1. Given an oracle that outputs the function: $f(x, y) = \sum_{ij} a_{ij}x_iy_j$, where x and y are n bit vectors, and A is an nxn boolean matrix. Show that there is a quantum algorithm that reconstructs A in $O(n)$ queries. Show that n queries are necessary.

   Now suppose the oracle outputs: $f(x) = \sum_{ij} a_{ij}x_ix_j$. Show that you can still reconstruct A using $O(n)$ queries.

2. Use the BV algorithm to show that the communication complexity of the inner product function is $\Omega(n)$. i.e. show that if Alice has input $u \in \{0, 1\}^n$, and Bob has input $v \in \{0, 1\}^n$, and they wish to compute $u \cdot v \bmod 2$, then they must exchange $\Omega(n)$ bits of information.

3. A pure state is separable (unentangled) if it can be written as a tensor product of states of each qubit. A mixed state is separable if it can be written as a probability distribution over separable pure states.

   (a) Consider the mixed state: $Prob$ $1/2 : 1/\sqrt{2}(|00\rangle + |11\rangle$
   $Prob$ $1/2 : 1/\sqrt{2}(|01\rangle + |10\rangle$
   .
   Show that even though this state does not appear to be a separable state as written, it is in fact separable.

   (b) Suppose that $H \subseteq Z_2^n$. To solve the hidden subgroup problem, we creat the mixed state which is a uniform superposition over a random coset of H. Give an example of a subgroup H where each superposition in this mixture is highly entangled.

   (c) Now show that for H, a uniformly random coset state is a separable mixed state.
   More generally it is not known whether separable mixed state quantum computation is efficiently simulable classically or whether it might be as powerful as BQP. In this model, at each step the state of the computer is a separable mixed state.

4. Prove that $QMA_{\log n} = BQP$. i.e. show that if there are only $\log n$ qubits in the quantum proof, then the verifier can only accept languages in BQP.

5. Show how to efficiently implement the quantum walk operator: the reflection about the subspace X spanned by the states $\phi_x = \sum_y \sqrt{p_{x,y}}|x\rangle\,|y\rangle$.

6. Suppose you are given a quantum circuit C for a language $L \in BQP$. How would you boost the success probability of C to $1-2^{-k}$. Assume that C uses $n+m$ qubits on inputs of size n. Can you achieve the desired boosting with a quantum circuit that operates on $n + m + O(k)$ qubits?

   One consequence of this fact is that $BQP^{BQP} = BQP$.