1. Revision.

(a) Imagine we have a quantum state $|\psi\rangle$ of $n$ qubits, where $|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$, and we measure the first qubit of $|\psi\rangle$ in the computational basis. What is the probability that the measurement outcome is 1, in terms of the $\alpha_x$ coefficients?

(b) What is the state of the system after the measurement?

(c) Let $M$ be the matrix defined by $M = \frac{1}{\sqrt{2}} \left( \begin{array}{cc} 1 & 1 \\ i & -i \end{array} \right)$. Is $M$ unitary?

(d) Write down the matrix corresponding to the operator $H \otimes H$, in the computational basis, where $H$ is the Hadamard operator.

2. The quantum circuit model.

(a) Consider the following quantum circuit $C$:

```
                 H
                 ———
             Z

                 ———
             H
```

i. Calculate the matrix of the unitary operation $U$ corresponding to $C$, with respect to the computational basis.

ii. Write down a quantum circuit corresponding to the inverse operation $U^{-1}$.

iii. If $C$ is applied to the initial state $|0\rangle|0\rangle$ and is followed by a measurement of each qubit in the computational basis, what is the distribution on measurement outcomes?

(b) The SWAP gate for 2 qubits is defined as $\text{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$ for $x, y \in \{0,1\}$ and is denoted by the circuit element $\bigotimes$. Show that SWAP can be implemented as a product of CNOT gates and write down the corresponding circuit.

(c) Show that a $CZ$ gate can be implemented using a CNOT gate and Hadamard gates and write down the corresponding circuit.

(d) The classical OR gate takes as input a pair of bits $x, y \in \{0,1\}$ and outputs 1 if either $x$ or $y$ is equal to 1, and 0 otherwise. Use the generic construction of reversible functions discussed in the lecture notes to write down a unitary operation on 3 qubits which corresponds to a reversible implementation of the OR gate.
3. **The Bernstein-Vazirani algorithm.**

A parity function $f_s : \{0, 1\}^n \rightarrow \{0, 1\}$, for some $s \in \{0, 1\}^n$, is a function of the form $f_s(x) = x \cdot s$, where the inner product is taken modulo 2. For example, with $n = 3$, $f_{110}(x)$ is the function $x_1 \oplus x_2$.

(a) Show that $f_s$ is a balanced function for all $s \neq 0^n$.

(b) Imagine we apply the circuit for the Deutsch-Jozsa algorithm with the oracle $U_{f_s}$. Show that the measured output is precisely the string $s$.

(c) Consider the following problem: given oracle access to a parity function $f_s$, determine $s$ using the minimal number of queries to $f_s$.

   i. Conclude from (b) that there is a quantum algorithm that solves this problem with one query to $f_s$.

   ii. Give an exact bound on the number of queries to $f_s$ required for a classical algorithm to solve the problem with certainty.

4. **Simulation of various kinds. (Optional)**

(a) Show that the phase oracle $U_f$ as defined in the lecture notes cannot be used to implement the bit oracle $O_f$ in general, even if $f$ only has 1 bit output.

(b) Imagine we are given a quantum circuit on $n$ qubits which consists of poly($n$) gates picked from the (universal) set $\{H, X, \text{CNOT}, T\}$, followed by a final measurement of all the qubits. Assume that at each step in the computation the quantum state is unentangled (i.e. is a product state of the $n$ qubits). Show that the circuit can be simulated efficiently classically: that is, there is an efficient classical algorithm for exactly sampling from the probability distribution on the final measurement outcomes.