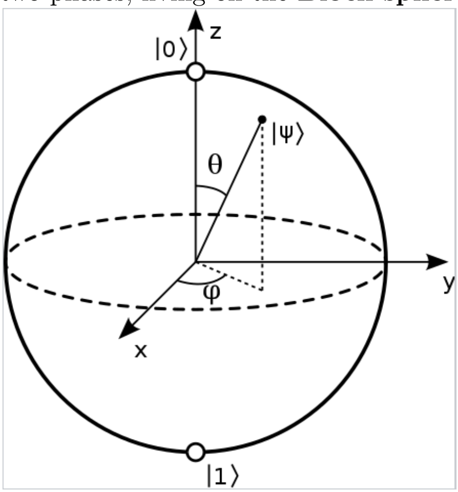
Quantum Computation 101 for Physicists

Class exercise 2

Today we will make the transition from classical computing to quantum computing. We already have most of the setting — we have introduced bits, reversible gates and circuits. Now all that is left is to turn our classical bits into quantum bits. A quantum bit, or **qubit** for short, is a quantum system with a Hilbert space of size 2. An example for such a system can be a $\frac{1}{2}-$spin or a photon's polarization, but as we mentioned last week, for our purposes it doesn't matter how the system is implemented. We take a basis of this Hilbert space which we can measure and denote it as **the computational basis**, and its two eigenstates as $|0\rangle$ and $|1\rangle$.

A single qubit state is not $|0\rangle$ or $|1\rangle$ like a classical state, but some combination $e^{i\Phi}(\cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle)$, with $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$. This is the most general form of a qubit state. We ignore the global phase Φ, that has no effect on the physics, and remain with a state represented by two phases, living on the **Bloch sphere**:



The Bloch sphere allows us to think of the qubit again as a spin 1/2 and introduce the Pauli matrices as 1-qubit operators:

$$\sigma_x \equiv X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y \equiv Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z \equiv Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We recall some properties of the Pauli matrices:

$$\sigma_i^2 = \mathbb{I},$$
$$\sigma_i\sigma_j = i\epsilon_{ijk}\sigma_k \text{ for } i \neq j.$$

Applying X (which is basically the NOT gate) rotates the state around the x axis on the Bloch sphere by π:

$$X(\cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle) = \cos(\frac{\theta}{2})|1\rangle + e^{i\phi}\sin(\frac{\theta}{2})|0\rangle \propto e^{-i\phi}\sin(\frac{\pi}{2} - \frac{\theta}{2})|1\rangle - \cos(\frac{\pi}{2} - \frac{\theta}{2})|0\rangle$$

$\theta \to \pi - \theta$, $\phi \to -\phi$. Applying Z rotates the state around the z axis by π, $\phi \to \phi + \pi$. Y can be constructed from X and Z by $Y = iXZ$, so we don't use it too often in quantum computation models (although it rotates the state around the y axis by π just as X and Z around their axes). Since any state can be described by a point on the Bloch sphere, any 1-qubit gate can be described by a multiplication of rotations around the three axes, $e^{i\frac{\varphi}{2}\hat{n}\cdot\vec{\sigma}} = \cos(\frac{\varphi}{2}) + i\sin(\frac{\varphi}{2})\hat{n}\cdot\vec{\sigma}$ (you will prove the last transition at home). The operator rotates a state around $\hat{n}$ by φ.

Now that our states do not have to be pure states anymore, our operator matrices do not have to be permutation matrices, but unitaries. Any quantum gate can now be expressed as a unitary.

We introduce another important 1-qubit gate called **the Hadamard gate**:

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

It takes the $|0\rangle$ states into the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ state, and the $|1\rangle$ state into the $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ state.

0.1 Question 1

1. Express the Hadamard gate in terms of X and Z.
2. Show that $HXH = Z, HZH = X$
3. Find φ and $\hat{n}$ for the Hadamard gate.

0.2 Solution

1. Directly from the matrix definition of the operators we get $H = \frac{1}{\sqrt{2}}(X + Z)$.
2. We use the result above to get:

$$HXH = \frac{1}{2}(X+Z)X(X+Z) = \frac{1}{2}(X^3+XXZ+ZXX+ZXZ) = \frac{1}{2}(X+2Z+iYZ) = \frac{1}{2}(X+2Z-X) = Z$$

$$HZH = \frac{1}{2}(X + Z)Z(X + Z) = \frac{1}{2}(Z^3 + ZZX + XZZ + XZX) = X$$

3. From $H = \frac{1}{\sqrt{2}}(X + Z)$, we see that $\cos(\frac{\varphi}{2}) = 0, \sin(\frac{\varphi}{2}) = 1$, so $\varphi = \pi$, and $\hat{n} = \frac{1}{\sqrt{2}}(1, 0, 1)$. So the Hadamard gate is a rotation around $\hat{n}$ by π.

0.3 Question 2

Express the CNOT gate using X and Z, and use it to reverse the CNOT gate, i.e. express CNOT_{ji} using CNOT_{ij} and Hadamard gates.

