Tutorial 4 (The Heisenberg uncertainty principle[1])
Suppose $|\psi\rangle$ is a quantum state and A and B are Hermitian operators. Verify that

$$4|\langle\psi|AB|\psi\rangle|^2 = |\langle\psi|\{A,B\}|\psi\rangle|^2 + |\langle\psi|[A,B]|\psi\rangle|^2, \tag{1}$$

where $\{A,B\} = AB + BA$ is the so-called *anti-commutator* of two operators.

The Cauchy-Schwarz inequality states that for any two vectors $|v\rangle$ and $|w\rangle$ it holds that

$$|\langle v|w\rangle|^2 \le \langle v|v\rangle\langle w|w\rangle. \tag{2}$$

Now let C and D be any observables. Substitute $A = C - \langle C\rangle$ and $B = D - \langle D\rangle$ into Eq. (1) and use Eq. (2) to derive the Heisenberg uncertainty principle,

$$\Delta C \Delta D \ge \frac{|\langle\psi|[C,D]|\psi\rangle|}{2}.$$

Interpret this formula.

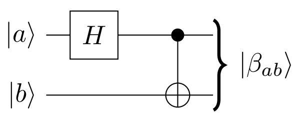
Recall that the expectation value of an observable C is $\langle C\rangle = \langle\psi|C|\psi\rangle$, and the standard deviation is defined as $\Delta C = \sqrt{\langle C^2\rangle - \langle C\rangle^2}$.

Exercise 4.1 (Bell states and superdense coding)
Recall that the *Bell states* are defined as

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

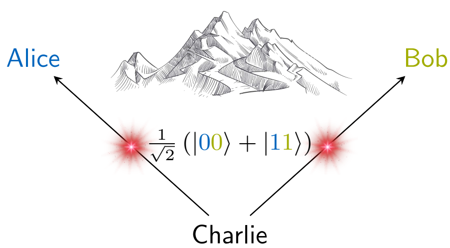
which can be summarized as $|\beta_{ab}\rangle = \frac{1}{\sqrt{2}}(|0,b\rangle + (-1)^a|1,1-b\rangle)$ for $a,b \in \{0,1\}$.

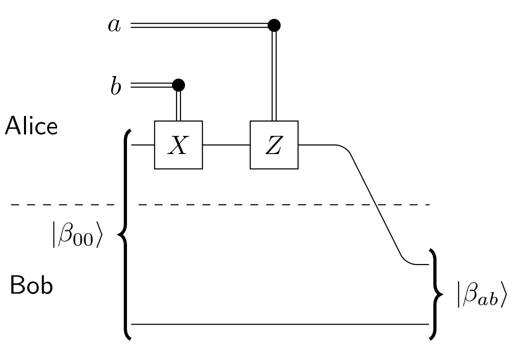
(a) Verify that the following quantum circuit creates the Bell states for inputs $|a,b\rangle$:



Note: this generalizes exercise 3.1(b). Since the circuit implements a unitary transformation of the standard basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, the Bell states form an orthonormal basis of the two qubit state space as well.

Superdense coding is a surprising use of entanglement to transmit two bits of classical information by sending just a single qubit! The setup agrees with quantum teleportation: two parties, usually referred to as Alice and Bob, live far from each other but share a pair of qubits in the entangled Bell state $|\beta_{00}\rangle$. They could have generated the pair during a visit in the past, or a common friend Charlie prepared it and sent one qubit to Alice and the other to Bob, as shown on the right.





Now Alice's task is to communicate two bits 'ab' of classical information to Bob. Alice can achieve that by applying X and/or Z gates to her qubit before sending it to Bob, depending on the information she wants to transmit: for '00', she does nothing to her qubit, for '01' she applies X, for '10' she applies Z, and for '11' she applies first X and then Z, i.e., $ZX = iY$. It turns out that the resulting states are precisely the Bell states, which Bob can distinguish by performing a measurement with respect to this basis. The diagram on the left summarizes the protocol.

