1. The uncertainty principle bounds how well a quantum state can be localized simultaneously in the standard basis and the Fourier basis. In this question, we will derive an uncertainty principle for a discrete system of n-qubits.

   Let $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$ be the state of an n-qubit system. A measure of the spread of $|\psi\rangle$ is $S(|\psi\rangle) \equiv \sum_x |\alpha_x|$. For example, for a completely localized state $|\psi\rangle = |y\rangle$ ($y \in \{0,1\}^n$), the spread is $S(|\psi\rangle) = 1$. For a maximally spread state $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$, $S(|\psi\rangle) = 2^n \cdot \frac{1}{\sqrt{2^n}} = \sqrt{2^n}$.

   a) Prove that for any quantum state $|\psi\rangle$ on n qubits, $S(|\psi\rangle) \le 2^{n/2}$. (Hint: use the Cauchy-Schwarz inequality,$\langle v | w \rangle \le \|v\| \cdot \|w\|$.)

   b) Suppose that $|\alpha_x| \le a$ for all x. Prove that $S(|\psi\rangle) \ge \frac{1}{a}$. (Hint: think about normalization....)

   c) In Problem Set 3 you showed that $H^{\otimes n}|x\rangle = \sum_y (-1)^{x\cdot y} |y\rangle$ ($x \cdot y \equiv \sum_{i=1}^n x_i y_i$). Hence we can obtain the action of $H^{\otimes n}$ on $|\psi\rangle$ as

   $$H^{\otimes n}|\psi\rangle = \sum_x \beta_x |x\rangle, \text{ where } \beta_x = \frac{1}{2^{n/2}} \sum_y (-1)^{x\cdot y} \alpha_y.$$

   Use this to prove that for all y, $|\beta_y| \le \frac{1}{2^{n/2}} S(|\psi\rangle)$. (Hint: use the triangle inequality.)

   d) Prove the uncertainty relation $S(|\psi\rangle) S(H^{\otimes n}|\psi\rangle) \ge 2^{n/2}$. Justify why it makes sense to call this an uncertainty relation.

2. Consider two qubits interacting with the Hamiltonian

   $$H_I = g\sigma_z^{(1)} \otimes \sigma_2^{(2)}.$$

   This is referred to as an Ising interaction and is a typical interaction between physical spins, e.g., between nuclear spins in liquids.

   Show that $X^{(2)} U(t) X^{(2)} = U^{-1}(t)$, where $U(t) = e^{-iH_I t}$.

   This result implies that $X^{(2)} U(t) X^{(2)} U(t) = 1$: the single qubit operations have effectively removed the interaction between the two qubits. This is referred to as 'refocusing' and can be used to remove undesired time evolution of interacting qubits when the interaction cannot be switched off.

3. This problem illustrates some of the issues about reversible computing touched on in Lecture 10.

   a) Write a quantum circuit for the following sequence of operations on two qubits: NOT gate on qubit 1, CNOT on qubits 1 and 2 (with qubit 1 the control. Now add a third, ancilla qubit which is assumed to be initialized to 0. Add to the circuit whatever gate is required to copy the second qubit output of the previous circuit to the ancilla qubit. Evaluate the full three-qubit output of this circuit for input state $|010\rangle$. Can you now extend the circuit to return the first two qubits to their original state, leaving the ancilla qubit unchanged? If yes, do so, if no, explain why not.

   b) Write a quantum circuit for the following sequence of operations on two qubits: Hadamard gate on qubit 1, CNOT on qubits 1 and 2 (with qubit 1 the control. Now add a third, ancilla qubit which is assumed to be initialized to 0, and add to the circuit whatever gate is required to copy the output of the previous circuit to the ancilla qubit. Evaluate the output of this circuit for input state $|010\rangle$. Can you now extend the circuit to return the first two qubits to their original state, leaving the ancilla qubit unchanged? If yes, do so, if no, explain why not.

4. This problem re-examines the question of whether there can be faster than light communication by an EPR device (you already know the answer....). Suppose you are given the two-electron total-spin 0 state $|\psi_-\rangle$ from the previous problem, and you have some way of separating the two electrons and sending them off to experimenters A and B. Experimenter A has a choice to measure x or z component of the spin of electron I. Electron II enters a multiplying device after A has performed a measurement on electron I. This mulitplying device produces a burst of N electrons all in exactly the same spin state as the single input electron. These N electrons are then examined by experimenter B with a Stern-Gerlach apparatus that measures the x component of spin.

   There are now 2 possibilities:

   a) A measures x component, so B receives and measures either N $S_x = +1/2$ or N $S_x = -1/2$ electrons.

   b) A measures z component, so the multiplier will have as input either an $S_z = +1/2$ electron or an$S_z = -1/2$ electron, each with probability 1/2. These are multiplied to N, and B then measures on average N/2 $S_x = +1/2$ electrons and N $S_x = -1/2$ electrons.

   So if B gets only $S_x = +1/2$ or only $S_x = -1/2$ values on measurement, he/she can conclude that A made an x measurement, whereas if B gets both $S_x = +1/2$ and $S_x = -1/2$ on measurement he/she concludes that A made a y measurement. This implies that B can find out which measurement A made, without receiving any information from A, i.e., superluminal communication appears to have occurred. What is the flaw in this argument? Hint: examine the multiplier closely.