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 the same is true with any other two orthogonal axes.

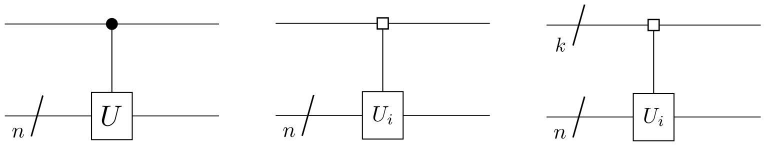
This week we will show how to implement an arbritary unitary operator, acting on many qubits, using a quantum circuit composed only of CNOT gates and elementary single-qubit gates, namely (again) rotations around the three axes,

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

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

First we will show a concrete construction that achieves universality, and then we will examine the size of the circuit and compare it 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 fewer and fewer 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 $\theta_0, \ldots, \theta_\ell$.

Solution. If C and S are diagonal matrices,

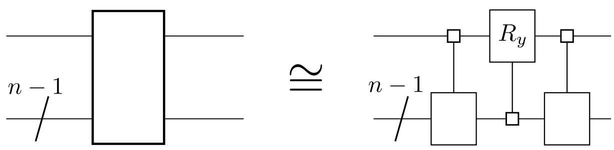
$$C = \begin{bmatrix} c_0 & & & \\ & c_1 & & \\ & & \ddots & \\ & & & c_\ell \end{bmatrix}, \quad S = \begin{bmatrix} s_0 & & & \\ & s_1 & & \\ & & \ddots & \\ & & & s_\ell \end{bmatrix},$$

then the condition $C^2 + S^2 = \mathbb{1}$ becomes

$$\begin{bmatrix} c_0^2 + s_0^2 & & & \\ & c_1^2 + s_1^2 & & \\ & & \ddots & \\ & & & c_\ell^2 + s_\ell^2 \end{bmatrix} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}.$$

But any two real numbers c and s such that $c^2 + s^2 = 1$ can be expressed as the cosine and the sine of an angle θ.

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



Solution. The two matrices

$$A = \begin{bmatrix} A_0 & 0 \\ 0 & A_1 \end{bmatrix}, \qquad B = \begin{bmatrix} B_0 & 0 \\ 0 & B_1 \end{bmatrix}$$

correspond to multiplexed gates. For instance, A acts as

$$\begin{aligned} A\left(|0\rangle \otimes |x\rangle\right) &= |0\rangle \otimes A_0|x\rangle \\ A\left(|1\rangle \otimes |x\rangle\right) &= |1\rangle \otimes A_1|x\rangle. \end{aligned}$$

To see this, note that

$$|0\rangle_1 \otimes |x\rangle_{(n-1)} = |x\rangle_n = \begin{bmatrix} 0_0 \\ \vdots \\ 1_x \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0_{2^n-1} \end{bmatrix}, \qquad |1\rangle_1 \otimes |x\rangle_{(n-1)} = |2^{n-1} + x\rangle_n = \begin{bmatrix} 0_0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 1_{2^{n-1}+x} \\ \vdots \\ 0_{2^n-1} \end{bmatrix},$$

where the green subscript indicates the position of the 0 or 1. Also, A can be written as

$$
\begin{aligned}
A &= \underbrace{\sum_{x,y=0}^{2^{n-1}-1} a_0^{x,y}\ |x\rangle\langle y|_n}_{A_0} + \underbrace{\sum_{x,y=0}^{2^{n-1}-1} a_1^{x,y}\ |2^{n-1}+x\rangle\langle 2_n^{n-1}+y|}_{A_1} \\
&= \sum_{x,y=0}^{2^{n-1}-1} a_0^{x,y}\ |0\rangle\langle 0|_1 \otimes |x\rangle\langle y|_{(n-1)} + \sum_{x,y=0}^{2^{n-1}-1} a_1^{x,y}\ |1\rangle\langle 1|_1 \otimes |x\rangle\langle y|_{(n-1)},
\end{aligned}
$$

