We define the following two operations for every \( x, y \in \{0, 1\}^n \)

\[ x \oplus y = (x_1 \oplus y_1, \ldots, x_n \oplus y_n), \quad \text{and} \quad x \odot y = (x_1 \cdot y_1) \oplus \cdots \oplus (x_n \cdot y_n), \]

where \( 0 \oplus 0 = 1 \oplus 1 = 0 \) and \( 0 \oplus 1 = 1 \oplus 0 = 1 \).

Let \( H \) be the Hadamard transform that maps \( |b\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle) \), for \( b = 0, 1 \). Let \( H \otimes^n \) be the transformation that applies \( H \) in each of the qubit of an \( n \)-qubit. You can use without justifying that for every \( x \in \{0, 1\}^n \)

\[ H \otimes^n |x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0, 1\}^n} (-1)^{x \odot y} |y\rangle. \]

**Question 1** Show that

\[ H \otimes^n \left( \frac{1}{2^{n/2}} \sum_{y \in \{0, 1\}^n} (-1)^{x \odot y} |y\rangle \right) = |x\rangle. \]

**Question 2** For any value \( i \in \{1, \ldots, n\} \), explain how to construct a quantum circuit \( A_i \) that maps \( |0\log^n 0\rangle |0\rangle \mapsto |0\log^n 0\rangle |0\rangle \) and \( |0\log^n 1\rangle |i\rangle \mapsto |i\rangle |1\rangle \).

Assume from now that \( x \in \{0, 1\}^n \) is some input given by a quantum unitary \( O_x \) such that

\[ O_x |i\rangle \mapsto \begin{cases} (-1)^x |i\rangle & \text{if } 1 \leq i \leq n, \\ |i\rangle & \text{if } i = 0. \end{cases} \]

Also assume that other than by using \( O_x \) it is impossible to learn anything about \( x \).

**Question 3** Give a quantum circuit \( B \) that realizes the map \( |y\rangle \mapsto (-1)^{x \odot y} |y\rangle \), for \( y \in \{0, 1\}^n \), using at most \( n \) times the unitary \( O_x \). Your circuit can use auxiliary qubits initialized to \( |0\rangle \) and that come back to \( |0\rangle \) at the end of the computation. (Therefore, to be more precise, the map is in fact \( |y\rangle |0^\ell\rangle \mapsto (-1)^{x \odot y} |y\rangle |0^\ell\rangle \), for some integer \( \ell \) of your choice.)

Compute the output of your circuit when the input state is \( \frac{1}{2^{n/2}} \sum_{y \in \{0, 1\}^n} |y\rangle \).

Last, complete the circuit with some gates other than \( O_x \), such that the final output is \( |x\rangle \).

Call \( C \) this final circuit.
For \( y \in \{0, 1 \}^n \), we denote by \( \| y \| = \sum_{i=1}^{n} y_i \) the Hamming weight of \( y \), and by \( I(y) = (i_1, \ldots, i_{\| y \|}) \) the increasing sequence of indices where \( y \) has bit value 1, that is such that \( i_1 < \cdots < i_{\| y \|} \) and \( y_{i_j} = 1 \) for \( j = 1, \ldots, \| y \| \).

**Question 4** Fix some integer \( k \leq n \). Justify why there exists a quantum circuit \( D_k \) that realizes the map
\[
|y\rangle \mapsto \begin{cases} 
|y\rangle|I(y), 0^{k-\| y \|}\rangle & \text{if } \| y \| \leq k, \\
|y\rangle|0^k\rangle & \text{if } \| y \| > k,
\end{cases}
\]
where \( y \in \{0, 1\}^n \), and with possibly auxiliary qubits as in Question 3.

**Question 5** Fix some integer \( k \leq n \). Give a quantum circuit \( E_k \) that uses at most \( k \) times the unitary \( O_x \) to realize the map
\[
|y\rangle \mapsto \begin{cases} 
(-1)^{x \cdot y} |y\rangle & \text{if } \| y \| \leq k, \\
|y\rangle & \text{if } \| y \| > k,
\end{cases}
\]
where \( y \in \{0, 1\}^n \), and with possibly auxiliary qubits as in Question 3.

