Quantum computing: algorithms and complexity

Assignment 1

Due: 01.04.2023, 23:59

Problem 1 (Useful identities)

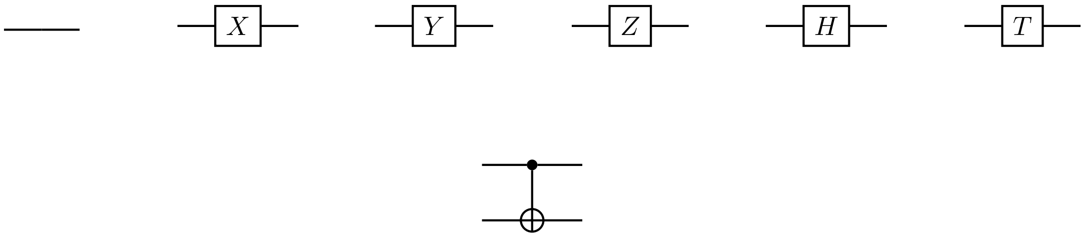
Recall some of the main unitary gates we encountered in the lectures:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

and

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

As circuits, these take the following form:



A. Prove the following relations:

1. $H = \frac{1}{\sqrt{2}}(X + Z)$.

2. $HXH = Z, HYH = -Y, HZH = X$.

3. $XZ = -ZX$, $XY = -YX$, $ZY = -YZ$.

4. $TZ = ZT$.

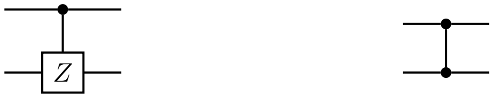
5. $(X \otimes X)CNOT = CNOT(X \otimes I)$ and $(I \otimes X)CNOT = CNOT(I \otimes X)$.

   Hint: for this, it's easier to use the actions of $CNOT$ and X on the computational basis states, rather than the matrix representations.

B. Now consider the controlled-Z operation, which applies a Z gate to the second qubit, conditioned on the first qubit being in a $|1\rangle$ state:

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

In circuit form, we represent CZ in one of two ways:



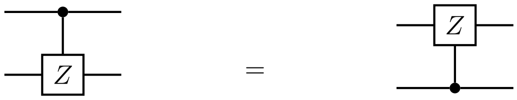
Notice that in the second picture the gate looks symmetrical, in the sense that there aren't obvious control and target qubits (unlike the first picture, where the top qubit is the control qubit and the bottom is the target qubit). Indeed, you will have to show that CZ is symmetrical.

Start by first showing, using the matrix representation, that

$$CZ\,|00\rangle = |00\rangle \quad CZ\,|01\rangle = |01\rangle \quad CZ\,|10\rangle = |10\rangle \quad CZ\,|11\rangle = -\,|11\rangle\,.$$

For controlled gates, let us introduce the notation $CZ_{1,2}$ (or $CNOT_{1,2}$, respectively) to indicate that qubit 1 is the control qubit and qubit 2 is the target qubit. That is to say, $CZ_{1,2}$ means "controlled on qubit 1 being $|1\rangle$, apply a Z gate to qubit 2." Prove the following relations:

1. $CZ_{1,2} = CZ_{2,1}$ (CZ is symmetric under qubit swapping). In circuit form, we have:



2. $CNOT_{1,2} \neq CNOT_{2,1}$. For this it suffices to show that there's at least one state $|\psi\rangle$ such that $CNOT_{1,2}\,|\psi\rangle \neq CNOT_{2,1}\,|\psi\rangle$.

3. $(I \otimes H)CZ_{1,2}(I \otimes H) = CNOT_{1,2}$.

4. $(H \otimes H)CNOT_{1,2}(H \otimes H) = CNOT_{2,1}$.

Problem 2 (States and unitaries)

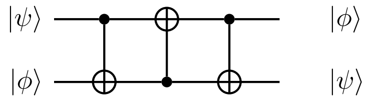
A. Express the 2-qubit Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in the $(|{++}\rangle, |{+-}\rangle, |{-+}\rangle, |{--}\rangle)$ basis, where recall that $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Next, express the 3-qubit GHZ state $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ in the $(|{+++}\rangle, |{++-}\rangle, ... |{---}\rangle)$ basis.

B. Compute $CNOT\,|{++}\rangle$. Is this state a product state? I.e., can it be expressed as $|\psi\rangle \otimes |\phi\rangle$ for some $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, $|\phi\rangle = c\,|0\rangle + d\,|1\rangle$?

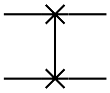
C. Compute $CZ\,|{++}\rangle$. Is this state a product state?

