ΝΑΝΟΗΛΕΚΤΡΟΝΙΚΗ & ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ

7^{η} Διάλεξη

Βιβλιογραφία: EXPLORATIONS IN QUANTUM COMPUTING, Colin P. Williams (2nd edition, Springer-Verlag, 2011), chapter 2.

Quantum Logic Gates

- Definitions of Quantum logic gate and network
- From Quantum Dynamics to Quantum Gates
- 1-Qubit Gates
- Rotations About the x-, y-, and z-Axes
- Controlled Quantum Gates

Definition of Quantum logic gate

A quantum logic gate is a device that carries out a given unitary operation on its input qubits in a fixed period of time.

- Any quantum gate is described by unitary matrices, their action is always logically reversible and are related to physical processes.
- Any quantum gate is implemented physically as the quantum mechanical evolution of an isolated quantum system:

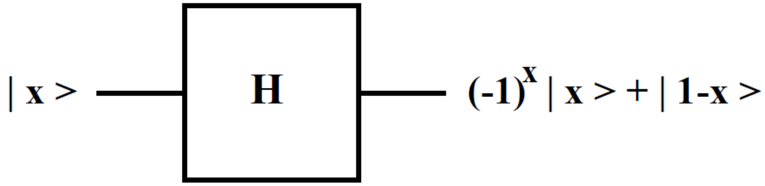
1. The transformation it achieves is given by	*Schrödinger's equation:* $i\hbar\partial\|\psi\rangle/\partial t = \mathcal{H}\|\psi\rangle$
2. Unitary matrices are related to physical processes	*via the equation:* $U = \exp(-i\mathcal{H}t/\hbar)$
3. Time evolution is described by a unitary transformation of an initial state $\|\psi(0)\rangle$	*to a final state:* $\|\psi(t)\rangle = \exp(-i\mathcal{H}t/\hbar)\|\psi(0)\rangle = U\|\psi(0)\rangle$
4. It transforms state $\|\psi(0)\rangle$ unitarily until a measurement of an observable is made with	*outcome one eigenvalue λ_j of the observable, with probability $p(\lambda_j)$ for the collapsed state.*

✓ *A linear function maps a qubit to a qubit (it preserves normalized vectors) if it is unitary.*

✓ *Unitarity is the only requirement on linear maps for quantum evolution.*

✓ *Any unitary linear map defines a valid single qubit quantum circuit.*

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ Hadamard gate



Special 1-Qubit Gates: Pauli Spin Matrices

Any 1-qubit Hamiltonian can always be written as weighted sum of the Pauli matrices:

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Some common forms for Hamiltonians that arise in practice are	
1. The Ising interaction	$\mathcal{H} = Z^{(1)} Z^{(2)}$
2. The XY interaction	$\mathcal{H} = X^{(1)} \otimes X^{(2)} + Y^{(1)} \otimes Y^{(2)}$
3. The form	$\mathcal{H} = 2X^{(1)} \otimes X^{(2)} + Y^{(1)} \otimes Y^{(2)}$
where the parenthetical superscripts labels which of two qubits the operator acts upon	

The Pauli X matrix is the **classical** (reversible) NOT gate

$$X \equiv \mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{cases} X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \\ X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \end{cases}$$

X negates the computational basis states $|0\rangle$ and $|1\rangle$, correctly as these correspond to the classical bits, 0 and 1.

Is Pauli X a NOT Gate for Qubits?

- ✓ The NOT gate has the effect of mapping a state at the North pole of the Bloch sphere into a state at the South pole and vice versa.
- ✓ But, is a NOT gate the operation that maps a qubit $|\psi\rangle$, lying at any point on the surface of Bloch sphere, into its antipodal state $|\psi^{\perp}\rangle$, on the opposite side of the Bloch sphere?

arbitrary starting state $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$ Check whether: $X|\psi\rangle = |\psi^{\perp}\rangle$

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \begin{pmatrix} e^{i\phi}\sin\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right) \end{pmatrix} = e^{i\phi}\sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)|1\rangle$$

the antipodal state is: $|\psi^{\perp}\rangle = \cos\left(\frac{\pi-\theta}{2}\right)|0\rangle + e^{i(\phi+\pi)}\sin\left(\frac{\pi-\theta}{2}\right)|1\rangle$

$$|\psi^{\perp}\rangle = \cos\left(\frac{\pi-\theta}{2}\right)|0\rangle - e^{i(\phi)}\sin\left(\frac{\pi-\theta}{2}\right)|1\rangle = \sin\left(\frac{\theta}{2}\right)|0\rangle - e^{i\phi}\cos\left(\frac{\theta}{2}\right)|1\rangle$$

Hence, the result of $X|\psi\rangle \neq |\psi^{\perp}\rangle$ The Pauli X gate cannot "negate" an arbitrary superposition state, and is not a universal NOT gate for qubits.

$$|0\rangle \;-\boxed{X}-\; |1\rangle$$

$$|1\rangle \;-\boxed{X}-\; |0\rangle$$

$$a\,|0\rangle + b\,|1\rangle \;-\boxed{X}-\; b\,|0\rangle + a\,|1\rangle$$

Special 1-Qubit Gates: $\sqrt{\text{NOT}}$ Gate

The simplest 1-qubit **non-classical** gate is a fractional power of NOT gate, such as:

$$\sqrt{\text{NOT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{\frac{1}{2}} = \begin{pmatrix} \frac{1}{2}+\frac{i}{2} & \frac{1}{2}-\frac{i}{2} \\ \frac{1}{2}-\frac{i}{2} & \frac{1}{2}+\frac{i}{2} \end{pmatrix}$$

