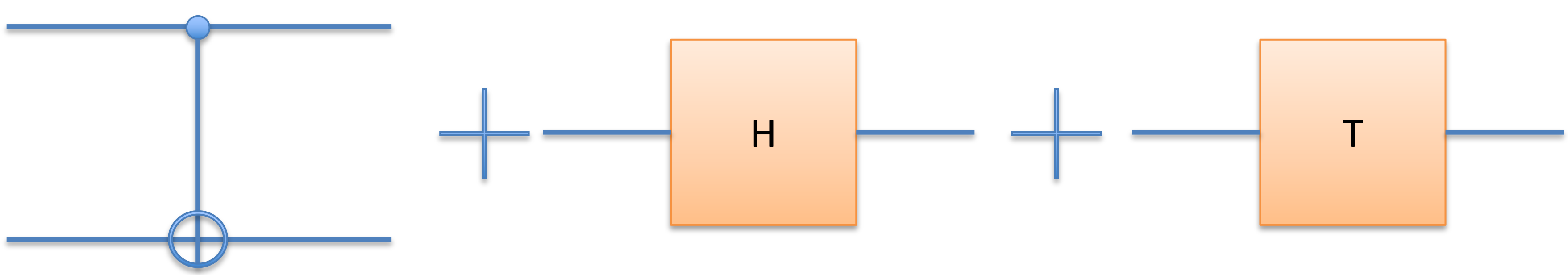
Single Qubit Rotations

Universality

In classical computing the NAND gate is universal, i.e. every Boolean function can be implemented as a sequence of NAND (NOT AND) gates:



In quantum computing every quantum circuit can be expressed as a sequence of:



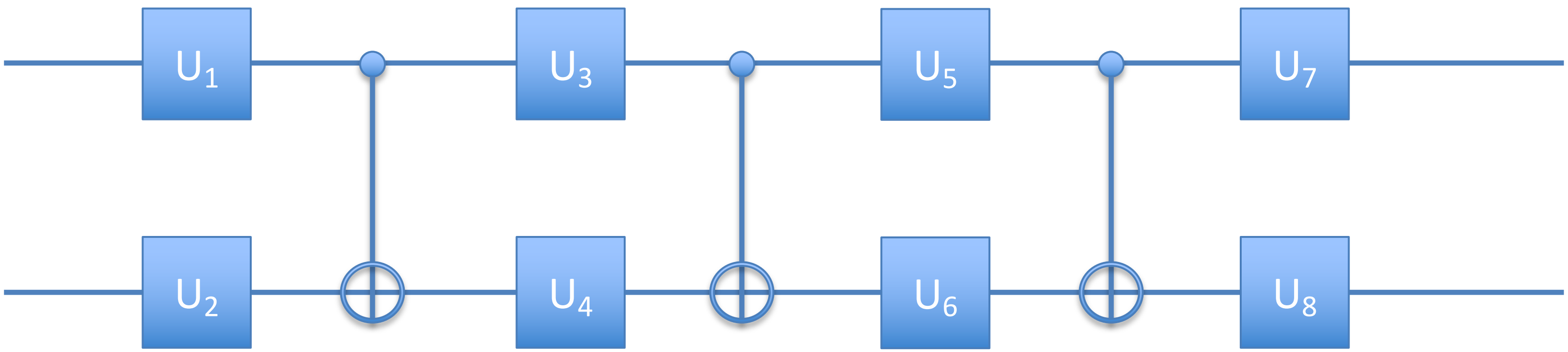
CNOT

Hadamard

T Gate
(pi/8)

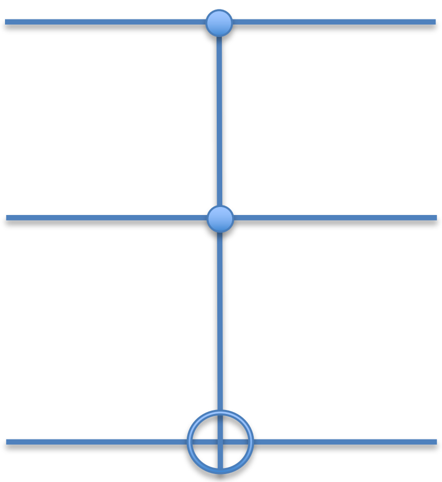
Construction for *any* two qubit unitary

Any two qubit gate can be decomposed into just 3 CNOTs and single qubit rotations:



Challenge problem

How can you decompose Tofolli as CNOTs and single qubit rotations?



