Quantum Systems

(Lecture 4: Quantum gates and the circuit model)

Luís Soares Barbosa

Universidade do Minho

The circuit model

Classical reversible circuits (which can simulate any non-reversible one with modest overhead) generalise to quantum circuits where

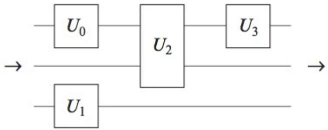
- logical qubits are carried along wires,
- quantum gates, corresponding to unitary transformations, act on them,
- and measurements of a quantum state $|\phi\rangle = \sum_i \alpha_i |i\rangle$result in a state $|i\rangle$, with probability given by the norm squared of its amplitude, $\| \alpha_i \|^2$, together with a classical label i indicating which outcome was obtained.

The circuit model

Quantum gates

A gate is a transformation that acts on only a small number of qubits
Differently from the classical case, they do not necessarily correspond to physical objects

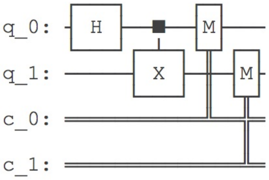
Notation



The circuit model

Circuits in Qiskit

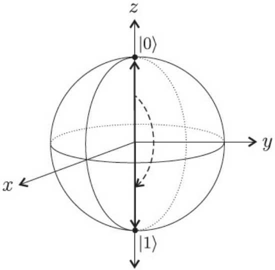
```python
from qiskit import QuantumCircuit

qc = QuantumCircuit(2, 2)
qc.h(0)
qc.cx(0, 1)
qc.measure([0, 1], [0, 1])
qc.draw()
```



1-Gates

The action of a 1-gate U on a quantum state $|\phi\rangle$ can be thought of as a rotation of the Bloch vector for $|\phi\rangle$ to the Bloch vector for $U|\phi\rangle$, eg.

Example: X



is a rotation about the x axis.

1-Gates

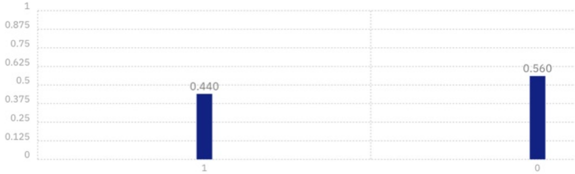
The $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ gate

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

1-Gates

The Hadamard gate creates superpositions

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



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

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

1-Gates

The phase shift gate

$$R_\phi = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

$$\begin{aligned} R_\phi \left|0\right\rangle &= \left|0\right\rangle \\ R_\phi \left|1\right\rangle &= e^{i\phi}\left|1\right\rangle \end{aligned}$$

The T (or $\frac{\pi}{8}$) gate

$$T = R_{\frac{\pi}{4}} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

which, up to a global phase factor $e^{i\frac{\pi}{8}}$, is equivalent to

$$\begin{bmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix}$$

1-Gates

Pauli gates

$$
\begin{aligned}
I &= |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
X &= |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
Z &= |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = R_\pi \\
Y &= i(-|1\rangle\langle 0| + |0\rangle\langle 1|) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}
\end{aligned}
$$

1-Gates

Rotation gates

Correspond to rotations about the three axes of the Bloch sphere, and are computed as Pauli gates squared.

$$R_e(\theta) \;\widehat{=}\; e^{\frac{-i\theta E}{2}} = \cos\left(\frac{\theta}{2}\right) I - i \sin\frac{\theta}{2} E$$

where $e \;\widehat{=}\; x, y, z$ and $E \;\widehat{=}\; X, Y, Z$.

because, for any real number r and matrix R st $R^2 = I$, which is the case for X, Y, and Z,

$$e^{irR} = cos(r) I + i \sin(r) R$$

1-Gates

Rotation gates as matrices in the computational basis

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

$$R_y(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

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

1-Gates

Compute $R_z(\theta)|\psi\rangle$ for $|\psi\rangle = \cos\left(\frac{\sigma}{2}\right)|0\rangle + e^{i\gamma}\sin\left(\frac{\sigma}{2}\right)|1\rangle$

$$\begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix} \begin{bmatrix} \cos\left(\frac{\sigma}{2}\right) \\ e^{i\gamma}\sin\left(\frac{\sigma}{2}\right) \end{bmatrix} = \begin{bmatrix} e^{-i\frac{\theta}{2}}\cos\left(\frac{\sigma}{2}\right) \\ e^{i\frac{\theta}{2}}e^{i\gamma}\sin\left(\frac{\sigma}{2}\right) \end{bmatrix}$$
$$= e^{-i\frac{\theta}{2}} \begin{bmatrix} \cos\left(\frac{\sigma}{2}\right) \\ e^{i\theta}e^{i\gamma}\sin\left(\frac{\sigma}{2}\right) \end{bmatrix}$$
$$= e^{-i\frac{\theta}{2}} \left(\cos\left(\frac{\sigma}{2}\right)|0\rangle + e^{i(\gamma+\theta)}\sin\left(\frac{\sigma}{2}\right)|1\rangle\right)$$

