Quantum Information Theory
SoSe 2023

Universität Tübingen
Ángela Capel
Paul Gondolf

Sheet 3

15. May 2023

Quantum circuits

Warm-up exercises

Problem 1. Consider a two qubit unitary gate U that accomplishes the following transformation:

- $|00\rangle \mapsto |{+}{+}\rangle$,
- $|10\rangle \mapsto |{-}{+}\rangle$,
- $|01\rangle \mapsto |{+}{-}\rangle$,
- $|11\rangle \mapsto \mathrm{e}^{i\varphi} |{-}{-}\rangle$.

Find φ such that

1. $U = U_A \otimes U_B$ for some single qubit unitaries U_A and U_B.
2. $U \neq U_A \otimes U_B$ for any single qubit unitaries U_A and U_B.

Problem 2. Prove that a state $|\psi\rangle$ of a composite system AB is a product state if, and only if, it has Schmidt rank 1. Prove that $|\psi\rangle$ is a product state if, and only if, for $\rho_{AB} := |\psi\rangle \langle\psi|$, ρ_A (and thus ρ_B) is a pure state.

Hint: Recall that ρ is a pure state if it can be written as $\rho = |\phi\rangle \langle\phi|$.

Graded exercises

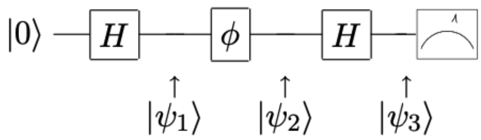
Problem 3.

1. Construct a reversible circuit which, when given two input bits x and y, it outputs $(x, y, c, x \oplus y)$, where c is the carry bit when x and y are added.

   Hint: c should be 1 if $x = y = 1$ and 0 elsewhere.

2. Construct a quantum circuit to add two two-bit numbers x and y modulo 4. That is, the circuit should perform the transformation $|x, y\rangle \mapsto |x, x + y \bmod 4\rangle$.

Problem 4. Consider this single qubit model of an interferometer, where the goal is to estimate an unknown phase ϕ:

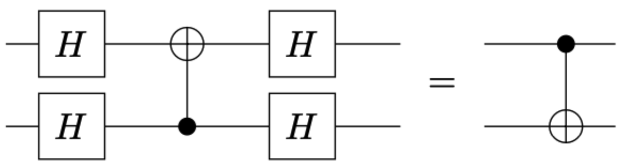


Let the box with ϕ map $|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $e^{i\phi}|1\rangle$.

- Give the states $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle$.
- What is the probability p of measuring the final qubit to be one?
- If this experiment is repeated n times, what is the standard deviation Δp of the value estimated for p from the measurement results? Also, give the uncertainty in the resulting estimate for ϕ, given by $\Delta\phi = \Delta p / \mid dp/d\phi \mid$.

  Hint: The standard deviation Δp is given by $\sqrt{< p^2 > - < p >^2}$, where $< \cdot, \cdot >$ here denotes 'expectation'.

Problem 5. The role of the control and target qubit of a CNOT gate can be reversed by switching to a different basis. First, show that the following equality of circuits holds:



Use this identity to derive the following relations:

- $CNOT\,|{+}{+}\rangle = |{+}{+}\rangle$,
- $CNOT\,|{-}{+}\rangle = |{-}{+}\rangle$,
- $CNOT\,|{+}{-}\rangle = |{-}{-}\rangle$,
- $CNOT\,|{-}{-}\rangle = |{+}{-}\rangle$.

Hint: Recall that

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\,.$$

Challenge exercise

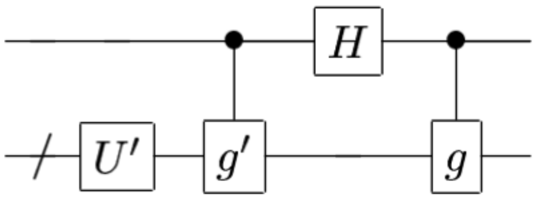
Problem 6. An essential result in quantum computation is that H, CNOT, and the Pauli gates are **not** universal for quantum computation. In fact, any quantum circuit composed from those gates (together with standard input states and measurements in the computational basis) can be simulated efficiently by a classical computer! This result is known as the *Gottesman-Knill theorem.* The purpose of this problem is to prove the key result behind the theorem.

Let G_n denote the Pauli group on n qubits (that is, matrix multiplication acting on the set of n-fold tensor products of Pauli matrices, including multiplicative factors ± 1, $\pm i$). By definition, we say the set of U such that $UG_nU^* = G_n$ is the *normalizer* of G_n, and denote it by $N(G_n)$. The following theorem about the normalizer of the Pauli group holds:

Suppose U is any unitary operator on n qubits with the property that if $g \in G_n$ then $UgU^* \in G_n$. Then, up to a global phase, U may be composed from $O(n^2)$ H, phase and CNOT gates.

We can construct an inductive proof of this theorem as follows:

1. Prove that the Hadamard and phase gates can be used to perform any normalizer operation on a single qubit.
2. Suppose that U is an $n+1$ qubit gate in $N(G_{n+1})$ such that $UZ_1U^* = X_1 \otimes g$ and $UX_1U^* = Z_1 \otimes g'$ for some elements $g, g' \in G_n$. Define U' on n qubits by $U' |\psi\rangle = \sqrt{2} \langle 0| U(|0\rangle \otimes |\psi\rangle)$. Use the inductive hypothesis to show that this construction for U:



   may be implemented using $O(n^2)$ Hadamard, phase and CNOT gates.
3. Show that any gate $U \in N(G_{n+1})$ may be implemented using $O(n^2)$ Hadamard, phase and CNOT gates.

Hint: You can use the following two lemmas without proving them:

Lemma 1: Given any Pauli operator g, there is some product of Hadamards and phase gates N such that $NgN^* = Z$.

Lemma 2: Given any two different Pauli matrices $\sigma \neq \sigma'$, there is some product of Hadamards and phase gates N such that $N\sigma N^* = X$ and $N\sigma' N^* = Z$. Therefore,

$$N \cdot SWAP_{1j} \cdot U \cdot Z_1 \cdot (N \cdot SWAP_{1j} \cdot U)^* = X_1 \otimes g\,,$$
$$N \cdot SWAP_{1j} \cdot U \cdot X_1 \cdot (N \cdot SWAP_{1j} \cdot U)^* = Z_1 \otimes g\,.$$