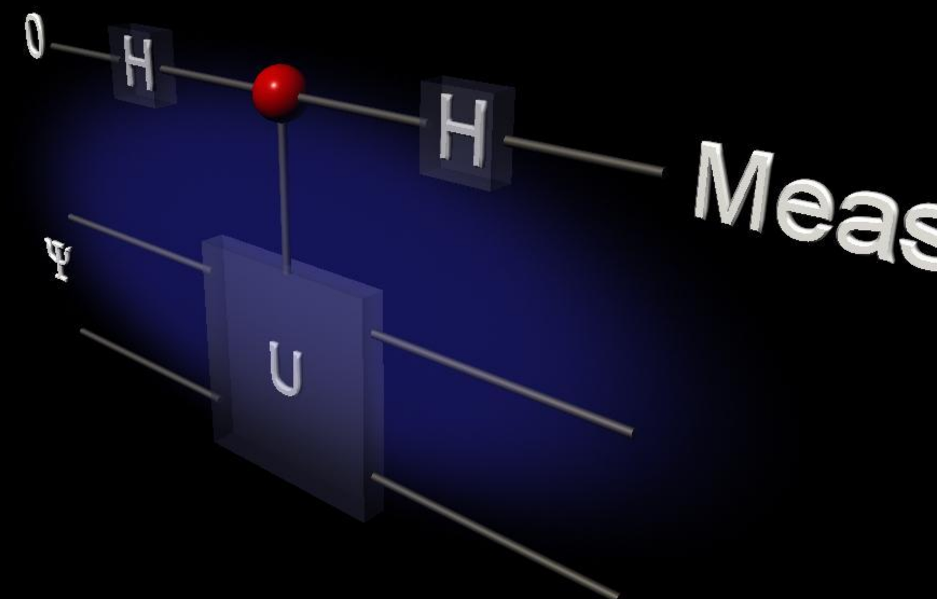
Introduction to Quantum Information Processing



CO481 CS467 PHYS467

Michele Mosca mmosca@iqc.uwaterloo.ca

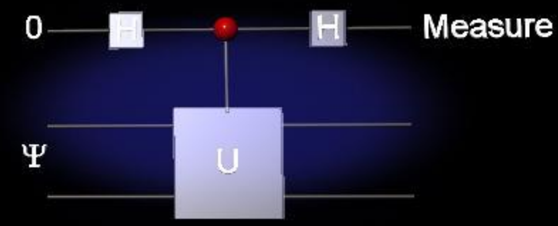
Lecture 3 (15 January 2013) by Dr. David Gosset

IQC Institute for Quantum Computing

UNIVERSITY OF WATERLOO

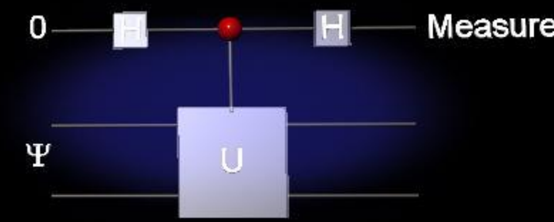
PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

Overview



- Quantum circuit model (sections 1.7 and 4.1)
- A bit more about Dirac notation (sections 2.1, 2.2, 2.3)
- Quantum universality (Page 56, Sections 2.4 – 2.6, 4.1, 4.2.1, 4.3, 4.4, 6.1)
  - The Bloch Sphere
  - Single qubit gates
  - Universal sets of quantum gates
  - Efficiency of approximating unitary transformations