Properties
1. A repeated application of the gate is equivalent to NOT: $\sqrt{\text{NOT}} \cdot \sqrt{\text{NOT}} = \text{NOT}$
2. A single application results in a **quantum state** that neither corresponds to the classical bit 0 or 1.
3. $\sqrt{\text{NOT}}$ is the first truly 1-qubit **non-classical** gate:

$$|0\rangle \xrightarrow{\sqrt{\text{NOT}}} \left(\frac{1}{2}+\frac{i}{2}\right)|0\rangle + \left(\frac{1}{2}-\frac{i}{2}\right)|1\rangle \xrightarrow{\sqrt{\text{NOT}}} |1\rangle$$

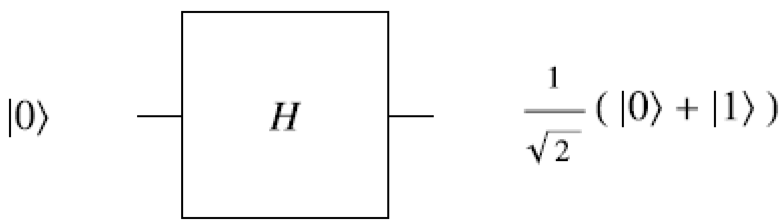
$$|1\rangle \xrightarrow{\sqrt{\text{NOT}}} \left(\frac{1}{2}-\frac{i}{2}\right)|0\rangle + \left(\frac{1}{2}+\frac{i}{2}\right)|1\rangle \xrightarrow{\sqrt{\text{NOT}}} |0\rangle$$

Special 1-Qubit Gates: Hadamard Gate

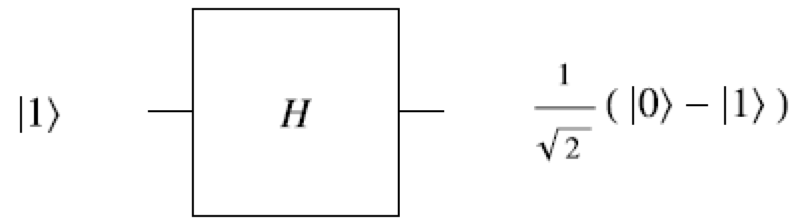
The most useful single qubit gate is the Walsh-Hadamard gate, *H*: $$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

It acts so as to map computational basis states into superposition states and vice versa:

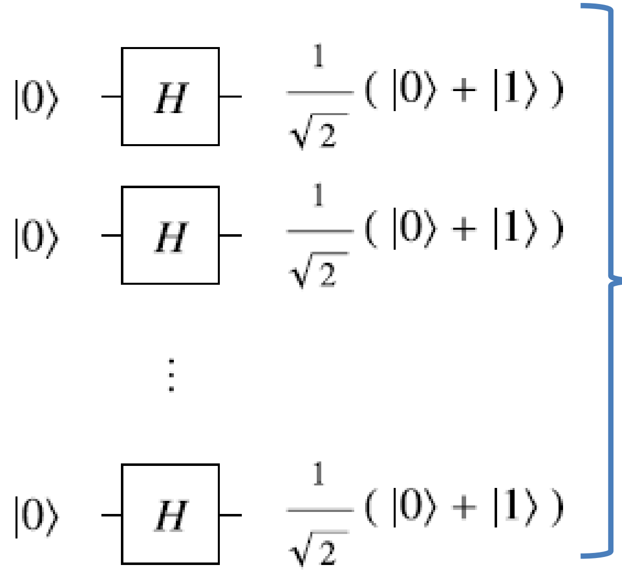
$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



By applying in parallel, n *H*-gates independently to n qubits, an n-qubit superposition is created whose component eigenstates are the binary representation of all the integers in the range 0 to $2^n - 1$.



$$\equiv \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle$$

A superposition containing exponentially many terms can be prepared using only a polynomial number of operations.

H-gate transforms the input according to

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$$

Rotations About the x-, y-, and z-Axes

What is the most general kind of quantum gate for a single qubit?

- ✓ We have to show how to implement a controlled *U* gate, *C(U)*, for any single qubit unitary transformation *U*. For any matrix or linear map ***A*** we formally write:

$$e^A = I + \frac{A^1}{1!} + \frac{A^2}{2!} + \cdots + \frac{A^n}{n!} + \cdots.$$

- ✓ If $\boldsymbol{A^2} = I$, then we have:

$$e^{iAx} \quad = \quad I + i\frac{x^1}{1!}A - \frac{x^2}{2!}I - i\frac{x^3}{3!}A + \cdots \quad = \quad \cos(x)I + i\sin(x)A$$

- ✓ In particular, this holds for the Pauli matrices *X*, *Y* and *Z* since $X^2 = Y^2 = Z^2 = I$

Definition

The rotation operators around the x, y and z axes of the Bloch sphere are respectively defined as:

