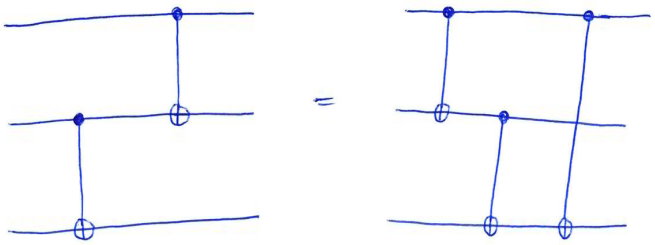
EXERCISES 8

Excercise 1. Show the following circuit identity involving CNOT gates.

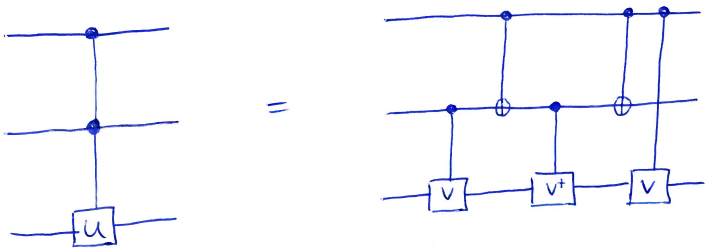


Excercise 2. Consider a single-qubit unitary $U \in \mathcal{U}(\mathbb{C}^2)$. In this exercise, we study how to implement the controlled unitary $C^2(U) : (\mathbb{C}^2)^{\otimes 2} \otimes \mathbb{C}^2 \to (\mathbb{C}^2)^{\otimes 2} \otimes \mathbb{C}^2$ with two control qubits and one target qubit defined as

$$C^2(U)(|c_1c_2\rangle \otimes |t\rangle) = |c_1c_2\rangle \otimes U^{c_1 \cdot c_2}|t\rangle,$$

on the computational basis states.

(1) Let $V \in \mathcal{U}(\mathbb{C}^2)$ denote a unitary such that $V^2 = U$. Verify that the following circuit implements $C^2(U)$.



(2) Find an implementation of $C^2(U)$ for any single-qubit unitary U using at most 8 single-qubit gates and at most 6 CNOT gates. **Hint:** Use the first exercise.

(3) The Toffoli gate is given by $C^2(X)$. Find a circuit implementing the Toffoli gate using as few gates from the gate set $\{H, T, T^{-1}, CNOT\}$ as possible.

Excercise 3. Consider a single-qubit unitary $U \in \mathcal{U}(\mathbb{C}^2)$. In this exercise, we study how to implement the controlled unitary $C^n(U) : (\mathbb{C}^2)^{\otimes n} \otimes \mathbb{C}^2 \to (\mathbb{C}^2)^{\otimes n} \otimes \mathbb{C}^2$ with n control qubits and one target qubit defined as

$$C^n(U)(|c_1c_2 \cdots c_n\rangle \otimes |t\rangle) = |c_1c_2 \cdots c_n\rangle \otimes U^{c_1 \cdot c_2 \cdots c_n}|t\rangle,$$

on the computational basis states.

(1) Let $V \in \mathcal{U}(\mathbb{C}^2)$ denote a single-qubit unitary such that $V^2 = U$. Show that $(C^n(V))^2 = C^n(U)$.

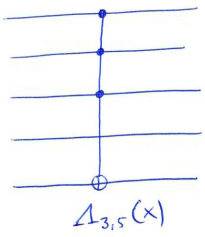
(2) Adapt the construction from the second exercise to implement the unitary $C^n(U)$ using only CNOT gates and the unitaries $C^{n-1}(V)$ and $C^{n-1}(V^\dagger)$.

(3) Let $V_1, \cdots, V_n \in \mathcal{U}(\mathbb{C}^2)$ denote single-qubit unitaries such that $V_1^2 = U$ and $V_{i+1}^2 = V_i$ for all $i \in \{1, \ldots, n-1\}$. Iterate the procedure from the previous subexercise to find a circuit only using CNOT gates and single qubit unitaries to implement the unitary $C^n(U)$. How many CNOT gates are needed for this construction?

The construction from the previous exercise is only feasible for small n. In the final two exercises we aim to find a better construction of the controlled unitary $C^n(U)$ for a single-qubit unitary U. To explain how this can be done, we introduce the notation $\Lambda_{m,n}(U)$ for the controlled unitary acting as