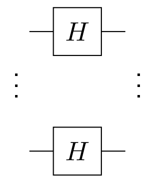
[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Box 2.4

(b) Verify for all combinations of $a, b \in \{0,1\}$ that the output of the circuit is indeed the Bell state $|\beta_{ab}\rangle$.

(c) Suppose E is an operator on Alice's qubit (e.g., $E = M_m^\dagger M_m$ in the general measurement framework, with M_m a measurement operator). Show that $\langle\beta_{ab}|E \otimes I|\beta_{ab}\rangle$ takes the same value for all four Bell states. Assuming an adversarial "Eve" intercepts Alice's qubit on the way to Bob, can Eve infer anything about the classical information which Alice tries to send?

Exercise 4.2 (Quantum parallelism and the Deutsch-Jozsa algorithm)

(a) We consider n Hadamard gates acting in parallel on n qubits, known as Hadamard transform and written as $H^{\otimes n}$. Show that, for computational basis states as input, the output is

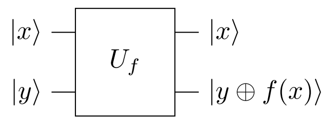


$$H^{\otimes n}\,|x_1, \dots, x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1,\dots,z_n} (-1)^{x_1 z_1 + \cdots + x_n z_n} |z_1, \dots, z_n\rangle.$$

Here the sum is over all $z \in \{0,1\}^n$. Note that this relation can be succinctly summarized as $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x \cdot z} |z\rangle$, where $x \cdot z$ is the bitwise inner product of x and z modulo 2.

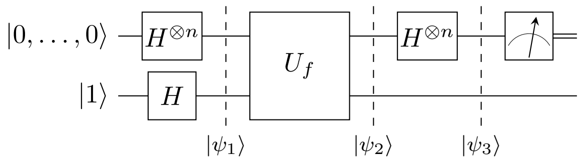
Hint: First verify that the action of the Hadamard gate on a single qubit can be represented as $H|x\rangle = \sum_{z=0}^{1} (-1)^{xz} |z\rangle / \sqrt{2}$ for $x \in \{0,1\}$.

In essence, *quantum parallelism* allows to evaluate a function $f(x)$ for many different values of x simultaneously. Here we consider functions $f : \{0,1\}^n \to \{0,1\}$, and assume that we have the unitary gate U_f acting on $n+1$ qubits as shown on the right available. With respect to the computational basis, U_f leaves the first n qubits invariant and outputs $|y \oplus f(x)\rangle$ as last qubit, where $\oplus$ is addition modulo 2.



Deutsch's problem considers functions f which are either constant or balanced, i.e., $f(x)$ is equal to 1 for half of all possible x and 0 for the other half. The task is to determine with certainty which kind a given f is. This somewhat contrived problem serves as demonstration of quantum parallelism; note that classically, at worst $2^{n-1} + 1$ function evaluations are necessary since the first 2^{n-1} evaluations may all give 0s even when f is balanced.

The *Deutsch-Jozsa algorithm* solves this problem via the following circuit:



The input is $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle \equiv |0, \dots, 0, 1\rangle$. According to (a), the state after the first Hadamard transform reads

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

(b) Argue that the state after applying U_f is given by

$$|\psi_2\rangle = U_f|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Again using (a), the state after the last Hadamard transform on the first n qubits is

$$|\psi_3\rangle = \sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} \frac{(-1)^{x \cdot z + f(x)}|z\rangle}{2^n} \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Finally, one performs a measurement of the first n qubits of $|\psi_3\rangle$ with respect to the computational basis. In case f is constant, the coefficient of $|0, \dots, 0\rangle$ is $(-1)^{f(0)}$ (since $x \cdot 0 = 0$) and thus the measurement result will be $0, \dots, 0$ with probability $|(-1)^{f(0)}|^2 = 1$. Conversely, in case f is balanced, the coefficient of $|0, \dots, 0\rangle$ is zero and thus the measurement outcome will certainly be different from $0, \dots, 0$. In summary, one can discern the two kinds of functions by a single application of U_f.