Two-qubit projective measurement

Examples of two-qubit projectors. Eg. For measuring the first qubit in the computational basis:

$$P_0 = |0\rangle\langle 0| \otimes I$$
$$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$P_1 = |1\rangle\langle 1| \otimes I$$
$$= \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Two-qubit measurement

Measurement on a two-qubit state:

(1) Apply projector into the measured state
(2) Renormalize the state

$$|\psi'\rangle = \frac{P_m |\psi\rangle}{\sqrt{p(m)}}$$

For example, consider the general two-qubit state:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

If the first qubit were measured to be "0", apply P_0 and renormalize to get the collapsed state:

$$|\psi'\rangle = \frac{a|00\rangle + b|01\rangle}{\sqrt{|a|^2 + |b|^2}}$$

normalization

If the first qubit were measured to be "1", apply P_1 and renormalize to get the collapsed state:

$$|\psi'\rangle = \frac{c|10\rangle + d|11\rangle}{\sqrt{|c|^2 + |d|^2}}$$

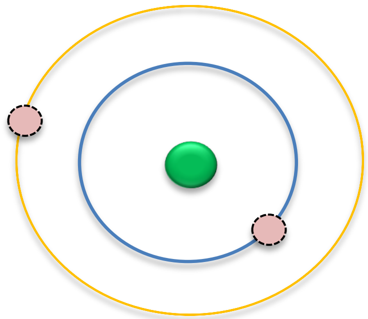
Later (and Lab 3): this generalizes to measurements on multi-qubit states.

5.2 Entanglement

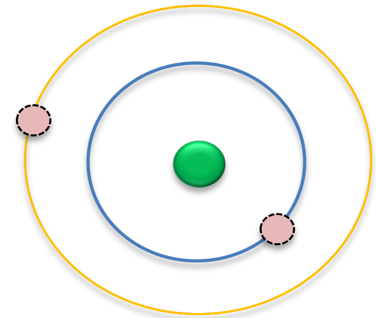
MULT90063

Lecture 5

Separable states



$$|\psi\rangle = a|0\rangle + b|1\rangle$$



$$|\phi\rangle = c|0\rangle + d|1\rangle$$

A separable state is one which can be written as

$$|\Phi\rangle = |\psi\rangle \otimes |\phi\rangle$$

All separable states (of two qubits) can be written as:

$$|\psi\rangle = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle$$

Examples of separable states

Consider the state:

$$|\psi\rangle = \frac{|00\rangle + |01\rangle}{\sqrt{2}}$$

It is *separable* because:

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

Consider the state:

$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

It is also *separable* because:

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

Constructing a Bell state

This is one of four states named after the physicist John Bell (who figured out how to experimentally explore reality of entanglement).

Consider the following circuit in the QUI:

Execution: $$|00\rangle \underset{\text{H}}{\rightarrow} \frac{|00\rangle + |10\rangle}{\sqrt{2}} \underset{\text{CNOT}}{\rightarrow} \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Question: Is $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ separable?

Entanglement

Answer: No! We can never find a, b, c, d, i.e.

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \neq (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle)$$

A state which is not separable is called an **entangled** state.

Entanglement is a uniquely quantum mechanical property, with no direct classical analogue.

Entanglement Measure

We would like to have a measure of *how much* entanglement a state has. Some states are more entangled than others:

$\|00\rangle$	Not entangled, separable
$\sqrt{0.99}\,\|00\rangle + \sqrt{0.01}\,\|11\rangle$	Entangled, but close to a separable state
$\frac{1}{\sqrt{2}}\,\|00\rangle + \frac{1}{\sqrt{2}}\,\|11\rangle$	Maximally entangled

One simple measure is to ask: How many Bell states (asymptotically) do would Alice and Bob need to share to construct this state, given they are allowed to do Local Operations and Classical Communication *(LOCC)*, but not interact their qubits directly. For pure states, this is equivalent to the *Entropy of Entanglement*.

Entropy of entanglement

Entanglement is a type of correlation between two systems, say A and B.

To see how much correlation there is between A and B: We will measure B, throw away the result, and ask how many bits information of information do we need to determine the state of A?

For example, taking the state (with Alice controlling the first qubit, Bob the second):

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

We measure the state of the second (Bob's) qubit, and forget the result.

50% of the time, the first qubit (Alice's) collapses to the state $|0\rangle$

50% of the time, the first qubit (Alice's) collapses to the state $|1\rangle$

Entropy of Entanglement

Bob needs some information to determine Alice's state. How much? That's measured by the *entropy*.

Entanglement entropy is given by:

$$S = -\sum_i p_i \log p_i$$

where p_i is the probability of measuring ith state of Alice's qubit.

For this case of a Bell state, p_0=50%, p_1=50%,

$$S = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{2}\log\frac{1}{2} = \frac{1}{2} + \frac{1}{2} = 1$$

Here, and throughout this subject, logarithms are taken base 2.

Therefore, a Bell State has 1 bit of entanglement (max possible).

Entropy measure of a separable state

For the separable state: $|00\rangle$

We measure the state of the second (Bob's) qubit.
100% of the time, the first qubit (Alice's) collapses to the state $|0\rangle$

The entropy of entanglement is therefore: $S = -1 \times \log 1 = 0$

All separable states have an entropy of entanglement of 0.

