Quantum gates

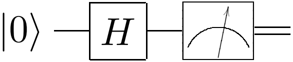
Quantum computing

G. Chênevert

January 13, 2023

Last time

Your first quantum program: a True Random Bit Generator



where H is the **Hadamard gate** that turns $|0\rangle$ into $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

Today: what other programs can we run on `imbq_armonk`? (QC with 1 qubit)

Quantum gates

Equivalent states

Consider $|\psi\rangle = \sum_{n<N} \alpha_n |n\rangle \in \mathcal{V}_N \setminus \{0\}$

Remark that for any globally proportional state: $|\phi\rangle = \alpha |\psi\rangle$ $(\alpha \neq 0)$ we have

$$\mathbb{P}\left[\, \mathcal{M}|\phi\rangle = |n\rangle \,\right] = \frac{|\langle \phi \mid n \rangle|^2}{\|\phi\|^2} = \frac{|\alpha|^2 \, |\langle \psi \mid n \rangle|^2}{|\alpha|^2 \, \|\psi\|^2} = \mathbb{P}\left[\, \mathcal{M}|\psi\rangle = |n\rangle \,\right]$$

Thus $|\phi\rangle$ and $|\psi\rangle$ cannot be distinguished by measurements: we write $|\phi\rangle \sim |\psi\rangle$.

Equivalence and normalization

Quantum states should really be thought of as *equivalence classes of vectors*

$$\{\, \alpha \,|\phi\rangle \;\mid\; \alpha \neq 0 \,\} \qquad \textit{i.e. } \text{lines in } \mathcal{V}$$

Clearly any quantum state is equivalent to a normalized state

$$|\phi\rangle \;\sim\; \frac{1}{\|\phi\|}\,|\phi\rangle$$

but such a normalized state is *not* unique:

$$|\phi\rangle \;\sim\; \alpha\,|\phi\rangle,$$

another state with the same norm, iff $|\alpha| = 1$, *i.e.* $\alpha = e^{it} \;\; (t \in \mathbb{R})$

Visualizing qubit states

So consider a qubit in quantum state

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathcal{V}_2 \setminus \{0\}.$$

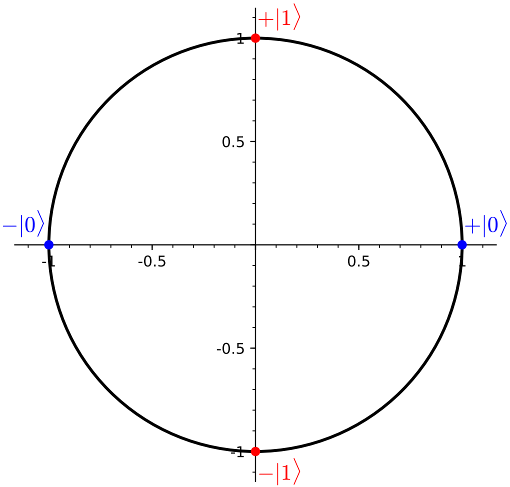
In general α and β are complex numbers: hard to visualize! $(\dim_{\mathbb{R}} \mathcal{V}_2 = 4)$

Let us assume for the moment that $\alpha, \beta \in \mathbb{R}$.

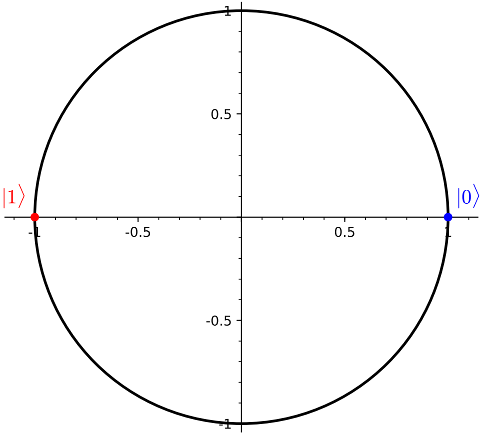
Since $|\psi\rangle \sim \dfrac{1}{\|\psi\|}|\psi\rangle$, we can assume without loss of generality that $\alpha^2 + \beta^2 = 1$.