$$R_x(\theta) = e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X,$$

$$R_y(\theta) = e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y,$$

$$R_z(\theta) = e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z.$$

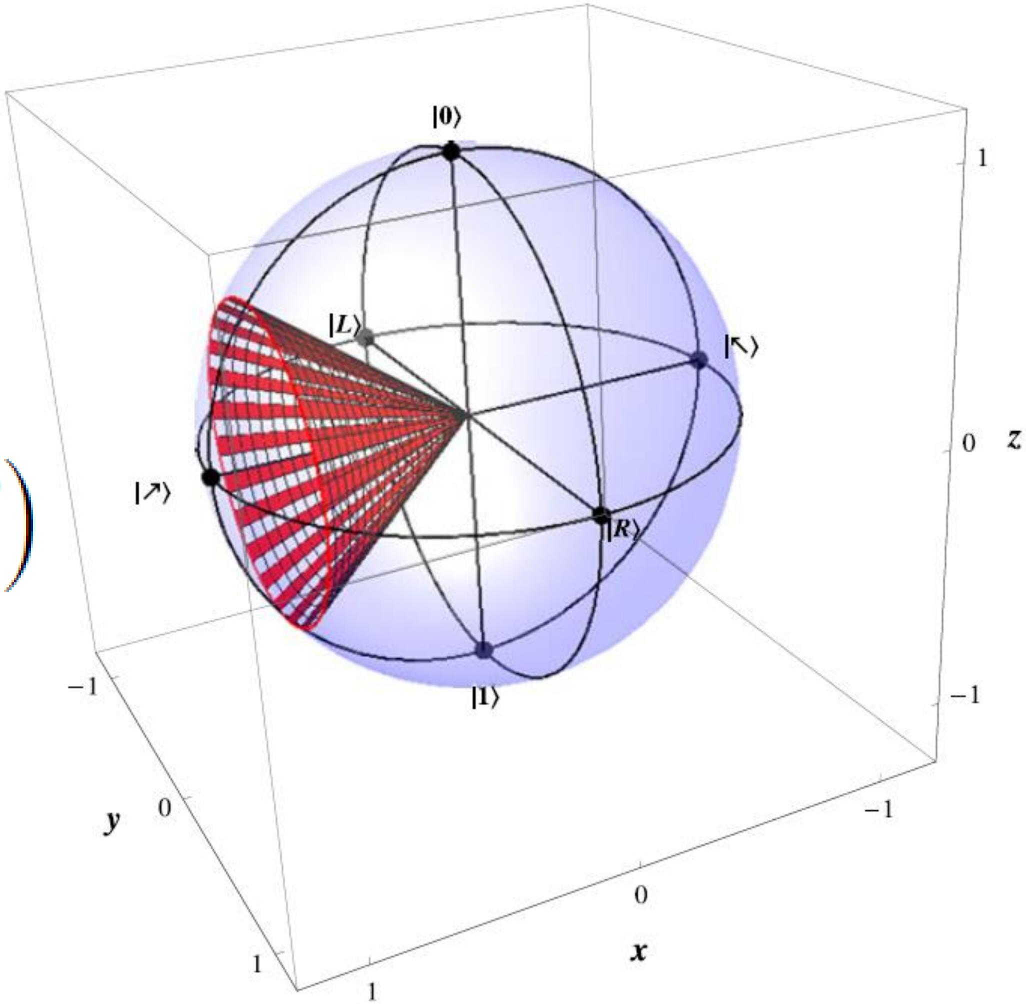
$R_x(\theta)$ gate

An $R_x(\theta)$ gate maps a state $|\psi\rangle$ on the surface of the Bloch sphere to a new state, $R_x(\theta)|\psi\rangle$, represented by the point obtained by rotating a radius vector from the center of the Bloch sphere to $|\psi\rangle$ through an angle θ/2 around the x-axis.

A rotation of 4π is needed to return to the original state.

$$R_x(\alpha) = \exp(-i\alpha X/2) =$$

$$= \begin{pmatrix} \cos(\frac{\alpha}{2}) & -i\sin(\frac{\alpha}{2}) \\ -i\sin(\frac{\alpha}{2}) & \cos(\frac{\alpha}{2}) \end{pmatrix}$$



