Today's outline - January 26, 2023

- Simple gates
- The CNOT gate
- General controlled gate
- The SWAP gate
- Quirk implemetations

Reading Assignment: Reiffel: 5.3-5.4 Wong: 6.4-6.5

Homework Assignment #03:
due Thursday, February 02, 2023

Homework Assignment #04:
due Thursday, February 09, 2023

Common single qubit gates

The most common single qubit transformations are the Pauli transformations and the Hadamard gate

$I = \vert 0\rangle\langle 0\vert + \vert 1\rangle\langle 1\vert$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$-\boxed{I}-$	returns the same qubit
$X = \vert 1\rangle\langle 0\vert + \vert 0\rangle\langle 1\vert$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$-\boxed{X}-$	negates the qubit
$Z = \vert 0\rangle\langle 0\vert - \vert 1\rangle\langle 1\vert$	$\begin{pmatrix} 1 & 0 \\ 0 & \bar{1} \end{pmatrix}$	$-\boxed{Z}-$	changes phase of qubit
$Y = \vert 0\rangle\langle 1\vert - \vert 1\rangle\langle 0\vert$	$\begin{pmatrix} 0 & 1 \\ \bar{1} & 0 \end{pmatrix}$	$-\boxed{Y}-$	negate and change phase of qubit
$H = \frac{1}{\sqrt{2}}(\vert 0\rangle\langle 0\vert + \vert 1\rangle\langle 0\vert + \vert 0\rangle\langle 1\vert - \vert 1\rangle\langle 1\vert)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & \bar{1} \end{pmatrix}$	$-\boxed{H}-$	Hadamard gate

The Hadamard gate

The Hadamard gate is particularly important as it transforms pure single qubit states into even superpositions

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

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle\langle 0|0\rangle + |1\rangle\langle 0|0\rangle + |0\rangle\cancelto{0}{\langle 1|0\rangle} - |1\rangle\cancelto{0}{\langle 1|0\rangle}) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \end{aligned}$$

$$\begin{aligned} H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle\cancelto{0}{\langle 0|1\rangle} + |1\rangle\cancelto{0}{\langle 0|1\rangle} + |0\rangle\langle 1|1\rangle - |1\rangle\langle 1|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \end{aligned}$$

the Hadamard gate is its own inverse

$$HH|0\rangle = H\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] = I|0\rangle$$

$$HH|1\rangle = H\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(H|0\rangle - H|1\rangle) = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] = I|1\rangle$$

Controlled-NOT gate

Multiple qubit gates can be constructed as tensor products of single qubit gates but they cannot affect entanglement

The most interesting multiple qubit transformations (gates) are those which change the entanglement of the system

The controlled-NOT (C_{not}) gate is described as

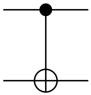
$$C_{not} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

This flips the second qubit if the first qubit is $|1\rangle$ and leaves it unchanged otherwise

$$C_{not}|00\rangle \longrightarrow |00\rangle, \qquad C_{not}|01\rangle \longrightarrow |01\rangle$$

$$C_{not}|10\rangle \longrightarrow |11\rangle, \qquad C_{not}|11\rangle \longrightarrow |10\rangle$$

$$C_{not} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

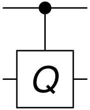


C_{not} is unitary, its own inverse and cannot be decomposed into a product of two single-qubit transformations, however it can change the entanglement between two qubits

$$C_{not}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle\right] = \frac{1}{\sqrt{2}}\left[C_{not}|00\rangle + C_{not}|10\rangle\right] = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$$

General controlled gate

A more generalized controlled gate is one that performs a single-qubit transformation Q on the second qubit only when the first qubit is $|1\rangle$



this kind of gate is represented by the shorthand:
$\bigwedge Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q$ and a 4×4 matrix

$$\bigwedge Q = \begin{pmatrix} I & 0 \\ 0 & Q \end{pmatrix}$$

the controlled phase shift gate, represented by $\bigwedge e^{i\theta} I \equiv \bigwedge e^{i\theta}$ is

