Last week we showed that any single-qubit unitary can be implemented using three rotations around two axes. We used

$$U = e^{i\alpha}\ R_z(\beta)\ R_y(\gamma)\ R_z(\delta), \tag{1}$$

but we the same is true with any other two orthogonal axes.

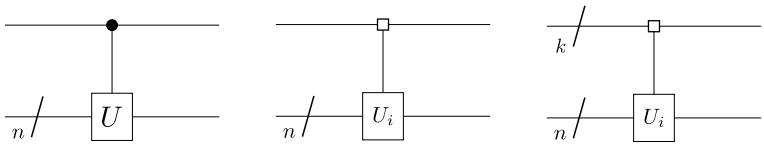
This week we will show how to implement an arbritary unitary operator, acting in many qubits, using a quantum circuit composed only of CNOT gates and elementary single-qubit gates, namely (again) rotations around the three axes,

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

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

First we will show a concrete construction that achieves universality, and then we will examine the size of the circuit and compare is with theoretical lower bounds.

We will use two types of controlled gates. Controlled gates (left) mean apply U if the control qubit is $|1\rangle$, otherwise apply the identity. Multiplexed gates (center and right) mean apply U_i if the state of the control qubit(s) is $|i\rangle$.



For instance, controlled gates with one control qubit have the matrix form $\begin{bmatrix} \mathbb{1} & 0 \\ 0 & U \end{bmatrix}$, and multiplexed gates with one control qubit correspond to the matrix $\begin{bmatrix} U_0 & 0 \\ 0 & U_1 \end{bmatrix}$.

Exercise 1. ***Universal construction***

This is an elegant recursive construction. We will start with an arbitrary unitary U acting on n qubits, and will successively break it down into gates that act on less and less qubits, until we are left with elementary rotations and CNOTs.

(a) The cosine-sine decomposition of $2\ell \times 2\ell$ unitary matrices gives us the relation

$$U = \begin{bmatrix} A_0 & 0 \\ 0 & A_1 \end{bmatrix} \begin{bmatrix} C & -S \\ S & C \end{bmatrix} \begin{bmatrix} B_0 & 0 \\ 0 & B_1 \end{bmatrix}, \tag{2}$$

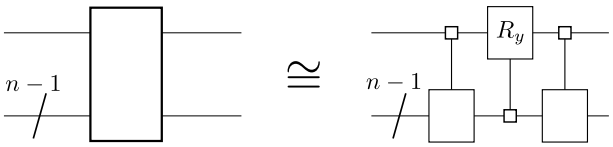
where A_0, A_1, B_0, B_1 are unitary $\ell \times \ell$ matrices, and C and S are real diagonal matrices such that $C^2 + S^2 = 1$.

Show that we can write

$$C = \begin{bmatrix} \cos\theta_0 & & & \\ & \cos\theta_1 & & \\ & & \ddots & \\ & & & \cos\theta_\ell \end{bmatrix}, \quad S = \begin{bmatrix} \sin\theta_0 & & & \\ & \sin\theta_1 & & \\ & & \ddots & \\ & & & \sin\theta_\ell \end{bmatrix}, \tag{3}$$

for some angles $\theta_0, \ldots, \theta_\ell$.

Show that the cosine-sine decomposition corresponds to the following circuit identity:



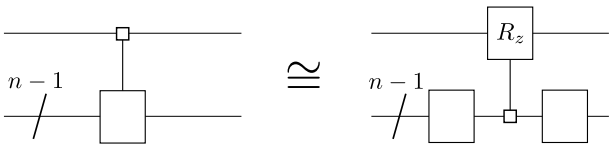
(b) We will now break down the multiplexed unitary gate using the relation

$$\begin{bmatrix} U_0 & 0 \\ 0 & U_1 \end{bmatrix} = \begin{bmatrix} V & 0 \\ 0 & V \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & D^\dagger \end{bmatrix} \begin{bmatrix} W & 0 \\ 0 & W \end{bmatrix}, \tag{4}$$

