Quantum gates II

Quantum computing

G. Chênevert

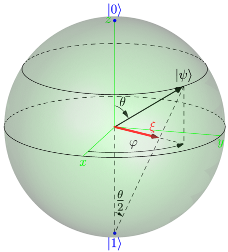
Jan. 22, 2021

Last time

- Every qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is equivalent to a state of the form

$$\cos(\tfrac{\theta}{2})|0\rangle + e^{i\varphi}\sin(\tfrac{\theta}{2})|1\rangle$$

corresponding to a (unique) point on the Bloch sphere.



http://stla.github.io/stlapblog/posts/BlochSphere.html

Certain qubit operations can be represented by 2×2 matrices :

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

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

$$P = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \qquad U = \begin{bmatrix} \cos(\frac{\theta}{2}) & -e^{i\lambda}\sin(\frac{\theta}{2}) \\ e^{i\phi}\sin(\frac{\theta}{2}) & e^{i(\lambda+\phi)}\cos(\frac{\theta}{2}) \end{bmatrix}$$

Review quiz: `https://www.wooclap.com/QCOMP2`

Quantum gates II

Single qubit gates

Multiple qubit gates

General single qubit gate

Theorem

The time evolution operator on the space of stationary states of a quantum system is represented by a unitary matrix.

Proof.

Consider a time-dependent potential $V(\mathbf{x}, t)$, $0 \leq t \leq 1$ with $V(\mathbf{x}, 0) = V(\mathbf{x}, 1)$.

The application G induced on the spaces of instantaneous solutions

$$G : \mathcal{V}_{t=0} \longrightarrow \mathcal{V}_{t=1}$$

is linear and preserves orthogonality. □

Unitary matrices

Remark:

$$\langle G\psi \mid G\phi \rangle = \langle \psi \mid \phi \rangle \quad \forall_{\psi,\phi} \qquad \Longleftrightarrow \qquad G^\dagger G = I$$

In general we have $|\det G| = 1$; up to matrix equivalence we may assume $\det G = 1$.

Then $G^{-1} = G^\dagger$ for $N = 2$ means

$$G = \begin{bmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{bmatrix}, \qquad |\alpha|^2 + |\beta|^2 = 1.$$

Special unitary group

$$\mathrm{SU}_2(\mathbb{C}) = \left\{ \begin{bmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{bmatrix} \,\middle|\, \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1 \right\}$$

Two such matrices G_1 and G_2 are equivalent $\iff G_1 = \pm G_2$.

Thus the set (group) of single qubit gates, up to equivalence, is

$$\mathrm{SU}_2(\mathbb{C})/\{\pm I\} =: \mathrm{PU}(2) = \mathrm{U}_2(\mathbb{C})/\{e^{i\theta} I \mid \theta \in \mathbb{R}\}$$

a 3-dimensional geometric space (Lie group)

General single qubit gate

Any single qubit gate G admits an orthogonal eigenbasis $|\psi_0\rangle$, $|\psi_1\rangle$ for which

$$\begin{cases} G\,|\psi_0\rangle = e^{+i\sigma}\,|\psi_0\rangle \\ G\,|\psi_1\rangle = e^{-i\sigma}\,|\psi_1\rangle \end{cases}$$

If $Q\,|0\rangle = |\psi_0\rangle$ and $Q\,|1\rangle = |\psi_1\rangle$, then

$$Q^\dagger G Q = \begin{bmatrix} e^{+i\sigma} & 0 \\ 0 & e^{-i\sigma} \end{bmatrix} \sim P(-2\sigma).$$

On the Bloch sphere, G *is a rotation of angle* -2σ *around the axis through the orthogonal states* $|\psi_0\rangle$ *and* $|\psi_1\rangle$.

Other point of view

Consider the images

$$\begin{cases} |\phi_0\rangle = G\,|0\rangle \\ |\phi_1\rangle = G\,|1\rangle \end{cases}$$

and write Bloch parameters

$$|\phi_0\rangle = \cos(\tfrac{\theta}{2})\,|0\rangle + \sin(\tfrac{\theta}{2})\,e^{i\varphi}\,|1\rangle.$$

Then $|\phi_1\rangle \sim -\sin(\frac{\theta}{2})\,|0\rangle + \cos(\frac{\theta}{2})\,e^{i\varphi}\,|1\rangle$ with phase factor, say, $e^{i\lambda}$

$$\implies G = \begin{bmatrix} |\phi_0\rangle & |\phi_1\rangle \end{bmatrix} = \begin{bmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\,e^{i\lambda} \\ \sin(\frac{\theta}{2})\,e^{i\varphi} & \cos(\frac{\theta}{2})\,e^{i(\varphi+\lambda)} \end{bmatrix} = U(\theta,\varphi,\lambda)$$

Two points of view

- axis $\mathbf{u}$ and rotation angle σ
- image of vertical axis $\mathbf{z}$ and phase parameter λ

The relationship between these two representations is a bit complicated...