0.4 Solution

We recall the CNOT gate matrix:

$$\text{CNOT}_{ij} = \begin{array}{c c} & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}.$$

The $i = 0$ block can be expressed by $\frac{1}{2}(\mathbb{I} + Z_i)$. The $i = 1$ block can be expressed by $\frac{1}{2}(\mathbb{I} - Z_i)X_j$, so in total,

$$\begin{aligned} CNOT_{ij} =& \frac{1}{2}(\mathbb{I} + Z_i) + \frac{1}{2}(\mathbb{I} - Z_i)X_j = \\ & \frac{1}{2}(\mathbb{I} + X_j) + \frac{1}{2}(\mathbb{I} - X_j)Z_i. \end{aligned}$$

Following the result of the last question, we see:

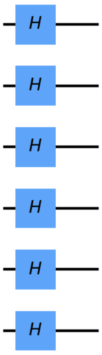
$$CNOT_{ji} = H_i H_j CNOT_{ij} H_j H_i.$$

0.5 Question 3

Draw a $n-$qubit circuit that takes as an input $|0\rangle^{\otimes n}$ and outputs $\frac{1}{2^{n/2}} \sum_{i=0}^{2^n} |i\rangle$.

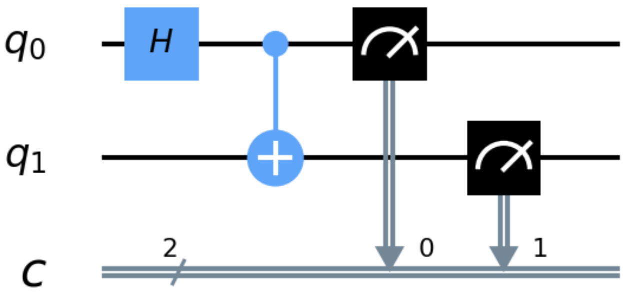
0.6 Solution

We notice that the output state should have the same amplitude for each computational basis eigenstate of the string, so also the same amplitude for each eigenstate $|0\rangle$ or $|1\rangle$ of each separate qubit. Having this insight, we understand that the circuit will be:



So now we see that we can get a superposition of all classical bit strings by applying only 1-qubit gates (which are the easiest to apply). So we can create this state, and by applying the right unitary we can perform the calculation on all of the possible strings in parallel. But How can we access the classical information in our quantum state?

We need to introduce our next important component in quantum circuit - measurement. A measurement can be performed on each qubit individually and is notated like the black symbols here:



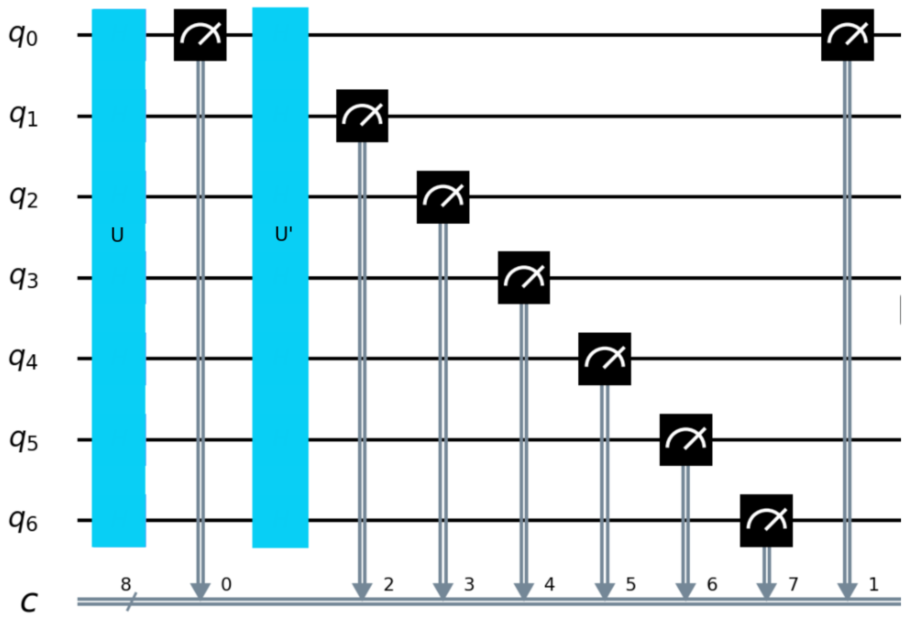
The black symbols represent a measurement, and the bottom gray lines are classical bits of information in which the information is stored. The result of the measurement, like you already know from QM courses, will be based on the amplitude of the state, and will have the qubit collapse into the measured state. So if our qubits are in the state $|\psi\rangle = \alpha_0|0\rangle_1|\psi_0\rangle_{n-1} + \alpha_1|1\rangle_1|\psi_1\rangle_{n-1}$ (with $|\psi_0\rangle_{n-1}$ and $|\psi_1\rangle_{n-1}$ not necessarily orthogonal), the result will be 0 (1) in probability $\alpha_0(\alpha_1)$. We can usually measure only in the computational basis, but since we can rotate the qubits by applying some unitary, we can usually effectively measure in any 1-qubit basis.