As global phase is insignificant, the angle mapping $\gamma \mapsto \gamma + \theta$ is a rotation of θ around the z-axis of the Bloch sphere.

1-Gates

Theorem

Let U be a 1-gate, and v, w any two non-parallel axes of the Bloch sphere. Then there exist real numbers $\alpha, \beta\, \gamma, \delta$ st

$$U \;=\; e^{i\alpha} R_v(\beta) R_w(\gamma) R_v(\delta)$$

which means that any 1-gate can be expressed as a sequence of two rotations about an axis and one rotation about another non parallel axis, multiplied by a suitable phase factor.

proof hint: Recall U is unitary and unfold the definition of rotation gate.

2-gates: *CNOT*

Acts on the standard basis for a 2-qubit system, flipping the second bit if the first bit is 1 and leaving it unchanged otherwise.

$$
\begin{aligned}
CNOT &= |0\rangle\langle 0| \otimes I \ + \ |1\rangle\langle 1| \otimes X \\
&= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) \ + \ |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) \\
&= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}
\end{aligned}
$$

CNOT is unitary and is its own inverse, and cannot be decomposed into a tensor product of two 1-qubit transformations

2-gates: $CNOT$

The importance of $CNOT$ is its ability to change the entanglement between two qubits, e.g.

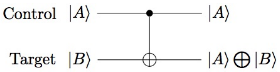
$$\begin{aligned} CNOT\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle\right) &= CNOT\left(\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)\right) \\ &= \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \end{aligned}$$

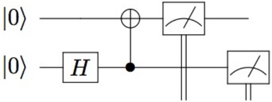
Being its own inverse, also takes an entangled state to an unentangled one.

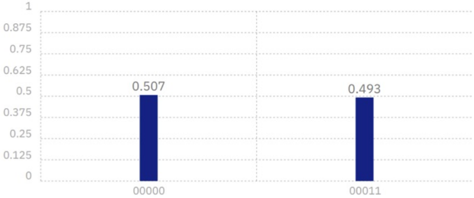
Note that entanglement is not a local property in the sense that transformations that act separately on two or more subsystems cannot affect the entanglement between those subsystems:

$(U \otimes V)\,|v\rangle$ is entangled iff $|v\rangle$ is

2-gates: *CNOT*


Control $|A\rangle$
Target $|B\rangle$
$|A\rangle$
$|A\rangle \oplus |B\rangle$


$|0\rangle$
$|0\rangle$
H

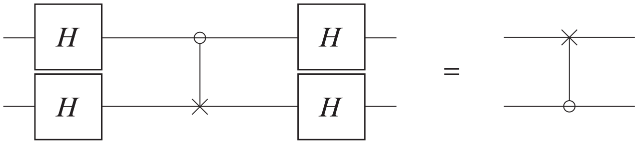

1
0.875
0.75
0.625
0.5
0.375
0.25
0.125
0
0.507
0.493
00000
00011

2-gates: *CNOT*

The notions of control/target bit in *CNOT* are arbitrary: they depend on what basis is considered. The standard behaviour is obtained in the computational basis. However, roles are interchanged in the Hadamard basis in which the effect of *CNOT* is

$$|++\rangle \mapsto |++\rangle \quad |+-\rangle \mapsto |--\rangle \quad |-+\rangle \mapsto |-+\rangle \quad |--\rangle \mapsto |+-\rangle$$

