Deutsch’s Problem:

1. Let \( f \) be a function from \( \{0,1\} \) into itself. Let \( U_f \) be the gate described in Fig. 1, where \( y + f(x) \) is computed mod2. Compute the outgoing state \( |\psi\rangle \).

2. How can the ingoing state in Fig. 1 be produced using the Hadamard gate?

3. In Fig. 2, the top left line is made of \( n \) wires in parallel, each holding a Hadamard gate. In this way this line holds a state of the tensor product \( \mathcal{H}^{\otimes n} \), if \( \mathcal{H} = \mathbb{C}^2 \), and the Hadamard gates acts like \( H^{\otimes n} \). Show that if the top left ingoing state is \( |00\cdots0\rangle \) (all bits are set to 0), then \( H^{\otimes n} \) transforms it into
This exercise consists in building the gates $U_f$ shown in Fig. 1,2. Namely the goal is to built a gate transforming $|x\rangle \otimes |y\rangle$ into $|x\rangle \otimes |y \oplus f(x)\rangle$.

1. Give the list of 0, 1-valued functions of one binary bit. For each of them propose a 2-qubit quantum circuit giving the gate $U_f$. (Hint: use only $X$ and CNOT gates.)

2. More generally how many functions $x = (x_1, \ldots, x_n) \in \{0, 1\}^n \mapsto f(x_1, \ldots, x_n) \in \{0, 1\}$ with values in $\{0, 1\}$ do exist?

3. For $y \in \{0, 1\}^n$ let $\delta_y$ be the function taking on the value 1 if $x = y$ and zero otherwise. Show that any function $f$ with values in $\{0, 1\}$ is a sum of such $\delta_y$’s.

4. Show that, if $f, g$ are two such functions, then $U_{f \oplus g}$ (see Fig. 2) can be obtained by applying successively $U_f$ and then $U_g$. (Hint: here $f(x) \oplus g(x)$ is the addition modulo 2.)

5. Shows that $\delta_0$ can be implemented by a controlled gate with an $n$ control qubit register representing $x$ and one working qubit computing $f(x)$ giving a quantum circuit for $U_{\delta_0}$.

6. Extend the previous construction to $\delta_y$. (Hint: first transform each $x_i$ for which $y_i = 1$ through an $X$-gate and apply the previous construction. Be careful to get $x$ back in the outgoing state.)

Deutsch’s oracle :

This exercise consists in building the gates $H^\otimes n$ shown in Fig. 1,2. Namely the goal is to built a gate transforming $|x\rangle \otimes |y\rangle$ into $|x\rangle \otimes |y \oplus f(x)\rangle$.

$$H^\otimes n |00 \cdots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle,$$

where $|x\rangle$ denotes the state $|x_0, \ldots, x_{n-1}\rangle$ if the bits $x_0, \ldots, x_{n-1}$ are the digits of the binary decomposition of $x \in [0, 2^n - 1]$. (Hint: consider the cases $n = 2, 3$ first and generalize.)

4. More generally, show that, for any family of $n$-bits

$$H^\otimes n |x_0, \ldots, x_{n-1}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_0, \ldots, z_{n-1}} (-1)^{x_0z_0 + \cdots + x_{n-1}z_{n-1}} |z_0, \ldots, z_{n-1}\rangle.$$

5. Consider the circuit in Fig. 2 with $n = 1$. Compute the resulting states $|\psi_i\rangle$ for $i = 0, 1, 2, 3$.

Show that $|\psi_i\rangle$ can be expressed as $\pm |f(0) + f(1)| |0\rangle - |1\rangle| / \sqrt{2}$.

6. Let now $n$ be arbitrary and let $f : x \in [0, 2^n - 1] \mapsto f(x) \in \{0, 1\}$ be some function prepared by Bob. Starting on the left from the ingoing state $|00 \cdots 01\rangle = |0\rangle^\otimes n |1\rangle$, compute the resulting states $|\psi_i\rangle$ for $i = 0, 1, 2, 3$. (Hint: it will be convenient to use the notation $x \cdot z$ to represent the sum $x_0z_0 + \cdots + x_{n-1}z_{n-1}$.)