Different acyclic circuit models

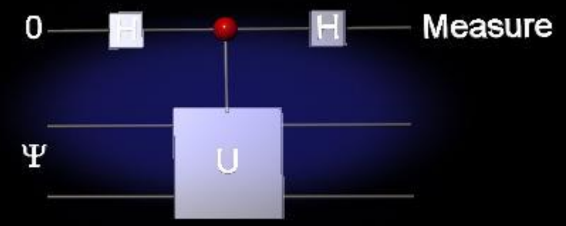


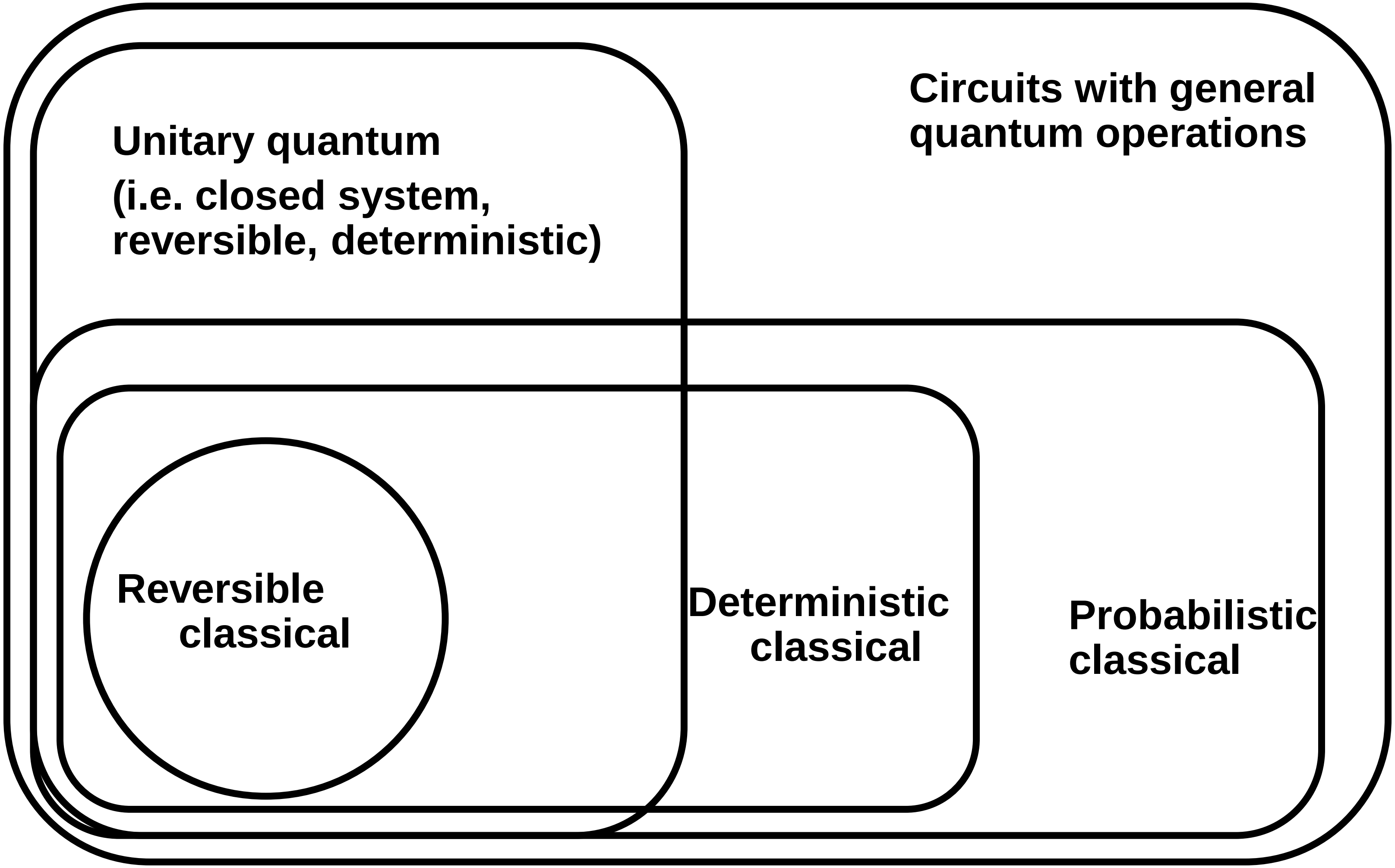
increasing capabilities →

increasing capabilities ↓

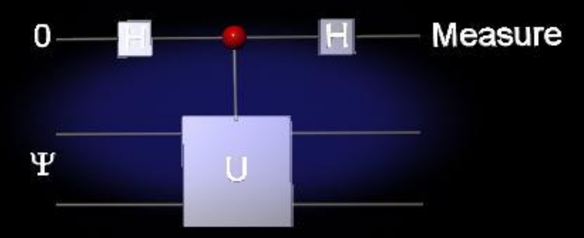
	Closed system (i.e. reversible)	Open system (i.e. not necessarily reversible)	
classical	Classical reversible circuit model	(without randomness) Deterministic classical circuit model	(with randomness) Probabilistic classical circuit model
quantum	Quantum circuit model with unitary gates	Quantum circuit model with general quantum gates	