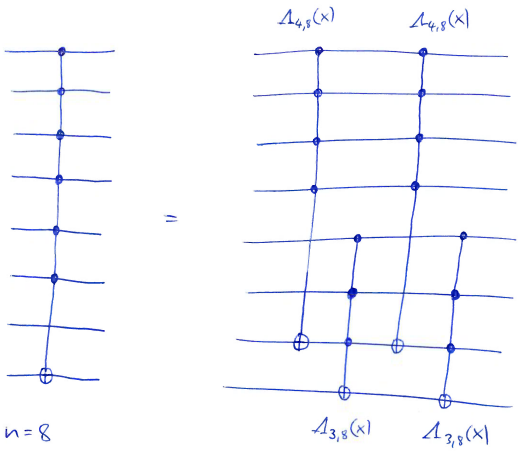
$$\Lambda_{m,n}(U)(|c_1 c_2 \cdots c_m\rangle \otimes |s_1 \cdots s_{n-m-1}\rangle \otimes |t\rangle) \\ = |c_1 c_2 \cdots c_m\rangle \otimes |s_1 \cdots s_{n-m-1}\rangle \otimes U^{c_1 \cdot c_2 \cdots c_m}|t\rangle,$$

i.e., where the first m qubits are the control, the last qubit is the target and the remaining qubits do are not acted upon (but they may be in any state). In the next Figure you can see a depiction of $\Lambda_{3,5}(X)$.



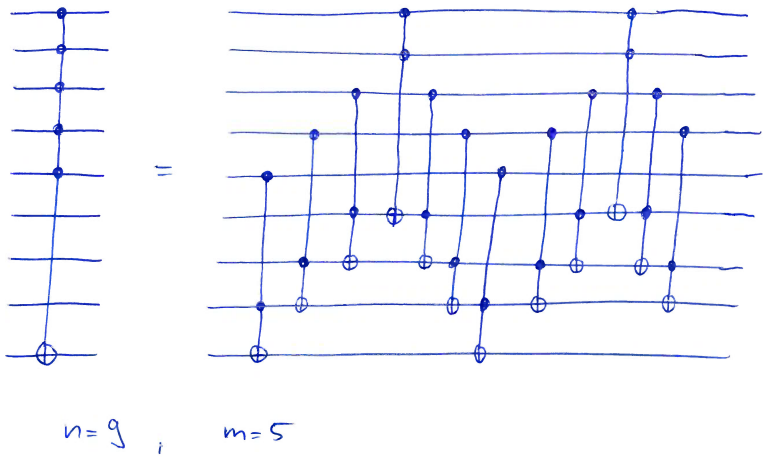
Excercise 4. In this exercise, we aim to implement unitaries of the type $\Lambda_{m,n}(X)$ and in particular $\Lambda_{n-2,n}(X)$. These will turn out to be important building blocks in the final exercise.

(1) Verify the following circuit:



Find a generalization of this circuit for $n \geqslant 5$ and $m \in \{2, \ldots, n-3\}$ implementing $\Lambda_{n-2,n}(X)$ using two instances of $\Lambda_{m,n}(X)$ and two instances of $\Lambda_{n-m-1,n}(X)$.

(2) Verify the following circuit:

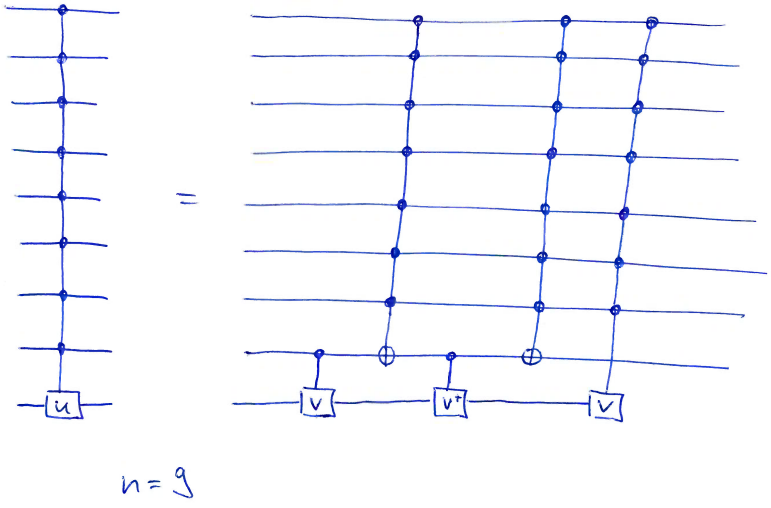


Find a generalization of this circuit for $n \geqslant 5$ and $m \in \{3, \ldots, \lceil \frac{n}{2} \rceil\}$ implementing $\Lambda_{m,n}(X)$ using $4(m-2)$ Toffoli gates.

(3) For $n \geqslant 7$ use the previous two exercises to implement the unitary $\Lambda_{n-2,n}(X)$ using $8(n-5)$ Toffoli gates.

Excercise 5. Finally, consider a single-qubit unitary U and a single-qubit unitary V such that $V^2 = U$. We will now find a better way of implementing the controlled gate $C^n(U)$ using Toffoli gates.

(1) Verify the following circuit:



(2) Use the previous exercises to show that $C^n(U)$ can be implemented using $O(n^2)$ Toffoli gates. Show that this means that $C^n(U)$ may be implemented by a circuit using $O(n^2)$ gates from the set $\{H, T, CNOT\}$.