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

$$\bigwedge e^{i\theta} I : \quad \begin{array}{ccr} |00\rangle & \rightarrow & |00\rangle \\ |01\rangle & \rightarrow & |01\rangle \\ |10\rangle & \rightarrow & e^{i\theta}|10\rangle \\ |11\rangle & \rightarrow & e^{i\theta}|11\rangle \end{array} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\theta} & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}$$

Note the $\rightarrow$ and not $\mapsto$, the former being a transformation in a complex vector space while the latter works in the complex projective space where $e^{i\theta}|11\rangle \sim |11\rangle$

More about controlled gates

Applying a phase shift to a single qubit is meaningless since global phase shifts can be factored out however, as part of a conditional transformation, this gate is gate is non-trivial as it changes the relative phase of the elements of a superposition

$$\bigwedge e^{i\theta}\left[\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right] \to \frac{1}{\sqrt{2}}(|00\rangle + e^{i\theta}|11\rangle)$$

Another common controlled gate is the one which swaps the two bits of a 2-qubit state

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$|00\rangle \mapsto |00\rangle, \qquad |01\rangle \mapsto |10\rangle, \qquad |10\rangle \mapsto |01\rangle, \qquad |11\rangle \mapsto |11\rangle$$

Things to remember . . .

As mentioned previously, the action of a unitary transformation is completely defined within the complex vector space (denoted by $\to$) while there is ambiguity (global phase) in the complex projective space (denoted by $\mapsto$)

A controlled gate with qubits is not identical to that of a classical computer since one can change basis and the gate may modify both qubits

Consider a 2-qubit system in the Hadamard basis

$$
\begin{aligned}
|++\rangle &= \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\
|+-\rangle &= \tfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \\
|-+\rangle &= \tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) \\
|--\rangle &= \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)
\end{aligned}
$$

Now apply the C_{not} gate: $C_{not} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$

$$
\begin{aligned}
C_{not} : \quad |++\rangle &\to \tfrac{1}{2}(|00\rangle + |01\rangle + |11\rangle + |10\rangle) = |++\rangle \\
|+-\rangle &\to \tfrac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle) = |--\rangle \\
|-+\rangle &\to \tfrac{1}{2}(|00\rangle + |01\rangle - |11\rangle - |10\rangle) = |-+\rangle \\
|--\rangle &\to \tfrac{1}{2}(|00\rangle - |01\rangle - |11\rangle + |10\rangle) = |+-\rangle
\end{aligned}
$$

Things to remember . . .

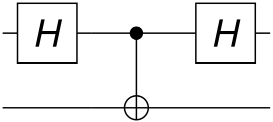
It is not even relevant to define control and target qubits since C_{not} takes a separable 2-qubit state and entangles it

$$
\begin{aligned}
C_{not}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle &= (|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|)\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)
\end{aligned}
$$

Finally, it is important to work out the circuits without assuming their function

Consider the circuit with 2 Hadamard gates and a C_{not}

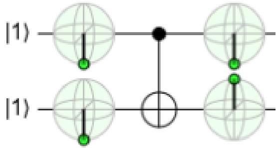
This might seem to leave the $|00\rangle$ state unchanged but



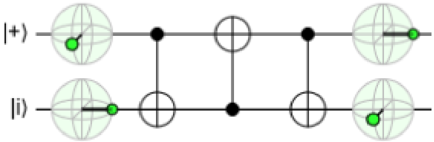
$$
\begin{aligned}
(H \otimes I)C_{not}(H \otimes I)|0\rangle|0\rangle &= (H \otimes I)C_{not}\frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)|0\rangle|0\rangle \\
&= (H \otimes I)C_{not}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = (H \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)
\end{aligned}
$$

Quirk implementations

C_{not} gate



SWAP gate



What happens when the inputs are not in the Standard basis?

How do we make a primitve C_{not} in Quirk?

[Start Quirk]

Remember that in Quirk the low order qubit is at the top, opposite of how we generally think of matrices