0.7 Question 4

It is possible to avoid doing any intermediate measurements in a quantum circuit, using one auxiliary qubit for each 1-qubit measurement that needs to be delayed until the end of the computation. Show how.

0.8 Solution

We look at a general intermediate measurement:

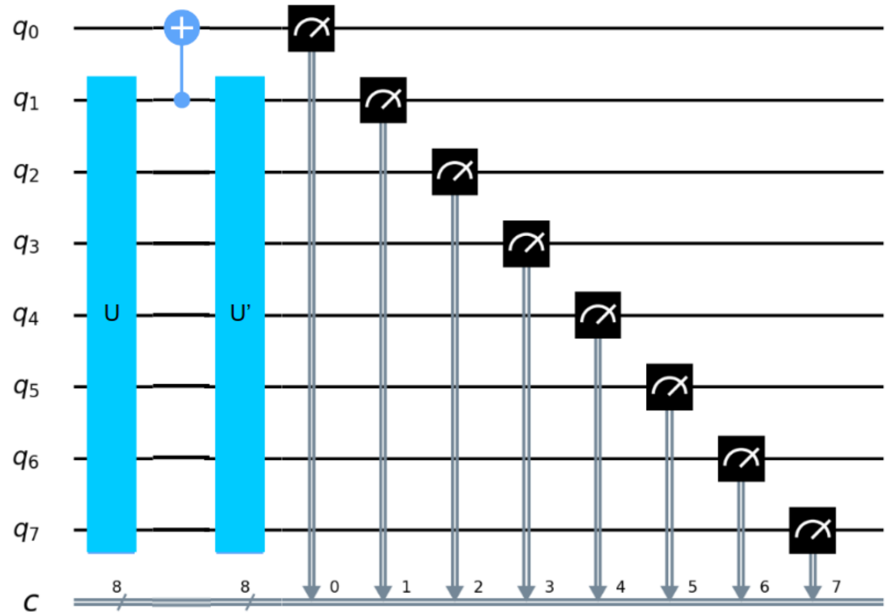


We define $|\psi_0\rangle_{n-1}$ and $|\psi_1\rangle_{n-1}$ as:

$$U|0\rangle_n = \alpha_0|0\rangle_1|\psi_0\rangle_{n-1} + \alpha_1|1\rangle_1|\psi_1\rangle_{n-1},$$

and see that the resulting state will be $U'[|0\rangle|\psi_0\rangle_{n-1}]$ with probability $|\alpha_0|^2$ and $U'[|1\rangle|\psi_1\rangle_{n-1}]$ with probability $|\alpha_1|^2$.

Now assume that instead we add an auxiliary (also called ancilla) qubit started as $|0\rangle$, and create the circuit:



Now, after the application of U, the state is: $U|0\rangle_{n+1} = |0\rangle \otimes (\alpha_0|0\rangle_1|\psi_0\rangle_{n-1} + \alpha_1|1\rangle_1|\psi_1\rangle_{n-1})$, so after applying the CNOT, we get:

$$\mathrm{CNOT}(1,0)U|0\rangle_{n+1} = \alpha_0|00\rangle_2|\psi_0\rangle_{n-1} + \alpha_1|11\rangle_2|\psi_1\rangle_{n-1}.$$

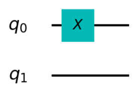
We apply U' and get:

$$U'_{2\ldots n+1}\mathrm{CNOT}(1,0)U_{2\ldots n+1}|0\rangle_{n+1} = \alpha_0|0\rangle_1 U'[|0\rangle_1|\psi_0\rangle_{n-1}] + \alpha_1|1\rangle_1 U'[|1\rangle_1|\psi_1\rangle_{n-1}].$$

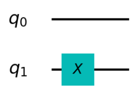
Measuring the ancilla qubit now will give us the same result as in the former circuit.

0.9 Question 5

We know in physics that if we have two separate systems, we can describe their state as $|\psi\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2$. Operators that act separately on the two systems are also described by a tensor product, $U = U_1 \otimes U_2$. When we write the operators as matrices, this tensor product is manifested by the **Kronecker product**: $\hat{A} \otimes \hat{B} = \begin{pmatrix} A_{11}\hat{B} & A_{12}\hat{B} & \dots & A_{1n}\hat{B} \\ A_{21}\hat{b} & \dots & \dots & A_{2n}\hat{B} \\ \dots & \dots & \dots & \dots \end{pmatrix}$

1. Find the two-particle matrix of $X \otimes \mathbb{I}_2$, 

.

2. Find the two-particle matrix of $\mathbb{I}_2 \otimes X$, 

.

3. Show the two matrices above commute.

0.10 Solution

1. $X \otimes \mathbb{I}_2 = \begin{pmatrix} 0 & \mathbb{I}_2 \\ \mathbb{I}_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$.

2. $\mathbb{I}_2 \otimes X = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

3. $\begin{pmatrix} 0 & \mathbb{I}_2 \\ \mathbb{I}_2 & 0 \end{pmatrix} \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} - \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} 0 & \mathbb{I}_2 \\ \mathbb{I}_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix} - \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix}$.