Quantum Computing for Computer Scientists

The gate quantum computation model

Why learn quantum computing?

- Quantum supremacy expected this year
  - Microsoft, Google, Intel, IBM all investing in quantum computer development
- Several exciting applications already known
  - Efficiently factor large composite numbers, breaking RSA encryption (Shor's algorithm, 1994)
  - Search an unordered list in O($\sqrt{n}$) time (Grover's algorithm, 1996)
  - Believed exponential speedup in simulating quantum mechanical systems
- Intellectually interesting – quantum mechanics is outside your intuition!
  - Get a small glimpse of what you don't know you don't know

Learning objectives

- Representing computation with basic linear algebra (vectors and matrices)
- Qbits, superposition, and quantum logic gates
- The simplest problem where a quantum computer beats a classical computer
- Bonus topics: quantum entanglement and teleportation

Representing classical bits as a vector

One bit with the value 0, also written as $|0\rangle$ (Dirac vector notation)

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

One bit with the value 1, also written as $|1\rangle$

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

Review: matrix multiplication

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax + by + cz \\ dx + ey + fz \\ gx + hy + iz \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

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

Operations on one classical bit (cbit)

Identity	$f(x) = x$	$\begin{tikzcd} 0 \arrow[r] & 0 \\ 1 \arrow[r] & 1 \end{tikzcd}$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$
Negation	$f(x) = \neg x$	$\begin{tikzcd} 0 \arrow[dr] & 0 \\ 1 \arrow[ur] & 1 \end{tikzcd}$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$
Constant-0	$f(x) = 0$	$\begin{tikzcd} 0 \arrow[r] & 0 \\ 1 \arrow[ur] & 1 \end{tikzcd}$	$\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$
Constant-1	$f(x) = 1$	$\begin{tikzcd} 0 \arrow[dr] & 0 \\ 1 \arrow[r] & 1 \end{tikzcd}$	$\begin{pmatrix}0 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$

Reversible computing

- Reversible means given the operation and output value, you can find the input value
  - For $Ax = b$, given b and A, you can uniquely find x
- Operations which permute are reversible; operations which erase & overwrite are not
  - Identity and Negation are reversible
  - Constant-0 and Constant-1 are not reversible
- Quantum computers use only reversible operations, so we will only care about those
  - In fact, all quantum operators *are their own inverses*

Review: tensor product of vectors

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \\ x_1 \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 6 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \otimes \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 z_0 \\ x_0 y_0 z_1 \\ x_0 y_1 z_0 \\ x_0 y_1 z_1 \\ x_1 y_0 z_0 \\ x_1 y_0 z_1 \\ x_1 y_1 z_0 \\ x_1 y_1 z_1 \end{pmatrix}$$

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

Representing multiple cbits

$$|00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$|01\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

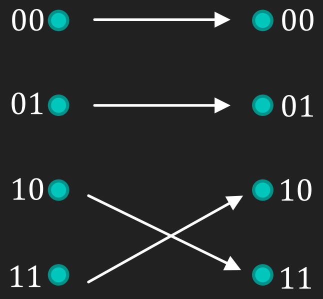
$$|11\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

$$|4\rangle = |100\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}$$

- We call this tensored representation the **product state**
- We can **factor** the product state back into the **individual state** representation
- The product state of n bits is a vector of size 2^n

Operations on multiple cbits: CNOT

- Operates on pairs of bits, one of which is the "control" bit and the other the "target" bit
- If the control bit is 1, then the target bit is flipped
- If the control bit is 0, then the target bit is unchanged
- The control bit is always unchanged
- With most-significant bit as control and least-significant bit as target, action is as follows:



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

Operations on multiple cbits: CNOT

$$C|10\rangle = C\left(\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = |11\rangle$$

$$C|11\rangle = C\left(\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = |10\rangle$$

Operations on multiple cbits: CNOT

$$C|00\rangle = C\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = |00\rangle$$

$$C|01\rangle = C\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = |01\rangle$$

Recap

- We represent classical bits in vector form as $\binom{1}{0}$ for 0 and $\binom{0}{1}$ for 1
- Operations on bits are represented by matrix multiplication on bit vectors
- Quantum computers only use reversible operations
- Multi-bit states are written as the tensor product of single-bit vectors
- The CNOT gate is a fundamental building block of reversible computing

Qbits and superposition

- Surprise! We've actually been using qbits all along!
- The cbit vectors we've been using are just special cases of qbit vectors
- A qbit is represented by $\binom{a}{b}$ where a and b are Complex numbers and $||a||^2 + ||b||^2 = 1$
  - The cbit vectors $\binom{1}{0}$ and $\binom{0}{1}$ fit within this definition
  - Don't worry! For this presentation, we'll only use familiar Real numbers.
- Example qbit values:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} \quad \begin{pmatrix} -1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$$

Qbits and superposition

- How can a qbit to have a value which is not 0 or 1? This is called superposition.
- Superposition means the qbit is both 0 and 1 and the same time
- When we **measure** the qbit, it **collapses** to an actual value of 0 or 1
  - We usually do this at the end of a quantum computation to get the result
- If a qbit has value $\binom{a}{b}$ then it collapses to 0 with probability $||a||^2$ and 1 with probability $||b||^2$
  - For example, qbit $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ has a $\left\|\frac{1}{\sqrt{2}}\right\|^2 = \frac{1}{2}$ chance of collapsing to 0 or 1 (coin flip)
  - The qbit $\binom{1}{0}$ has a 100% chance of collapsing to 0, and $\binom{0}{1}$ has a 100% chance of collapsing to 1

Qbits and superposition

- Multiple qbits are similarly represented by the tensor product $\binom{a}{b} \otimes \binom{c}{d} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$
  - Note that $\|ac\|^2 + \|ad\|^2 + \|bc\|^2 + \|bd\|^2 = 1$
- For example, the system $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$ (note that $\left\|\frac{1}{2}\right\|^2 = \frac{1}{4}$, and $\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$)
  - There's a ¼ chance each of collapsing to $|00\rangle, |01\rangle, |10\rangle$, or $|11\rangle$

Operations on qbits

- How do we operate on qbits? The same way we operate on cbits: with matrices!
- All the matrix operators we've seen also work on qbits (bit flip, CNOT, etc.)
- Matrix operators model the effect of some device which manipulates qbit spin/polarization without measuring and collapsing it

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{pmatrix}$$

- There are several important matrix operators which only make sense in a quantum context

The Hadamard gate

- The Hadamard gate takes a 0- or 1-bit and puts it into exactly equal superposition

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \qquad H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$$

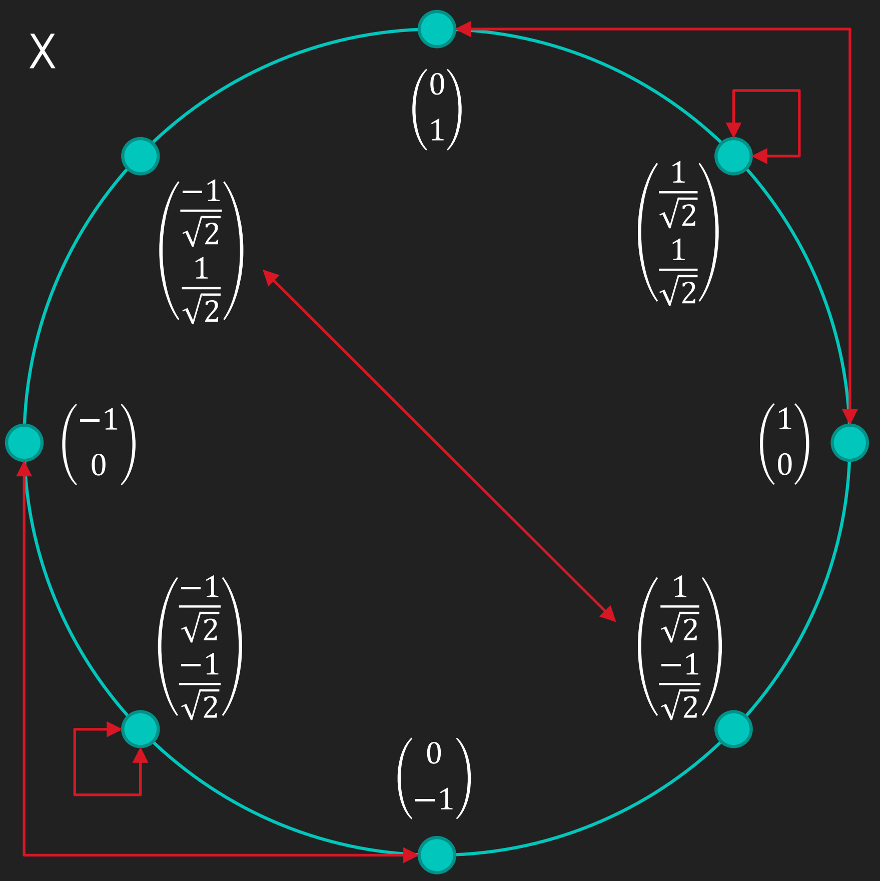
The Hadamard gate

- The Hadamard gate also takes a qbit in exactly-equal superposition, and transforms it into a 0- or 1-bit! (This should be unsurprising – remember operations are their own inverse!)