and therefore their product comes

$$
\begin{aligned}
A\left(|0\rangle \otimes |x'\rangle\right) &= \sum_{x,y=0}^{2^{n-1}-1} a_0^{x,y}\ |0\rangle \underbrace{\langle 0|0\rangle}_{=1} \otimes |x\rangle\langle y|x'\rangle + \sum_{x,y=0}^{2^{n-1}-1} a_1^{x,y}\ |1\rangle \underbrace{\langle 1|0\rangle}_{=0} \otimes |x\rangle\langle y|x'\rangle \\
&= |0\rangle \otimes \sum_{x,y=0}^{2^{n-1}-1} a_0^{x,y}|x\rangle\langle y|x'\rangle \\
&= |0\rangle \otimes A_0|x'\rangle, \\
A\left(|1\rangle \otimes |x'\rangle\right) &= \sum_{x,y=0}^{2^{n-1}-1} a_0^{x,y}\ |0\rangle \underbrace{\langle 0|1\rangle}_{=0} \otimes |x\rangle\langle y|x'\rangle + \sum_{x,y=0}^{2^{n-1}-1} a_1^{x,y}\ |1\rangle \underbrace{\langle 1|1\rangle}_{=1} \otimes |x\rangle\langle y|x'\rangle \\
&= |1\rangle \otimes \sum_{x,y=0}^{2^{n-1}-1} a_0^{x,y}|x\rangle\langle y|x'\rangle \\
&= |1\rangle \otimes A_0|x'\rangle.
\end{aligned}
$$

The middle matrix is a multiplexed rotation of a single qubit, conditioned on the state of the remaining $n-1$ qubits,

$$
R = \begin{bmatrix}
\cos\theta_0 & & & & -\sin\theta_0 & & & \\
& \cos\theta_1 & & & & -\sin\theta_1 & & \\
& & \ddots & & & & \ddots & \\
& & & \cos\theta_\ell & & & & -\sin\theta_\ell \\
\sin\theta_0 & & & & \cos\theta_0 & & & \\
& \sin\theta_1 & & & & \cos\theta_1 & & \\
& & \ddots & & & & \ddots & \\
& & & \sin\theta_\ell & & & & \cos\theta_\ell.
\end{bmatrix}
$$

This matrix acts as

$$
R\left(|k\rangle_1 \otimes |x\rangle_{(n-1)}\right) = R_k|k\rangle_1 \otimes |x\rangle_{(n-1)}, \qquad R_x = \begin{bmatrix} \cos\theta_x & -\sin\theta_x \\ \sin\theta_x & \cos\theta_x \end{bmatrix}.
$$

To see this, note that we can write R as

$$
\begin{aligned}
R &= \sum_{y=0}^{2^{n-1}-1} \left(\cos\theta_y|0\rangle\langle 0| \otimes |y\rangle\langle y| - \sin\theta_y|0\rangle\langle 1| \otimes |y\rangle\langle y| + \sin\theta_y|1\rangle\langle 0| \otimes |y\rangle\langle y| + \cos\theta_y|1\rangle\langle 1| \otimes |y\rangle\langle y|\right) \\
&= \sum_{y=0}^{2^{n-1}-1} \left(\cos\theta_y|0\rangle\langle 0| - \sin\theta_y|0\rangle\langle 1| + \sin\theta_y|1\rangle\langle 0| + \cos\theta_y|1\rangle\langle 1|\right) \otimes |y\rangle\langle y| \\
&= \sum_{y=0}^{2^{n-1}-1} R_y \otimes |y\rangle\langle y|.
\end{aligned}
$$

Applying R on a state $|k\rangle \otimes |x\rangle$ results in

$$
\begin{aligned}
R(|k\rangle_1 \otimes |x\rangle_{(n-1)}) &= \sum_{y=0}^{2^{n-1}-1} R_y|k\rangle \otimes |y\rangle \underbrace{\langle y|x\rangle}_{=\delta_{xy}} \\
&= R_x|k\rangle \otimes |x\rangle.
\end{aligned}
$$

We can see that R is a multiplexed rotation: it applies a rotation around the y-axis by an angle θ_x on the first qubit if the other $n-1$ qubits are in state $|x\rangle$.

