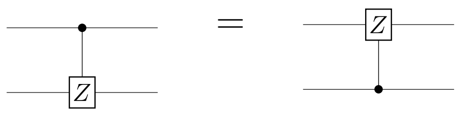
Exercise 1. *Controlled gates*

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

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

respectively, in the computational basis.

(a) [previously *b*)] Show that



Solution. For clarity, let's call the top qubit A and the bottom qubit B. In Dirac notation, we can express the controlled-Z gate, with control qubit A and target qubit B, as

$$CZ = |0_A 0_B\rangle\langle 0_A 0_B| + |0_A 1_B\rangle\langle 0_A 1_B| + |1_A 0_B\rangle\langle 1_A 0_B| - |1_A 1_B\rangle\langle 1_A 1_B|.$$

But a controlled-Z gate with control qubit B and target A has exactly the same expression,

$$|0_A 0_B\rangle\langle 0_A 0_B| + |1_A 0_B\rangle\langle 1_A 0_B| + |0_A 1_B\rangle\langle 0_A 1_B| - |1_A 1_B\rangle\langle 1_A 1_B| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Note: the same is not true of, for instance, the CNOT gate: if the control qubit is A and the target B, we have

$$\mathrm{CNOT} = |0_A 0_B\rangle\langle 0_A 0_B| + |0_A 1_B\rangle\langle 0_A 1_B| + |1_A 0_B\rangle\langle 1_A 1_B| + |1_A 1_B\rangle\langle 1_A 0_B|.$$

However, if the control is B and the target is A, we get

$$|0_A 0_B\rangle\langle 0_A 0_B| + |1_A 0_B\rangle\langle 1_A 0_B| + |0_A 1_B\rangle\langle 1_A 1_B| + |1_A 1_B\rangle\langle 0_A 1_B| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

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

Solution. Since the Hadamard matrix only applies to one qubit, we have to tensor it with the identity to obtain the global unitary acting on the two qubits: $H_A \otimes \mathbb{1}_B$ if we apply the Hadamard gate on the first qubit, and $\mathbb{1}_A \otimes H_B$ if we apply it on the second. Let's do both to see how it works.

$$\begin{aligned} H_A \otimes \mathbb{1}_B &= \frac{1}{\sqrt{2}} \left(|0_A\rangle\langle 0_A| + |0_A\rangle\langle 1_A| + |1_A\rangle\langle 0_A| - |1_A\rangle\langle 1_A| \right) \otimes \left(|0_B\rangle\langle 0_B| + |1_B\rangle\langle 1_B| \right) \\ &= \frac{1}{\sqrt{2}} \left(|0_A 0_B\rangle\langle 0_A 0_B| + |0_A 0_B\rangle\langle 1_A 0_B| + |1_A 0_B\rangle\langle 0_A 0_B| - |1_A 0_B\rangle\langle 1_A 0_B| \right. \\ &\quad \left. + |0_A 1_B\rangle\langle 0_A 1_B| + |0_A 1_B\rangle\langle 1_A 1_B| + |1_A 1_B\rangle\langle 0_A 1_B| - |1_A 1_B\rangle\langle 1_A 1_B| \right) \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}, \end{aligned}$$

$$
\begin{aligned}
\mathbb{1}_A \otimes H_B &= (|0_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A|) \otimes \frac{1}{\sqrt{2}} (|0_B\rangle\langle 0_B| + |0_B\rangle\langle 1_B| + |1_B\rangle\langle 0_B| - |1_B\rangle\langle 1_B|) \\
&= \frac{1}{\sqrt{2}} (|0_A 0_B\rangle\langle 0_A 0_B| + |0_A 0_B\rangle\langle 0_A 1_B| + |0_A 1_B\rangle\langle 0_A 0_B| - |0_A 1_B\rangle\langle 0_A 1_B| \\
&\qquad + |1_A 0_B\rangle\langle 1_A 0_B| + |1_A 0_B\rangle\langle 1_A 1_B| + |1_A 1_B\rangle\langle 0_A 0_B| - |1_A 1_B\rangle\langle 1_A 1_B|) \\
&= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}.
\end{aligned}
$$

Now we can try to build the circuit. One combination that works is

$$
(\mathbb{1}_A \otimes H_B) CZ (\mathbb{1}_A \otimes H_B) = \frac{1}{2} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.
$$

Note that the result of part a) implies that $(H_A \otimes \mathbb{1}_B) CZ (H_A \otimes \mathbb{1}_B)$ gives us a CNOT with control qubit B and target A.