Unless one is willing to work with quaternions

$$\mathbb{H} = \{a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}.$$

Universal family

Remark: every single qubit gate G can be expressed as a combination of

$$H \qquad \text{and} \qquad P(\theta) \qquad (\theta \in \mathbb{R}) \qquad \text{only.}$$

Idea:

- express G as a combination of $R_x(\alpha)$, $R_y(\beta)$, $R_z(\gamma)$
- explicit formulas for these 3 kinds of rotations

Corollary: every single qubit gate G can be *approximated* by a combination of

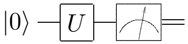
$$H \qquad \text{and} \qquad P(\tfrac{2\pi}{n}) \qquad (n \gg 0) \qquad \text{only.}$$

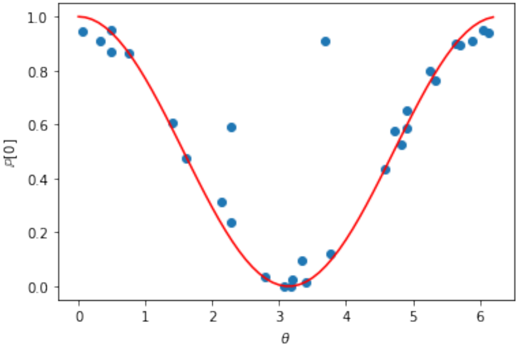
Great!

You now understand all possible programs that can run on `imbq_armonk`

$$\mathbb{Z}/2\mathbb{Z} = \{I, X\} \qquad \textit{vs.} \qquad \mathrm{PU}_2(\mathbb{C}) = \{U(\theta, \phi, \lambda)\}_{\theta,\phi,\lambda} = \mathrm{SO}_3(\mathbb{R})$$

Measurement lab





Quantum gates II

Single qubit gates

Multiple qubit gates

2-qubit system

Consider a system with two qubits A and B. Suppose:

A in state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

B in state $|\phi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$

Then the system (A, B) is in state

$$|\psi\rangle \otimes |\phi\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle)$$

$$= \alpha\gamma\,|0\rangle \otimes |0\rangle + \alpha\delta\,|0\rangle \otimes |1\rangle + \beta\gamma\,|1\rangle \otimes |0\rangle + \beta\delta\,|1\rangle \otimes |1\rangle$$

$$= \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle$$

2-qubit system

More generally: the 2-qubit system can be in *any* linear combination state

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \in \mathcal{V}_2 \otimes \mathcal{V}_2$$

Some of these can*not* be written in the form $|\psi\rangle \otimes |\phi\rangle$: called **entangled**

Example

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

Two qubit gates

Do we have the analogues of the classical AND, OR, XOR, NAND, ... gates for quantum bits?

NO! They lose information...

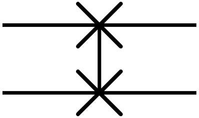
Recall: the space of quantum states for a system of 2 qubits is

$$\mathcal{V}_2 \otimes \mathcal{V}_2 \cong \mathcal{V}_4$$

basis $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$ or $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ or $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$

2-qubit gates are represented by 4×4 unitary matrices

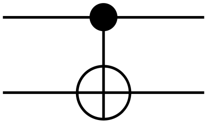
SWAP gate



$$|\psi\rangle \otimes |\phi\rangle \;\mapsto\; |\phi\rangle \otimes |\psi\rangle$$

$$\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \mathrm{diag}(1, X, 1)$$

CNOT = CX gate



$$\mathrm{CX}(|x\rangle \otimes |y\rangle) \text{ "} = \text{" } X^x|y\rangle = \begin{cases} |y\rangle & \text{if } |x\rangle = |0\rangle \\ X|y\rangle & \text{if } |x\rangle = |1\rangle \end{cases} = |x \oplus y\rangle$$

To be able to go back we must output $|x\rangle$ as well:

$$\text{"}\,\mathrm{CX}\begin{bmatrix} |x\rangle \\ |y\rangle \end{bmatrix} = \begin{bmatrix} |x\rangle \\ |x \oplus y\rangle \end{bmatrix}\text{"}$$

CNOT = CX gate

$$\mathrm{CX}(|x\rangle \otimes |y\rangle) = |x\rangle \otimes (|x \oplus y\rangle)$$

$$\mathrm{CX}\big(|0\rangle \otimes |\phi\rangle\big) = |0\rangle \otimes |\phi\rangle \qquad \mathrm{CX}\big(|1\rangle \otimes |\phi\rangle\big) = |1\rangle \otimes X|\phi\rangle$$

$$\mathrm{CX} = \mathrm{diag}(I, X) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Reversible operation ! $\mathrm{CX}^2 = I$

Exercise

What is the matrix representation of the 2-qubit gate corresponding to the application of X on the first qubit and H on the second qubit?

Quantum gates, general case

General case of a n-qubit system:

$$\underbrace{\mathcal{V}_2 \otimes \cdots \otimes \mathcal{V}_2}_{n} \cong \mathcal{V}_{2^n}$$

Any reversible quantum operation can be viewed as a $2^n \times 2^n$ unitary matrix:

$$G \in \mathrm{U}(2^n).$$

Usually described as a **quantum circuit** made of gates on smaller numbers of qubits.