Lecture 4

From reversible to quantum circuits

Last time

- The circuit model describes computations (graphically) as compositions of gates
- We interpret the meaning of circuits using some mathematical structure(s)

Classical circuits

states: bitstrings $\vec{x} \in \mathbb{F}_2^n$

gates : functions $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$

Reversible circuits

states : unit vectors $|\vec{x}\rangle \in \mathbb{F}_2^{2^n}$

gates : invertible linear operators

$$A : \mathbb{F}_2^{2^n} \longrightarrow \mathbb{F}_2^{2^n} \leftarrow \text{permutation matrices!}$$

Quantum circuits

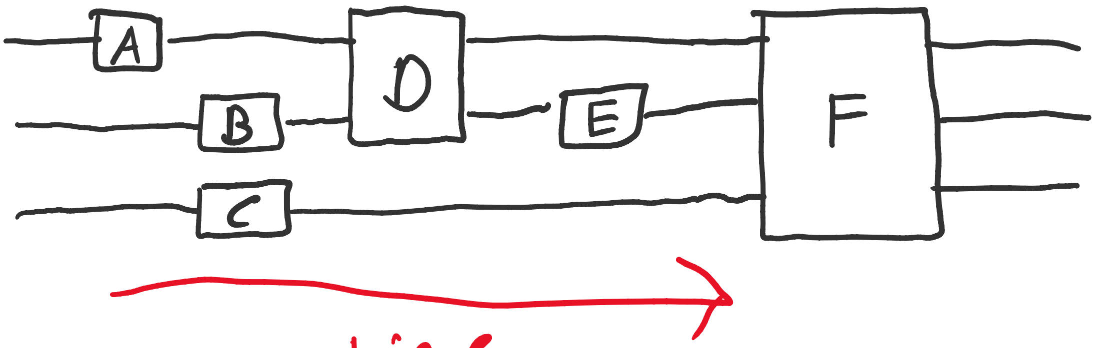
States: unit vectors $|\psi\rangle \in \mathbb{C}^{2^n}$

gates : unitary operators

$$U : \mathbb{C}^{2^n} \longrightarrow \mathbb{C}^{2^n}$$

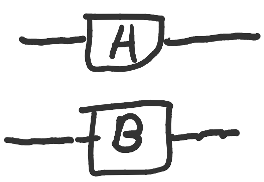
Note: reversible circuits $\subsetneq$ quantum circuits which only permute basis states

Quantum circuit diagrams



Algebraically,

is BA



is $A \otimes B$

Ex.

The above circuit diagram can be written as

$$F(I \otimes E \otimes I)(D \otimes I)(I \otimes B \otimes C)(A \otimes I \otimes I)$$

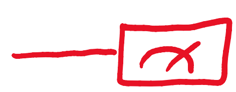
↖ identity operator

Note: algebraically

since

$$(I \otimes B)(A \otimes I) = IA \otimes BI = AI \otimes IB = (A \otimes I)(I \otimes B)$$

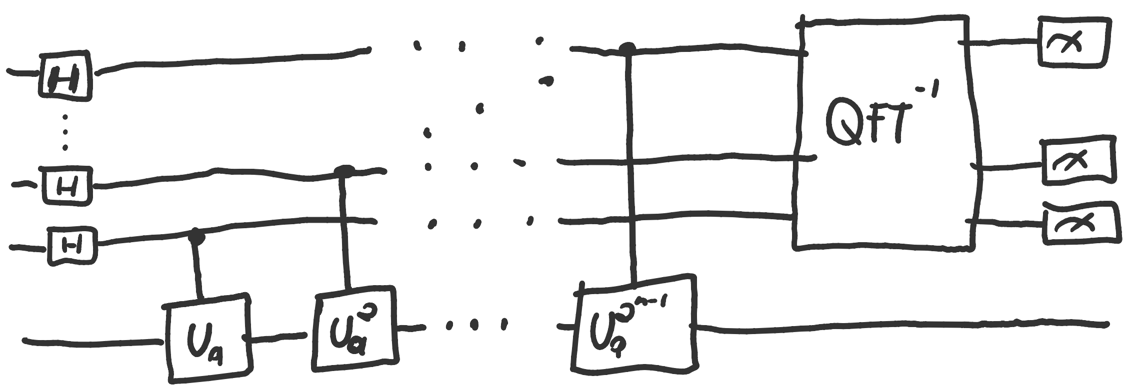
Note:

Measurement, denoted by , isn't a linear op. on the state space $\mathbb{C}^{2^n}$, so we stick to unitary circuits for now (i.e. no measurement) which can be shown to be equally powerful

Gate sets & compilation

Quantum algorithms are described as high-level circuits.

E.g. Shor's algorithm
(actually the period finding part)



To actually implement such an algorithm just like in classical computing we need to know how to decompose or compile it down to basic gates (quantum instruction set) which can be performed by the computer. Moreover, this implementation should be efficient in its time and space use.

We first look at generic techniques aimed at showing that unitary operators can in fact be factorized into small sets of physical gates.

Later on we'll look at
- Compilation problems for specific platforms
- Compilation problems for specific unitary groups

Single qubit unitaries

Classically we had exactly two single bit ops:

$$\text{———} = -\boxed{I}- = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\text{———} = -\boxed{X}- = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = -\oplus-$$

Quantumly, we have any 2x2 unitary matrix:

$$\begin{bmatrix} a & -e^{i\theta} b^* \\ b & e^{i\theta} a^* \end{bmatrix}, \quad |a|^2 + |b|^2 = 1$$

This gives an uncountable continuum of gates on just 1 qubit.

<u>Ex.</u> Important single qubit gates include

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

(Pauli gates)

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

Note that X, Y, Z, and H are all self-inverse, i.e.

$$X^2 = Y^2 = Z^2 = H^2 = I$$

Single qubit gates correspond to rotations of a 3-dimensional sphere called the Bloch sphere

The Bloch sphere

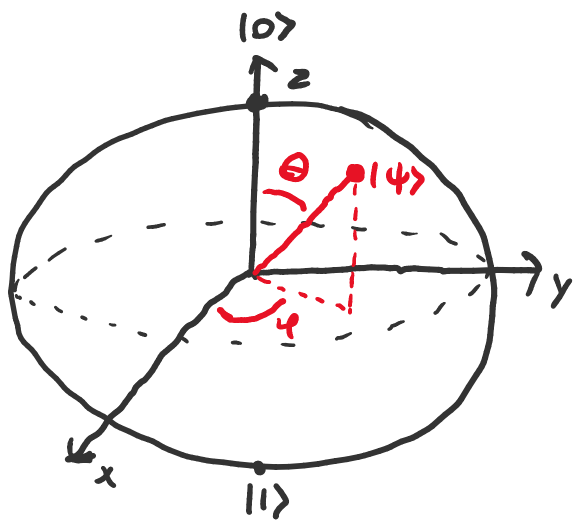
Recall that the state of a single qubit is

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

We may write this up to global phase as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

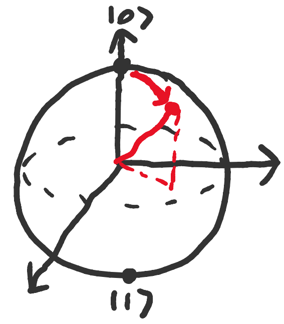
Together, θ & φ define a point on a 3-dimensional unit sphere called the Bloch sphere



Since 1-qubit states are points on the Bloch sphere, a 1-qubit gate rotates the Bloch sphere. If we write

$$U = \begin{bmatrix} a & -e^{i\varphi}b^* \\ b & e^{i\varphi}a^* \end{bmatrix}$$

then that rotation sends the $|0\rangle$ pole to the point $|\psi\rangle = a|0\rangle + b|1\rangle$



Rotation gates

Pauli exponentials give rise to rotations about the X, Y, and Z axes

$$R_x(\theta) = e^{-i\theta X/2}$$
$$R_y(\theta) = e^{-i\theta Y/2}$$
$$R_z(\theta) = e^{-i\theta Z/2}$$

what?