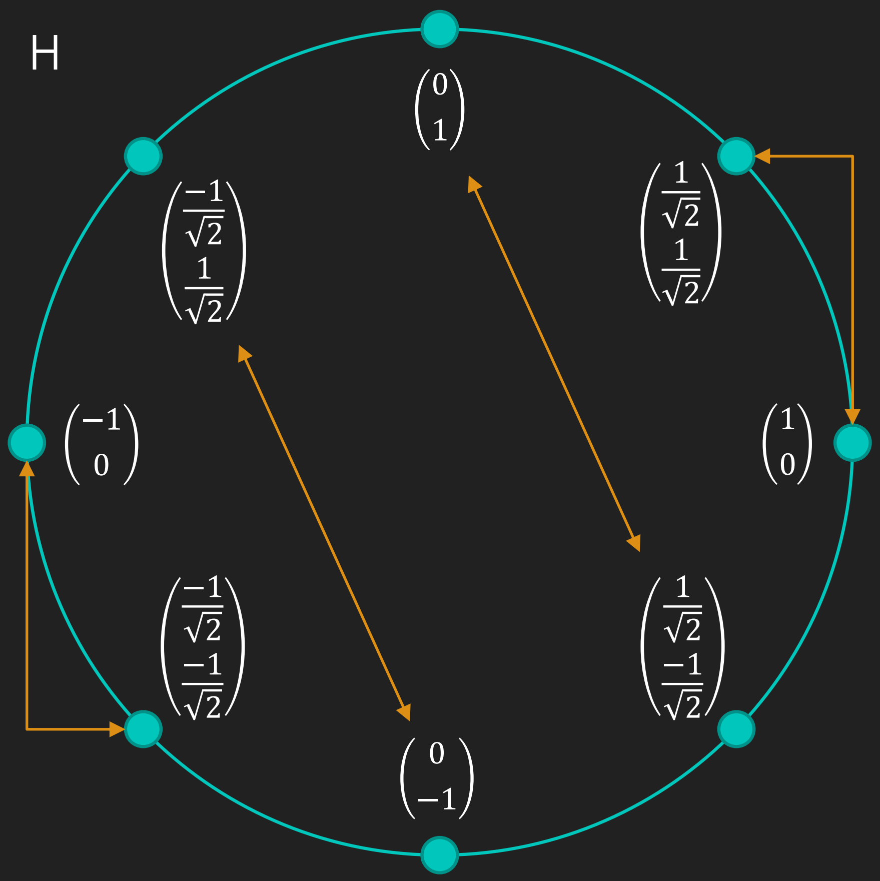
$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- We can transition out of superposition without measurement!
- We can thus structure quantum computation deterministically instead of probabilistically

The unit circle state machine

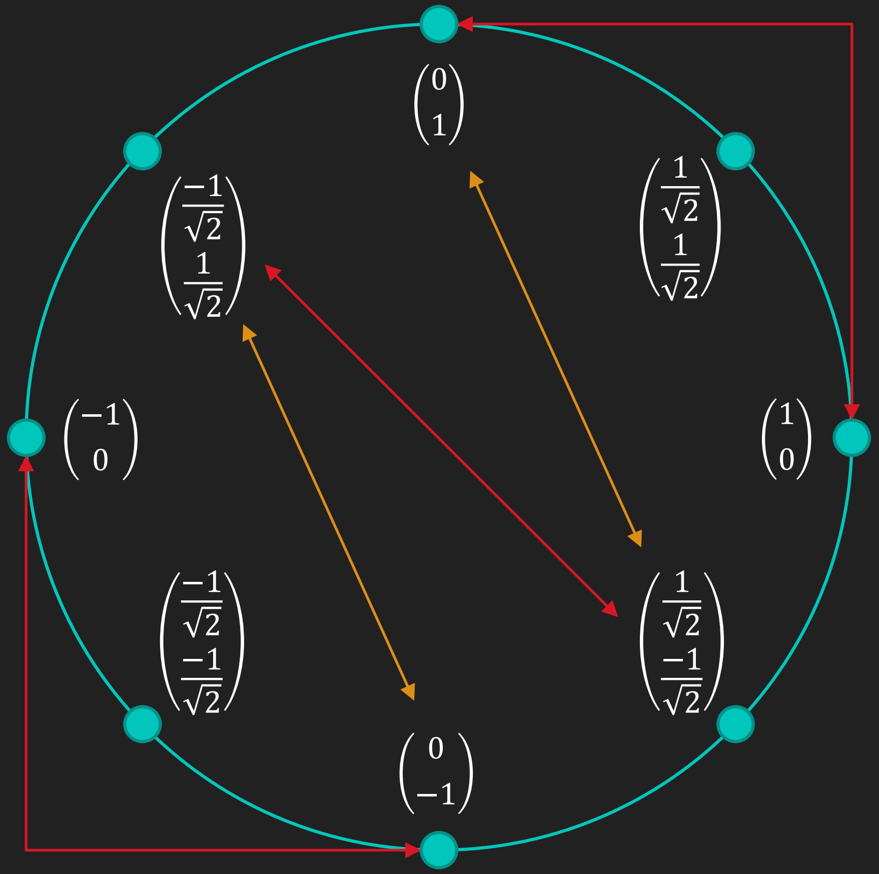


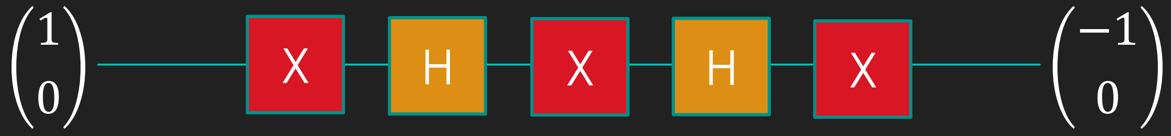
X
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$



H
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$

The unit circle state machine


$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$


$\begin{pmatrix}1\\0\end{pmatrix}$
X
H
X
H
X
$\begin{pmatrix}-1\\0\end{pmatrix}$

Recap

- Cbits are just a special case of qbits, which are 2-vectors of Complex numbers
- Qbits can be in superposition, and are probabilistically collapsed to cbits by measurement
- Multi-qbit systems are tensor products of single-qbit systems, like with cbits
- Matrices represent operations on qbits, same as with cbits
- The Hadamard gate takes 0- and 1-bits to equal superposition, and back
- We can think of qbits and their operations as forming a state machine on the unit circle
    - Actually the unit sphere if we use complex numbers

The Deutsch oracle

- Imagine someone gives you a black box containing a function on one bit
  - Recall! What are the four possible functions on one bit?
- You don’t know which function is inside the box, but can try inputs and see outputs
- How many queries would it take to determine the function on a classical computer?
- How many on a quantum computer?

The Deutsch oracle

- What if you want to check whether the unknown function is constant, or variable?
  - Constant-0 & constant-1 are constant, identity & negation are variable
- How many queries would it take on a classical computer?
- How many on a quantum computer?

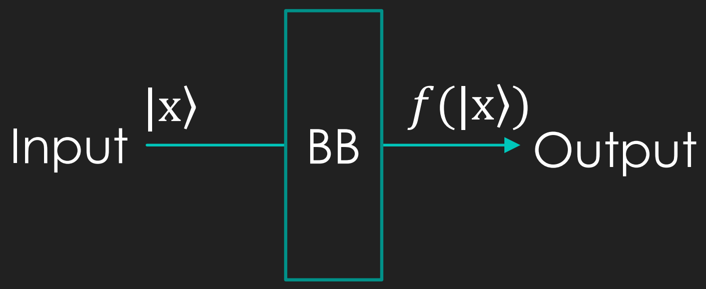
The Deutsch oracle

- How can it be done in a single query!?
- We can do it with the magic of superposition!
- First, we have to define what each of the four functions look like on a quantum computer
  - We have an immediate problem with the constant functions

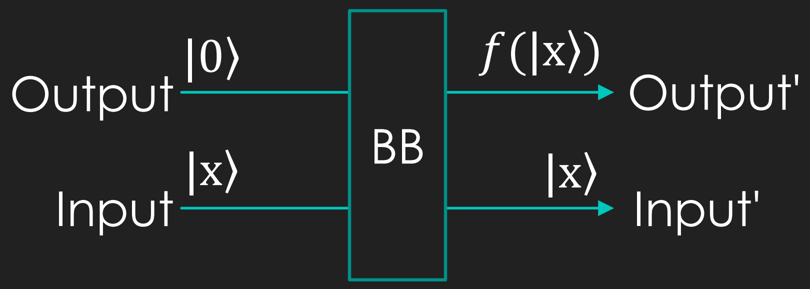
The Deutsch oracle

- How do we write nonreversible functions in a reversible way?
- Common hack: add an additional **output qbit** to which the function action is applied
- We thus have to rewire our black box:

Before:

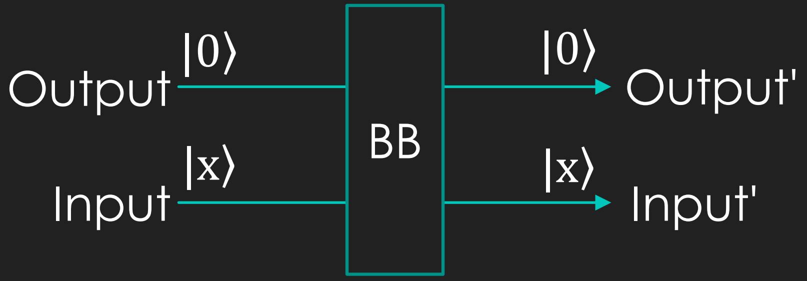


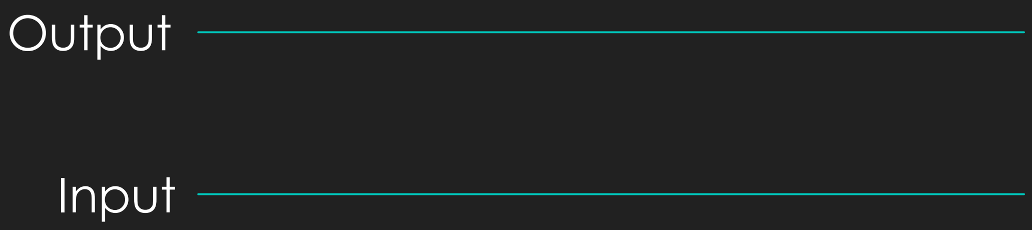
After:



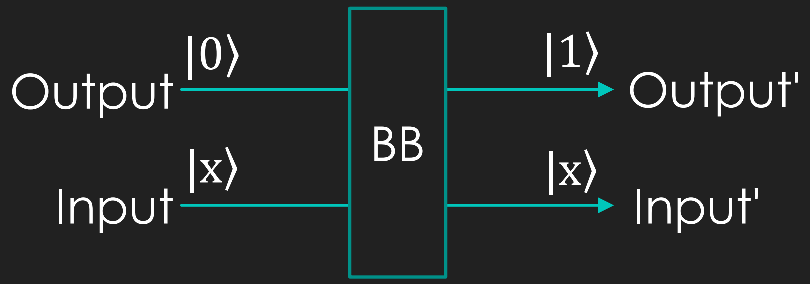
- The black box leaves the **input qbit** unchanged, writing function output to **output qbit**