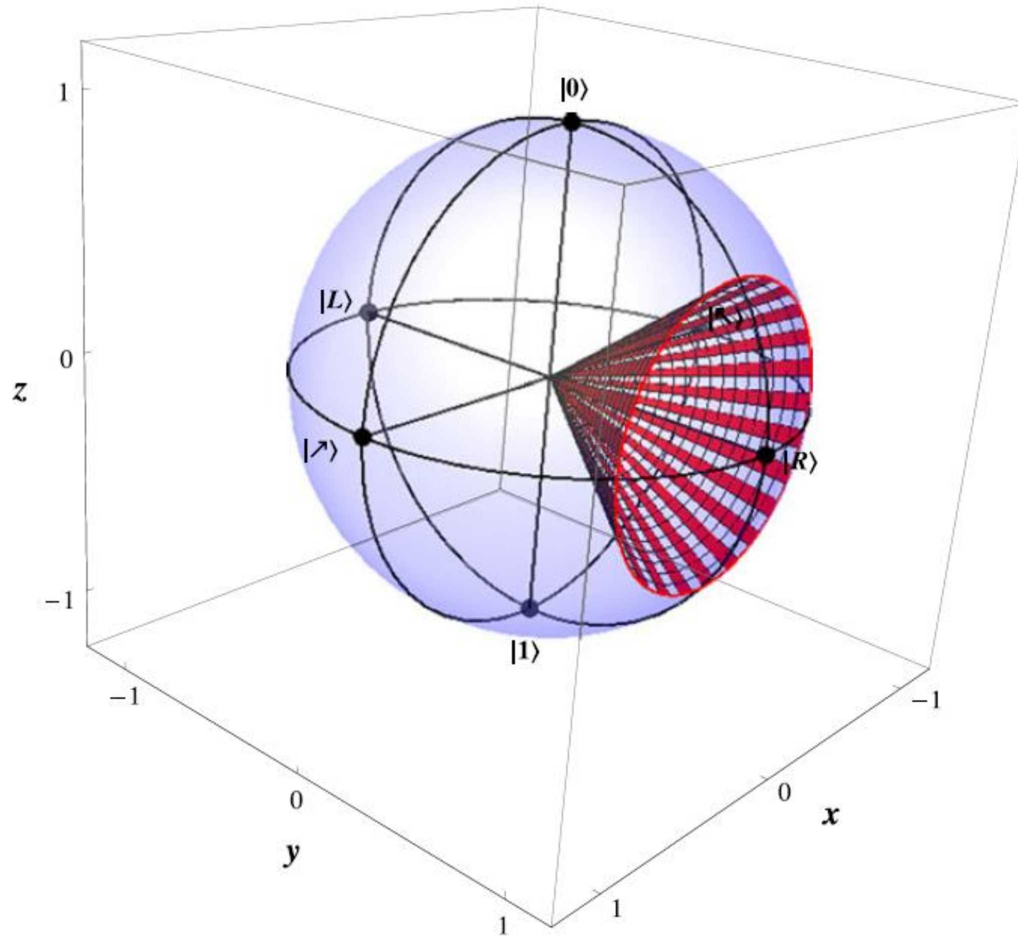
$R_y(\theta)$ gate

An $R_y(\theta)$ gate maps a state $|\psi\rangle$ on the surface of the Bloch sphere to a new state, $R_y(\theta)|\psi\rangle$, represented by the point obtained by rotating a radius vector from the center of the Bloch sphere to $|\psi\rangle$ through an angle θ/2 around the y-axis.

A rotation of 4π is needed to return to the original state.

$$R_y(\alpha) = \exp(-i\alpha Y/2) =$$

$$= \begin{pmatrix} \cos(\frac{\alpha}{2}) & -\sin(\frac{\alpha}{2}) \\ \sin(\frac{\alpha}{2}) & \cos(\frac{\alpha}{2}) \end{pmatrix}$$



$R_z(\theta)$ a *z-rotation* gate

An $R_z(\theta)$ gate maps a state $|\psi\rangle$ on the surface of the Bloch sphere to a new state, $R_z(\theta|\psi\rangle$, represented by the point obtained by rotating a radius vector from the center of the Bloch sphere to $|\psi\rangle$ through an angle θ/2 around the z-axis.

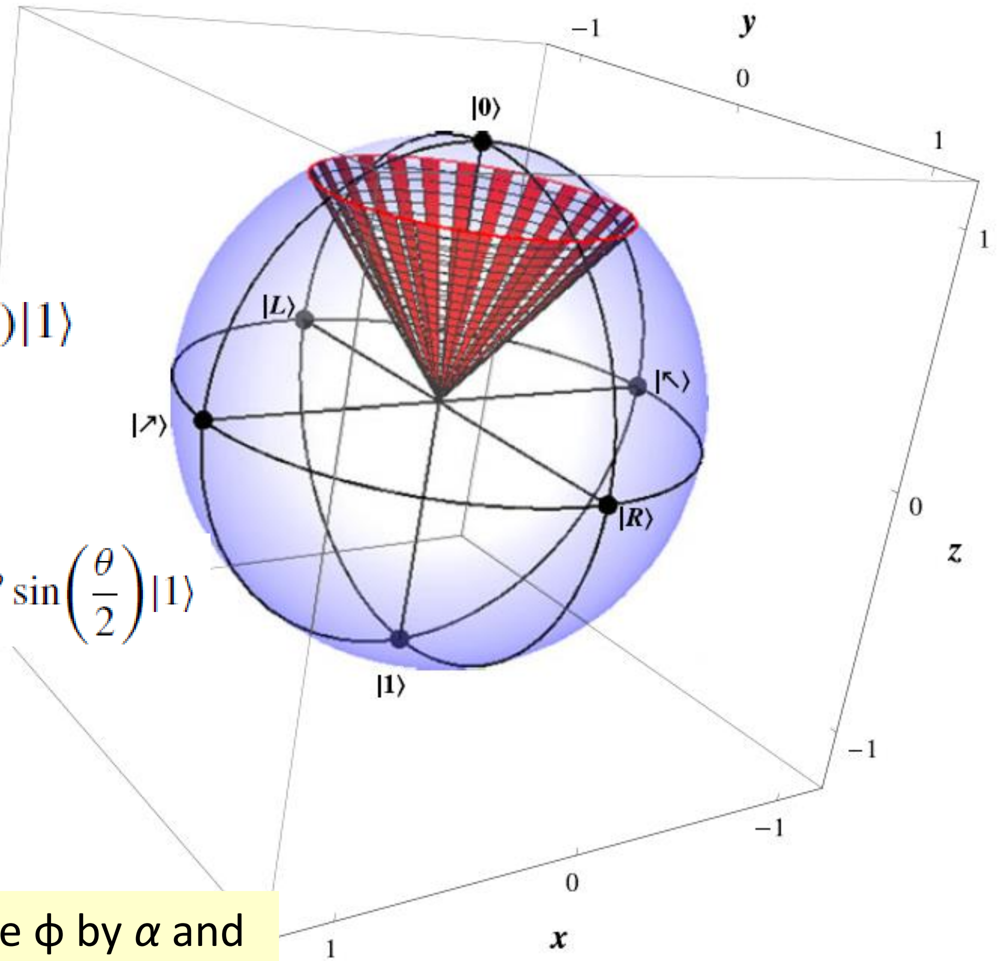
A rotation of 4π is needed to return to the original state.

$$R_z(\alpha) = \exp(-i\alpha Z/2) = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix}$$

Action of $R_z(\alpha)$ on $|\psi\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle$

$$R_z(\alpha)|\psi\rangle = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix} \cdot \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix}$$

$$= \begin{pmatrix} e^{-i\alpha/2}\cos\left(\frac{\theta}{2}\right) \\ e^{i\alpha/2}e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} = e^{-i\alpha/2}\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\alpha/2}e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$



If we multiply by a phase factor of *exp*($i\alpha/2$):

$$R_z(\alpha)|\psi\rangle \equiv \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i(\phi+\alpha)}\sin\left(\frac{\theta}{2}\right)$$

The action of $R_z(\alpha)$ gate is to advance the angle ϕ by α and hence rotate the state about the z-axis through angle α.