(Operator functions)

Let $f : \mathbb{C} \to \mathbb{C}$ and $A = \sum_{e_i} a_i |e_i\rangle\langle e_i|$

where $\{e_i\}$ is an orthonormal basis. Then

$$f(A) = \sum_{e_i} f(a_i) |e_i\rangle\langle e_i|$$

Ex.

Recall that $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Then

$$\begin{aligned}\sqrt{Z} &= \sqrt{1}\,|0\rangle\langle 0| + \sqrt{-1}\,|1\rangle\langle 1| \\ &= |0\rangle\langle 0| + i|1\rangle\langle 1| \\ &= S\left(= \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\right)\end{aligned}$$

We can verify that $S^2 = Z$:

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

Likewise, $T = \sqrt{S}$ since

$$\sqrt{S} = |0\rangle\langle 0| + \sqrt{i}\,|1\rangle\langle 1| = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$$

The spectral decomposition

What if $A \neq \sum a_i |i\rangle\langle i|$?

e.g. $X = |0\rangle\langle 1| + |1\rangle\langle 0|$

We say $A: V \to V$ is diagonalizable if there exists an orthonormal basis $\{|e_i\rangle\}$ such that

$$A = \sum a_i |e_i\rangle\langle e_i|$$

Thm. (spectral decomposition)

An operator A is diagonalizable if and only if it is normal ($AA^\dagger = A^\dagger A$)

Cor.

Any normal operator A can be written as

$$U \Lambda U^\dagger$$

where U is unitary and Λ is diagonal in the standard (computational) basis. The columns of U encode the eigenvectors of A and the entries of Λ are the eigenvalues

<u>Ex.</u>

$$X|+\rangle = X\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right) = \tfrac{1}{\sqrt{2}}|1\rangle + \tfrac{1}{\sqrt{2}}|0\rangle = |+\rangle$$

$$X|-\rangle = X\left(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle\right) = \tfrac{1}{\sqrt{2}}|1\rangle - \tfrac{1}{\sqrt{2}}|0\rangle = -|-\rangle$$

$$\therefore X = \tfrac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\tfrac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = HZH!$$

Back to exponentials

Let $f: \mathbb{C} \to \mathbb{C}$ and M be normal. Then

$$f(M) = \sum_i f(a_i) |e_i\rangle\langle e_i| = U f(\Lambda) U^\dagger$$

Now we can evaluate $R_z(\theta)$, $R_x(\theta)$, $R_Y(\theta)$:

$$R_z(\theta) = e^{-i\theta Z/2} = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

$$R_x(\theta) = e^{-i\theta X/2} = He^{-i\theta Z/2}H = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} e^{-i\theta/2} & -e^{-i\theta/2} \\ e^{i\theta/2} & -e^{i\theta/2} \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} e^{-i\theta/2}+e^{i\theta/2} & e^{-i\theta/2}-e^{i\theta/2} \\ e^{-i\theta/2}-e^{i\theta/2} & e^{-i\theta/2}+e^{i\theta/2} \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} 2\mathrm{Re}(e^{i\theta/2}) & 2\mathrm{Im}(e^{i\theta/2}) \\ -2\mathrm{Im}(e^{i\theta/2}) & 2\mathrm{Re}(e^{i\theta/2}) \end{bmatrix}$$

$$= \begin{bmatrix} \cos\theta/2 & i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{bmatrix}$$

$$R_y(\theta) = e^{-i\theta Y/2} = \begin{bmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{bmatrix}$$

Exercise:

Diagonalize Y by finding 2 orthonormal eigenvectors

$$Y|+_y\rangle = |+_y\rangle$$

$$Y|-_y\rangle = -|-_y\rangle$$

More rotations

Lemma.