Note: What about input states that are not diagonal in the computational basis? We can simply expand them in this basis, and apply the operators linearly.

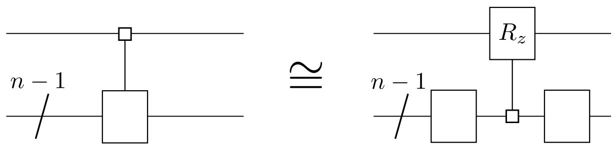
(b) We will now break down the multiplexed unitary gate using the relation

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

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:



Solution. Notation: $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} = |0\rangle\langle 0| \otimes A + |1\rangle\langle 1| \otimes B$ is the direct sum of operators A and B, denoted by $A \oplus B$. You can check that $(A \oplus B)(\tilde{A} \oplus \tilde{B}) = (A\tilde{A}) \oplus (B\tilde{B})$, if the matrices have the same size.

If U_0 and U_1 are unitary matrices, then $U_1 \oplus U_2$ is unitary. Since $V \oplus V$ and $W \oplus W$ are also unitary, it follows from Eq. 4 that $D \oplus D^\dagger$ must be unitary. This means that $D \oplus D^\dagger$ is already of the form $\mathrm{C} - R_z$, and $D' = \mathbb{1}$.

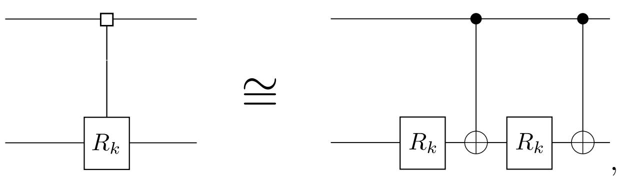
[The following was not asked in the exercise.] Here is how to derive the matrices V, D and W. $U_1 U_2^\dagger$ is a unitary matrix, and therefore has a spectral decomposition

$$U_1 U_2^\dagger = V \tilde{D} V^\dagger,$$

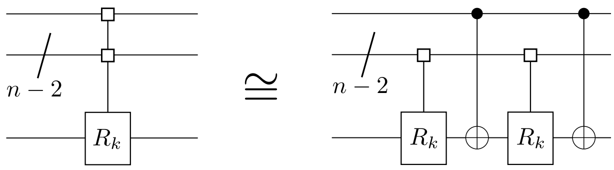
where $\tilde{D}$ is the diagonal matrix whose entries are the eigenvalues of $U_1 U_2^\dagger$, and the columns of V are the corresponding eigenvectors. Now take $D := \sqrt{\tilde{D}}$, and $W := D V^\dagger U_2$. We can check that this choice of matrices works,

$$\begin{aligned} (V \oplus V)(D \oplus D^\dagger)(W \oplus W) &= (VDW) \oplus (VD^\dagger W) \\ &= (VDDV^\dagger U_2) \oplus (VDD^\dagger V^\dagger U_2) \\ &= (U_1 U_2^\dagger U_2) \oplus (VV^\dagger U_2) \\ &= U_1 \oplus U_2. \end{aligned}$$

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



with $k = y, z$. These identities can be generalized to



Solution. Note: remember that circuits read from left to right and matrix multiplication is the other way around. The factor of 2 for instance in $R_z(2\alpha)$ is there so the rotation matrices don't have factors of 1/2 floating around.