Relationship between some acyclic circuit models



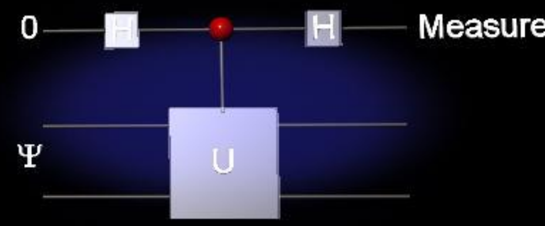


Relationship between these models

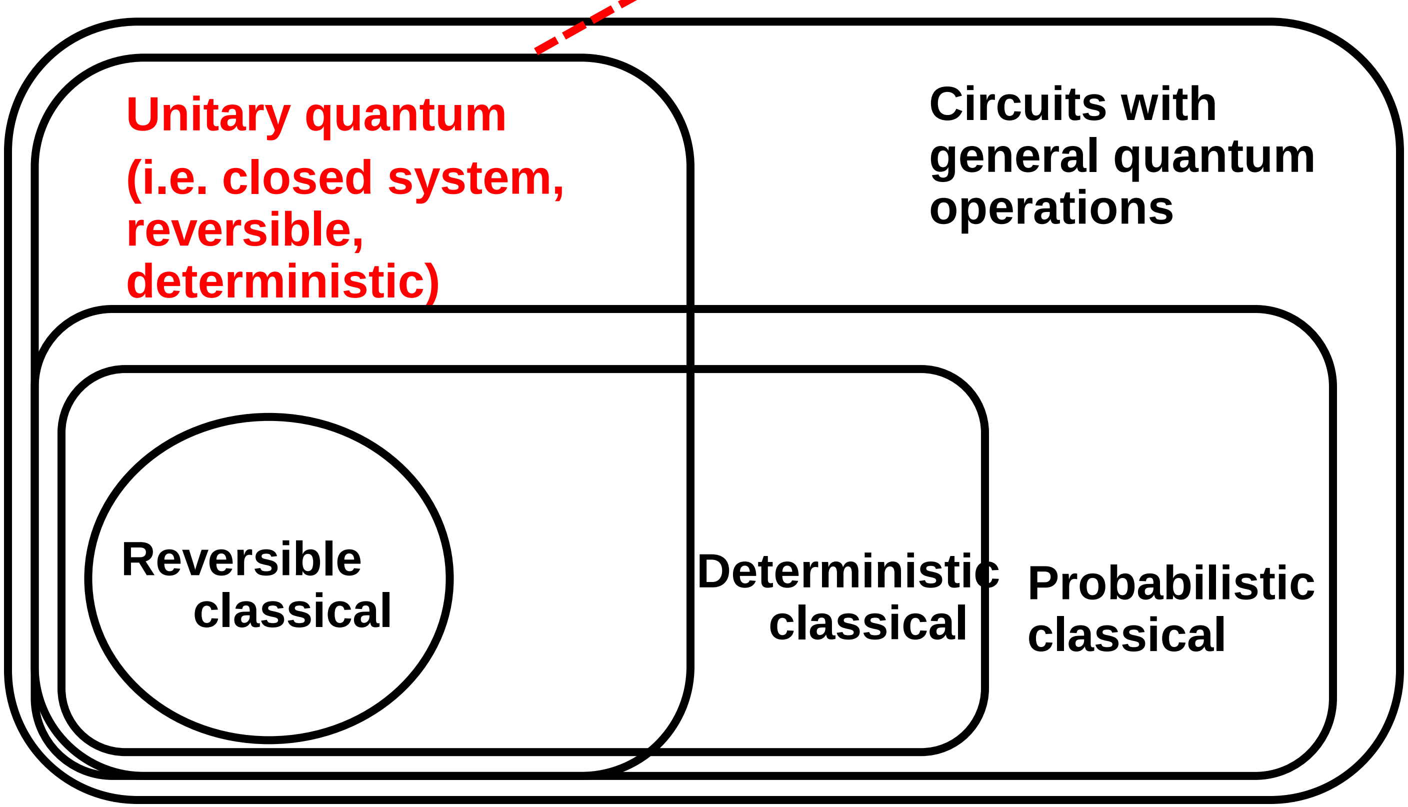


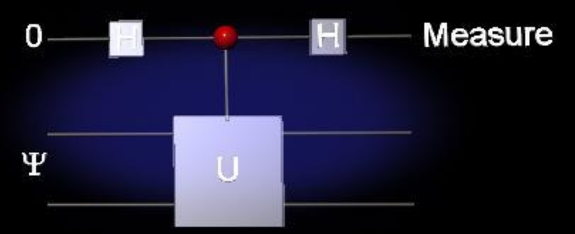
- If the operations of circuit model A are a subset of the operations of circuit model B, then clearly circuit model B is at least as powerful as circuit model A.
- We have also seen that the reversible classical circuit model can efficiently simulate general deterministic circuit model
- It is still not known whether probabilistic classical circuits are computationally more powerful than deterministic classical circuits (i.e. is BPP = P?)
- Unitary quantum circuits can efficiently simulate quantum circuits with general quantum gates
- Any universal set of gates for the reversible classical circuit model needs a 3-bit gate. This contrasts with the quantum case, where we only need 2-qubit interactions to achieve universality.

Relationship between some acyclic circuit models



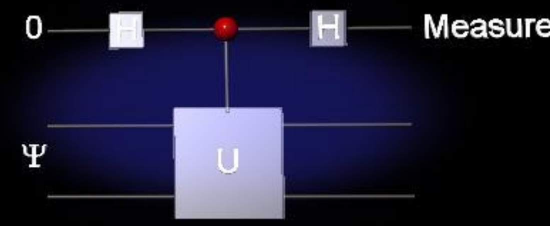
Unitary quantum model can efficiently simulate all the other computational models.





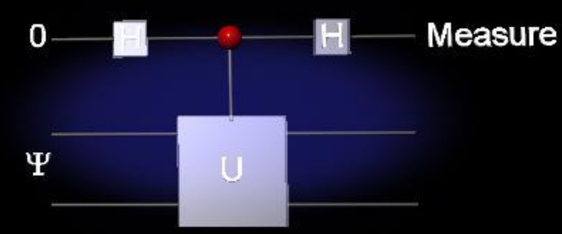
Summary

- For most of this course we restrict attention to the unitary circuit model. Why?
- As mentioned already, this model has the full computational power of the more general circuit model.
- The notation for the unitary circuit model is much simpler.
- Most of the literature and books, especially introductory material, focus on this model.



Dirac notation

Dirac notation

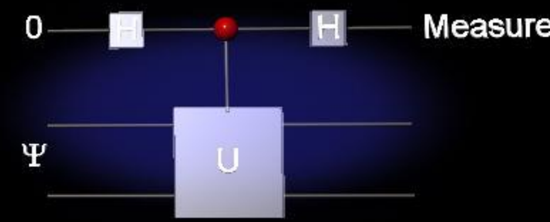


For any vector $|\psi\rangle$, we let $\langle\psi|$ denote $|\psi\rangle^\dagger$, the complex conjugate of $|\psi\rangle$.

e.g. If $$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

then $$\langle\psi| = \alpha^*\langle 0| + \beta^*\langle 1| \equiv \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$$

We denote by $\langle\phi|\psi\rangle = \langle\phi|\cdot|\psi\rangle$ the inner product between two vectors $|\psi\rangle$ and $|\varphi\rangle$.



Dirac notation

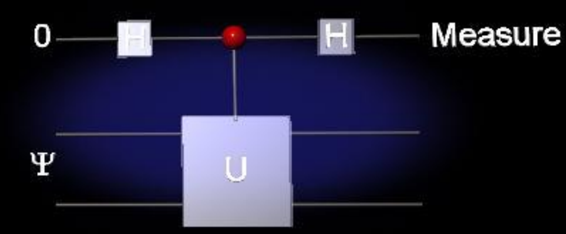
e.g. $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ $\qquad |\varphi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$

$$\langle\phi|\psi\rangle = \langle\phi|\cdot|\psi\rangle = \left(\frac{1}{\sqrt{2}}\langle 0| - \frac{i}{\sqrt{2}}\langle 1|\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$= \frac{1}{2}\langle 0||\cdot|0\rangle + \frac{1}{2}\langle 0||\cdot|1\rangle - \frac{i}{2}\langle 1||\cdot|0\rangle - \frac{i}{2}\langle 1||\cdot|1\rangle$$

$$= \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot 0 - \frac{i}{2}\cdot 0 - \frac{i}{2}\cdot 1 = \frac{1+i}{2}$$