[Insert diagrams]

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 $X^2 = Y^2 = Z^2 = \mathbb{1}$.

Solution. This is direct,

$$
X^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},
$$

and so on.

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

Solution. We start from the usual expansion of the exponential, and split it into even and odd terms,

$$
\begin{aligned}
e^{ixA} &= \sum_{k=0}^{\infty} \frac{1}{k!} (ixA)^k \\
&= \sum_{k=0}^{\infty} \frac{1}{(2k)!} i^{2k} x^{2k} \underbrace{A^{2k}}_{\mathbb{1}^k} + \sum_{k=1}^{\infty} \frac{1}{(2k-1)!} \underbrace{i^{2k-1}}_{i \cdot i^{2k-2}} x^{2k-1} A \underbrace{A^{2k}}_{\mathbb{1}^k} \\
&= \mathbb{1} \sum_{k=0}^{\infty} \frac{1}{(2k)!} (-1)^k \, x^{2k} + iA \sum_{k=1}^{\infty} \frac{1}{(2k-1)!} (-1)^{k-1} \, x^{2k-1} \\
&= \mathbb{1} \cos x + iA \sin x.
\end{aligned}
$$

(c) Use the previous step to show that

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

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

Solution.

$$\begin{aligned} e^{-i\frac{\theta}{2}Y} &= \mathbb{1}\cos\left(-\frac{\theta}{2}\right) + iY\sin\left(-\frac{\theta}{2}\right) = \cos\frac{\theta}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - i\sin\frac{\theta}{2}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ &= \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}, \\ e^{-i\frac{\theta}{2}Z} &= \mathbb{1}\cos\left(-\frac{\theta}{2}\right) + iZ\sin\left(-\frac{\theta}{2}\right) = \cos\frac{\theta}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + i\sin\frac{\theta}{2}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} - i\sin\frac{\theta}{2} & 0 \\ 0 & \cos\frac{\theta}{2} + i\sin\frac{\theta}{2} \end{bmatrix} \\ &= \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}. \end{aligned}$$

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

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

Solution. A complex 2×2 matrix U is unitary if $UU^\dagger = U^\dagger U = \mathbb{1}$. This implies that the rows and columns of U are orthonormal. [some gymnastics gives us the result]

(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

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

Solution. This follows directly from the definition of rotation matrices.

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,

$$\left\{ \begin{array}{ll} |\phi_0\rangle = \frac{1}{\sqrt{2}} \left(|0_S 0_A\rangle + |1_S 1_A\rangle \right), & |\phi_1\rangle = \frac{1}{\sqrt{2}} \left(|0_S 0_A\rangle - |1_S 1_A\rangle \right), \\ |\phi_2\rangle = \frac{1}{\sqrt{2}} \left(|0_S 1_A\rangle + |1_S 0_A\rangle \right), & |\phi_3\rangle = \frac{1}{\sqrt{2}} \left(|0_S 1_A\rangle - |1_S 0_A\rangle \right) \end{array} \right\}. \tag{8}$$

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?

Solution. Let's do this properly. First we write down the POVM elements of Alice's measurement,

$$\begin{aligned} P_0 &= |\phi_0\rangle\langle\phi_0| = \frac{1}{2} \left(|0\rangle_S |0\rangle_A + |1\rangle_S |1\rangle_A \right) \left(\langle 0|_S \langle 0|_A + \langle 1|_S \langle 1|_A \right), \\ P_1 &= |\phi_1\rangle\langle\phi_1| = \frac{1}{2} \left(|0\rangle_S |0\rangle_A - |1\rangle_S |1\rangle_A \right) \left(\langle 0|_S \langle 0|_A - \langle 1|_S \langle 1|_A \right), \\ P_2 &= |\phi_2\rangle\langle\phi_2| = \frac{1}{2} \left(|0\rangle_S |1\rangle_A + |1\rangle_S |0\rangle_A \right) \left(\langle 0|_S \langle 1|_A + \langle 1|_S \langle 0|_A \right), \\ P_3 &= |\phi_3\rangle\langle\phi_3| = \frac{1}{2} \left(|0\rangle_S |1\rangle_A - |1\rangle_S |0\rangle_A \right) \left(\langle 0|_S \langle 1|_A - \langle 1|_S \langle 0|_A \right). \end{aligned}$$

Note that $P_0 + P_1 + P_2 + P_3 = \mathbb{1}_{SA}$, as should be for a POVM.