Exercise



The proof

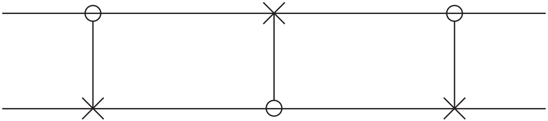
$$
\begin{aligned}
LHS &= \frac{1}{2}\begin{bmatrix} H & H \\ H & -H \end{bmatrix} \overbrace{\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}}^{CNOT} \begin{bmatrix} H & H \\ H & -H \end{bmatrix} \\
&= \frac{1}{2}\begin{bmatrix} H & HX \\ H & -HX \end{bmatrix} \begin{bmatrix} H & H \\ H & -H \end{bmatrix} \\
&= \frac{1}{2}\begin{bmatrix} I + HXH & I - HXH \\ I - HXH & I + HXH \end{bmatrix} \;=\; \frac{1}{2}\begin{bmatrix} I + Z & I - Z \\ I - Z & I + Z \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \\
&= I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1| \;=\; RHS
\end{aligned}
$$

noting that

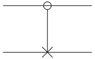
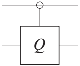
$$
H \otimes H = (I \otimes H)(H \otimes I) = \frac{1}{\sqrt{2}}\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix} \begin{bmatrix} I & I \\ I & -I \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} H & H \\ H & -H \end{bmatrix}
$$

Exercise

Discuss



Controlled Q-gates

From  to 

$$
\begin{aligned}
C_Q|0\rangle|\varphi\rangle &= |0\rangle|\varphi\rangle \\
C_Q|1\rangle|\varphi\rangle &= |1\rangle Q|\varphi\rangle
\end{aligned}
$$

$$C_Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q$$

corresponding to the following matrix in the standard basis:

$$C_Q = \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix}$$

Controlled phase shift gate

$$C_{e^{i\theta}} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\theta}|10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11|$$

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

Transforming a global into a local phase

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \longrightarrow \frac{1}{\sqrt{2}}(|00\rangle + e^{i\theta}|11\rangle)$$

Actually, a unitary transformation is completely determined by its action on a basis, but not by specifying what states the states corresponding to basis states are sent to.

Example: $e^{i\theta}$ takes the four quantum states to themselves (because e.g. $|10\rangle$ and $e^{i\theta}|10\rangle$ represent the same state), but a global phase can be transformed into a local one, as above

CCNOT or Toffoli gate

A 3-bit gate corresponding to controlled *CNOT*. If the first two bits are in the state $|1\rangle$ applies X the third bit, else it does nothing:

$$|q_1 q_2 q_3\rangle \;\mapsto\; |q_1 q_2, q_3 \oplus (q_1 \wedge q_2)\rangle$$

In matrix form,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Universal set of gates?

Is there a universal set of quantum gates?

In general no: there are uncountably many quantum transformations, and a finite set of generators can only generate countably many elements. However, it is possible for finite sets of gates to generate arbitrarily close approximations to all unitary transformations.

Definitions

- The error in approximating U by V is

$$Er(U,V) = \max_{|\phi\rangle} \| (U-V)|\phi\rangle \|$$

- An operator U can be approximated to arbitrary accuracy if for any positive ϵ there exists another unitary transformation V st $Er(U,V) \leq \epsilon$.
- A set of gates is universal if for any integer $n \geq 1$, any n-qubit unitary operator can be approximated to arbitrary accuracy by a quantum circuit using only gates from that set.

Universal set of gates?

Some examples

- The set $\{H, T\}$ is universal for 1-gates.
- The set $\{H, T, CNOT\}$ is a universal set of gates.

How efficient is an approximation?

To approximate an unitary transformation encoding some specific computation, one would expect to use a number of gates from the universal set which is polynomial in the number of qubits and the inverse of the quality factor ϵ.

Main result: theorem of Solovay-Kitaev

Teleportation

Aim: to transmit, using two classical bits, the state of a single qubit.

Surprisingly,

- shows that two classical bits suffice to communicate a qubit state, which has an infinite number of configurations
- provides a mechanism for the transmission of an unknown quantum state, in spite of the no-cloning theorem

Note that the original state cannot be preserved (precisely because of the no-cloning result), which motivates the name of the protocol ...