The phase $Ph(\delta)$ gate

If U is a single qubit unitary operation, then there exist α, β, γ and δ such that $U = e^{i\delta}R_z(\alpha)R_y(\beta)R_z(\gamma)$.

$$U \equiv -\boxed{R_z(a)}-\boxed{R_y(b)}-\boxed{R_z(c)}-\boxed{Ph(d)}-$$

A phase $Ph(\delta)$ gate is defined by the identity matrix I: $Ph(\delta) = e^{i\delta}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

The NOT, √NOT, and Hadamard gates can be obtained via sequences of rotation gates:

$$\text{NOT} \equiv R_x(\pi) \cdot Ph\left(\frac{\pi}{2}\right)$$

$$\text{NOT} \equiv R_y(\pi) \cdot R_z(\pi) \cdot Ph\left(\frac{\pi}{2}\right)$$

$$\sqrt{\text{NOT}} \equiv R_x\left(\frac{\pi}{2}\right) \cdot Ph\left(\frac{\pi}{4}\right)$$

$$\sqrt{\text{NOT}} \equiv R_z\left(-\frac{\pi}{2}\right) \cdot R_y\left(\frac{\pi}{2}\right) \cdot R_z\left(\frac{\pi}{2}\right) \cdot Ph\left(\frac{\pi}{4}\right)$$

$$H \equiv R_x(\pi) \cdot R_y\left(\frac{\pi}{2}\right) \cdot Ph\left(\frac{\pi}{2}\right)$$

$$H \equiv R_y\left(\frac{\pi}{2}\right) \cdot R_z(\pi) \cdot Ph\left(\frac{\pi}{2}\right)$$

The Hadamard gate, the phase gates π/2 and π/4, and the CNOT gate together form a finite universal set of gates: any unitary transformation on two or more qubits can be efficiently approximated as accurately as desired by a circuit with a finite number of these gates.

Decomposition of $R_x(\theta)$ Gate

Since any arbitrary 1-qubit gate can be achieved without performing a rotation about the x-axis, we note that it is possible to express rotations about the x-axis purely in terms of rotations about the y- and z-axes.

$$R_x(\theta) = \exp(-i\theta X/2) = \begin{pmatrix} \cos(\frac{\theta}{2}) & i\sin(\frac{\theta}{2}) \\ i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$$

$$\equiv R_z(-\pi/2)\cdot R_y(\theta)\cdot R_z(\pi/2)$$

$$\equiv R_y(\pi/2)\cdot R_z(\theta)\cdot R_y(-\pi/2)$$

where **≡** is to be read as "equal up to an unimportant arbitrary overall phase factor".

Exercise

Check that $XYX = -Y$ and $XZX = -Z$;

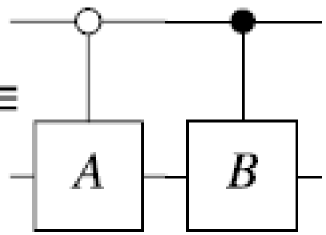
then show that $XR_y(\theta)X = R_y(-\theta)$ and $XR_z(\theta)X = R_z(-\theta)$.

Controlled Quantum Gates

- Non-trivial computations change the operation applied to one set of qubits depending upon the values of some other set of qubits.
- The gates that implement these "if-then-else" type operations are called controlled gates.

The quantum circuit corresponding to a gate that performs different control actions according to whether the top qubit is $|0\rangle$ or $|1\rangle$.

$A \oplus B \equiv$



- ✓ If a controlled quantum gate acts on a superposition state all of the control actions are performed in parallel and we do not need to read control bits during its application.
- ✓ Let A and B be a pair of unitary matrices corresponding to arbitrary 1-qubit quantum gates. Then the gate defined by their direct sum:

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} & 0 & 0 \\ A_{21} & A_{22} & 0 & 0 \\ 0 & 0 & B_{11} & B_{12} \\ 0 & 0 & B_{21} & B_{22} \end{pmatrix}$$

performs a "controlled" operation in the following sense.

“Controlled” Gate in the Quantum Context

- ✓ If the first qubit is in state $|0\rangle$, the input state is: $|0\rangle(a|0\rangle + b|1\rangle)$, and upon the gate action:

$$(A \oplus B)(|0\rangle \otimes (a|0\rangle + b|1\rangle)) = \begin{pmatrix} A_{11} & A_{12} & 0 & 0 \\ A_{21} & A_{22} & 0 & 0 \\ 0 & 0 & B_{11} & B_{12} \\ 0 & 0 & B_{21} & B_{22} \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} aA_{11} + bA_{12} \\ aA_{21} + bA_{22} \\ 0 \\ 0 \end{pmatrix}$$

$$= (aA_{11} + bA_{12})|00\rangle + (aA_{21} + bA_{22})|01\rangle = |0\rangle \otimes A(a|0\rangle + b|1\rangle)$$

- ✓ If the first qubit is in state $|1\rangle$, the input state is: $|1\rangle(a|0\rangle + b|1\rangle)$, and upon the gate action:

$$(A \oplus B)(|1\rangle \otimes (a|0\rangle + b|1\rangle)) = \begin{pmatrix} A_{11} & A_{12} & 0 & 0 \\ A_{21} & A_{22} & 0 & 0 \\ 0 & 0 & B_{11} & B_{12} \\ 0 & 0 & B_{21} & B_{22} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ aB_{11} + bB_{12} \\ aB_{21} + bB_{22} \end{pmatrix}$$

$$= (aB_{11} + bB_{12})|10\rangle + (aB_{21} + bB_{22})|11\rangle = |1\rangle \otimes B(a|0\rangle + b|1\rangle)$$

Overall, when the 2-qubit controlled gate (A ⊕ B) acts on a general 2-qubit superposition state $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ the control qubit is no longer purely $|0\rangle$ or purely $|1\rangle$.