D. For $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, compute $CNOT\,|\psi\rangle\,|-\rangle$. Is this state a product state? You should notice that the relative phase of the first qubit changes as a result of the $CNOT$ operation (even though, intuitively, the control qubit should remain unchanged). This is called the *phase kickback* effect and is an important part of certain quantum algorithms.

E. Show that $CNOT_{1,2}\ CNOT_{2,1}\ CNOT_{1,2}\ (|\psi\rangle \otimes |\phi\rangle) = |\phi\rangle \otimes |\psi\rangle$, where $|\psi\rangle$ and $|\phi\rangle$ are single-qubit states. In circuit form, you have to show the following:



This operation is referred to as $SWAP$ and is sometimes promoted to the status of a fundamental gate, represented as:



Hint: Since every unitary is fully determined by its action on a basis, consider the action of that circuit on the computational basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$.

F. Which 2-qubit unitary (expressed in terms of the elementary gates we've seen so far) performs the mapping:

$$|00\rangle \to |00\rangle \qquad |01\rangle \to -|01\rangle \qquad |10\rangle \to -|10\rangle \qquad |11\rangle \to |11\rangle?$$

What about:

$$|00\rangle \to |00\rangle \qquad |01\rangle \to |01\rangle \qquad |10\rangle \to |11\rangle \qquad |11\rangle \to -|10\rangle?$$

Problem 3 (Fun with Hadamard)

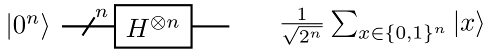
Recall the action of the Hadamard gate on the computational basis: $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$.

We used $H \otimes H$ to denote the 2-qubit gate which consists of Hadamard acting on the first qubit and on the second qubit. We typically write this in the more compact form $H^{\otimes 2} = H \otimes H$. In general, $H^{\otimes n} = H \otimes H \otimes ... \otimes H$, denotes n Hadamard gates acting in parallel on n qubits. This notation also applies to states. For instance $|0\rangle^{\otimes 2} = |0\rangle \otimes |0\rangle = |00\rangle$. In general, $|0\rangle^{\otimes n} = |00..0\rangle$. The latter state is also sometimes denoted $|0^n\rangle$.

A. Show that $H^{\otimes 2}|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$. Generalize this by showing that:

$$H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle .$$

Here, $|x\rangle$ is the computational basis state associated to the n-bit string x. In circuit form, we write:



B. For $b \in \{0,1\}$, we can compactly write the action of Hadamard on the computational basis states as:

$$H|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b |1\rangle).$$

Generalize this by showing:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle . \tag{1}$$

This is an extremely useful relation which will come up a number of times in the lectures.

Here, $x \cdot y$ denotes the modulo 2 inner product between x and y as vectors of bits. That is, if $x = x_1 x_2 ... x_n$ and $y = y_1 y_2 ... y_n$, with $x_i, y_i \in \{0,1\}$, then

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \bmod 2.$$

Equivalently,

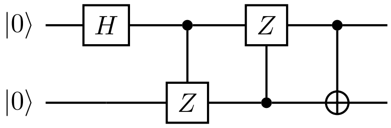
$$x \cdot y = x_1 y_1 \oplus x_2 y_2 \oplus ... \oplus x_n y_n,$$

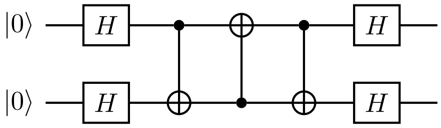
since the xor operation $\oplus$ is addition modulo 2.

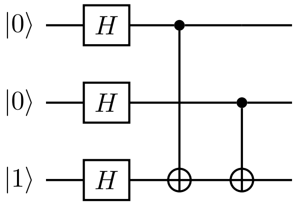
Hint: To show Equation 1, start by showing the $n = 2$ case to get a feel for what the relation is saying. You can then prove the general statement by induction.

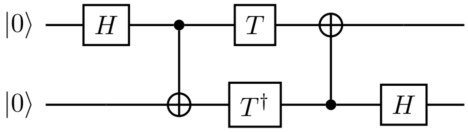
Problem 4 (Quantum circuits)

A. Compute the output quantum state for each of the following circuits:









Where $T^\dagger$ is the inverse of T.

B. Using only gates from the set $\{X, H, T, CNOT\}$, write circuits for the following operations:[1]

1. $T^\dagger$. Note that while T is part of the set, $T^\dagger$ is not, so you have to somehow express it in terms of the operations in the set. **Hint:** $T^8 = I$.
2. The unitary performing the mapping $|x\rangle |y\rangle |z\rangle \to |y\rangle |x\rangle |x \oplus y \oplus z\rangle$, where $x, y, z \in \{0, 1\}$.
3. The unitary which maps the computational basis to the eigenbasis of Y. That is $|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$, $|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$.
4. Any unitary that maps $|0000\rangle \to \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$.

