1. Alice is given as input a random bit a_{in} and Bob a random bit b_{in}. Without communicating with each other, Alice and Bob wish to output bits a_{out} and b_{out} respectively such that $a_{in} \cdot b_{in} = a_{out} + b_{out} \ (mod\ 2)$. Prove that any classical protocol that Alice and Bob follow has success probability at most $3/4$. Hint: you should consider both deterministic and non-deterministic strategies. For a non-deterministic strategy, Alice and Bob could, e.g., independently flip coins to decide whether to output 0 or 1. Or they could decide to use non-equal probabilities for outputting 0 or 1. Use this strategy with general probabilities - e.g., p_A and p_B for Alice and Bob to output 1, respectively, given input 0, and correspondingly, probabilities p'_A and p'_B for them to output 1 given input 1 - to construct the corresponding probability of success in such a non-deterministic strategy. This must then be maximized.

2. Write the 4×4 matrix of the unitary operation on two qubits resulting from performing a Hadamard transform on the first qubit and a phase flip on the second qubit (a phase flip is a one-qubit gate that takes $|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $-|1\rangle$).

3. Prove that the Bell state $|\psi^-\rangle$ is rotationally invariant: i.e. $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|vv^\perp\rangle - |v^\perp v\rangle)$, where $|v\rangle$ is *any* unit vector and $|v^\perp\rangle$ the unit vector perpendicular to $|v\rangle$ (i.e. $|v\rangle$ and $|v^\perp\rangle$ are basis vectors in an arbitrary orthornormal basis).

4. Give a quantum circuit that outputs the four Bell states $|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^-\rangle$ on input of the four basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (not necessarily in the same order), verifying the circuit explicitly for each case.
   Hint: Experiment with putting together a CNOT-gate and various single-qubit gates. You should be able to do this with very simple circuits, but you will need at least one CNOT-gate (or generally at least one two-qubit gate, try to think of why this is the case).