Dirac notation



Can also think of $\langle\psi|$ as a linear function that maps $|\phi\rangle \mapsto \langle\psi|\phi\rangle$

i.e. $\langle\psi|\left(|\phi\rangle\right) = \langle\psi|\phi\rangle$

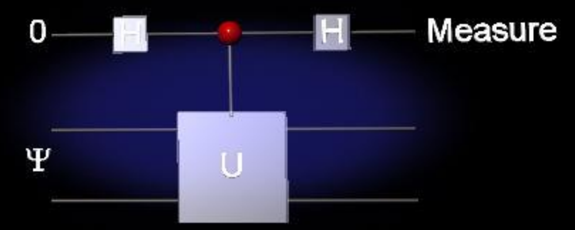
… it maps any state $|\varphi\rangle$ to the coefficient of its $|\psi\rangle$ component

e.g. $|\psi_+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ $\quad |\psi_-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$

$$|\varphi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = \frac{1+i}{2}|\psi_+\rangle + \frac{1-i}{2}|\psi_-\rangle$$

$$\langle\psi_+\|\varphi\rangle = \langle\psi_+\|\left(\frac{1+i}{2}|\psi_+\rangle + \frac{1-i}{2}|\psi_-\rangle\right) = \frac{1+i}{2}\langle\psi_+\|\psi_+\rangle + \frac{1-i}{2}\langle\psi_+\|\psi_-\rangle = \frac{1+i}{2}$$

Describing operators in Dirac notation



$|\psi\rangle\langle\psi|$ defines a linear operator that maps

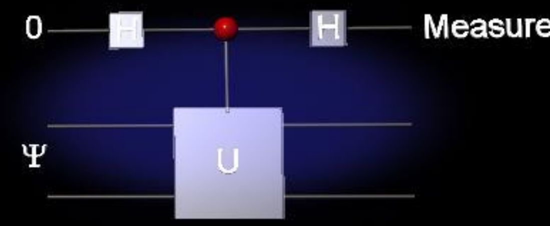
$$|\psi\rangle\langle\psi||\varphi\rangle \rightarrow |\psi\rangle\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle|\psi\rangle$$

(i.e. projects a state to its $|\psi\rangle$ component)

e.g. $$\left(|\psi_+\rangle\langle\psi_+|\right)|\varphi\rangle = |\psi_+\rangle\left(\langle\psi_+||\varphi\rangle\right) = |\psi_+\rangle\frac{1+i}{2} = \frac{1+i}{2}|\psi_+\rangle$$

(Aside: this projection operator also corresponds to the "density matrix" for $|\psi\rangle$)

Describing operators in Dirac notation

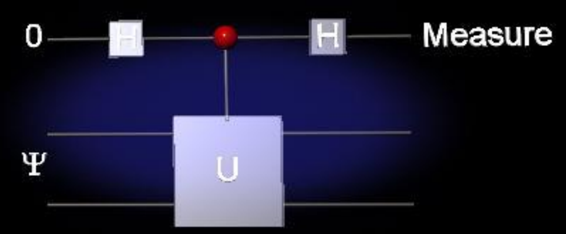


More generally, we can also have operators like

$$|\theta\rangle\langle\psi|$$

$$|\theta\rangle\langle\psi\|\varphi\rangle \rightarrow |\theta\rangle\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle|\theta\rangle$$

or sums of such “outer product” terms.



For example, the one-qubit NOT gate corresponds to the operator

$$|0\rangle\langle 1| + |1\rangle\langle 0|$$

e.g. $$\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right)\left(|0\rangle\right)$$

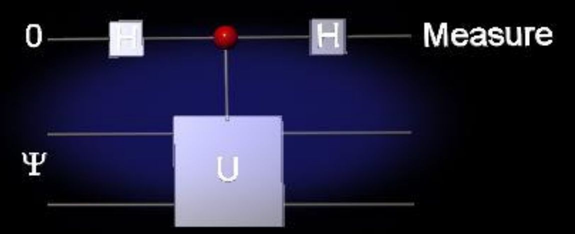
$$= |0\rangle\langle 1||0\rangle + |1\rangle\langle 0||0\rangle$$

$$= |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle$$

$$= 0|0\rangle + 1|1\rangle$$

$$= |1\rangle$$

Special unitaries: Pauli Matrices



The NOT operation, is often called the X or σ_X operation.

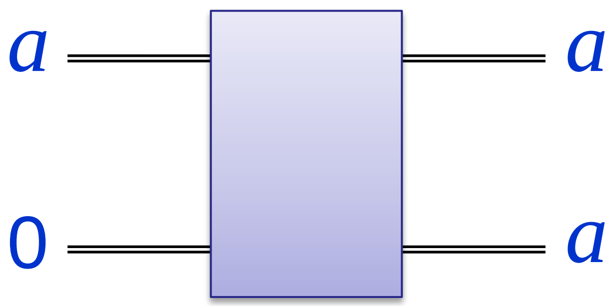
$$X = \sigma_X = NOT = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

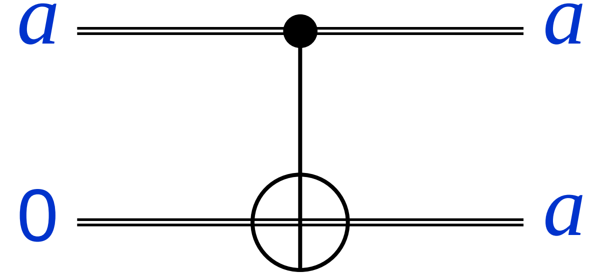
$$Z = \sigma_Z = phaseflip = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$Y = \sigma_Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0| = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