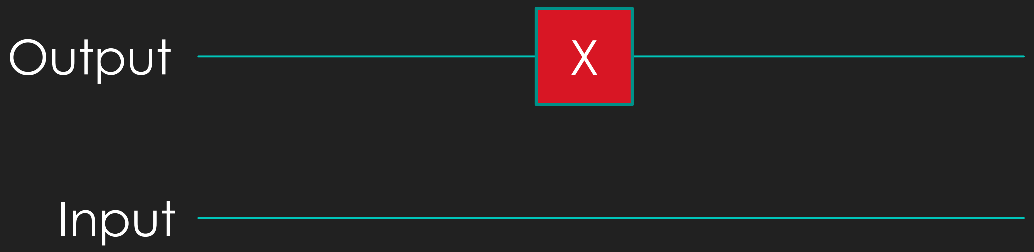
The Deutsch oracle: constant-0



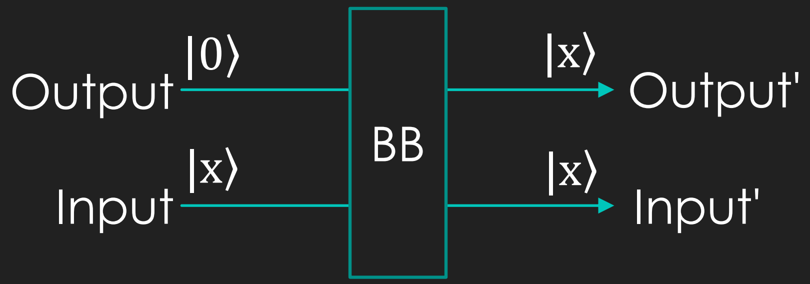


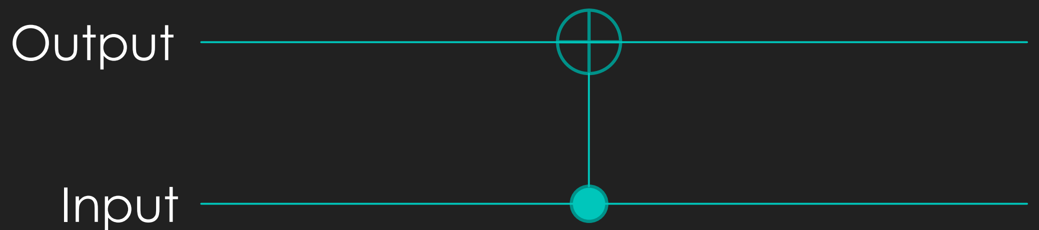
The Deutsch oracle: constant-1



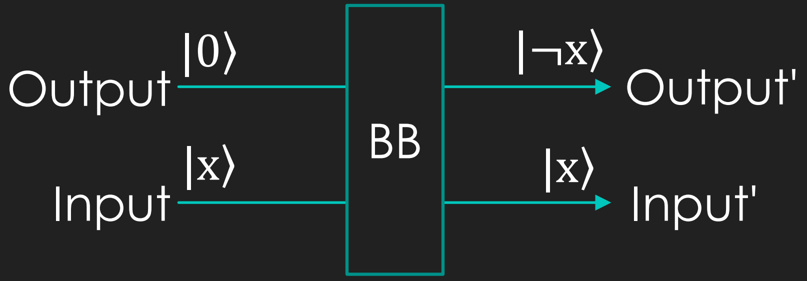


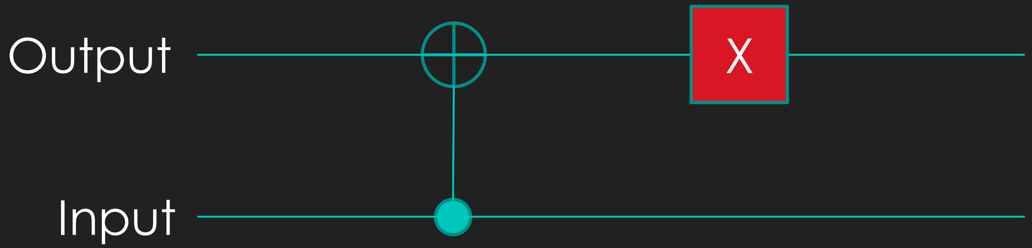
The Deutsch oracle: identity





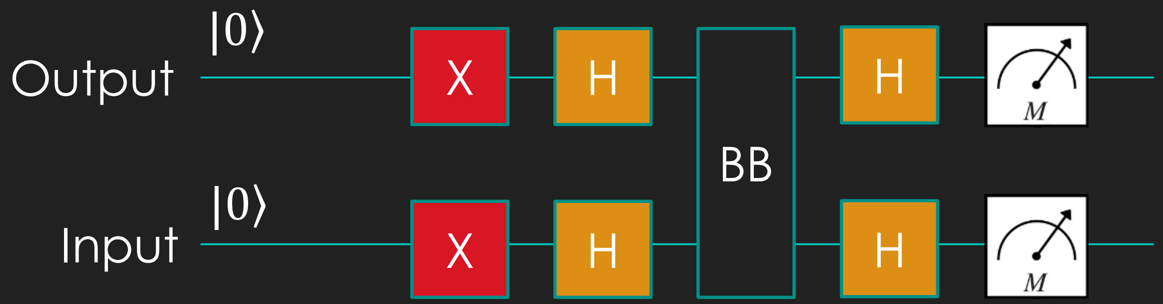
The Deutsch oracle: negation





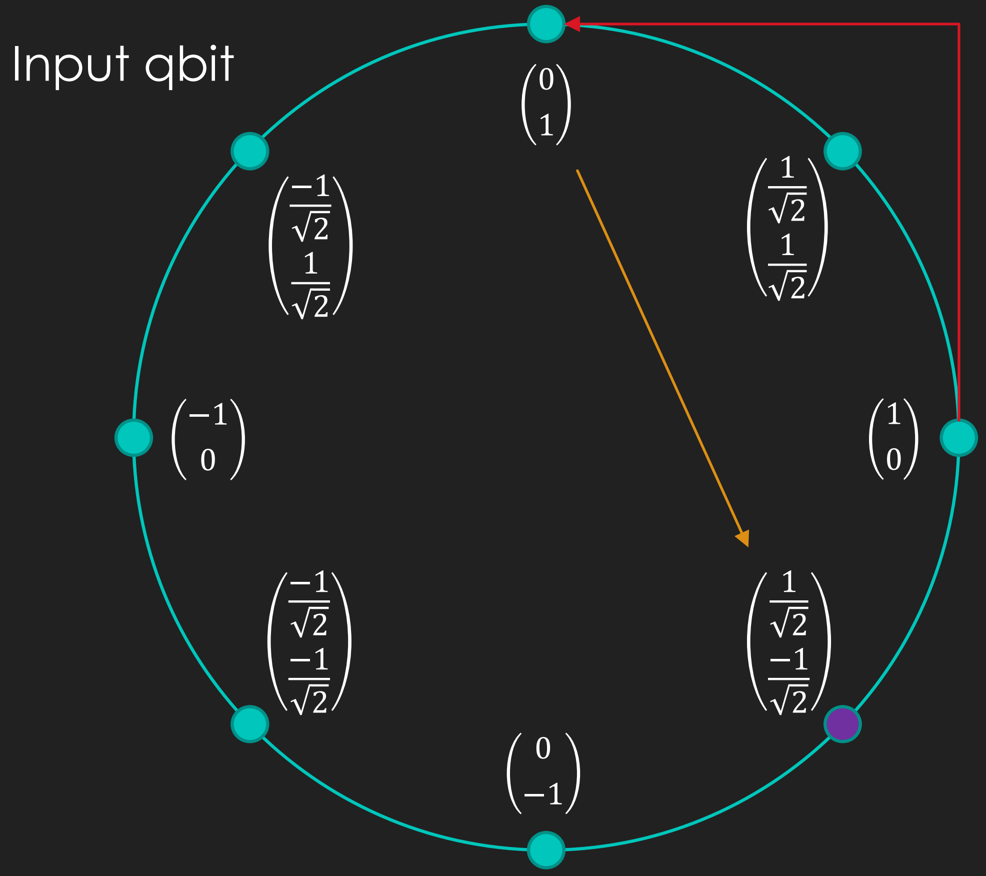
The Deutsch oracle

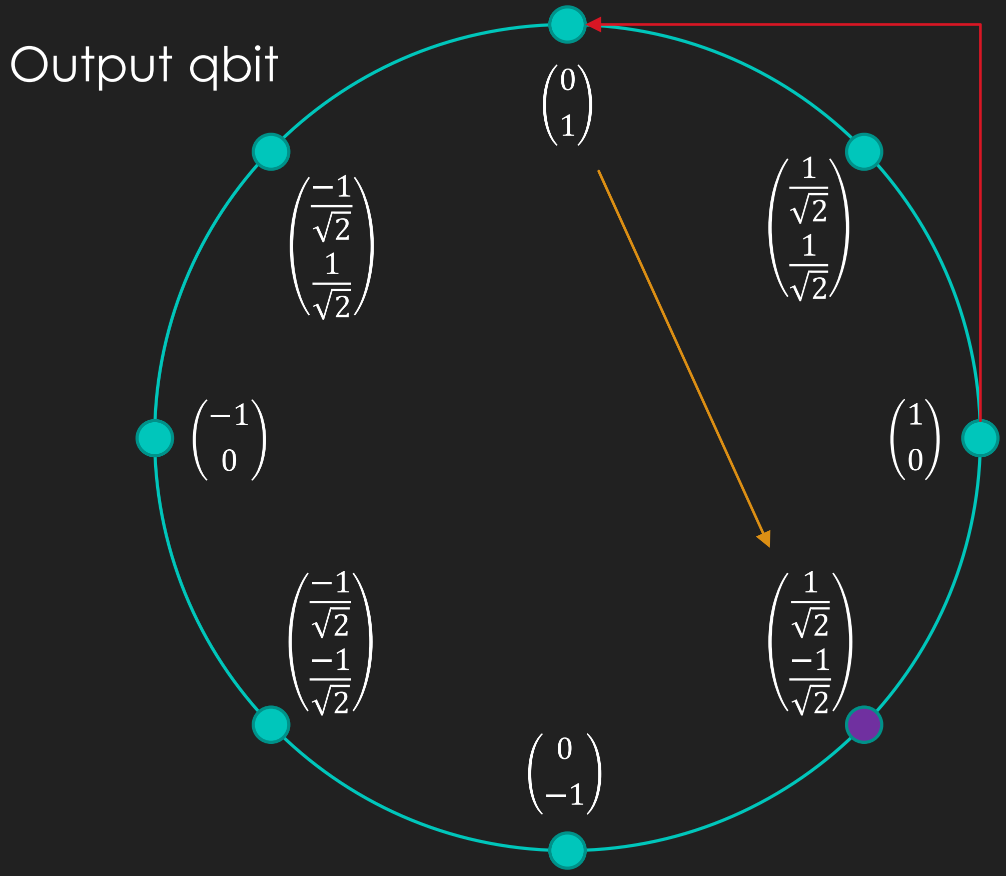
- How do we solve it on a quantum computer in one query?



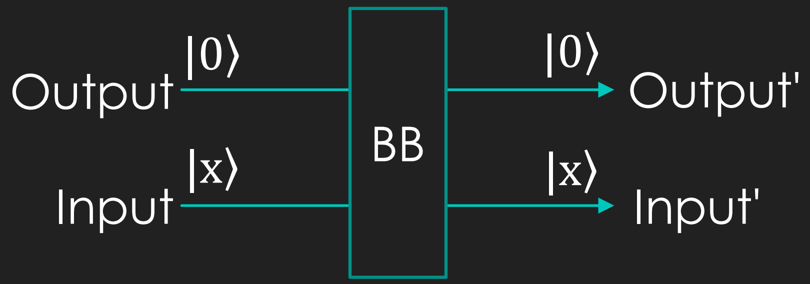
- If the black-box function is constant, system will be in state $|11\rangle$ after measurement
- If the black-box function is variable, system will be in state $|01\rangle$ after measurement