7. Show that the amplitude of the outgoing state along the direction of $|0\rangle^\otimes n$ (for the top line) is given by $\sum_x (-1)^{f(x)} / 2^n$.

8. Bob has promised to Alice to choose $f$ with the property that, either $f$ is constant (namely $f(x) = 0$ for all $x$’s or $f(x) = 1$ for all $x$’s) or it takes on values 0 as many times than 1. Show that by measuring the final state along the direction of $|0\rangle^\otimes n$ (for the top line) Alice can figure out in one measurement whether $f$ is constant or not.

9. In a classical computer Alice may send Bob only one value of $x$ at a time. How many time must she, classically, query Bob to get the same result? Compare the performances of the two computers.
Quantum Fourier transform:

1. A *swap* is a 2-qubit gate which transforms the ingoing state \(|xy\rangle = |x\rangle \otimes |y\rangle\) into the outgoing state \(|yx\rangle = |y\rangle \otimes |x\rangle\), namely it exchanges the content of the two lines of the corresponding circuit. Compute the corresponding unitary matrix.

2. By using only three \texttt{cnot} gates, build a 2-qubit circuit which *swaps* the two qubits.

3. Describe the circuit giving the quantum Fourier transform algorithm for 4 qubits.

4. Give the expression of the unitary matrix described by the previous of the Fourier transform circuit.

Binary Fourier transform:

In this section, \(\mathbb{Z}_2\) is the additive group \(\{0,1\}\) with two elements. For \(n > 1\) an integer, let \(G\) denote the group \(\mathbb{Z}_2^n\) of families \(x = (x_1,\ldots,x_n)\) with \(x_k \in \mathbb{Z}_2\) endowed with the addition \(x+y = (x_1+y_1,\ldots,x_n+y_n)\). It will be convenient to use the following notation \(x \cdot y = x_1y_1 + \cdots + x_ny_n\).

1. Give the definition of a *character* of \(G\). Give the definition of the *dual group* \(G^*\). Give the definition of the Hilbert space \(\ell^2(G)\). (Hint: namely define it as a set, then as a complex vector space and give the expression of the inner product.)

2. Let \(\chi\) be a character of \(G\). Show that for every \(x \in G\), \(\chi(x) = \pm 1\). (Hint: compute the square and use the definition of a character.)

3. Given \(y \in G\), show that the map \(\chi_y : x \in G \mapsto \chi_y(x) = \prod_i (-1)^{x_iy_i} = (1)^{x \cdot y}\) is a *character* of \(G\).

4. Let \(e_i \in G\) be the element with 1 at coordinate \(i\) and 0 at all other coordinates. Show that any \(x \in G\) can be written in a unique way as \(x = x_1e_1 + \cdots + x_ne_n\). Conclude that, if \(\chi\) is a character of \(G\), then there is a unique \(y \in G\) such that \(\chi = \chi_y\). (Hint: define \(y_i\) from the value of \(\chi(e_i)\).)

5. Show that the map \(y \in G \mapsto \chi_y \in G^*\) is a group isomorphism. (Hint: it transforms the addition in \(G\) into the multiplication in \(G^*\) and it is a bijection.)

6. Show that \(|y\rangle := 2^{-n/2}\chi_y\) defines an orthonormal basis of \(\ell^2(G)\).

7. Let \(f \in \ell^2(G)\) then compute \(\hat{f}(y) = \langle y|f\rangle\) and show that it is the Fourier transform of \(f\). Show that the inverse Fourier transform is obtained from the decomposition \(f = \sum_y \hat{f}(y)|y\rangle\).

8. Compute \(\|f\|^2\) (norm in \(\ell^2(G)\)) and conclude that

\[
\sum_{x \in G} |f(x)|^2 = \sum_{y \in G} |\hat{f}(y)|^2.
\]