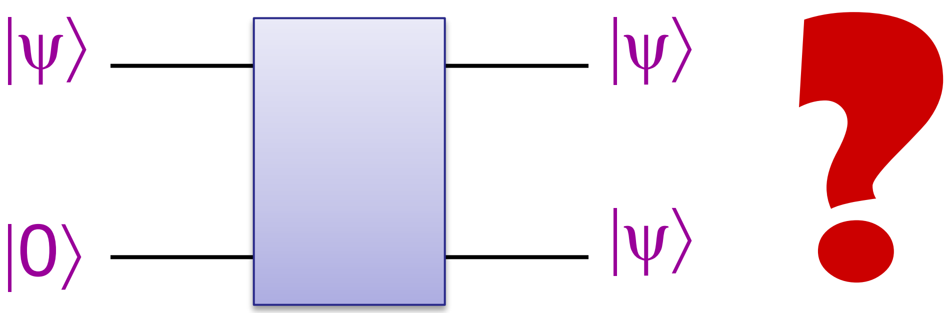
No-cloning theorem

Classical information can be copied

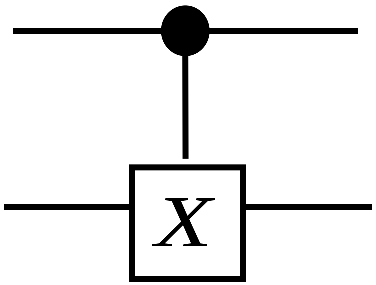




What about quantum information?



Candidate:



works fine for $|\psi\rangle = |0\rangle$ and $|\psi\rangle = |1\rangle$

... but it fails for $|\psi\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ ...

... where it yields output $(1/\sqrt{2})(|00\rangle + |11\rangle)$

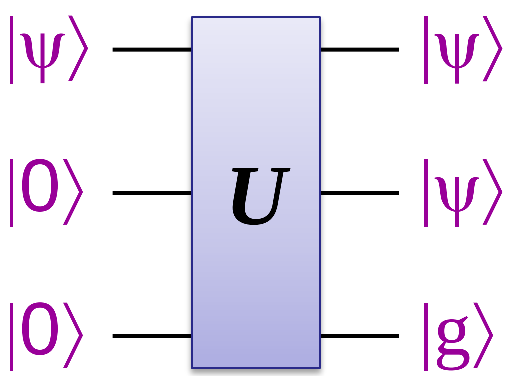
instead of $|\psi\rangle|\psi\rangle = (1/4)(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

No-cloning theorem (thm10.4.1)

Theorem:

There is ***no*** valid quantum operation that maps an arbitrary state $|\psi\rangle$ to $|\psi\rangle|\psi\rangle$;
This also holds if we restrict to $|\psi\rangle$ from a set containing at least two non-orthogonal vectors.

Proof:



Let $|\psi\rangle$ and $|\psi'\rangle$ be two distinct input states with
$0 < |\langle\psi|\psi'\rangle| < 1$, yielding outputs $|\psi\rangle|\psi\rangle|g\rangle$ and $|\psi'\rangle|\psi'\rangle|g'\rangle$ respectively

Since U preserves inner products:
$\langle\psi|\psi'\rangle\,\langle 0|0\rangle\,\langle 0|0\rangle = \langle\psi|\psi'\rangle\langle\psi|\psi'\rangle\langle g|g'\rangle$ so
$\langle\psi|\psi'\rangle(1- \langle\psi|\psi'\rangle\langle g|g'\rangle) = 0$ so
$|\langle\psi|\psi'\rangle| = 0$ or 1
We have a contradiction

Quantum universality

- The Bloch Sphere
- Single qubit gates
- Universal sets of quantum gates
- Efficiency of approximating unitary transformations

Density matrices

Consider a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Let ρ be $$|\psi\rangle\langle\psi| = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix} = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}$$

We call ρ the *density matrix* for the state. Note that it always has trace one.

Bloch Sphere

These four matrices form a basis (over **R**) for the 2x2 Hermitian matrices:

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(Pauli matrices)

So every density matrix can be written as

$$\rho = \frac{1}{2}\left(I + a_x X + a_y Y + a_z Z\right)$$

In this decomposition, just think of X, Y and Z as matrices; they are not "operating" on or transforming state vectors as we saw earlier.

Bloch Sphere

We associate with every one-qubit state

$$\rho = \frac{1}{2}(I + a_x X + a_y Y + a_z Z)$$

the vector

$$(a_x, a_y, a_z)$$

If $\rho = |\Psi\rangle\langle\Psi|$ for a state

$$|\Psi\rangle = e^{i\alpha}\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right)$$