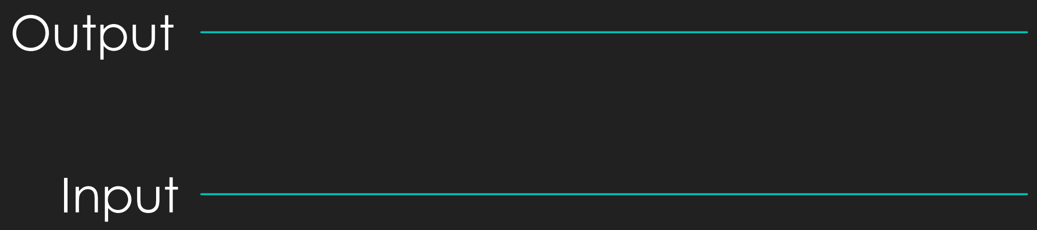
The Deutsch oracle: preprocessing


Input qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$

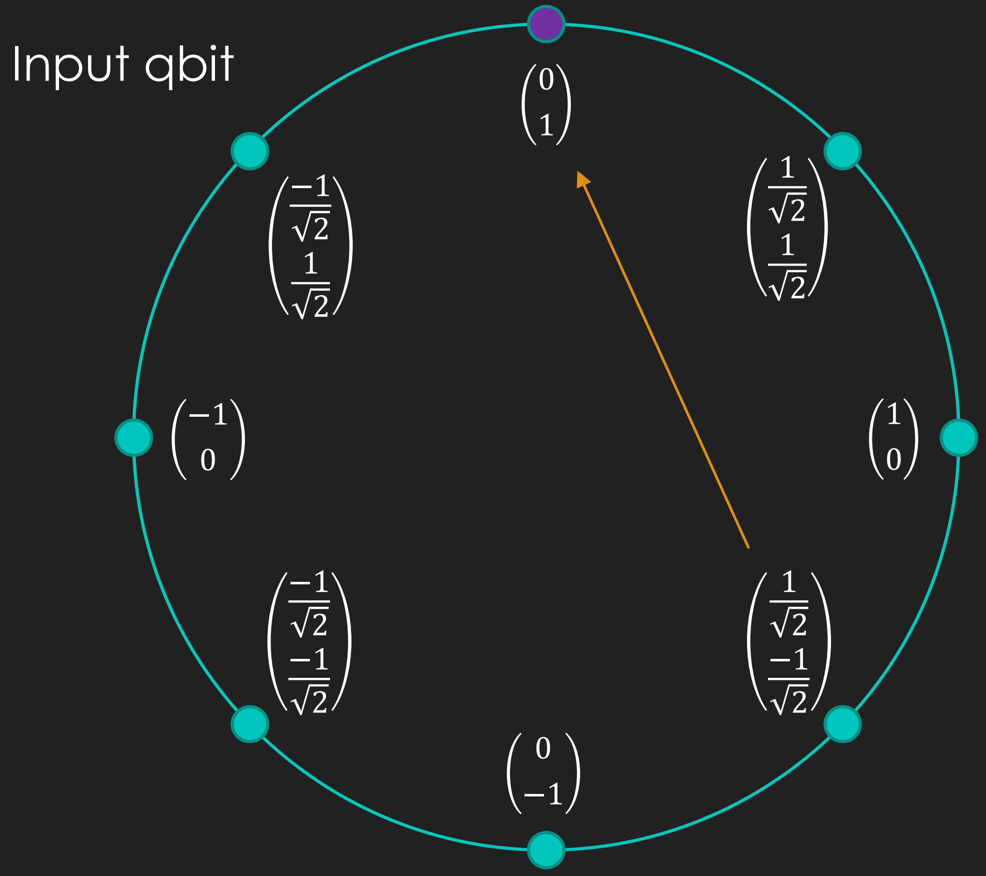

Output qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$

The Deutsch oracle: constant-0

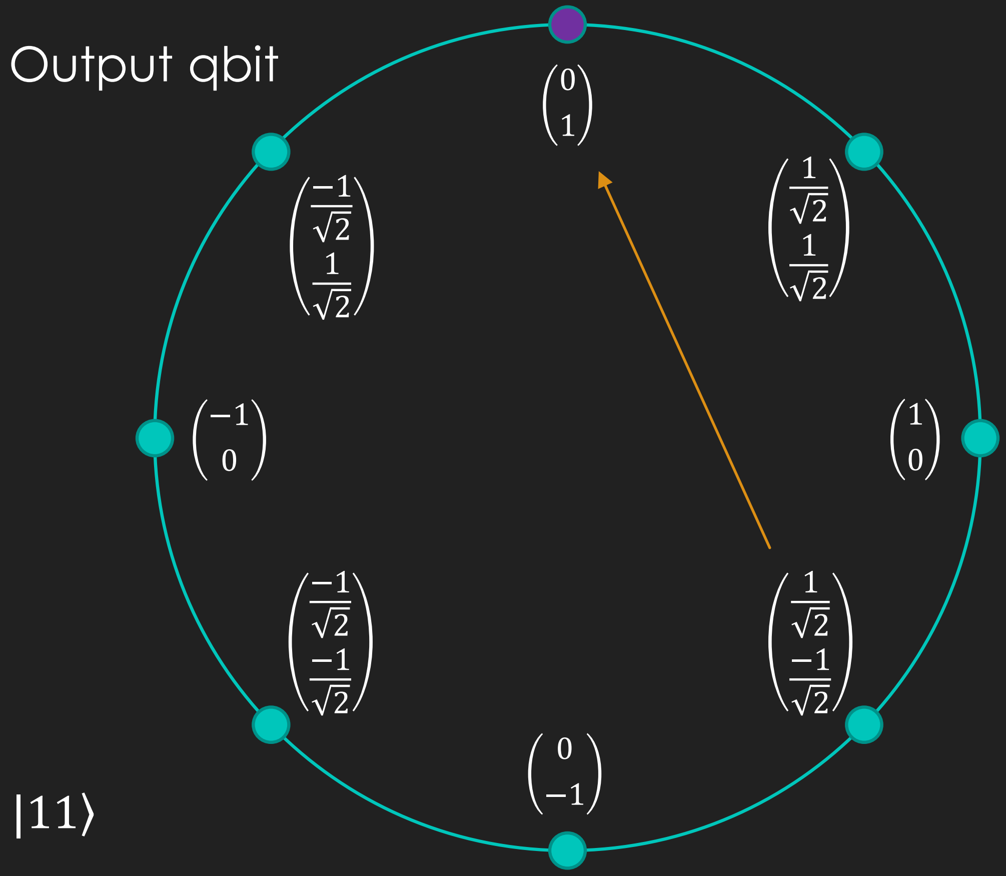




The Deutsch oracle: constant-0



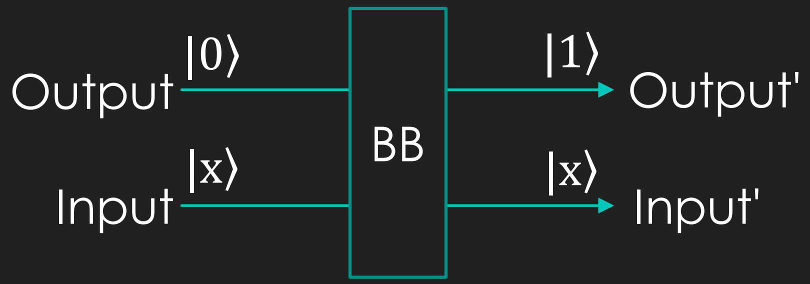
Input qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$