Let \( S_k = \{ y \in \{0, 1\}^n : \| y \| \leq k \} \), \( M_k = \sum_{i=0}^{k} \binom{n}{i} \) and \( |\psi_k\rangle = \frac{1}{\sqrt{M_k}} \sum_{y \in S_k} |y\rangle \). Without any justification you can use that \( |\psi_k\rangle \) has norm 1, and that \( M_k \geq 0.95 \times 2^n \) when \( k \geq \frac{n}{2} + \sqrt{n} \).

**Question 6** Use circuit \( C \) of Question 2 with input state \( |\psi_k\rangle \). Prove that the measure of the output gives \( x \) with probability \( M_k/2^n \). What happens if \( B \) is replaced by \( E_k \)? Conclude that \( x \) can be learned with bounded error 5\% and using at most \( (\frac{n}{2} + \sqrt{n}) \) times the unitary \( O_x \).

**Part II**

We define the following communication problems:

- \( IP : \{0, 1\}^n \times \{0, 1\}^n \longrightarrow \{0, 1\} \) defined by \( IP(x, y) = \sum_{i=1}^{n} x_i \cdot y_i \mod 2 \) (the inner product of \( x \) and \( y \), viewed as \( n \)-dimensional vectors over \( Z_2 \)).

- \( SEND \), where Alice has a string \( x \in \{0, 1\}^n \); at the end of the protocol, Bob produces \( x \) as his output.

**Question 7**

1. Out of the \( 2^n \) inputs \( (x, y) \in \{0, 1\}^n \times \{0, 1\}^n \) to \( IP \), show that \( 2^{2n}/2 \) of them evaluate to 0.

2. For any set of vectors \( A \) in \( Z_2^n \), denote by \( A' \) the span of the elements in \( A \) (the span of \( A \) is the subspace composed of all vectors that can be obtained as linear combinations of vectors in \( A \)). Show that if \( A \times B \) is a rectangle such that \( \forall (x, y) \in A \times B, f(x, y) = 0 \), then it is also the case that \( \forall (x, y) \in A' \times B', f(x, y) = 0 \).
3. Let $A \times B$ be a rectangle such that $\forall (x, y) \in A \times B, f(x, y) = 0$. Give an upper bound on $\dim(A') + \dim(B')$.

4. Give an upper bound on the cardinality of any such rectangle $A \times B$. How many rectangles are necessary to cover all the 0 values in the communication matrix of $IP$?

5. Give a lower bound on the deterministic communication complexity of $IP$.

6. Generalize the previous result to any function $f : X \times Y \rightarrow Z$. Let $\text{rect}_z(f)$ be the size of the largest rectangle $R = A \times B$ such that $\forall (x, y) \in A \times B, f(x, y) = z$. Prove that $\forall f, D(f) \geq \max_{z \in Z} \text{rect}_z(f)$.

**Question 8** Recall that

$$O_x|i\rangle \mapsto \begin{cases} (-1)^{x_i}|i\rangle & \text{if } 1 \leq i \leq n, \\ |i\rangle & \text{if } i = 0. \end{cases}$$

Construct a circuit that computes the mapping $U_x|i\rangle|b\rangle \mapsto |i\rangle|x_i \oplus b\rangle$, using a single call to the unitary $O_x$. Hint: define a circuit control-$O_x$ and start by applying control-$O_x$ to an appropriate state.

**Question 9** Let us consider a restricted version of $IP$ where there is a promise that input $y$ has small Hamming weight, that is, $\|y\| \leq k$. Based on the circuits in Part I, give an efficient quantum protocol for this restricted version of $IP$, and give its communication complexity in terms of $n$ and $k$.

You may use without proof that the quantum communication complexity of $SEND$ is

$$Q(SEND) \geq \lceil \frac{n}{2} \rceil.$$ 

**Question 10** Show that if there is a protocol for $IP$ that uses $t$ qubits of communication, then it can be used to obtain a protocol for $SEND$ that uses the same number of qubits. Give a linear lower bound (including constants) on the quantum communication of $IP$. 