We start with R_z. We want to find the rotation angles α and β such that

$$R_z(2\phi_0) \oplus R_z(2\phi_1) = \textsc{cnot}\ (\mathbb{1} \otimes R_z(2\alpha))\ \textsc{cnot}\ (\mathbb{1} \otimes R_z(2\beta)).$$

On the left-hand side we have

$$R_z(2\phi_0) \oplus R_z(2\phi_1) = \begin{bmatrix} e^{-i\phi_0} & & & \\ & e^{i\phi_0} & & \\ & & e^{-i\phi_1} & \\ & & & e^{i\phi_1} \end{bmatrix},$$

and, on the right-hand side,

$$\begin{aligned} &\textsc{cnot}\ (\mathbb{1} \otimes R_z(2\alpha))\ \textsc{cnot}\ (\mathbb{1} \otimes R_z(2\beta)) = \\ &= \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \begin{bmatrix} e^{-i\alpha} & & & \\ & e^{i\alpha} & & \\ & & e^{-i\alpha} & \\ & & & e^{i\alpha} \end{bmatrix} \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \begin{bmatrix} e^{-i\beta} & & & \\ & e^{i\beta} & & \\ & & e^{-i\beta} & \\ & & & e^{i\beta} \end{bmatrix} \\ &= \begin{bmatrix} e^{-i(\alpha+\beta)} & & & \\ & e^{i(\alpha+\beta)} & & \\ & & e^{i(\alpha-\beta)} & \\ & & & e^{-i(\alpha-\beta)} \end{bmatrix}. \end{aligned}$$

This means we have to pick α, β such that $\alpha + \beta = \phi_0$ and $-\alpha + \beta = \phi_1$; in other words,

$$\alpha = \frac{\phi_0 - \phi_1}{2}, \qquad \beta = \frac{\phi_0 + \phi_1}{2}.$$

For R_y we need to satisfy

$$R_y(2\phi_0) \oplus R_y(2\phi_1) = \textsc{cnot}\ (\mathbb{1} \otimes R_y(2\alpha))\ \textsc{cnot}\ (\mathbb{1} \otimes R_y(2\beta))$$

On the left-hand side, we have

$$R_y(2\phi_0) \oplus R_y(2\phi_1) = \begin{bmatrix} \cos\phi_0 & -\sin\phi_0 & & \\ \sin\phi_0 & \cos\phi_0 & & \\ & & \cos\phi_1 & -\sin\phi_1 \\ & & \sin\phi_1 & \cos\phi_1 \end{bmatrix},$$

and, on the right-hand side,

$$\begin{aligned} &\textsc{cnot}\ (\mathbb{1} \otimes R_y(2\alpha))\ \textsc{cnot}\ (\mathbb{1} \otimes R_y(2\beta)) = \\ &= \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\alpha & -\sin\alpha & & \\ \sin\alpha & \cos\alpha & & \\ & & \cos\alpha & -\sin\alpha \\ & & \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta & & \\ \sin\beta & \cos\beta & & \\ & & \cos\beta & -\sin\beta \\ & & \sin\beta & \cos\beta \end{bmatrix} \\ &= \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\sin\alpha\cos\beta - \cos\alpha\sin\beta & & \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta & & \\ & & \cos\alpha\cos\beta + \sin\alpha\sin\beta & \sin\alpha\cos\beta - \cos\alpha\sin\beta \\ & & -\sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta + \sin\alpha\sin\beta \end{bmatrix} \\ &= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) & & \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) & & \\ & & \cos(-\alpha+\beta) & -\sin(-\alpha+\beta) \\ & & \sin(-\alpha+\beta) & \cos(-\alpha+\beta) \end{bmatrix}. \end{aligned}$$

Again, we have to choose α, β such that $\alpha+\beta = \phi_0, -\alpha+\beta = \phi_1$. To summarize, we obtained the identities

$$R_z(2\phi_0) \oplus R_z(2\phi_1) = \text{CNOT } (\mathbb{1} \otimes R_z(\phi_0 - \phi_1)) \text{ CNOT } (\mathbb{1} \otimes R_z(\phi_0 + \phi_1)),$$
$$R_y(2\phi_0) \oplus R_y(2\phi_1) = \text{CNOT } (\mathbb{1} \otimes R_y(\phi_0 - \psi_1)) \text{ CNOT } (\mathbb{1} \otimes R_y(\phi_0 + \phi_1)).$$