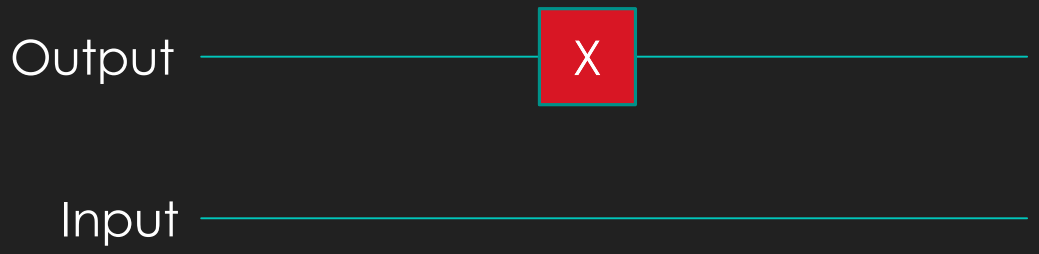


Output qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$

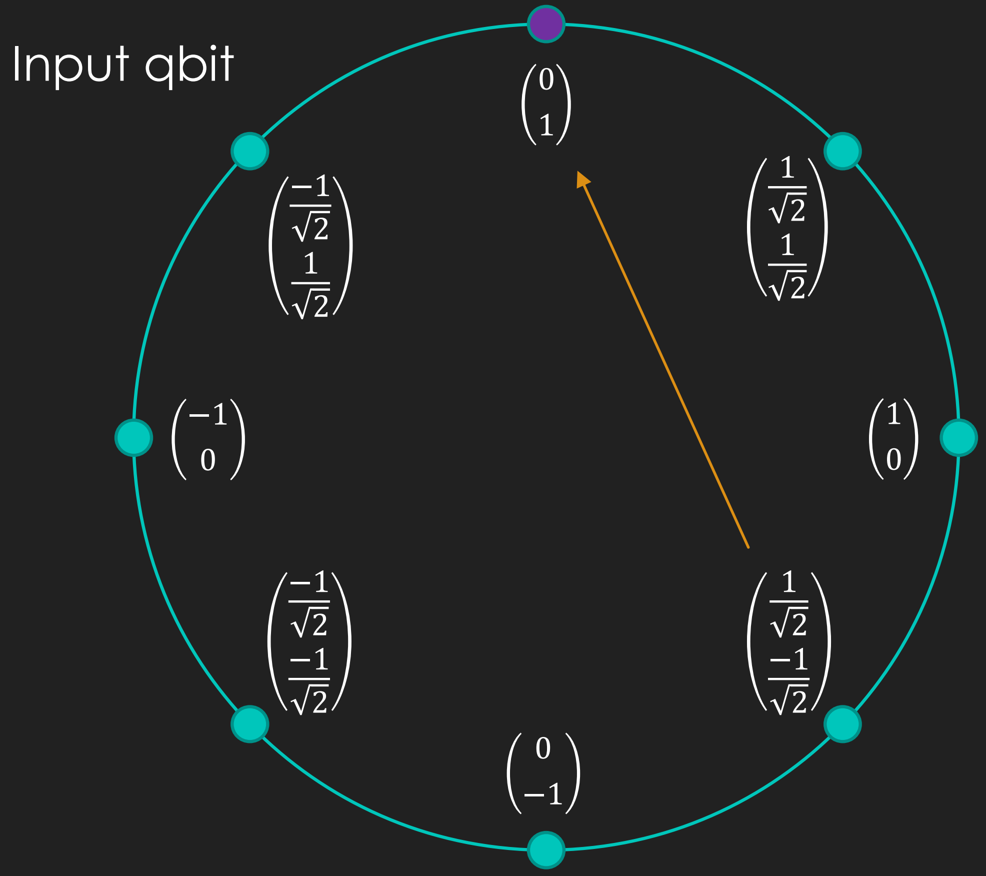
Result: $|11\rangle$

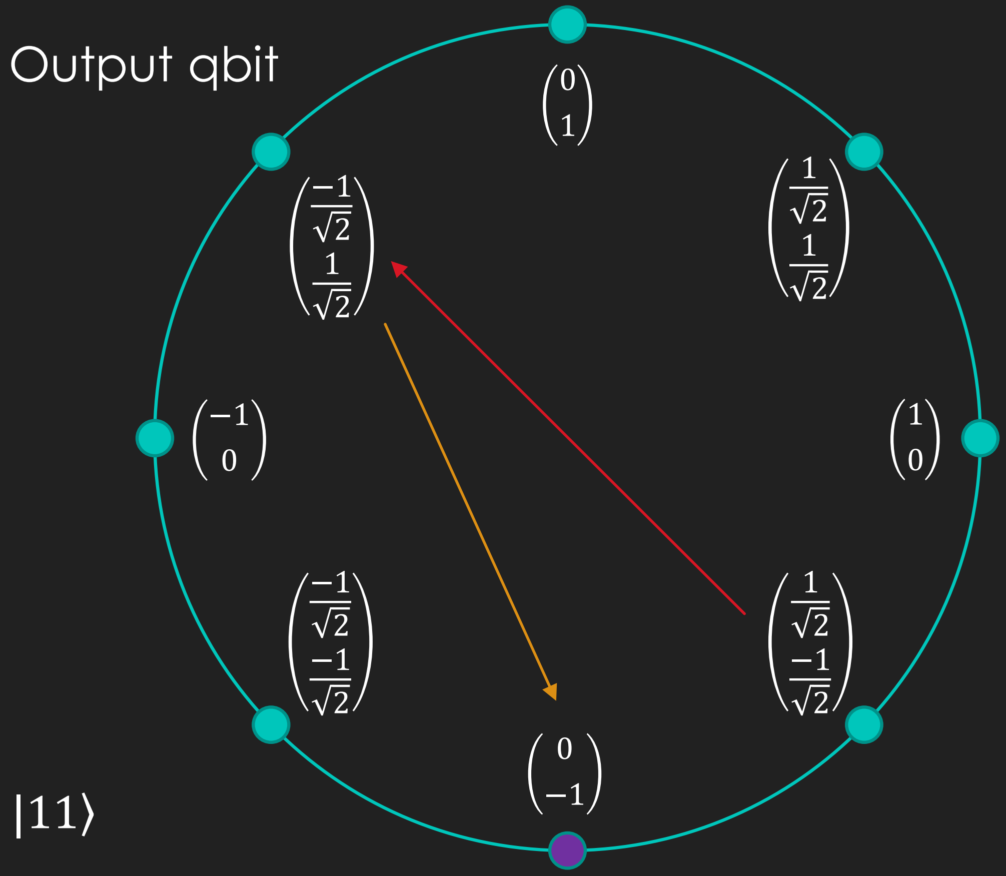
The Deutsch oracle: constant-1





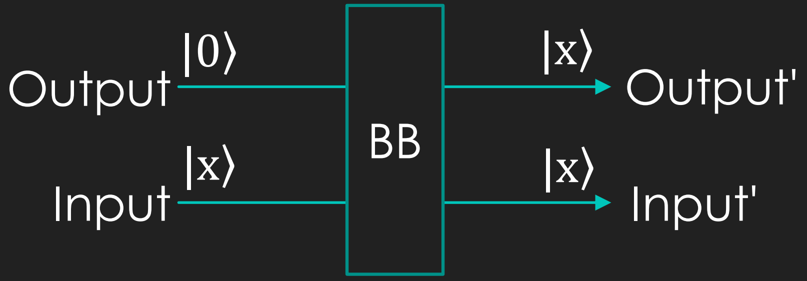
The Deutsch oracle: constant-1

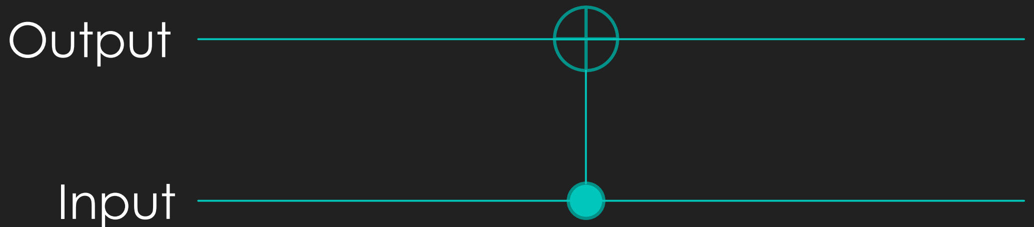

Input qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$


Output qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$

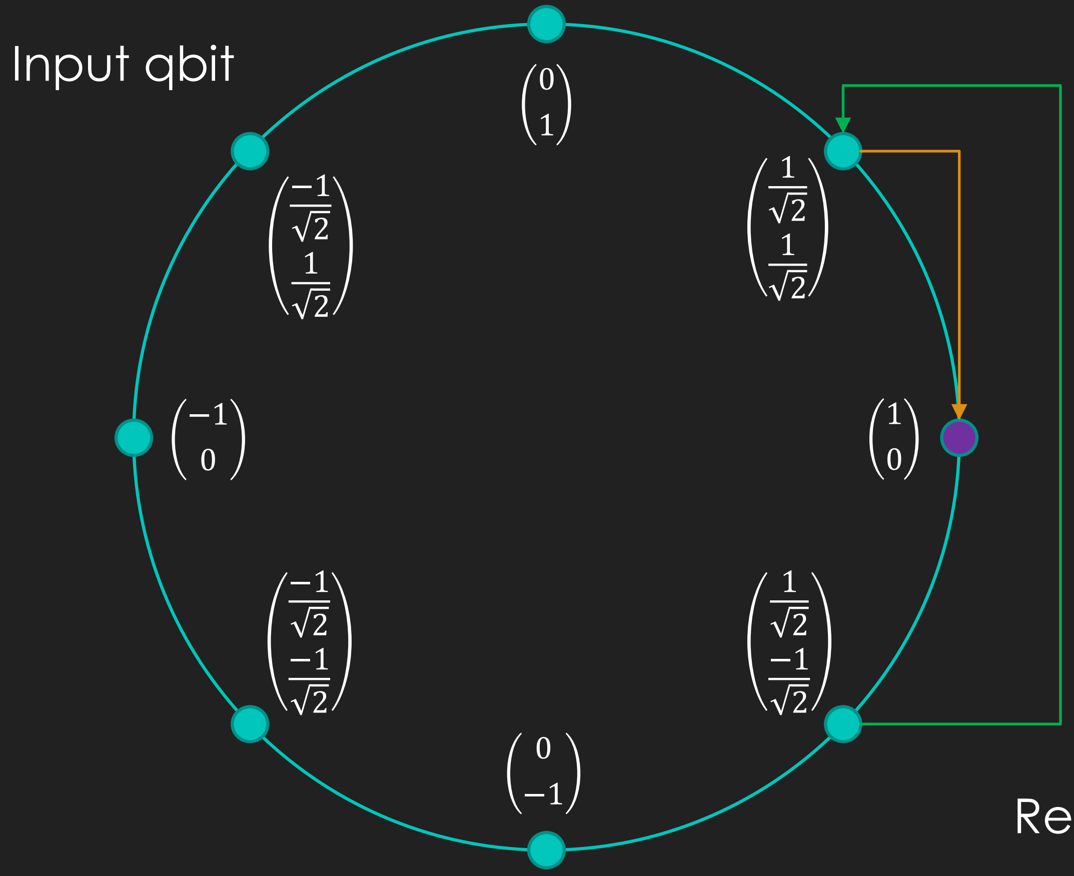
Result: $|11\rangle$

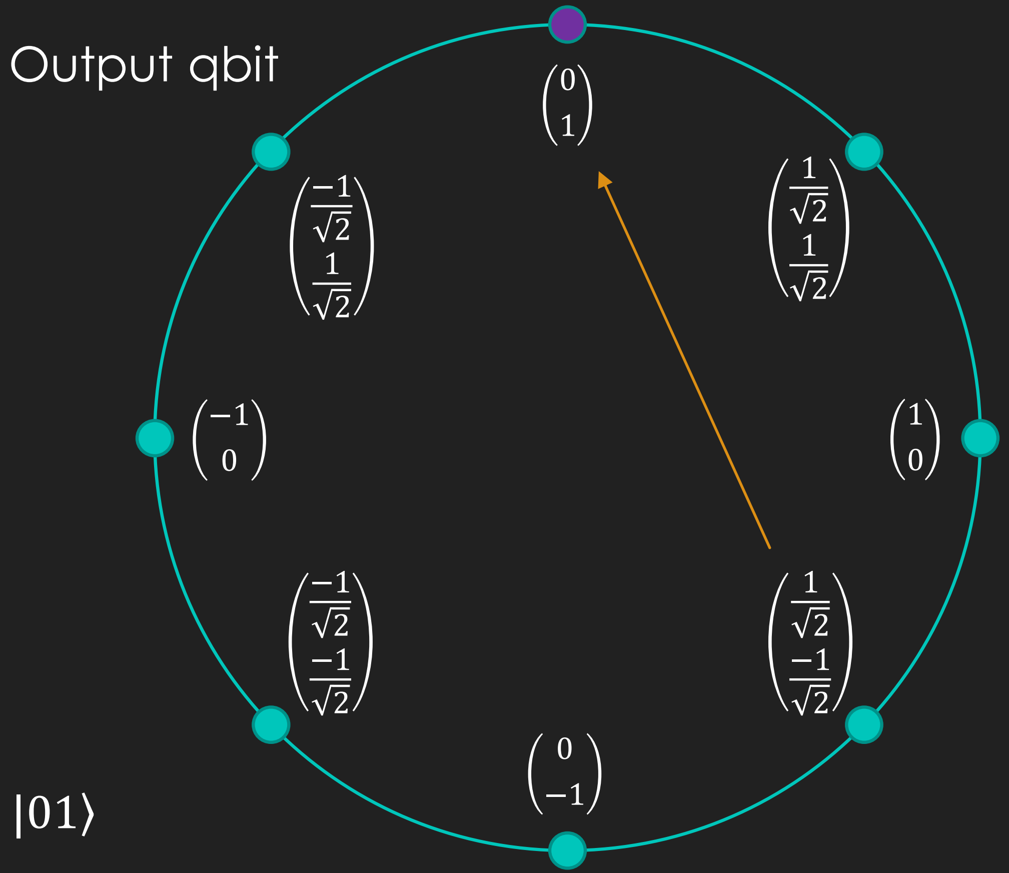
The Deutsch oracle: identity





The Deutsch oracle: identity


Input qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$

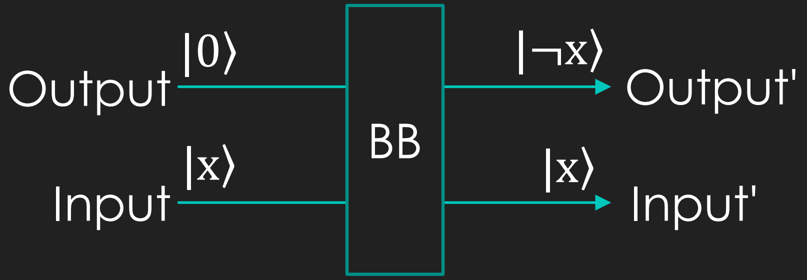

Output qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$

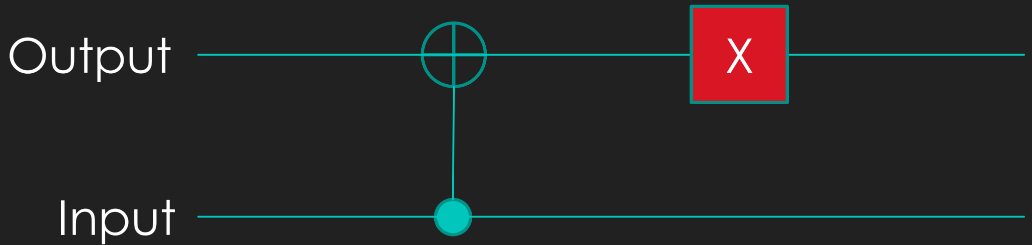
Result: $|01\rangle$

The Deutsch oracle: identity

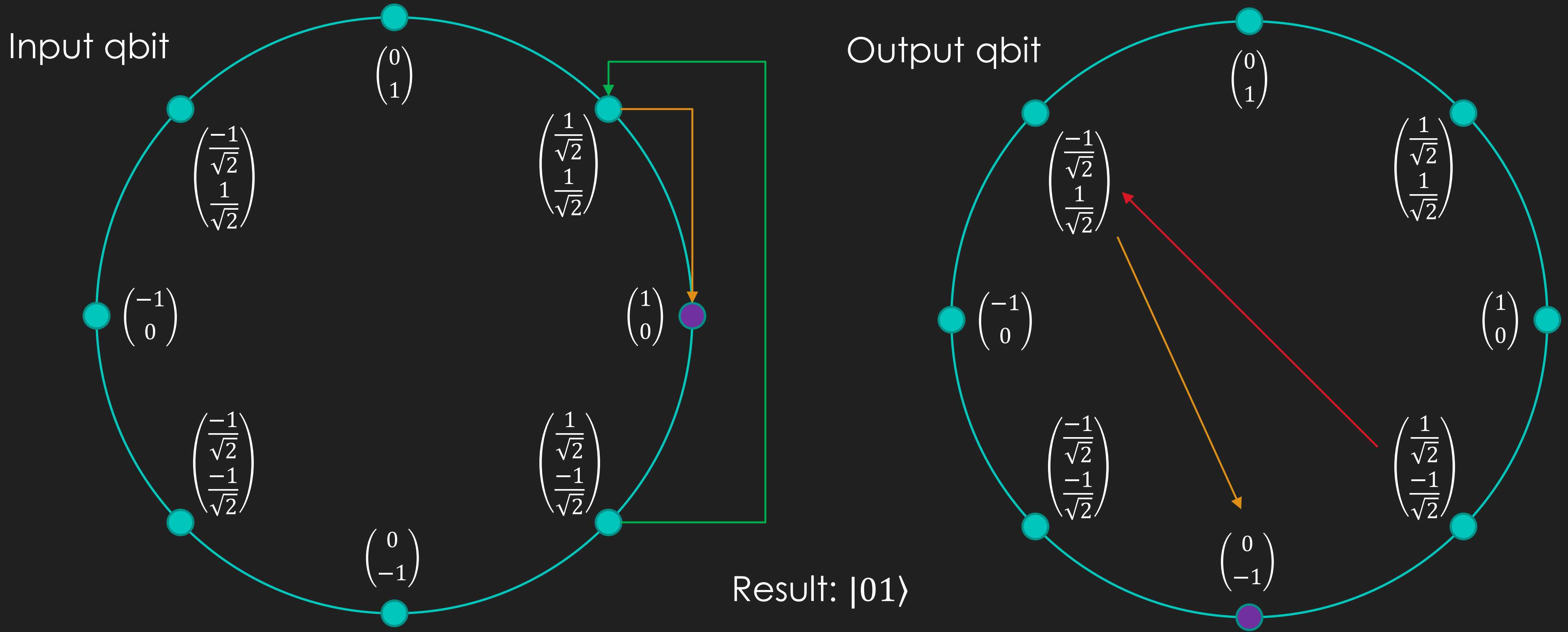
$$C\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{pmatrix}\right)=C\begin{pmatrix}\frac{1}{2}\\ \frac{-1}{2}\\ \frac{-1}{2}\\ \frac{1}{2}\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{pmatrix}$$

The Deutsch oracle: negation





The Deutsch oracle: negation


Input qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$
Output qbit
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}-1\\0\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}\frac{-1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\end{pmatrix}$
$\begin{pmatrix}0\\-1\end{pmatrix}$

Result: $|01\rangle$

The Deutsch oracle

- We did it! We determined whether the function was constant or variable in a single query!
- Intuition: the difference *within* the categories (negation) was neutralized, while the difference *between* the categories (CNOT) was magnified
- This problem seems pretty contrived (and it was, when it was published)
- A generalized version with an n-bit black box also exists (Deutsch-Josza problem)
  - Determine whether the function returns the same value for all 2^n inputs (i.e. is constant)
- A variant of the generalized version was an inspiration for Shor's algorithm!