For the state: $\sqrt{0.99}\,|00\rangle + \sqrt{0.01}\,|11\rangle$ $\qquad S = 0.08$

This measure of entanglement generalizes between two subsystems of qubits A and B, and is how the measure of entanglement is calculated in the QUI.

Schmidt Decomposition

How much entanglement is present in a general state?

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

Can be hard to tell. It's not in anything like product form. For that we will use SVD.
Arrange as a matrix:

$$A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix}$$

Taking Singular Value Decomposition (SVD):

$$A = \sum \lambda_i |u_i\rangle \langle v_i|$$

Allows us to express the state in this convenient form:

$$|\psi\rangle = \sum \lambda_i |u_i\rangle |v_i\rangle$$

This from is known as the "Schmidt Decomposition"

Schmidt Rank

$$|\psi\rangle = \sum \lambda_i |u_i\rangle |v_i\rangle$$

Several terms might have a singular value of 0. The number of non-zero terms is called the **Schmidt rank**.

If a state has a Schmidt rank of 1:

$$|\psi\rangle = |u_0\rangle \otimes |v_0\rangle$$

Then the state is separable, and not entangled.

If a state has a Schmidt rank greater than 1, then the state is entangled. Schmidt rank is a very coarse measure of entanglement. We would like a finer measure.

Entanglement Entropy

$$|\psi\rangle = \sum \lambda_i |u_i\rangle |v_i\rangle$$

A more fine-grained measure of entanglement is the **entanglement entropy**. Form a probability distribution:

$$p_i = \lambda_i^2$$

From which you can calculate the entanglement entropy:

$$S = -\sum_i p_i \log p_i$$

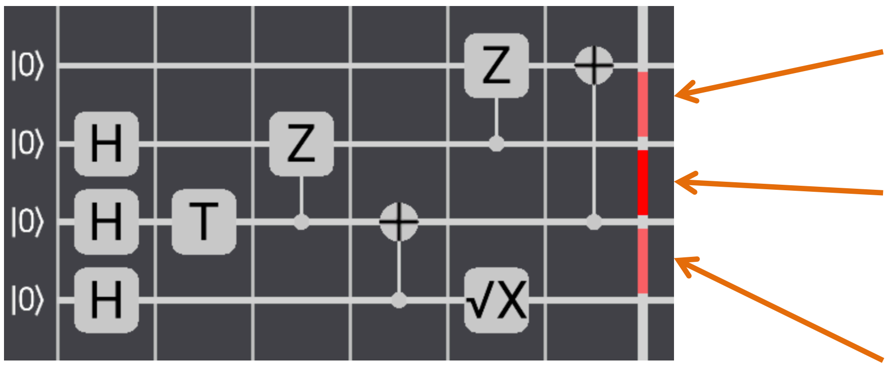
This is a measure of entanglement. The higher the entanglement entropy, the more entanglement.

Entanglement in the QUI

The time scrubber is the vertical bar which moves left and right to show the quantum state at each time step.

The entropy of entanglement is shown in a red colour scale between min and max values possible. Each segment corresponds to the entropy between the system of qubits above and below for that particular bi-partition.

qubit-1
qubit-2
qubit-3
qubit-4



Entanglement entropy between qubit 1 and qubits {2 & 3 & 4} partition

Entanglement entropy between qubits {1 &2} and qubits {3 & 4} partitions

Entanglement entropy between qubit 4 and qubits {1 & 2 & 3} partition

QUBIT ENTANGLEMENT

Entanglement level: 2.000

Quantum entanglement can occur between each qubit and every other qubit. This entanglement segment represents the total entanglement between qubits above and qubits below.

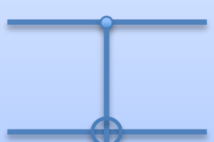
Lecture 5 Summary

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$$

Tensor Product

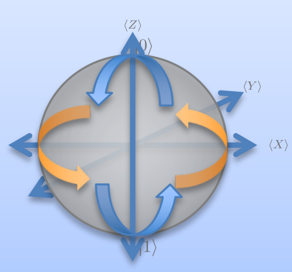
A state which is not separable is called an **entangled** state.

Universal set of gates



CNOT

+



Single Qubit Rotations

Two qubit gates

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Week by week

(1) Introduction to quantum computing
(2) Single qubit representation and operations
(3) Multi-qubit systems
(4) Simple quantum algorithms
(5) Quantum search (Grover's algorithm)
(6) Quantum factorization (Shor's algorithm)
(7) Quantum supremacy and noise
(8) Programming real quantum computers (IBM Q)
(9) Quantum error correction (QEC)
(10) QUBO problems and Adiabatic Quantum Computation (AQC)
(11) Variational/hybrid quantum algorithms (QAOA and VQE)
(12) Solving linear equations, QC computing hardware