Exercise 1. ***Controlled gates***

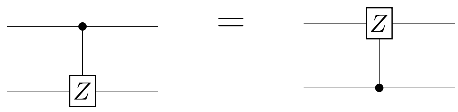
The controlled-Z gate, the CNOT gate and the Hadamard gates are implemented by the unitary matrices

$$\mathrm{C}Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \quad \mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{1}$$

respectively, in the computational basis.

(a) Construct a CNOT gate using one controlled-Z gate and two Hadamard gates. Draw the circuit, specifying the control and target qubits.

(b) Show that



Exercise 2. ***$Z - Y$ decomposition on a single qubit***

Recall that the Pauli matrices are given by

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{2}$$

in the computational basis.

We will see that exponentiating Pauli matrices give us unitary matrices that correspond to rotations around each axis of the Bloch sphere. Then we will show that any unitary gate on a single qubit can be implemented using only Z and Y rotations.

(a) Show that $X^2 = Y^2 = Z^2 = \mathbb{1}$.

(b) Show that, if A is a matrix such that $A^2 = \mathbb{1}$, then, for any real number x, $e^{ixA} = \cos(x)\mathbb{1} + i\sin(x)A$.

(c) Use the previous step to show that

$$R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}, \tag{3}$$

$$R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}. \tag{4}$$

(d) Show that if U is a unitary matrix acting on a qubit, then there exist real numbers $\alpha, \beta, \gamma, \delta$ such that

$$U = \begin{bmatrix} e^{i(\alpha-\beta-\delta)}\cos\gamma & -e^{i(\alpha-\beta+\delta)}\sin\gamma \\ e^{i(\alpha+\beta-\delta)}\sin\gamma & e^{i(\alpha+\beta+\delta)}\cos\gamma \end{bmatrix}. \tag{5}$$

(e) Use all of the above to show that, for any reversible gate U acting on a single qubit, there exist real numbers $\alpha, \beta, \gamma, \delta$ such that U can be implemented as

$$U = e^{i\alpha} R_z(2\beta) R_y(2\gamma) R_z(2\delta). \tag{6}$$

Exercise 3. ***Quantum teleportation***

Imagine that Alice (A) has state S in her lab, in pure state $|\psi\rangle_S$. She wants to send the state to Bob, who lives on the moon, without the expensive costs of shipping a coherent qubit on a space rocket. We will see that if Alice and Bob share some initial entanglement, Alice can "teleport" the state $|\psi\rangle$ to Bob's lab, using only local operations and classical communication.

Formally, we have three systems $S \otimes A \otimes B$. Alice controls systems S and A, and Bob controls B. In this exercise we will assume all three systems are qubits. The initial state is

$$|\psi\rangle_S \otimes \frac{1}{\sqrt{2}} \left(|0_A 0_B\rangle + |1_A 1_B\rangle \right), \tag{7}$$

i.e. A and B are fully entangled in a Bell state. We may write $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

(a) In a first step, Alice will measure systems S and A jointly in the Bell basis,

$$\left\{ \begin{array}{ll} \frac{1}{\sqrt{2}} \left(|0_S 0_A\rangle + |1_S 1_A\rangle \right), & \frac{1}{\sqrt{2}} \left(|0_S 0_A\rangle - |1_S 1_A\rangle \right), \\ \frac{1}{\sqrt{2}} \left(|0_S 1_A\rangle + |1_S 0_A\rangle \right), & \frac{1}{\sqrt{2}} \left(|0_S 1_A\rangle - |1_S 0_A\rangle \right) \end{array} \right\}. \tag{8}$$

Alice then communicates the result of her measurement to Bob: this takes two bits of classical information. What is the reduced state of Bob's system (B) for each of the possible outcomes?

(b) Depending on the outcome of the measurement by Alice, Bob may have to perform certain unitary operations on his qubit so that he recovers $|\psi\rangle$. Which operations are these?

(c) Suppose that Alice does not manage to tell Bob the outcome of her measurement. Show that in this case he does not have any information about his reduced state and therefore does not know which operation to apply in order to obtain $|\psi\rangle$.

(d) **[extra]** In general, the state of S is not pure: it might be correlated with some other system that Alice and Bob do not control. Consider a purification of ρ_S on a reference system R,

$$\rho_S = \mathrm{tr}_R \, |\phi\rangle\langle\phi|_{SR}. \tag{9}$$

Show that if you apply the quantum teleportation protocol on $S \otimes A \otimes B$, without touching the reference system, the final state on $B \otimes R$ is $|\phi\rangle$.

This implies that quantum teleportation preserves entanglement — it simply transfers it from [S and R] to [B and R].