The linearity of quantum mechanics guarantees that the correct control actions are performed, in the correct proportions, on the target qubit:

$$(A \oplus B)|\psi\rangle = |0\rangle \otimes A(a|0\rangle + b|1\rangle) + |1\rangle \otimes B(c|0\rangle + d|1\rangle)$$

Classical reversible gates *vs* quantum gates

- ✓ CNOT, FREDKIN (controlled-SWAP), and TOFFOLI (controlled-controlled-NOT) are classical reversible gates, but in addition they are also quantum gates because the transformations (permutations of computational basis states) are unitary.
- ✓ However, controlled quantum gates can be far more sophisticated than controlled classical gates.
- ✓ For example, the quantum generalization of the CNOT gate is the controlled-U gate:

$$\text{controlled-}U \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix} \qquad \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \text{ is an arbitrary 1-qubit gate.}$$

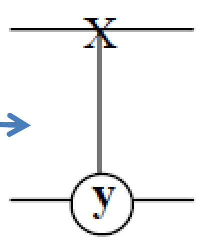
Any *d*-dimensional unitary matrix on $\mathbb{C}^d$ can be written as the composition of at most: *d*(*d*−1)/2, two-dimensional unitary matrices.

A general way of writing a 2-dimensional unitary matrix, except for an overall phase factor, is

$$y(\lambda,\nu,\phi) = \begin{bmatrix} \cos\lambda & -e^{i\nu}\sin\lambda \\ e^{i(\varphi-\nu)}\sin\lambda & e^{i\varphi}\cos\lambda \end{bmatrix}$$

A family of universal 2-qubit gates can be built using y,

$$\Gamma_2[y] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\lambda & -e^{i\nu}\sin\lambda \\ 0 & 0 & e^{i(\varphi-\nu)}\sin\lambda & e^{i\varphi}\cos\lambda \end{bmatrix} \longleftrightarrow$$

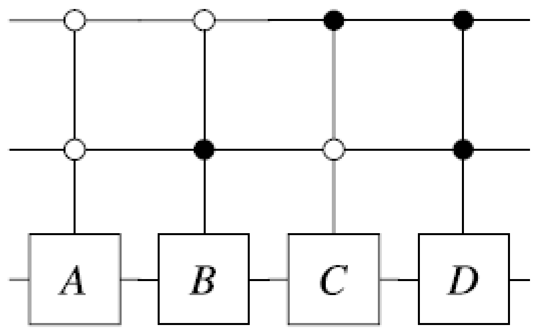


The Γ_2[y] means that this is a 2-qubit gate which applies y to the 2nd qubit conditional on the 1st qubit being in $|1\rangle$.

Multiply-Controlled Gates

Controlled gates can be generalized to have multiple controls, where a different operation is performed on the third qubit depending on the state of the top two qubits.

✓ For example, the quantum circuit corresponding to a gate that performs different control actions according to whether the top two qubits are $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$, is:



$$\equiv \begin{pmatrix} A & 0 & 0 & 0 \\ 0 & B & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & D \end{pmatrix} \equiv A \oplus B \oplus C \oplus D$$

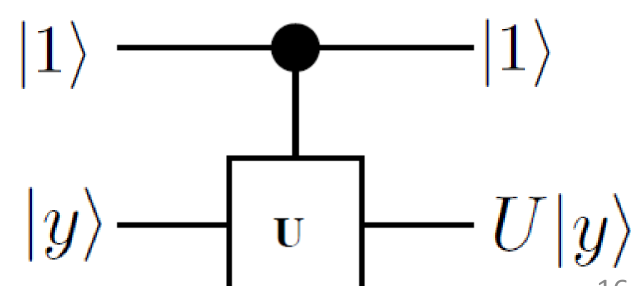
The number of distinct states of the controls grows exponentially with the number of controls!

Such controlled gates can be decomposed into a simpler set of standard gates by factoring a controlled gate as in $A \oplus B = (\mathbb{1} \otimes A) \cdot (\mathbb{1} \otimes A^{-1} \cdot B)$ where $\mathbb{1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

The core "controlled" component of the gate is $\begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} = A^{-1} \cdot B$, of the controlled-U.

Generally, the controlled-U transform for any 1-qubit unitary transform U, maps

$$\begin{cases} |0\rangle|y\rangle \longrightarrow |0\rangle|y\rangle \\ |1\rangle|y\rangle \longrightarrow |1\rangle(U|y\rangle \end{cases}$$



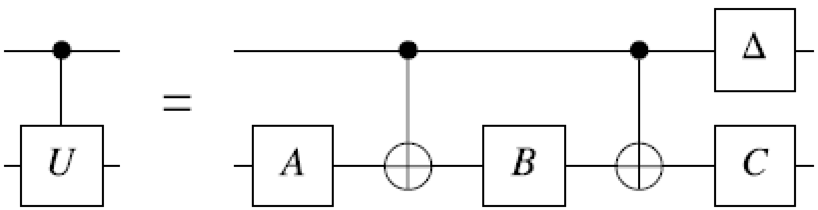
Quantum circuit for a 2-qubit controlled-U gate

Given the quantum circuit decomposition for computing $U = e^{ia} R_z(b) \cdot R_y(c) \cdot R_z(d)$, what is a quantum circuit that computes controlled-U?