then the corresponding vector is

$$(a_x, a_y, a_z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

Bloch Sphere

Notice that the vectors

$$(a_x, a_y, a_z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

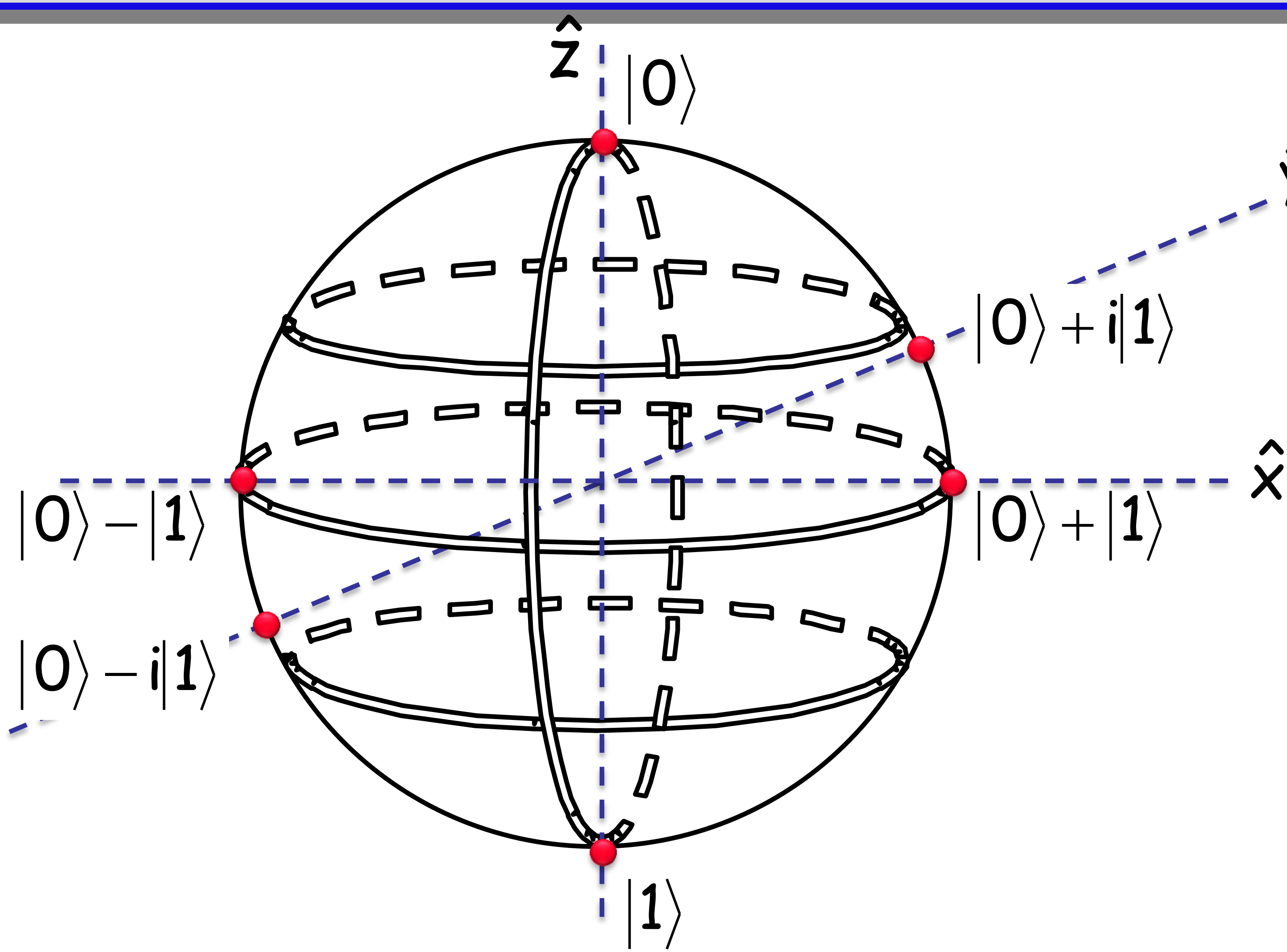
satisfy

$$|a_x|^2 + |a_y|^2 + |a_z|^2 = 1$$

Thus the quantum states we have seen so far, also known as *pure states*, lie **on the surface of** the Bloch Sphere.

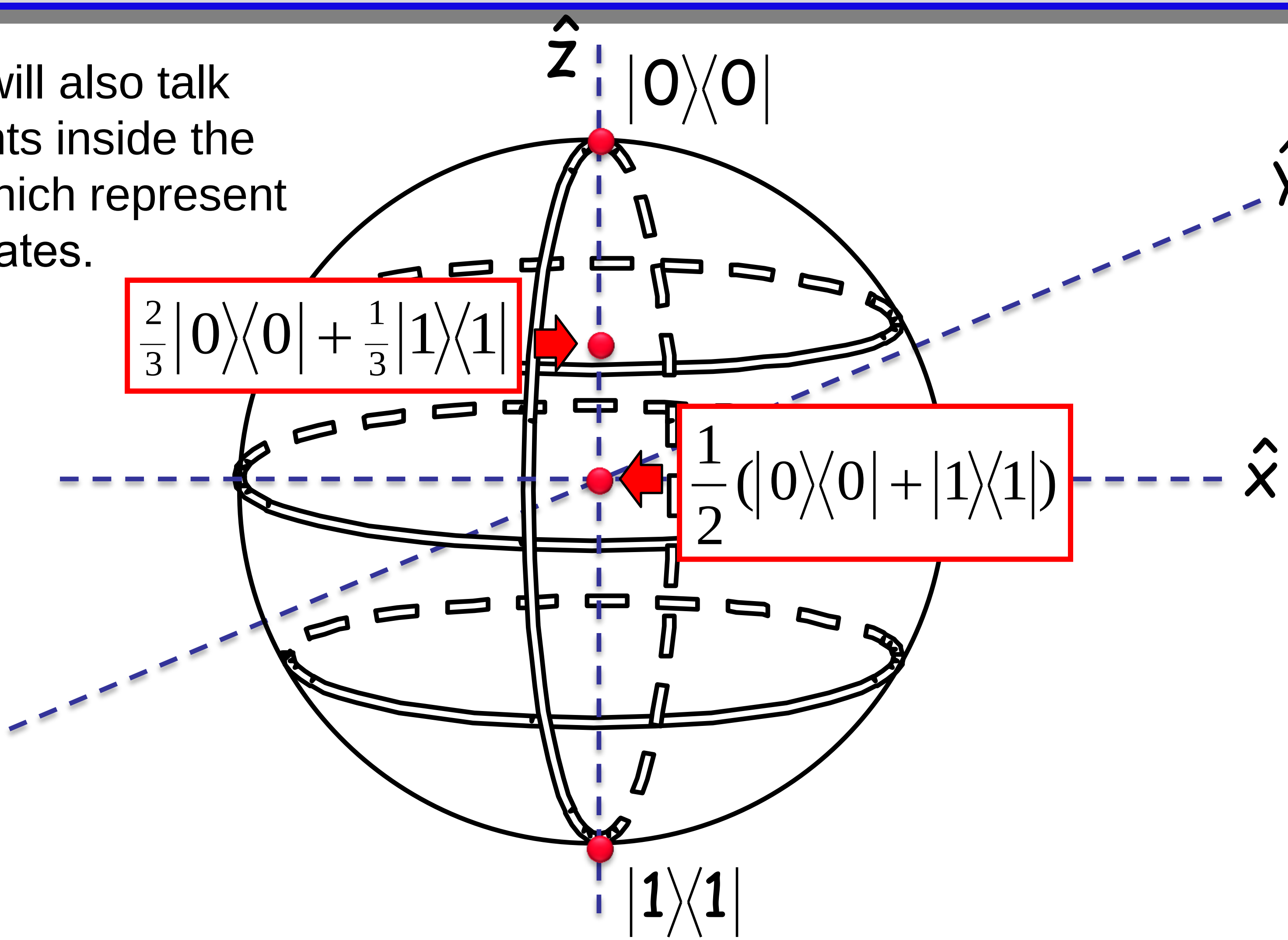
The vectors **within** the Bloch Sphere are also important as they represent mixtures of pure states (known as *mixed states*), which we will learn about later.