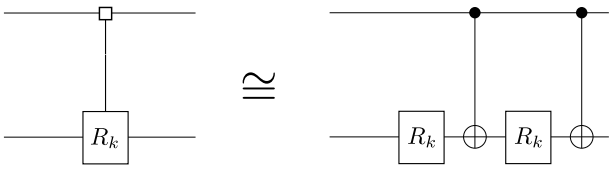
where V, D, W are unitary matrices, and D is diagonal. Show that we can write

$$\begin{bmatrix} D & 0 \\ 0 & D^\dagger \end{bmatrix} = \begin{bmatrix} D' & 0 \\ 0 & D' \end{bmatrix} \text{C-}R_z, \quad \text{C-}R_z = \begin{bmatrix} e^{i\phi_0} & & & & & \\ & \ddots & & & & \\ & & e^{i\phi_\ell} & & & \\ & & & e^{-i\phi_0} & & \\ & & & & \ddots & \\ & & & & & e^{-i\phi_\ell} \end{bmatrix}, \tag{5}$$

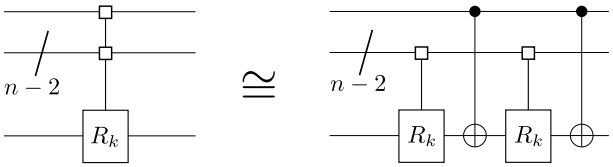
where D' is also unitary and diagonal. This gives us the following circuit identity:



(c) Now we only have to deal with multiplexed rotations R_y and R_z. Show that, for a single qubit control,



These identities can be generalized to

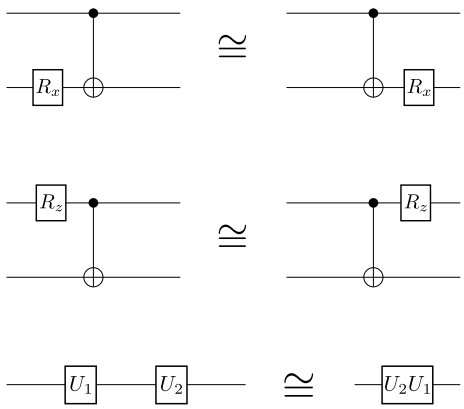


Exercise 2. ***Circuit size***

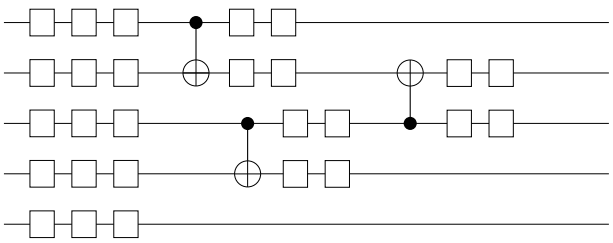
Now we will see how large a circuit we need to implement an arbritary unitary operation. In particular, we will look at the number of CNOT gates necessary. We start with the theoretical lower bound on the number of gates, and then we see if the construction from Exercise 1 performs, compared to that bound.

(a) Show that the dimension of the space of unitary matrices acting on n qubits (such that the global phase is irrelevant), $SU(2^n)$, is $4^n - 1$. This tells us that in order to achieve universality, a quantum circuit of n qubits must take $4^n - 1$ parameters.

(b) Prove the following circuit identities:



(c) Those identities allow us to compress the unitary gates that are applied after a CNOT. For instance,



Each CNOT only brings at most 4 new parameters. Show that the number of independent parameters implemented in an n-qubit circuit with c_n CNOTs is at most $3n + 4c_n$. Prove that the minimum number of CNOT gates necessary to implement an arbritary n-qubit unitary operation is given by

$$c_n \geq \frac{1}{4}(4^n - 3n - 1).$$

(d) Show that the number of CNOT gates used in the decomposition of Exercise 1 also scales as 4^n.