✓ We can construct a quantum circuit for a 2-qubit controlled-U gate in terms of CNOT gates and 1-qubit gates as follows. Given the angles *a*, *b*, *c*, and *d*, define matrices *A*, *B*, *C* as:

$$A = R_z\left(\frac{d-b}{2}\right) \quad B = R_y\left(-\frac{c}{2}\right) \cdot R_z\left(-\frac{d+b}{2}\right) \quad C = R_z(b) \cdot R_y\left(\frac{c}{2}\right) \quad \Delta = \mathrm{diag}(1, e^{ia})$$

A quantum circuit that computes an arbitrary 1-qubit controlled-U is:



The transformation to which the target qubit will be subject when the control qubit in the circuit is $|0\rangle$: $(C \cdot (B \cdot (A|\psi\rangle)))$ (*gate A first then gate B then gate C*)

The net effect of these three operations is the identity (as required).

$$C \cdot B \cdot A \equiv R_z(b) \cdot R_y\left(\frac{c}{2}\right) \cdot R_y\left(-\frac{c}{2}\right) \cdot R_z\left(-\frac{d+b}{2}\right) \cdot R_z\left(\frac{d-b}{2}\right) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The transformation to which the target qubit will be subject when the control qubit in the circuit is $|1\rangle$: $e^{ia} C \cdot X \cdot B \cdot X \cdot A$ (the control qubit first picks up a phase factor since $\Delta|1\rangle = e^{ia}|1\rangle$)

$$X \cdot R_y(\theta) \cdot X \equiv R_y(-\theta)$$

$$X \cdot R_z(\theta) \cdot X \equiv R_z(-\theta)$$

$$C \cdot X \cdot B \cdot X \cdot A = R_z(b) \cdot R_y\left(\frac{c}{2}\right) \cdot X \cdot R_y\left(-\frac{c}{2}\right) \cdot R_z\left(-\frac{d+b}{2}\right) \cdot X \cdot R_z\left(\frac{d-b}{2}\right)$$

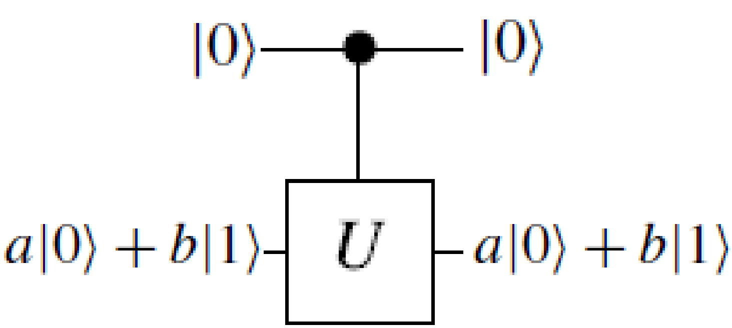
$$= R_z(b) \cdot R_y\left(\frac{c}{2}\right) \cdot R_y\left(\frac{c}{2}\right) \cdot R_z\left(\frac{b+d}{2}\right) \cdot R_z\left(\frac{d-b}{2}\right) = R_z(b) \cdot R_y(c) \cdot R_z(d)$$

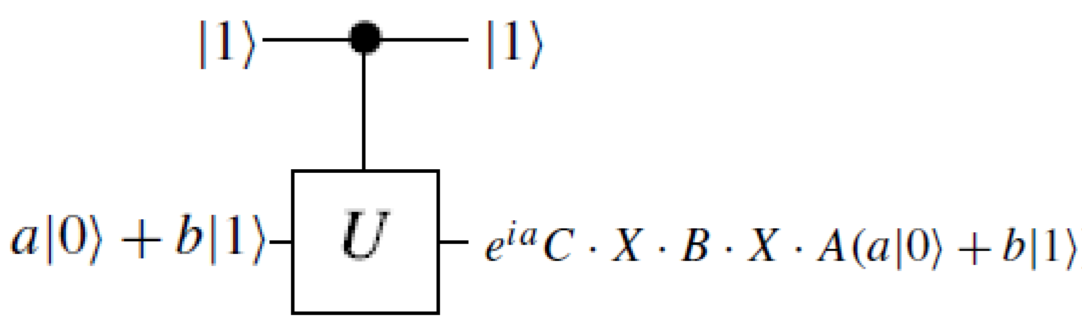
Quantum circuit for a 2-qubit controlled-U gate

Given the quantum circuit decomposition for computing $U = e^{ia} R_z(b) \cdot R_y(c) \cdot R_z(d)$, what is a quantum circuit that computes controlled-U?

✓ The circuit for controlled-U performs as follows:

$$
\begin{aligned}
\text{controlled-}U\ |0\rangle(a|0\rangle + b|1\rangle) &= |0\rangle \otimes C \cdot B \cdot A(a|0\rangle + b|1\rangle) \\
&= |0\rangle \otimes (a|0\rangle + b|1\rangle) \\
\text{controlled-}U\ |1\rangle(a|0\rangle + b|1\rangle) &= e^{ia}|1\rangle \otimes C \cdot X \cdot B \cdot X \cdot A(a|0\rangle + b|1\rangle) \\
&= |1\rangle \otimes e^{ia} C \cdot X \cdot B \cdot X \cdot A(a|0\rangle + b|1\rangle) \\
&= |1\rangle \otimes U(a|0\rangle + b|1\rangle)
\end{aligned}
$$