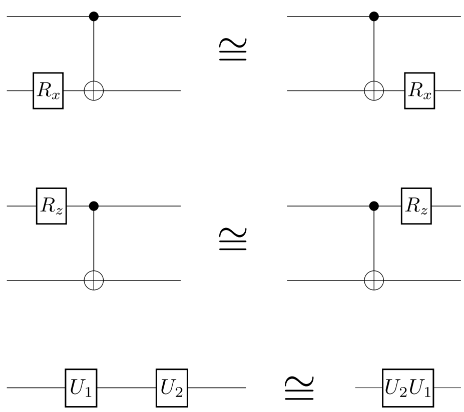
Exercise 2. *Circuit size*

Now we will see how large a circuit we need to implement an arbitrary 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.

Solution. A unitary acting on n qubits corresponds to a matrix of $2^n \times 2^n$ complex entries. That accounts for 2×4^n real parameters. However, the unitarity condition, $UU^\dagger = U^\dagger = \mathbb{1}$, imposes a system of 4^n linear equations on the matrix entries. This leaves room for $2 \times 4^n - 4^n = 4^n$ free parameters. If we want to implement any unitary up to the global phase (one real parameter less), we need to a circuit with $4^n - 1$ free parameters.

(b) Prove the following circuit identities:



Solution. For the top identity, we have

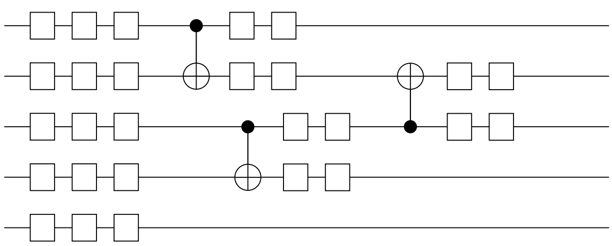
$$
\begin{aligned}
\textsc{cnot}\ (\mathbb{1}\otimes R_x(2\alpha)) &= \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\alpha & -i\sin\alpha & & \\ -i\sin\alpha & \cos\alpha & & \\ & & \cos\alpha & -i\sin\alpha \\ & & -i\sin\alpha & \cos\alpha \end{bmatrix} \\
&= \begin{bmatrix} \cos\alpha & -i\sin\alpha & & \\ -i\sin\alpha & \cos\alpha & & \\ & & -i\sin\alpha & \cos\alpha \\ & & \cos\alpha & -i\sin\alpha \end{bmatrix}, \\
(\mathbb{1}\otimes R_x(2\alpha))\ \textsc{cnot} &= \begin{bmatrix} \cos\alpha & -i\sin\alpha & & \\ -i\sin\alpha & \cos\alpha & & \\ & & \cos\alpha & -i\sin\alpha \\ & & -i\sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} \cos\alpha & -i\sin\alpha & & \\ -i\sin\alpha & \cos\alpha & & \\ & & -i\sin\alpha & \cos\alpha \\ & & \cos\alpha & -i\sin\alpha \end{bmatrix} = \textsc{cnot}\ (\mathbb{1}\otimes R_x(2\alpha)). \qquad \checkmark
\end{aligned}
$$

For the middle identity,

$$
\begin{aligned}
\textsc{cnot}\ (R_z(2\alpha)\otimes\mathbb{1}) &= \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \begin{bmatrix} e^{-i\alpha} & & & \\ & e^{-i\alpha} & & \\ & & e^{i\alpha} & \\ & & & e^{i\alpha} \end{bmatrix} \\
&= \begin{bmatrix} e^{-i\alpha} & & & \\ & e^{-i\alpha} & & \\ & & 0 & e^{i\alpha} \\ & & e^{i\alpha} & 0 \end{bmatrix} \\
(R_z(2\alpha)\otimes\mathbb{1})\ \textsc{cnot} &= \begin{bmatrix} e^{-i\alpha} & & & \\ & e^{-i\alpha} & & \\ & & e^{i\alpha} & \\ & & & e^{i\alpha} \end{bmatrix} \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} e^{-i\alpha} & & & \\ & e^{-i\alpha} & & \\ & & 0 & e^{i\alpha} \\ & & e^{i\alpha} & 0 \end{bmatrix} = \textsc{cnot}\ (\mathbb{1}\otimes R_x(2\alpha)). \qquad \checkmark
\end{aligned}
$$

Finally, the bottom identity is trivial, $(U_2)(U_1) = (U_2U_1)$. Indeed, it only tells us how to read circuits and write them as multiplication of matrices, from right to left.