Now, Alice's measurement device must have a classical registry X (like a screen or a hard drive) that saves the outcome of the measurement. A measurement corresponds to a unitary evolution on all the qubits and the classical registry,

$$|\text{ready to measure}\rangle\langle\text{ready to measure}|_X \otimes \rho_{SAB} \mapsto \sum_{k=0}^{3} |\text{outcome: } k\rangle\langle\text{outcome: } k|_X \otimes (P_k \otimes \mathbb{1}_B)\ \rho_{SAB}\ (P_k \otimes \mathbb{1}_B).$$

Notice that Bob has no access to the registry X, which tells Alice the outcome of the measurement, so from his perspective, the global state of the three qubits SAB is simply

$$\begin{aligned} \sigma_{SAB} &= \operatorname{tr}_X \left(\sum_{k=0}^{3} |\text{outcome: } k\rangle\langle\text{outcome: } k|_X \otimes (P_k \otimes \mathbb{1}_B)\ \rho_{SAB}\ (P_k \otimes \mathbb{1}_B) \right) \\ &= \sum_{k=0}^{3} (P_k \otimes \mathbb{1}_B)\ \rho_{SAB}\ (P_k \otimes \mathbb{1}_B) \end{aligned} \tag{S.1}$$

We will look at this state again in part c). Alice, on the other hand, has access to X, and can simply read the outcome of the measurement. If she reads "outcome: k", she knows that the global state is

$$\sigma_{SAB|X=k} = \frac{(P_k \otimes \mathbb{1}_B)\ \rho_{SAB}\ (P_k \otimes \mathbb{1}_B)}{\|(P_k \otimes \mathbb{1}_B)\ \rho_{SAB}\ (P_k \otimes \mathbb{1}_B)\|}.$$

The denominator is just the probability of obtaining outcome k.

If attributing two states to the same physical system seems confusing, think of the following analogy: Bob tells Alice to buy him a lottery ticket. She does, but does not tell him the number. If you ask Bob about his (financial state) after the results come out, he will say "I am very likely not a millionaire". Alice, on the other hand, has access to the lottery result and the ticket number, so she knows exactly whether he is a millionaire or not. After she shares the ticket number with Bob, he also has this knowledge.

Now let us apply this framework to our particular initial state, $|\psi\rangle_S \otimes \frac{1}{\sqrt{2}} \left(|0_A 0_B\rangle + |1_A 1_B\rangle \right)$. After Alice obtains the outcome k, the global state becomes, from her perspective,

$$\begin{aligned} |\gamma_k\rangle_{SAB} &= \frac{1}{\|\dots\|}\ (P_k \otimes \mathbb{1}_B)\ |\psi\rangle_S \otimes \frac{1}{\sqrt{2}} \left(|0_A 0_B\rangle + |1_A 1_B\rangle \right) \\ &= \frac{1}{\|\dots\|}\ (|\phi_k\rangle\langle\phi_k|_{SA} \otimes \mathbb{1}_B)\ |\psi\rangle_S \otimes \frac{1}{\sqrt{2}} \left(|0_A 0_B\rangle + |1_A 1_B\rangle \right), \end{aligned}$$

because the initial global state is pure. We will compute the final global state explicitly for the first outcome, $k=0$. Remember that we can expand $|\psi\rangle_S$ in the computational basis, $|\psi\rangle_S = \alpha|0\rangle_S + \beta|1\rangle_S$. This gives us