Full recap

- We learned how to model classical computation with basic linear algebra
- We learned about qbits, superposition, and the Hadamard gate
- We learned the Deutsch Oracle problem, where quantum outperforms classical

Bonus topics

- Quantum entanglement
- Quantum teleportation

Entanglement

- If the product state of two qbits cannot be factored, they are said to be **entangled**

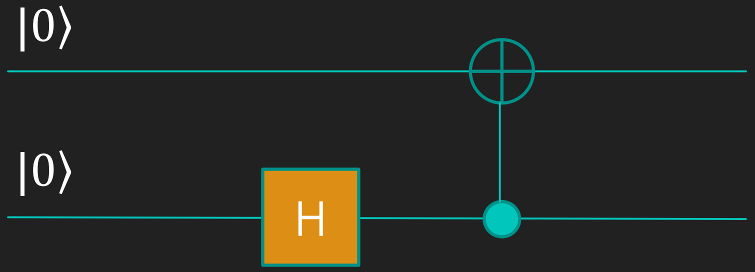
$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix}$$

$$\begin{aligned} ac &= \frac{1}{\sqrt{2}} \\ ad &= 0 \\ bc &= 0 \\ bd &= \frac{1}{\sqrt{2}} \end{aligned}$$

- The system of equations has no solution, so we cannot factor the quantum state!
- This has a 50% chance of collapsing to $|00\rangle$ and 50% chance of collapsing to $|11\rangle$

Entanglement

How can we reach an entangled state? Easy!



$$CH_1\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=C\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix}$$

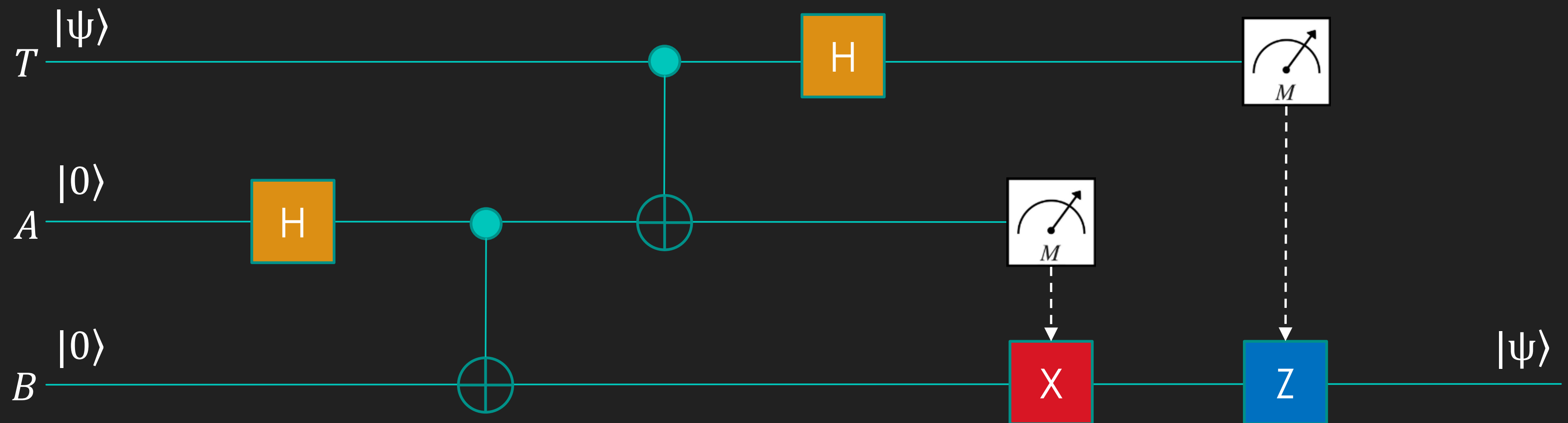
Entanglement

- What's going on here? The qbits seem to be coordinating in some way
  - Measuring one qbit also collapses the other in a correlated state
- This coordination happens even across vast stretches of space
- The coordination even happens faster than the speed of light! It is instantaneous.
  - A 2013 experiment measured particles within 0.01% of the travel time of light between them
- Surely the qbits "decided" at the time of entanglement what they would do?
  - No! This is called "hidden variable" theory and was disproved by John Bell in 1964
- This does indeed break locality through faster-than-light coordination
  - However – and this is the critical part – *no information can be communicated*

Teleportation

- **Quantum teleportation** is the process by which the state of an arbitrary qbit is transferred from one location to another by way of two other entangled qbits
- You can transfer qbit states (cut & paste) but you cannot clone them (copy & paste)
  - This is called the **No-cloning theorem**
- The teleportation is not faster-than-light, because some classical information must be sent