Let A be a normal operator s.t. $A^2 = I$. Then
$$e^{i\theta A} = \cos(\theta) I + i\sin(\theta) A$$

(Rotation about an arbitrary axis)

Let $v = (\alpha, \beta, \gamma)$ be a real unit vector in 3D. A rotation around v is
$$R_v(\theta) = e^{-i\theta(\alpha X + \beta Y + \gamma Z)/2}$$
$$= \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)(\alpha X + \beta Y + \gamma Z)$$

(Rotation about an arbitrary state $|\psi\rangle$)

Let $|\psi\rangle = \cos\theta/2\,|0\rangle + e^{i\varphi}\sin\theta/2\,|1\rangle$. Then
$$R_{\theta,\varphi}(\sigma)$$
is a rotation about the $|\psi\rangle$ defined by
$$R_{\theta,\varphi}(\sigma)|\psi\rangle = |\psi\rangle$$
$$R_{\theta,\varphi}(\sigma)|\psi^\perp\rangle = e^{i\sigma}|\psi^\perp\rangle$$
where $|\psi^\perp\rangle = \sin\theta/2\,|0\rangle - e^{i\varphi}\cos\theta/2\,|1\rangle$

Decomposition of 1-qubit unitaries

Since physical hardware can't directly implement an arbitrary single qubit rotation, we need to decompose or compile it into a sequence of implementable rotations. This is a fundamental problem in QC.

Thm.

Let U be a 1-qubit unitary. Then there exist $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ s.t.

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

Pf.

We know U may be written as

$$\begin{bmatrix} a & -e^{i2\alpha} b^* \\ b & e^{i2\alpha} a^* \end{bmatrix}$$

where $|a|^2 + |b|^2 = 1$. Recall that we may write

$$a = e^{i\theta} \cos \gamma/2 \qquad b = e^{i\varphi} \sin \gamma/2$$

Then

$$e^{-i\alpha} U = \begin{bmatrix} e^{i\overbrace{(\theta - \alpha)}^{\theta'}} \cos \gamma/2 & -e^{i\overbrace{(-\varphi + \alpha)}^{-\varphi'}} \sin \gamma/2 \\ e^{i\underbrace{(\varphi - \alpha)}_{\varphi'}} \sin \gamma/2 & e^{i\underbrace{(-\theta + \alpha)}_{-\theta'}} \cos \gamma/2 \end{bmatrix}$$

Now choose β, δ s.t.

$$\theta' = -\beta/2 - \delta/2$$

$$\varphi' = \beta/2 - \delta/2$$

(Note: set $\delta = -\theta' - \varphi'$. Then

$$\beta = -2\theta' - \delta$$
$$= -\theta' + \varphi'$$

check: $\frac{-\theta' + \varphi'}{2} - \frac{-\theta' - \varphi'}{2} = \frac{2\varphi'}{2} = \varphi'$)

So we have

$$e^{-i\alpha} U = \begin{bmatrix} e^{i(-\beta/2 - \delta/2)} \cos \gamma/2 & -e^{i(-\beta/2 + \delta/2)} \sin \gamma/2 \\ e^{i(\beta/2 - \delta/2)} \sin \gamma/2 & e^{i(\beta/2 + \delta/2)} \cos \gamma/2 \end{bmatrix}$$

$$= \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos \gamma/2 & -\sin \gamma/2 \\ \sin \gamma/2 & \cos \gamma/2 \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}$$

$$= R_z(\beta) R_y(\gamma) R_z(\delta)$$

Hence

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) \qquad \square$$

More about decompositions

Decomposition of rotations is an old topic not specific to quantum computing. The decomposition into $z \cdot y \cdot z$ rotations is an example of Euler angles used to describe a 3-D rotation. We can also choose other axes, such as $x \cdot z \cdot x$ to decompose a general 1-qubit unitary. In fact, any 2 orthogonal axes suffice:

Thm.

Let n, m be any two orthogonal axes of the Bloch sphere. Then any 1-qubit unitary U can be decomposed as

$$U = e^{i\alpha} R_n(\beta) R_m(\gamma) R_n(\delta)$$