1. Give a linear time quantum algorithm for the following problem: given n numbers $x_1, \ldots, x_n$, decide whether they are all distinct.

2. Let $\mathcal{A}$ be a quantum algorithm for some language $L \in BQP$. Suppose that there is a quantum algorithm $\mathcal{B}$ that correctly decides membership in L' in polynomial time, provided it is allowed oracle access to L (i.e. it is allowed to make queries, in superposition, about whether $x \in L$). We would like to claim that $\mathcal{B}$ can then call $\mathcal{A}$ as subroutine, thus yielding a polynomial time quantum algorithm for L'. The difficulty in doing this is that $\mathcal{A}$ might use scratch space during its computation, and the contents of that scratch space might prevent the desired quantum interference when $\mathcal{A}$ is called as a subroutine. Prove that any algorithm $\mathcal{A}$ can be modified into a clean algorithm $\mathcal{C}_\epsilon$with the following property: on input x, $\mathcal{C}_\epsilon$ outputs $|x\rangle\,|L(x)\rangle$ with amplitude squared at least $1-\epsilon$.

3. An (n, m, p) quantum random access code is a way of encoding n classical bits $x_1, \ldots, x_n$ into m quantum bits (where $m < n$) such that any single bit x_i can be recovered with error probability at most p by performing a suitably chosen measurement on the m quantum bits. Ideally we would like m to be much smaller than n. But why would this not contradict Holevo's theorem, which says that n quantum bits are necessary to transmit n classical bits? The hope is that the measurement to determine x_i might disturb the quantum state of the m qubits sufficiently to prevent any possibility of determining the remaining bits of x, thus making Holevo's bound inapplicable.

   (a) Prove that the following four states of a single qubit $cos\theta|0\rangle + sin\theta|1\rangle$ for $\theta = \pi/8, 3\pi/8, 5\pi/8, 7\pi/8$ can be used to create a $(2, 1, sin^2\pi/8)$ quantum random access code.

   (b) Prove that if there is an (n, m, p) random access code for some constant p, then there is also an $(\Omega(n/logn), m, 1/poly(n))$ code.

   (c) Prove that any (n, m, p) quantum random access code for constant p must have $m = 2^{\Omega(n/logn)}$. Hint: Use the hybrid argument and Holevo's bound.

4. A pure quantum state on n qubits is said to be separable or unentangled if it can be written as a tensor product of single qubit states. A mixed state is said to be unentangled if it is a probability distribution over separable pure states. However, since different mixtures can be equivalent (i.e. have the same density matrix) - thus a (mixed) quantum state that looks entangled, might actually be separable, since it might have an equivalent representation as a probability distribution over separable pure states.

   (a) Prove that the mixed state $|00\rangle + |11\rangle$ with probability 1/2 and $|01\rangle + |10\rangle$ with probability 1/2 is a separable mixed state.

   (b) Challenge: Prove that the following state is separable: let $C \subseteq Z_2^n$ be a subgroup of the group Z_2^n. Consider a uniform mixture of coset states $|C + x\rangle$. Prove that this is a separable mixed state.