Teleportation

Strategy:

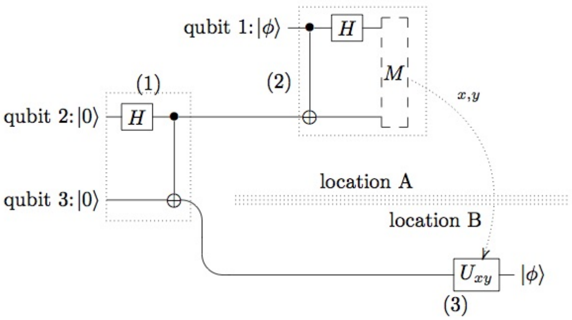
- Alice and Bob share a Bell state (also called a EPR pair)

$$|r\rangle \;=\; \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$$

  created ahead in time when both qubits were together and can be made to interact to produce an entangled state (through e.g. a *CNOT* gate).
- This entangled state becomes a resource which remains available when one qubit is taken away from the other.
- Then Alice encodes the unknown qubit with her part of the EPR pair, measures and transmits the (classical) result of the measurement.
- Finally, Bob decodes its part of the EPR pair based on the (classical) information received

Teleportation

Implementation:



The EPR pair

is the real resource

named after Einstein, Podolsky, and Rosen, from the *hidden-variable* controversy

Teleportation

Alice

... has a qubit whose state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ she does not know, but wants to send to Bob through classical channels.

The starting point is the 3-qubit state after stage (1) whose first 2 qubits are controlled by Alice and the last by Bob:

$$\begin{aligned} |\phi\rangle \otimes |r\rangle &= \frac{1}{\sqrt{2}}(\alpha|0\rangle \otimes \overbrace{(|00\rangle + |11\rangle)}^{\text{entangled}} + \beta|1\rangle \otimes \overbrace{(|00\rangle + |11\rangle)}^{\text{entangled}}) \\ &= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle) \end{aligned}$$

Teleportation

Alice

... then she applies $CNOT \otimes I$ and $H \otimes I \otimes I$ to obtain

$$
\begin{aligned}
&(H \otimes I \otimes I)(CNOT \otimes I)(|\phi\rangle \otimes |r\rangle) \\
&= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle) \\
&= \frac{1}{2}(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)) \\
&= \frac{1}{2}(|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) + \\
&\qquad + |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle))
\end{aligned}
$$

Teleportation

Alice

Alice measures the first two qubits and obtains one of the four standard basis states, $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, with equal probability.
Depending on the result of her measurement, the state of Bob's qubit is projected to

$$\alpha|0\rangle + \beta|1\rangle,\ \alpha|1\rangle + \beta|0\rangle,\ \alpha|0\rangle - \beta|1\rangle,\ \alpha|1\rangle - \beta|0\rangle$$

Then, Alice sends the result of her measurement as two classical bits to Bob.

After these transformations, crucial information about the original state $|\phi\rangle$ is contained in Bob's qubit, Alice's being destroyed ...

Teleportation

Bob

When Bob receives the two bits from Alice, he knows how the state of his half of the entangled pair compares to the original state of Alice's qubit.

Bob can reconstruct the original state of Alice's qubit, $|\phi\rangle$, by applying the appropriate decoding transformation to his qubit, originally part of the entangled pair.

Bits received	Bob's state	Transformation to decode
00	$\alpha\|0\rangle + \beta\|1\rangle$	I
01	$\alpha\|1\rangle + \beta\|0\rangle$	X
10	$\alpha\|0\rangle - \beta\|1\rangle$	Z
11	$\alpha\|1\rangle - \beta\|1\rangle$	Y

After decoding, Bob's qubit will be in the state $|\phi\rangle$

Dense coding

Aim: encode and transmit two classical bits with one qubit and a shared EPR pair.

This result is surprising, since only one bit can be extracted from a qubit

The idea is that, since entangled states can be distributed ahead of time, only one qubit needs to be physically transmitted to communicate two bits of information.

Let Alice (Bob) be sent and operate the first (second) qubit of the EPR pair

$$|r\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Dense coding

Alice

wishes to transmit the state of two classical bits encoding one of the numbers 0 through 3. Depending on this number, Alice performs one of the Pauli transformations on her qubit of the entangled pair $|r\rangle$, and sends her qubit to Bob.

	Transformation	New state
0	$(I \times I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	$(X \times I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
2	$(Z \times I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
3	$(Y \times I)\|r\rangle$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$

Dense coding

Bob

decodes the information applying a *CNOT* gate to the two qubits of the entangled pair and then H to the first qubit:

$$CNOT \longrightarrow \begin{bmatrix} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) \\ \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \\ \frac{1}{\sqrt{2}}(-|11\rangle + |01\rangle) \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \otimes |1\rangle \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(-|1\rangle + |0\rangle) \otimes |1\rangle \end{bmatrix}$$

$$H \otimes I \longrightarrow \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix}$$

Bob then measures the two qubits in the standard basis to obtain the 2-bit binary encoding of the number Alice wished to send