Problem 5 (Measurements)

A. Recall that a (projective) measurement is specified by a collection of *projectors*, $\{P_i\}_{i=1}^k$, where $P_i^2 = P_i$, $P_i P_j = 0$ (for $i \neq j$) and $\sum_{i=1}^k P_i = I$. Show that the following projectors constitute a valid projective measurement:

$$P_0 = |00\rangle\langle 00| + |11\rangle\langle 11| \qquad P_1 = |01\rangle\langle 01| + |10\rangle\langle 10| . \tag{2}$$

[1] You can implicitly also use the identity operation, I, which just means no gate.

Mathematically, projectors define a plane (or hyperplane) in Hilbert space onto which a state is projected when a measurement is performed. In this case, the measurement is referred to as the *parity* measurement. This is because P_0 projects onto the plane spanned by $|00\rangle$ and $|11\rangle$, the strings with parity 0,[2] while P_1 projects onto the plane spanned by the strings of parity 1.

B. Recall that performing the measurement $M = \{P_i\}_{i=1}^k$ on some state $|\psi\rangle$, will yield outcome i with probability $\langle\psi| P_i |\psi\rangle$, and the state after the measurement is $\frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}$. This is referred to as the *post-measurement state.*

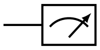
What are the two possible post-measurement states when the state $|{+}{+}\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ is measured with the measurement from Equation 2. What are the probabilities for the 2 possible outcomes?

What about for the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$?

C. Recall that a measurement of a single qubit in the computational basis is given by the projectors:

$$P_0 = |0\rangle\langle 0| \qquad\qquad P_1 = |1\rangle\langle 1|\,.$$

In circuit form, a computational basis measurement is represented as:

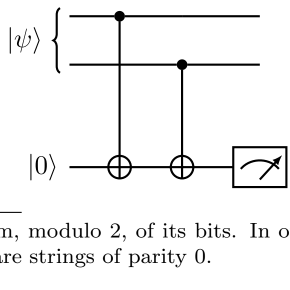


If we'd like to measure a single qubit (in the computational basis) from a multi-qubit state, the corresponding projectors are obtained by tensoring with identity operations on the unmeasured qubits. For instance, if we want to measure the first qubit of a 3-qubit state, the corresponding projectors would be:

$$P_0 = |0\rangle\langle 0| \otimes I \otimes I \qquad\qquad P_1 = |1\rangle\langle 1| \otimes I \otimes I.$$

What are the possible post-measurement states (and the probabilities for each) when measuring the first qubit of the GHZ state $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$? What about for $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$?

D. Is there a way to perform the parity measurement from Equation 2 using only a computational basis measurement? The answer is yes, and the idea is to simply compute the parity of the state into an extra qubit and then measure that qubit in the computational basis. Show that this is indeed the case by proving that the following circuit performs a parity measurement on the 2-qubit state $|\psi\rangle$.



[2] The parity of a bitstring x is simply the sum, modulo 2, of its bits. In other words, $Parity(x) = x_1 \oplus x_2 \oplus ... \oplus x_n$. It's clear that $0 \oplus 0 = 1 \oplus 1 = 0$, so that 00 and 11 are strings of parity 0.

In other words, show that when the bottom qubit is measured as being 0, the state $|\psi\rangle$ is projected to $\frac{P_0|\psi\rangle}{\sqrt{\langle\psi|P_0|\psi\rangle}}$ and, similarly, for outcome 1 we have projection onto $\frac{P_1|\psi\rangle}{\sqrt{\langle\psi|P_1|\psi\rangle}}$, where here P_0 and P_1 are the ones from Equation 2. You should assume here that $|\psi\rangle$ is an arbitrary 2 qubit state, $|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$.

E. Consider measuring a qubit in the $(|+\rangle\,, |-\rangle)$ basis. Write the projectors for this measurement. Compute the post-measurement states (and probabilities) for a $(|+\rangle\,, |-\rangle)$-basis measurement of the (first qubit of the) $|GHZ\rangle$ and $|W\rangle$ states.

F. In analogy to the parity measurement, we can also define a *phase parity* measurement with the projectors:

$$P_+ = |{+}{+}\rangle\,\langle{+}{+}| + |{-}{-}\rangle\,\langle{-}{-}| \qquad\qquad P_- = |{+}{-}\rangle\,\langle{+}{-}| + |{-}{+}\rangle\,\langle{-}{+}|\,.$$

As in **D**, give a circuit which implements the phase parity measurement using a single-qubit computational basis measurement.