Looks like a circle...

A circle ?



Yes: the Bloch circle



The (real) Bloch representation

According to the first picture we are tempted to write:

$$|\psi\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \qquad 0 \leq \theta < 2\pi$$

but this representation has the ambiguity $\theta \longleftrightarrow \theta + \pi$, $|\psi\rangle \sim -|\psi\rangle$.

In the second, more accurate picture, what we actually see is the point

$$P_{|\psi\rangle} = (\cos 2\theta,\, \sin 2\theta).$$

Thus in hindsight it would have been better to write, non-ambiguously,

$$|\psi\rangle = \cos(\tfrac{\theta}{2})\,|0\rangle + \sin(\tfrac{\theta}{2})\,|1\rangle.$$

Angle between two states

In the (real) Bloch representation:

$$\begin{cases} |\psi\rangle = \cos(\frac{\theta_1}{2})\,|0\rangle + \sin(\frac{\theta_1}{2})\,|1\rangle, \\ |\phi\rangle = \cos(\frac{\theta_2}{2})\,|0\rangle + \sin(\frac{\theta_2}{2})\,|1\rangle \end{cases}$$

we have

$$\langle \phi \,|\, \psi \rangle = \cos(\tfrac{\theta_1}{2})\cos(\tfrac{\theta_2}{2}) + \sin(\tfrac{\theta_1}{2})\sin(\tfrac{\theta_2}{2}) = \cos\tfrac{\theta_1 - \theta_2}{2}.$$

In particular:

$$\langle \phi \,|\, \psi \rangle = 0 \iff \tfrac{\theta_1 - \theta_2}{2} = \pm\tfrac{\pi}{2} \iff \theta_2 = \theta_1 \pm \pi.$$

Orthogonal states lie *opposite* on the Bloch circle.

Towards the Bloch representation

Now for a general state $0 \neq |\psi\rangle \in \mathcal{V}_2$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \qquad \alpha, \beta \in \mathbb{C}.$$

Without loss of generality we can assume $|\alpha|^2 + |\beta|^2 = 1$ (normalized state).

Equivalent normalized states: if $|\psi\rangle \sim |\phi\rangle$, then $|\psi\rangle = \gamma\,|\phi\rangle$ with $|\gamma| \; = 1$.

So: if $\alpha = A\,e^{ia}$, by multiplying by e^{-ia} we can reduce to the case

$$\alpha = A \text{ is real}, \quad \beta = B\,e^{ib}, \quad A^2 + B^2 = 1.$$

Bloch representation

$$|\psi\rangle \sim A\,|0\rangle + B\,e^{ib}\,|1\rangle, \quad A^2 + B^2 = 1.$$

From the real case we know we should write $A = \cos(\frac{\theta}{2})$, $B = \sin(\frac{\theta}{2})$.

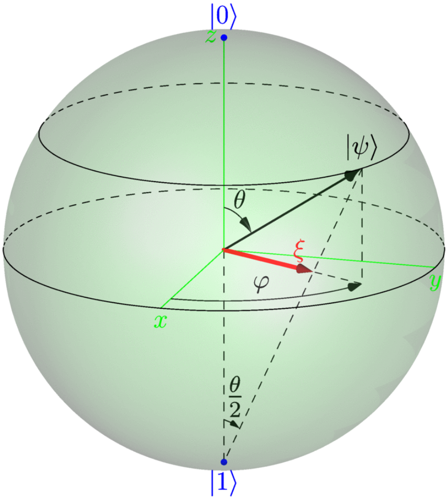
We have proved:

Every qubit state is equivalent to a unique normalized state of the form

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

These correspond to points $(\cos\varphi\,\sin\theta, \sin\varphi\,\sin\theta, \cos\theta)$ on a *sphere*.