$$\begin{aligned}
|\gamma_0\rangle_{SAB} &= \frac{1}{\|\ldots\|}\left(|\phi_0\rangle\langle\phi_0|_{SA}\otimes \mathbb{1}_B\right)\left(\alpha|0\rangle_S+\beta|1\rangle_S\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B\right)\\
&= \frac{1}{\|\ldots\|}\left[\frac{1}{2}\left(|0\rangle_S|0\rangle_A+|1\rangle_S|1\rangle_A\right)\left(\langle 0|_S\langle 0|_A+\langle 1|_S\langle 1|_A\right)\otimes\left(|0\rangle\langle 0|_B+|1\rangle\langle 1|_B\right)\right]\\
&\qquad\qquad \left(\alpha|0\rangle_S+\beta|1\rangle_S\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B\right)\\
&= \frac{1}{\|\ldots\|}\frac{1}{2}\left(|000\rangle\langle 000|+|001\rangle\langle 001|+|000\rangle\langle 110|+|001\rangle\langle 111|+|110\rangle\langle 000|+|111\rangle\langle 001|+|110\rangle\langle 110|+|111\rangle\langle 111|\right)\\
&\qquad\qquad \frac{1}{\sqrt{2}}\left(\alpha|000\rangle+\alpha|011\rangle+\beta|100\rangle+\beta|111\rangle\right)\\
&= \frac{1}{\frac{1}{2\sqrt{2}}\sqrt{|\alpha|^2+|\alpha|^2+|\beta|^2+|\beta|^2}}\frac{1}{2\sqrt{2}}\left(\alpha|000\rangle+\alpha|110\rangle+\beta|001\rangle+\beta|111\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left(\alpha|000\rangle+\alpha|110\rangle+\beta|001\rangle+\beta|111\rangle\right)\\
&= \frac{1}{\sqrt{2}}\left(|00\rangle_{SA}+|11\rangle_{SA}\right)\otimes\left(\alpha|0\rangle_B+\beta|1\rangle_B\right)\\
&= |\phi_0\rangle_{SA}\otimes|\psi\rangle_B.
\end{aligned}$$

The reduced state on Bob's qubit is simply $|\psi\rangle$. For anti-pedagogical purposes, we can show it explicitly by hand,

$$\begin{aligned}
\sigma_{B|X=0} &= \mathrm{tr}_{SA}\left(|\gamma_0\rangle\langle\gamma_0|_{SAB}\right)\\
&= \frac{1}{2}\mathrm{tr}_{SA}\left[\left(\alpha|000\rangle+\alpha|110\rangle+\beta|001\rangle+\beta|111\rangle\right)\left(\alpha^*\langle 000|+\alpha^*\langle 110|+\beta^*\langle 001|+\beta^*\langle 111|\right)\right]\\
&= \frac{1}{2}\left[|\alpha|^2|0\rangle\langle 0|+\alpha\beta^*|0\rangle\langle 1|+|\alpha|^2|0\rangle\langle 0|+\alpha\beta^*|0\rangle\langle 1|+\beta\alpha^*|1\rangle\langle 0|+|\beta|^2|1\rangle\langle 1|+\beta\alpha^*|1\rangle\langle 0|+|\beta|^2|1\rangle\langle 1|\right]\\
&= |\alpha|^2|0\rangle\langle 0|+\alpha\beta^*|0\rangle\langle 1|+\alpha^*\beta|1\rangle\langle 0|+|\beta|^2\\
&= (\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle 0|+\beta^*\langle 1|)\\
&=: |b_0\rangle\langle b_0| = |\psi\rangle\langle\psi|.
\end{aligned}$$

Similarly, for the other outcomes, we obtain

$$\begin{aligned}
|\gamma_1\rangle_{SAB} &= |\phi_1\rangle_{SA}\otimes|b_1\rangle_B, & |b_1\rangle &= \alpha|0\rangle-\beta|1\rangle,\\
|\gamma_2\rangle_{SAB} &= |\phi_2\rangle_{SA}\otimes|b_2\rangle_B, & |b_2\rangle &= \beta|0\rangle+\alpha|1\rangle,\\
|\gamma_3\rangle_{SAB} &= |\phi_3\rangle_{SA}\otimes|b_3\rangle_B, & |b_3\rangle &= \beta|0\rangle-\alpha|1\rangle.
\end{aligned}$$

(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?

Solution. These operations turn out to be the Pauli matrices and the identity,

$$\begin{aligned}
\mathbb{1}\,|b_0\rangle &= \begin{bmatrix}1&0\\0&1\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix}=\begin{bmatrix}\alpha\\\beta\end{bmatrix}, & Z\,|b_1\rangle &= \begin{bmatrix}1&0\\0&-1\end{bmatrix}\begin{bmatrix}\alpha\\-\beta\end{bmatrix}=\begin{bmatrix}\alpha\\\beta\end{bmatrix},\\
X\,|b_2\rangle &= \begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}\beta\\\alpha\end{bmatrix}=\begin{bmatrix}\alpha\\\beta\end{bmatrix}, & iY\,|b_2\rangle &= \begin{bmatrix}0&-1\\1&0\end{bmatrix}\begin{bmatrix}\beta\\-\alpha\end{bmatrix}=\begin{bmatrix}\alpha\\\beta\end{bmatrix},
\end{aligned}$$

Note that Bob has to know the outcome of Alice's measurement in order to choose the right operation.