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

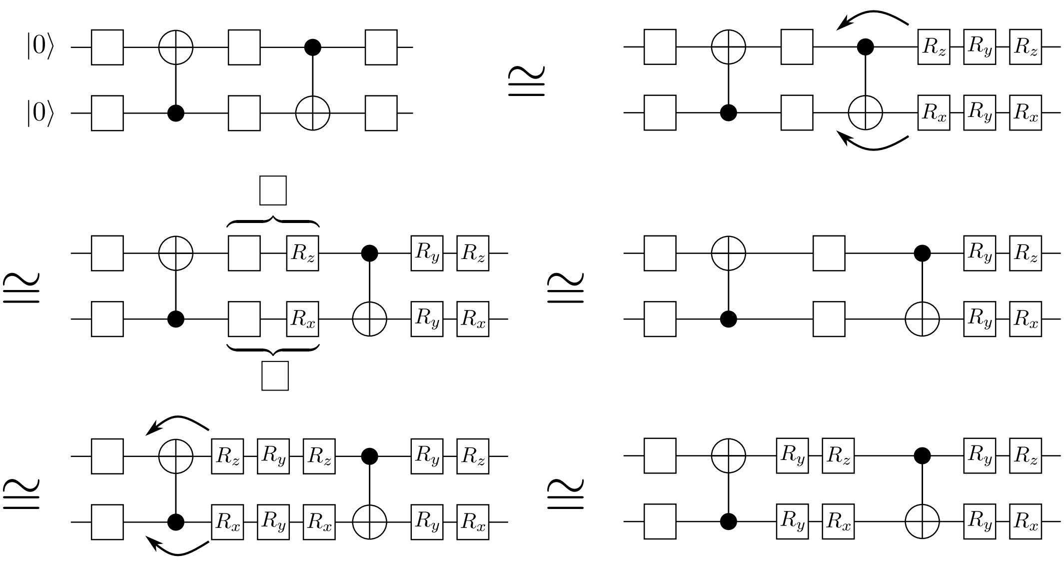


Each CNOT only brings at most 4 new parameters. Show that the number of independent parameters implemented in an n-qubit circuit with c_n CNOTs is at most $3n + 4c_n$.

Prove that the minimum number of CNOT gates necessary to implement an arbitrary n-qubit unitary operation is given by

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

Solution. Let's show (with pictures!) how each CNOT only allows for 4 new free parameters.



So, we implement at most 3 elementary rotations per qubit in the beginning of the computation (to initialize each qubit), and then 4 new elementary rotations per CNOT gate used. The minimum number of elementary rotations in a circuit with n qubits and c_n CNOT gates is $3n + 4c_n$. This corresponds to the number of free parameters in the circuit. In order to implement a unitary that acts on n qubits, we need $4^n - 1$ free parameters, so the total number of CNOTs is

$$4^n - 1 = p \leq 3n + 4c_n \quad \Rightarrow \quad c_n \geq \frac{1}{4}(4^n - 3n - 1).$$

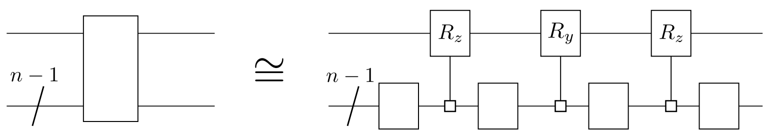
(d) Show that the number of CNOT gates used in the decomposition of Exercise 1 also scales as 4^n.