Bloch Sphere

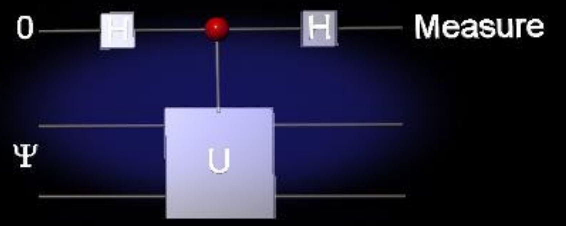


Mixed States

Later we will also talk about points inside the sphere, which represent “mixed” states.



Aside:What is e^{iH}??

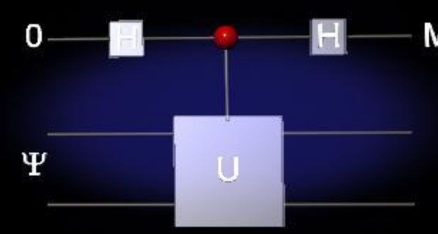


Recall $e^x = \sum_m \frac{1}{m!} x^m$? Let $x = iH$.

How am I supposed to calculate that??

Let’s start with the spectral theorem.

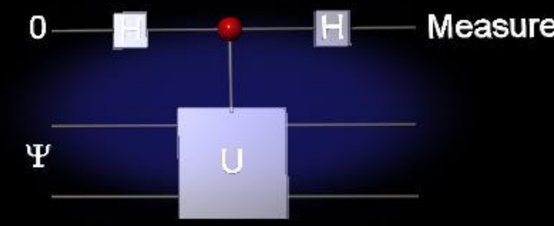
Spectral decomposition



- Definition: an operator (or matrix) M is “normal” if $MM^\dagger=M^\dagger M$

- E.g. Unitary matrices U satisfy $UU^\dagger=U^\dagger U=I$

- E.g. Density matrices and Hamiltonians (since they satisfy $\rho=\rho^\dagger$; i.e. “Hermitian”) are also normal



Spectral decomposition

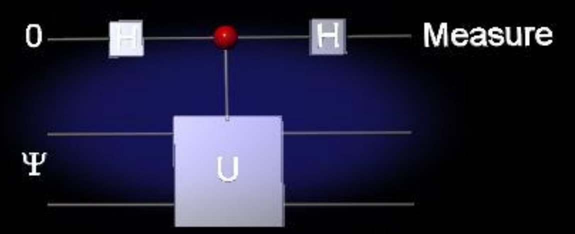
Theorem: For any normal matrix M, there is a unitary matrix P so that $M=P\Lambda P^{\dagger}$ where Λ is a diagonal matrix.

- The diagonal entries of Λ are the eigenvalues. The columns of P encode the eigenvectors.

- We can use this to prove that for a matrix M, and a function f defined as a series (as we did for e^x) as $f(M) = Pf(\Lambda)P$, where $f(\Lambda)$ is calculated element-wise, e.g.

$$f\left(\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}\right) = \begin{bmatrix} f(\lambda_1) & 0 \\ 0 & f(\lambda_2) \end{bmatrix}$$

Spectral decomposition for NOT gate



$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle \qquad X = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$[X]_{\{|0\rangle,|1\rangle\}} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}$$

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

$$X|+\rangle = |+\rangle \qquad X|-\rangle = -|-\rangle \qquad X = |+\rangle\langle +| - |-\rangle\langle -|$$

$$[X]_{\{|+\rangle,|-\rangle\}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Bloch Sphere

Rotations about the $\hat{x}$ axis are denoted

$$R_x(\theta) = e^{-i\theta X/2} = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right) X = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

Similar definitions for rotations about the $\hat{y}$ and $\hat{z}$ axes (section 4.2.1)

Bloch Sphere

We can define a rotation about any axis

$$\hat{n} = (n_x, n_y, n_z) \qquad n_x^2 + n_y^2 + n_z^2 = 1$$

$$R_{\hat{n}}(\theta) = e^{-i\theta\,\hat{n}\cdot(X,Y,Z)/2}$$

$$= \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right)\left(n_x X + n_y Y + n_z Z\right)$$

Bloch Sphere

Alternatively, we can describe these rotations as $R_{\alpha,\varphi}(\theta)$ where

$$\left|\Psi\right\rangle = \cos\left(\frac{\alpha}{2}\right)\left|0\right\rangle + e^{i\varphi}\sin\left(\frac{\alpha}{2}\right)\left|1\right\rangle$$

$$\left|\Psi^{\perp}\right\rangle = \sin\left(\frac{\alpha}{2}\right)\left|0\right\rangle - e^{i\varphi}\cos\left(\frac{\alpha}{2}\right)\left|1\right\rangle$$

$$R_{\alpha,\varphi}(\theta)\left|\Psi\right\rangle = \left|\Psi\right\rangle$$

$$R_{\alpha,\varphi}(\theta)\left|\Psi^{\perp}\right\rangle = e^{i\theta}\left|\Psi^{\perp}\right\rangle$$

Arbitrary one-qubit operations

Theorem 4.2.2 *** (see www.qcintro.com or** http://old.iqc.uwaterloo.ca/~klm-book/ **for errata)**

Let $\hat{n}$ and $\hat{m}$ be any two orthogonal axes of the Bloch sphere. Let U be a 1-qubit unitary.