Teleportation



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

Further learning goals

- Deutsch-Jozsa algorithm and Simon’s periodicity problem
  - Former yields oracle separation between EQP and P, latter between BQP and BPP
- Shor’s algorithm and Grover’s algorithm
- Quantum cryptographic key exchange
- How qbits, gates, and measurement are actually implemented
- Quantum error correction
- Quantum programming language design

Further reading

- Recommended textbook: *Quantum Computing for Computer Scientists*
  - Others have recommended *Quantum Computing: A Gentle Introduction*
  - For those with heavier math backgrounds, *Quantum Computer Science: An Introduction*
- The Microsoft Quantum Development Kit docs are nice [link]
  - The development kit contains a quantum computer simulator!
  - Exercise: implement the Deutsch Oracle tester in Q#
- Some skepticism about physically-realizable quantum computers [link]
  - Noise might increase exponentially with the number of physical qbits

Appendices

- Single-bit operations on multi-bit states
- Quantum teleportation math

Review: matrix multiplication associativity

$$(AB)x = A(Bx)$$

$$\left(\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\right)\begin{pmatrix}a\\b\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\left(\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}\right)$$

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

$$\begin{pmatrix}a\\b\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}$$

$$(HXH)x = Zx$$

$$\left(\frac{1}{2}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\right)\begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

$$\left(\frac{1}{2}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}1 & -1\\1 & 1\end{pmatrix}\right)\begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}\alpha\\-\beta\end{pmatrix}$$

$$\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}\alpha\\-\beta\end{pmatrix}$$

$$\begin{pmatrix}\alpha\\-\beta\end{pmatrix} = \begin{pmatrix}\alpha\\-\beta\end{pmatrix}$$

You only have to care about the *cumulative effect* of a series of gates; the specific sequence changes nothing.

Review: tensor product of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} a\begin{pmatrix} w & x \\ y & z \end{pmatrix} & b\begin{pmatrix} w & x \\ y & z \end{pmatrix} \\ c\begin{pmatrix} w & x \\ y & z \end{pmatrix} & d\begin{pmatrix} w & x \\ y & z \end{pmatrix} \end{pmatrix} = \begin{pmatrix} aw & ax & bw & bx \\ ay & az & by & bz \\ cw & cx & dw & dx \\ cy & cz & dy & dz \end{pmatrix}$$

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

Single-bit operations on multi-bit states

- When applying gates to multi-bit states, we want to specify which qbit we're modifying
- We use subscripts to identify the qbit
- The subscript value is the power of 2 associated with the significance of that qbit
  - So 0, 1, 2, 3, 4, etc. since any binary number is written as $\alpha_0 2^0 + \alpha_1 2^1 + \alpha_2 2^2 + \cdots$
- So X_2 refers to the bit-flip operator which flips the most-significant qbit in a 3-qbit system

Single-bit operations on multi-bit states

What if we want to operate on a single bit in the product state? What matrix do we use?

Example - flip the least-significant bit:

$$X_0|01\rangle = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$$

The operation we want is tensored with the identity matrix, in the position matching the significance of that bit.

Single-bit operations on multi-bit states

We can also tensor multiple one-bit operators together to operate on bits in parallel.

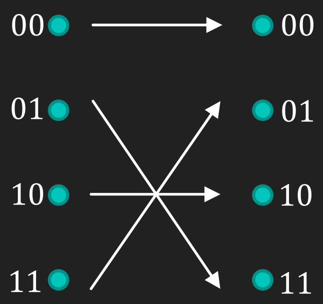
Example – flip both bits:

$$X_1 X_0 |01\rangle = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$$

Many useful operators are products of one-bit operators, but some (like CNOT) cannot be factored that way.

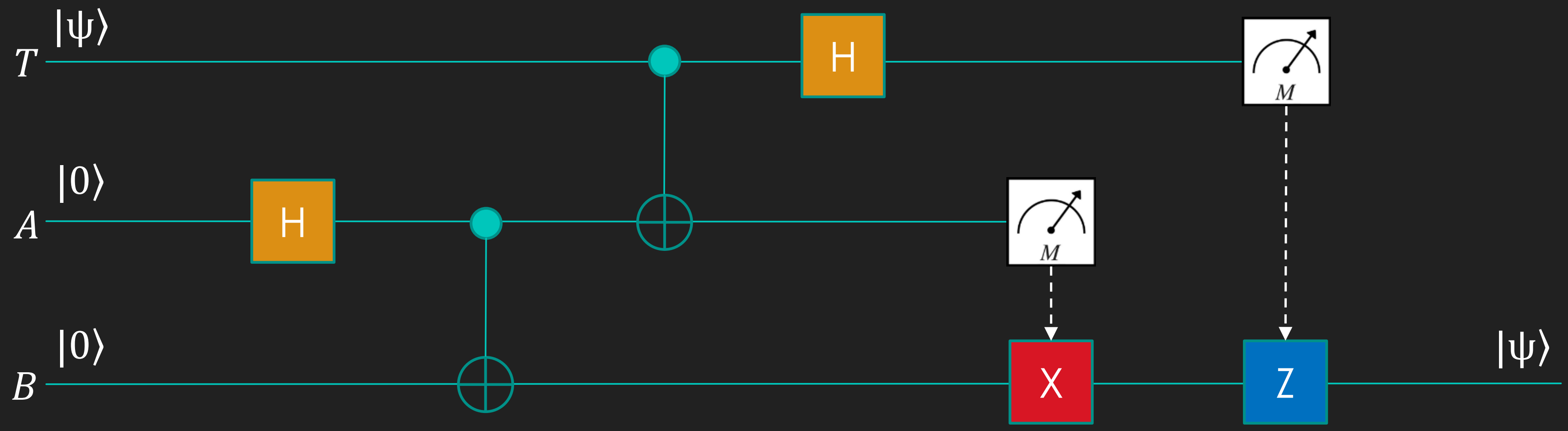
Single-bit operations on multi-bit states

- CNOT gate subscripts are of the form C_{ct} where c specifies control bit and t target bit
- We can tensor CNOT matrices with the identity to operate on adjacent bits out of multiple
- Throughout the presentation, the CNOT gate we used was C_{10}
- The C_{01} gate (with least-significant bit as control and most-significant target) is as follows:



$$C_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Quantum teleportation math



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

Quantum teleportation math

$$H_2C_{21}C_{10}H_1\left(\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\otimes\begin{pmatrix}1\\ 0\end{pmatrix}\otimes\begin{pmatrix}1\\ 0\end{pmatrix}\right)=H_2C_{21}C_{10}\left(\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\otimes\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}1\\ 0\end{pmatrix}\right)$$

$$=H_2C_{21}\left(\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\otimes\begin{pmatrix}\frac{1}{\sqrt{2}}\\ 0\\ 0\\ \frac{1}{\sqrt{2}}\end{pmatrix}\right)=H_2\left(\frac{1}{\sqrt{2}}\begin{pmatrix}\alpha\\ 0\\ 0\\ \alpha\\ 0\\ \beta\\ \beta\\ 0\end{pmatrix}\right)=\frac{1}{2}\begin{pmatrix}\alpha\\ \beta\\ \beta\\ \alpha\\ \alpha\\ -\beta\\ -\beta\\ \alpha\end{pmatrix}$$

Quantum teleportation math

The state right before measurement breaks down into four cases:

$$\frac{1}{2}\left(\begin{array}{c} \alpha \\ \beta \\ \hline \beta \\ \alpha \\ \hline \alpha \\ -\beta \\ \hline -\beta \\ \alpha \end{array}\right) = \frac{1}{2}\left(|00\rangle \begin{pmatrix} \alpha \\ \beta \end{pmatrix} + |01\rangle \begin{pmatrix} \beta \\ \alpha \end{pmatrix} + |10\rangle \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} + |11\rangle \begin{pmatrix} -\beta \\ \alpha \end{pmatrix} \right)$$

$$|00\rangle \longrightarrow \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$|01\rangle \longrightarrow \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

$$|10\rangle \longrightarrow \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$$

$$|11\rangle \longrightarrow \begin{pmatrix} -\beta \\ \alpha \end{pmatrix}$$

When Alice measures her two qbits, Bob’s qbit is forced into one of four states.
The bits measured by Alice determine the state into which Bob’s qbit was forced.
Bob needs to apply a transformation to get his qbit to the state that he wants.
Bob needs to know the values of Alice’s bits to know which transformation(s) to apply.

Quantum teleportation math

If Alice measured:	Then Bob has:	So Bob must apply:
$\|00\rangle$	$\binom{\alpha}{\beta}$	$I\binom{\alpha}{\beta} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\binom{\alpha}{\beta} = \binom{\alpha}{\beta}$
$\|01\rangle$	$\binom{\beta}{\alpha}$	$X\binom{\beta}{\alpha} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\binom{\beta}{\alpha} = \binom{\alpha}{\beta}$
$\|10\rangle$	$\binom{\alpha}{-\beta}$	$Z\binom{\alpha}{-\beta} = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\binom{\alpha}{-\beta} = \binom{\alpha}{\beta}$
$\|11\rangle$	$\binom{-\beta}{\alpha}$	$XZ\binom{-\beta}{\alpha} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\binom{-\beta}{\alpha} = \binom{\alpha}{\beta}$

Most-significant bit controls whether Z gate is applied, least-significant controls X gate.