Solution. The generalization of exercise 1 *c*) tells us that a multiplexed rotation R_y or R_z with k control qubits (k-multiplexed) can be decomposed into 2 CNOTs and 2 $(k-1)$-multiplexed rotations. Applying this decomposition recursively gives us the total number of gates necessary to implement the multiplexed rotation using only CNOTs and non-multiplexed rotations.

Let c be the number of CNOTs and r_k the number of k-multiplexed rotations with k. We have

$$\begin{bmatrix} \text{level} & \#\text{gates} \\ k & r_k \\ k-1 & 2c + 2r_{k-1} \\ k-2 & 2c + 2(2c + 2r_{k-1}) \\ k-3 & 2c + 2(2c + 2(2c + r_{k-2})) \\ \vdots & \\ 0 & \underbrace{\left(\sum_{j=1}^{k} 2^j\right)}_{2^{k+1}-2} c + 2^k r_0. \end{bmatrix}$$

The number of CNOTs necessary per k-multiplexed rotation would be $2^{k+1} - 2$. Not let's see how many of these rotations we need per unitary. Combining parts *a*) and *b*) of exercise 1, we can see that we can decompose a unitary that acts on k qubits into 4 unitaries acting on $k-1$ qubits and 3 $(k-1)$-multiplexed rotations,



Applying this decomposition recursively gives us

$$\begin{bmatrix} \text{level} & \#\text{gates} \\ k & u_k \\ k-1 & 3r_{k-1}+4u_{k-1} \\ k-2 & 3r_{k-1}+4(3r_{k-2}+4u_{k-2}) \\ k-3 & 3r_{k-1}+4(3r_{k-2}+4(3r_{k-3}+4u_{k-3})) \\ \vdots & \\ 1 & \left(\sum_{j=1}^{k-1} 4^{k-j-1}\ 3r_j\right)+4^k u_1. \end{bmatrix}$$

The total number of CNOTs necessary to implement a unitary acting on n qubits in this way is

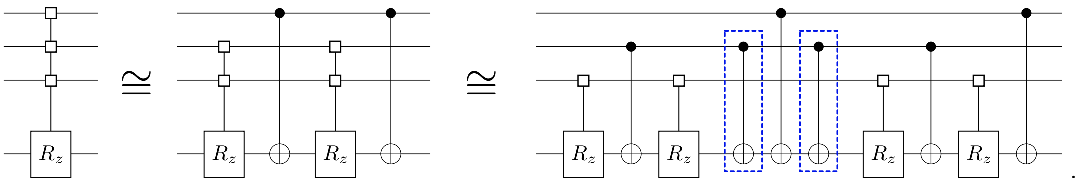
$$\begin{aligned} c_n &= \sum_{j=1}^{n-1} 4^{n-j-1}\ 3(2^{k+1}-2) \\ &= 4^n - 3(2^n) + 2, \end{aligned}$$

which grows with 4^n.

This decomposition can be optimized. For instance, using the identities

$$\begin{aligned} &\text{CNOT } (\mathbb{1} \otimes R_y(2\alpha)) \text{ CNOT } (\mathbb{1} \otimes R_y(2\beta)) = (\mathbb{1} \otimes R_y(2\beta)) \text{ CNOT } (\mathbb{1} \otimes R_y(2\alpha)) \text{ CNOT} \\ &\text{CNOT } (\mathbb{1} \otimes R_z(2\alpha)) \text{ CNOT } (\mathbb{1} \otimes R_z(2\beta)) = (\mathbb{1} \otimes R_z(2\beta)) \text{ CNOT } (\mathbb{1} \otimes R_z(2\alpha)) \text{ CNOT}, \end{aligned}$$

we can find a decomposition of multiplexed rotations such that some CNOTs cancel out:



This way we only need 2^k CNOTs to implement a k-multiplexed rotation. That brings us to a total of $\sum_{j=1}^{n-1} 4^{n-j-1}\ 3\ (2^j) = \frac{3}{4}4^n - \frac{3}{2}2^n$ CNOT gates to implement a unitary acting on n qubits. Further optimizations can be found in `http://arxiv.org/abs/quant-ph/0406176`.