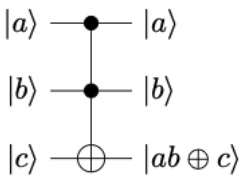
Quantum Information Theory **Universität Tübingen**
SoSe 2023 Ángela Capel
Paul Gondolf

Sheet 4 22. May 2023

Quantum algorithms

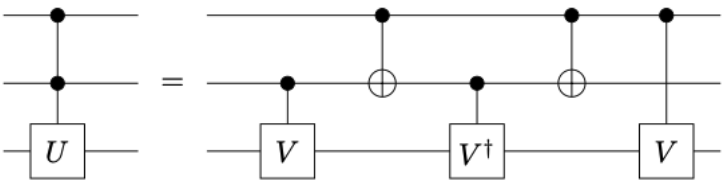
Graded exercises

Problem 1. 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> 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, is:



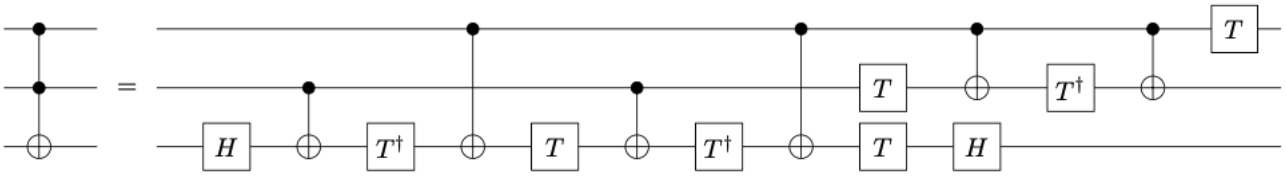
where V is a certain single-qubit gate depending on U. (The Toffoli gate corresponds to the special case $U = X$.)

1. 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.
2. Find the V gate corresponding to $U = X$.

The so-called Clifford gates play an important role for quantum error correction and the Gottesman-Knill theorem (see Exercise 6 of Sheet 3). 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, which is defined as

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\frac{i\pi}{4}} \end{pmatrix}.$$

It is possible to decompose the Toffoli gate in terms of these gates:



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

Problem 2. The uncertainty principle bounds how well a quantum state can be localized simultaneously in the standard basis and the Fourier basis. In this problem, we will derive an uncertainty principle for a discrete system of n-qubit.

Let $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$ be the state of an n-qubit system. A measure of the spread of $|\psi\rangle$ is $S(|\psi\rangle) = \sum_x |\alpha_x|$. For example,for a completely localized state $|\psi\rangle = |y\rangle$, with $y \in \{0,1\}^n$, the spread is $S(|\psi\rangle) = 1$. For a maximally spread state $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$, the spread is $S(|\psi\rangle) = \sqrt{2^n}$.

1. Prove that for any quantum state $|\psi\rangle$ on n qubits, $S(|\psi\rangle) \leq \sqrt{2^n}$.

   (Hint: Use Cauchy-Schwarz inequality)

2. Suppose that $|\alpha_x| \leq a$ for all x. Prove that $S(|\psi\rangle) \geq \frac{1}{a}$.

3. Show that $H^{\otimes n} |x\rangle = \sum_y (-1)^{x\cdot y} |y\rangle$.

   (Remainder: $x \cdot y = \sum_{i=1}^n x_i y_i$)

4. Now, we can write $H^{\otimes n} |\psi\rangle = \sum_x \beta_x |x\rangle$, where $\beta_x = \frac{1}{\sqrt{2^n}} (-1)^{x\cdot y} \alpha_y$. Use this to prove that for all y, $|\beta_y| \leq \frac{1}{\sqrt{2^n}} S(|\psi\rangle)$.

5. Prove the uncertainty relation

   $$S(|\psi\rangle) S(H^{\otimes n} |\psi\rangle) \geq \sqrt{2^n}.$$

   Justify why it makes sense to call it an uncertainty relation.

Problem 3. Consider the task of constructing a quantum circuit to compute $|x\rangle \mapsto |x + y (mod 2^n)\rangle$, where y is a fixed constant, and $0 \leq x < 2n$. Show that one efficient way to do this, for values of y such as 1, is to first perform a quantum Fourier transform, then to apply single qubit phase shifts, then an inverse Fourier transform. What values of y can be added easily this way, and how many operations are required?

Challenge exercise

Problem 4. Suppose we have a single qubit operator U with eigenvalues ± 1, so that U is both Hermitian and unitary, so it can be regarded both as an observable and a quantum gate. Suppose we wish to measure the observable U. That is, we desire to obtain a measurement result indicating one of the two eigenvalues, and leaving a post-measurement state which is the corresponding eigenvector. How can this be implemented by a quantum circuit?