(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 the reduced state of his qubit and therefore does not know which operation to apply in order to obtain $|\psi\rangle$.

Solution. If Bob does not know the outcome of the measurement, his knowledge about the state of the three qubits can be obtained by tracing out the registry X from the global state. This is done in Eq. S.1. Bob's knowledge of qubit B is obtained by tracing out S and A,

$$\begin{aligned}
\sigma_B &= \mathrm{tr}_{SA}\left(\sum_{k=0}^{3}(P_k \otimes \mathbb{1}_B)\ \rho_{SAB}\ (P_k \otimes \mathbb{1}_B)\right) \\
&= \sum_{q=0}^{3}(\langle\phi_q|_{SA} \otimes \mathbb{1}_B)\ \left(\sum_{k=0}^{3}(|\phi_k\rangle\langle\phi_k| \otimes \mathbb{1}_B)\ \rho_{SAB}\ (|\phi_k\rangle\langle\phi_k| \otimes \mathbb{1}_B)\right)(|\phi_q\rangle_{SA} \otimes \mathbb{1}_B) \\
&= \sum_{k=0}^{3}(\langle\phi_k|_{SA} \otimes \mathbb{1}_B)\ \rho_{SAB}\ (|\phi_k\rangle_{SA} \otimes \mathbb{1}_B) \\
&= \mathrm{tr}_{SA}(\rho_{SAB}) \\
&= \mathrm{tr}_{SA}\left(|\psi\rangle\langle\psi|_S \otimes \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}\,\frac{\langle 0|_A\langle 0|_B + \langle 1|_A\langle 1|_B}{\sqrt{2}}\right) \\
&= \frac{1}{2}(|0\rangle\langle 0|_B + |1\rangle\langle 1|_B) = \frac{\mathbb{1}_B}{2}.
\end{aligned}$$

This is a fully mixed state, which contains no information about which operation should be performed to recover $|\psi\rangle$.

(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,

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

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 $|\psi\rangle$.

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

Solution. We saw that, for an initial state $|\psi\rangle_S$, the teleportation protocol acts on systems SAB as

$$|\psi\rangle_S \otimes |\phi_0\rangle_{AB} \mapsto |\phi_0\rangle_{SA} \otimes |\psi\rangle_B$$

(we could also have $|\phi_k\rangle_{SA}$ as Alice's final state, but since she knows the outcome of her measurement, she can always apply a local unitary operation U_k on $|\phi_k\rangle_{SA}$ to rotate it to $|\phi_0\rangle_{SA}$).

Now we consider the more general case, where we want to transmit a mixed state ρ_S which may be correlated with a reference system, R: $\rho_S = \mathrm{tr}_R\,|\psi\rangle\langle\psi|_{RS}$. A Schmidt decomposition (QIT script, Section 4.1.5) of $|\psi\rangle$ gives

$$|\psi\rangle_{RS} = \sum_m \sqrt{\lambda_m}\ |\alpha_m\rangle_R \otimes |\beta_m\rangle_S,$$

where $\{|\alpha_m\rangle_R\}$ and $\{|\beta_m\rangle_S\}$ are the eigenstates of the reduced density matrices ρ_R and ρ_S respectively, and $\{\lambda_m\}$ the corresponding eigenvalues.

The teleportation protocol uses only linear maps (a measurement and unitary operations), and it does not act on R, so

$$|\psi\rangle_{RS} \otimes |\phi_0\rangle_{AB} = \sum_m \sqrt{\lambda_m}\ |\alpha_m\rangle_R \otimes |\beta_m\rangle_S \otimes |\phi_0\rangle_{AB} \mapsto \sum_m \sqrt{\lambda_m}\ |\alpha_m\rangle_R \otimes |\phi_0\rangle_{SA}|\beta_m\rangle_B.$$

The reduced state on RB is the original entangled state,

$$\sum_m \sqrt{\lambda_m}\ |\alpha_m\rangle_R \otimes |\beta_m\rangle_B = |\psi\rangle_{RB}.$$