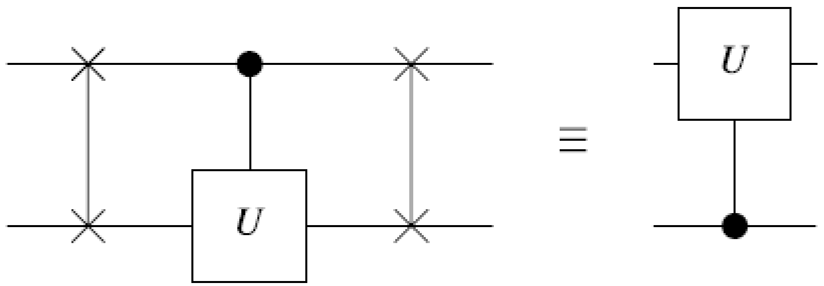
Flipping the Control and Target Qubits

- ✓ The control qubit does not have to be the topmost qubit in a quantum circuit.
- ✓ An upside down controlled-U gate would be given by:

$$\mathrm{SWAP}\cdot\text{controlled-}U\cdot\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & U_{11} & 0 & U_{12} \\ 0 & 0 & 1 & 0 \\ 0 & U_{21} & 0 & U_{22} \end{pmatrix}$$

The 2nd qubit is the control qubit and the 1st qubit the target qubit.

The result is the matrix corresponding to a 2-qubit controlled quantum gate inserted into a circuit "upside down".

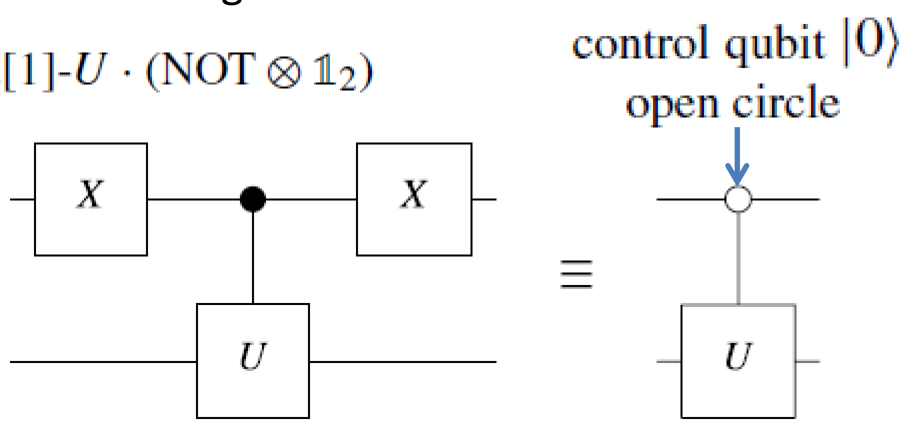


Control-on-$|0\rangle$ Quantum Gates

A 2-qubit quantum gate with the special action conditioned on the value of the first qubit being $|0\rangle$ instead of $|1\rangle$ is related to usual controlled gate as:

$$\text{controlled}[0]\text{-}U = (\mathrm{NOT}\otimes \mathbb{1}_2)\cdot\text{controlled}[1]\text{-}U\cdot(\mathrm{NOT}\otimes \mathbb{1}_2)$$

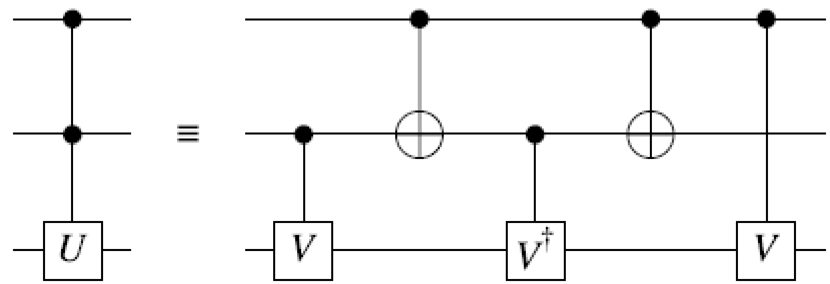
$$= \begin{pmatrix} U_{11} & U_{12} & 0 & 0 \\ U_{21} & U_{22} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



Circuit for Controlled-Controlled-U

Generalizing the controlled-controlled-NOT (TOFFOLI) gate leads us to consider a controlled-controlled-*U* gate, where *U* is an arbitrary 1-qubit gate:

$$\text{controlled-controlled-}U \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & 0 & 0 & 0 & 0 & U_{21} & U_{22} \end{pmatrix}$$



Any controlled-controlled-*U* gate is a circuit built from only CNOT gates and 1-qubit gates, such as that $V^2 = U$.

$$|000\rangle \xrightarrow{\text{ctrl-ctrl-}U} |000\rangle$$

$$|001\rangle \xrightarrow{\text{ctrl-ctrl-}U} |001\rangle$$

$$|010\rangle \xrightarrow{\text{ctrl-ctrl-}U} |01\rangle \otimes (V^\dagger \cdot V|0\rangle) = |010\rangle$$

$$|011\rangle \xrightarrow{\text{ctrl-ctrl-}U} |01\rangle \otimes (V^\dagger \cdot V|1\rangle) = |011\rangle$$

$$|100\rangle \xrightarrow{\text{ctrl-ctrl-}U} |10\rangle \otimes (V \cdot V^\dagger|0\rangle) = |100\rangle$$

$$|101\rangle \xrightarrow{\text{ctrl-ctrl-}U} |10\rangle \otimes (V \cdot V^\dagger|1\rangle) = |101\rangle$$

$$|110\rangle \xrightarrow{\text{ctrl-ctrl-}U} |11\rangle \otimes V^2|0\rangle = |11\rangle \otimes U|0\rangle$$

$$|111\rangle \xrightarrow{\text{ctrl-ctrl-U}} |11\rangle \otimes V^2|1\rangle = |11\rangle \otimes U|1\rangle$$

Operation of this circuit to the eight possible computational basis states of a 3-qubit system .