Then there exist real numbers $\alpha, \beta, \gamma, \delta$

such that

$$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta)$$

Arbitrary one-qubit operations

Theorem 4.2.2 ****

Let $\hat{n}$ and $\hat{m}$ be any two non-parallel axes of the Bloch sphere. Let U be any 1-qubit unitary.

Then there exists an integer t and a finite sequence of t real numbers $\alpha, \beta_1, \gamma_1, \beta_2, \gamma_2, \cdots, \beta_t, \gamma_t$ such that

$$U = e^{i\alpha} R_{\hat{n}}(\beta_1) R_{\hat{m}}(\gamma_1) R_{\hat{n}}(\beta_2) R_{\hat{m}}(\gamma_2) \cdots R_{\hat{n}}(\beta_t) R_{\hat{m}}(\gamma_t)$$

Universal set of quantum gates

Definition

A set of gates G is said to be universal if for any integer $n>0$, any n-qubit unitary operator can be approximated to arbitrary accuracy by a quantum circuit using only gates from G.

Results about universal gates give us guidelines for implementing universal quantum computation

Definition of *error* or *accuracy*

Suppose we approximate a desired unitary transformation *U* by some other unitary transformation *V*.

The *error* in the approximation is defined to be

$$E(U,V) \equiv \max_{|\psi\rangle} \| U|\psi\rangle - V|\psi\rangle \|$$

Universal set of quantum gates

Definition

A two-qubit gate is said to be <u>entangling</u> if for some input product state, the output of the gate is an entangled state.

$$\underbrace{|\phi\rangle|\psi\rangle}_{\text{Input state}} \xrightarrow{\text{Entangling gate}} \boxed{\text{Entangled state}}$$

Universal set of quantum gates

Theorem 4.3.3

A set composed of any two-qubit entangling gate, together with all one-qubit gates, is universal.

… a bit of an overkill, since such a set allows one to achieve any unitary <u>exactly</u>.

Also unrealistic, since one needs access to an infinite number of one-qubit gates.

Can we achieve universality with a finite set of gates?

Universal one-qubit computation

Definition 4.3.4

A set of gates G is said to be universal for 1-qubit computation if any 1-qubit unitary gate can be approximated to arbitrary accuracy by a quantum circuit using only gates from G.

Arbitrary one-qubit operations

Theorem 4.3.5

Let $\hat{n}$ and $\hat{m}$ be any two non-parallel axes of the Bloch sphere, and let β, γ be real numbers such that

$$\frac{\beta}{\pi}, \frac{\gamma}{\pi}$$

are not rational.

Then

$$G = \left\{ R_{\hat{n}}(\beta), R_{\hat{m}}(\gamma) \right\}$$

is universal for one-qubit gates.

Universal one-qubit computation

Theorem 4.3.6

The set

$$G = \{HTHT, THTH\}$$

satisfies the conditions of Theorem 4.3.5, and thus is universal for one-qubit computation.

Corollary 4.3.1

The set

$$G = \{H, T\}$$

is universal for one-qubit computation.

A universal set of gates

Theorem 4.3.7

The set

$$\mathrm{G} = \{\mathrm{H}, \mathrm{T}, \mathrm{CNOT}\}$$

is a universal set of gates.

i.e. any *n*-qubit unitary operator *U* can be approximated with error ε,
for any $\varepsilon > 0$, using a finite circuit with gates from *G*.

Efficiency of approximation

How does the size of a circuit scale as the desired accuracy improves?

$$e^{O\left(\frac{1}{\varepsilon}\right)} \text{ ?} \qquad O\left(\frac{1}{\varepsilon}\right) \text{ ?} \qquad O\left(\log\frac{1}{\varepsilon}\right) \text{ ?}$$

Efficiency of approximation

Example

What is the overhead when we simulate a circuit implementing *U* made from gates in

$$G_1 = \{CNOT, R_z(\theta), R_x(\theta) : \text{any } \theta\}$$

with a circuit made from gates in

$$G_2 = \{R_z(\alpha), R_x(\beta), CNOT\}$$

for some specific $0 < \alpha, \beta < 2\pi$?

Say there are *T* one-qubit gates, and O(T) *CNOT* gates. In order for the total error to not exceed $\boldsymbol{\varepsilon}$, we need each gate to be approximated with error <u>at most</u>

$$O\left(\frac{\varepsilon}{T}\right)$$

Efficiency of approximation

Suppose we can approximate any $R_z(\theta)$ with error ε / T using $O(T^2/\varepsilon^2)$ applications of $R_z(\alpha)$

and we can approximate any $R_x(\theta)$ with error ε / T using $O(T^2/\varepsilon^2)$ applications of $R_x(\beta)$.

Thus, the new circuit uses $O\left(\frac{1}{\varepsilon^2}T^3\right)$ gates from G_2.

Ok, but not great.

Some quantum algorithms offer "quadratic speed-up". We don't want to lose that when it comes time to synthesize circuits with specific gates.

Solovay-Kitaev theorem

Theorem 4.4.1

If *G* is a finite set of one-qubit gates satisfying the conditions of Theorem 4.3.5 and also

iii) for any gate $g \in G$, its inverse g^{-1} can be implemented exactly by a finite sequence of gates in *G*

➡ any one-qubit gate can be approximated with error at most ε using $O\left(\log^{c}(1/\varepsilon)\right)$ gates from *G*, where *c* is a positive constant.

Efficiency of approximation

Corollary

It is possible to approximate a circuit with *T* gates from any universal set with $O\left(T \log^c (T/\varepsilon)\right)$ gates from any finite universal set of gates satisfying condition *iii)*.

- Key points are sketched in section 4.4.
- More details in Appendix of N&C.
- Very recent developments allow us to set the constant c=1, for an important universal gate set. This approach bypasses the method from the Solovay-Kitaev theorem.