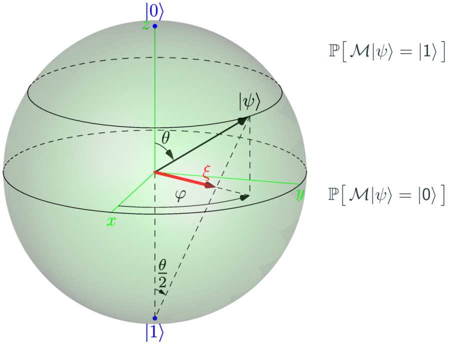
The Bloch sphere $\mathcal{B}$ (click title for interactive model)



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

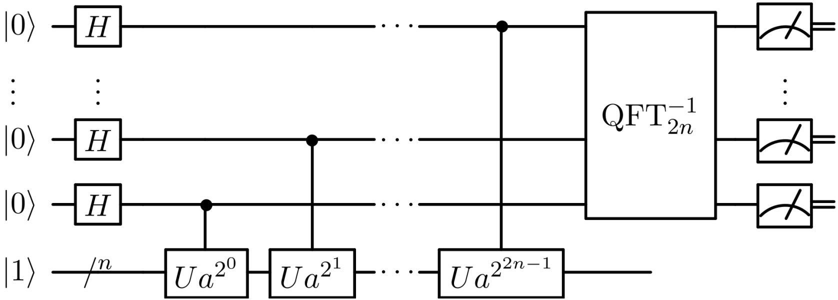
Properties of the Bloch representation

- Pairs of orthogonal states correspond to antipodal points on the Bloch sphere.
- The probability that $|\psi\rangle$ is measured as $|0\rangle$ or $|1\rangle$ can be interpreted as relative areas on the sphere.



Quantum gates

Spoilers ahead: Shor's algorithm



Quantum circuits

Quantum circuits are made up of

- **quantum registers** containing qubits
- **quantum logic gates** modifiying the state of these qubits
- **classical registers** containing regular bits
- **measurements** mapping quantum registers to classical registers

that can then be manipulated with a classical electronic circuit.

NOT gate

$$\begin{cases} \text{NOT}\,|0\rangle = |1\rangle \\ \text{NOT}\,|1\rangle = |0\rangle \end{cases}$$

$$\text{NOT}(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|1\rangle + \beta\,|0\rangle$$

$$\text{NOT}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \qquad \text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Interpretation on the Bloch sphere

Fixed points of NOT:

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

NOT can be thought of as a *rotation of* π *around the* x*-axis*

often called the **Pauli X** gate for this reason and written NOT, X or $\oplus$

Note: $X^2 = I$

Hadamard gate

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

Sends $|0\rangle$ to $H|0\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|1\rangle$ to the orthogonal state $H|1\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$.

Remark: $H^2 = I$ (isn't it?)

Phase gate $P = P(\theta)$

$$P = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

$$P|0\rangle = |0\rangle, \qquad P|1\rangle = e^{i\theta}$$

$$P(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|0\rangle + e^{i\theta}\,\beta\,|1\rangle$$

Remark : $Z := P(\pi) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ special case

Universal gate U

Depends on 3 parameters θ, φ and λ:

$$U = \begin{bmatrix} \cos(\frac{\theta}{2}) & -e^{i\lambda}\sin(\frac{\theta}{2}) \\ e^{i\varphi}\sin(\frac{\theta}{2}) & e^{i(\lambda+\varphi)}\cos(\frac{\theta}{2}) \end{bmatrix}$$

All gates encountered so far are special cases !

Remark: U is a unitary matrix ($U^\dagger U = I$)

Quantum gates

Visualizing qubit states

Examples of quantum gates

General single-qubit gate

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:

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

In other words: the columns of G form an orthonormal basis for the hermitian product.

In general if G is unitary 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

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

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 denotes the unitary transformation for which $Q\,|0\rangle = |\psi_0\rangle$ and $Q\,|1\rangle = |\psi_1\rangle$, then

$$Q^\dagger GQ = \begin{bmatrix} e^{+i\sigma} & 0 \\ 0 & e^{-i\sigma} \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & -2\sigma \end{bmatrix} = P(-2\sigma).$$

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`

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

Exercise for next time

Modify your TRNG so that the probability of getting $|1\rangle$ is, say, 62%.