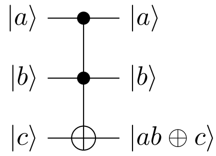
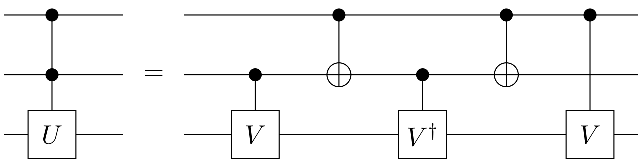
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Exercise 5.2 (Toffoli gate and quantum logic)
The Toffoli gate is also known as CCNOT or "controlled-controlled-NOT" operation. In classical circuits, this gate inverts the target wire when the input of its two control wires is 1. Thus, defining the Toffoli gate in terms of computational basis states leads to (for any $a, b, c \in \{0, 1\}$):



The bottom (target) qubit gets flipped precisely if both control qubits are in the $|1\rangle$ state; equivalently, the flip occurs if the product ab equals 1, which leads to the expression $ab \oplus c$.

Physical quantum computers only implement a finite gate-set as hardware operations. Thus it is typically necessary to decompose such multi-control operations in terms of gates with at most one control wire. One such decomposition of a controlled-controlled-U operation, known as the Sleator and Weinfurter construction[1], is:

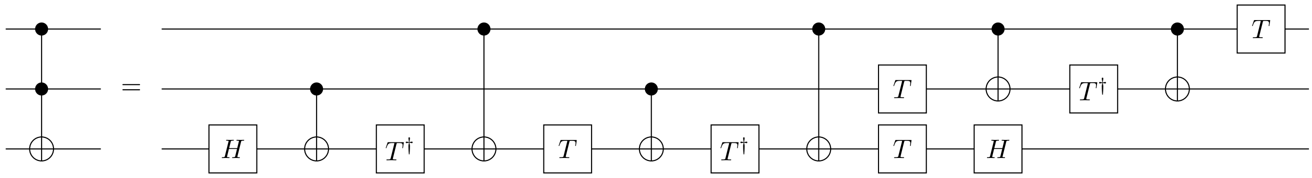


where V is a certain single-qubit gate depending on U. (The Toffoli gate corresponds to the special case $U = X$.)

(a) Which condition must V satisfy such that the equality holds? Verify your answer by inserting all four possible computational basis states for the control qubits.

(b) Find the V gate corresponding to $U = X$.
Hint: You can obtain a matrix power A^κ (with $\kappa \in \mathbb{R}$) of a normal matrix $A \in \mathbb{C}^{n\times n}$ by first computing its spectral decomposition: $A = U \operatorname{diag}(\lambda_1, \dots, \lambda_n)U^\dagger$ and U unitary; then exponentiate the eigenvalues, i.e., $A^\kappa = U \operatorname{diag}(\lambda_1^\kappa, \dots, \lambda_n^\kappa)U^\dagger$.

The so-called Clifford gates play an important role for quantum error correction and the Gottesman-Knill theorem.[2] Hence, most quantum computers support the "Clifford+T" gate set, which includes the Hadamard gate, the Pauli gates, the CNOT gate as well as the T gate, defined as $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$. It is possible to decompose the Toffoli gate in terms of these gates:



(c) Verify that the above circuit indeed implements the Toffoli gate.

Solution

(a) We first check the action of the circuit when the inputs on the control qubits are $|11\rangle$. We find that V^2 is applied to the target qubit. Hence, equality with the controlled-controlled-U operation requires that $V^2 = U$.

We can also verify the three other possible inputs on the control qubits, $|00\rangle, |01\rangle, |10\rangle$:

For $|00\rangle$, no gates are applied to the target qubit since all the controlled gates are inactive.

For $|01\rangle$, we see that $V^\dagger V = I$ is applied to the target qubit, and similarly for $|10\rangle$, $VV^\dagger = I$ is applied.

Hence, for the input states $|00\rangle, |01\rangle, |10\rangle$ on the control qubits, the circuit acts as identity, as required.

[1] T. Sleator, H. Weinfurter: *Realizable Universal Quantum Logic Gates*. Phys. Rev. Lett. 74, 4087 (1995)
[2] Quantum error correction will be part of the follow-up course "Advanced Concepts of Quantum Computing" next semester.

(b) We need to find $V = \sqrt{X}$, i.e., $\kappa = \frac{1}{2}$ in the hint. The spectral decomposition of the Pauli-X gate is

$$X = H\,\mathrm{diag}(1, -1)H,$$

with H the Hadamard gate (see previous exercises). Taking the square-root of the eigenvalues then leads to

$$\sqrt{X} = H\,\mathrm{diag}(1, i)H = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \frac{1+i}{2}I + \frac{1-i}{2}X.$$

(Multiplying the matrix on the right by itself indeed results in X, as expected.)

(c) Similar to part (a), we can simply check the action of the circuit for the four possible inputs in the computational basis on the control qubits. We first verify that no changes occur when the input to the control wires is not $|11\rangle$, noting that the T gate has no effect on qubits in the $|0\rangle$ state and $T^\dagger T = TT^\dagger = I$.

For $|00\rangle$, we see that $HTT^\dagger TT^\dagger H = I$ is applied to the target wire. (Note that the circuit diagram runs from left to right, while the order of applied matrices runs from right to left!) We then note that no changes occur in the control wires as they are both in the $|0\rangle$ state.

For $|01\rangle$, we see that $HTT^\dagger XTT^\dagger XH = I$ is applied to the target qubit. The output on the control wires is $(T\,|0\rangle) \otimes (T^\dagger T\,|1\rangle) = |01\rangle$.

For $|10\rangle$, we see that $HTXT^\dagger TXT^\dagger H = I$ is applied to the target wire. On the control wires, the action of the circuit is:

$$\begin{aligned}
&(T\,|1\rangle) \otimes (XT^\dagger XT\,|0\rangle) \\
&= (T\,|1\rangle) \otimes (XT^\dagger X\,|0\rangle) \\
&= e^{\frac{i\pi}{4}}\,|1\rangle \otimes (XT^\dagger\,|1\rangle) \\
&= e^{\frac{i\pi}{4}}\,|1\rangle \otimes (e^{\frac{-i\pi}{4}}X\,|1\rangle) \\
&= e^{\frac{i\pi}{4}}\,|1\rangle \otimes e^{\frac{-i\pi}{4}}\,|0\rangle = |10\rangle\,.
\end{aligned}$$

Finally, for $|11\rangle$, we see that $HT(XT^\dagger X)T(XT^\dagger X)H$ is applied to the target wire. We note the effect of conjugation by the Pauli-X gate is to flip the entries of a diagonal 2×2 matrix.

$$\begin{aligned}
XT^\dagger X &= \begin{pmatrix} \mathrm{e}^{-\frac{i\pi}{4}} & 0 \\ 0 & 1 \end{pmatrix}, \\
TXT^\dagger X &= \begin{pmatrix} \mathrm{e}^{-\frac{i\pi}{4}} & 0 \\ 0 & \mathrm{e}^{\frac{i\pi}{4}} \end{pmatrix}, \\
(TXT^\dagger X)^2 &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -iZ, \\
H(TXT^\dagger X)^2 H &= -iX.
\end{aligned}$$

We then note that the effect of the circuit on the control wires is effectively:

$$T\,|1\rangle \otimes T\,|1\rangle = i\,|11\rangle\,.$$

The final output of a circuit with input $|11x\rangle$, where $x \in \{0, 1\}$, is then

$$i\,|11\rangle \otimes (-iX\,|x\rangle) = |11\bar{x}\rangle\,,$$

which realizes the Toffoli gate.