**QUANTUM COMPUTATION - FALL 2006 - EXERCISE 2**

**Due: 7/12/05. Submition in triplets, to Ido's mailbox in Ross.**

## 1. Bell Basis

The Bell states are:

$$\begin{aligned} \left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ \left|\Phi^-\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ \left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ \left|\Psi^-\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}$$

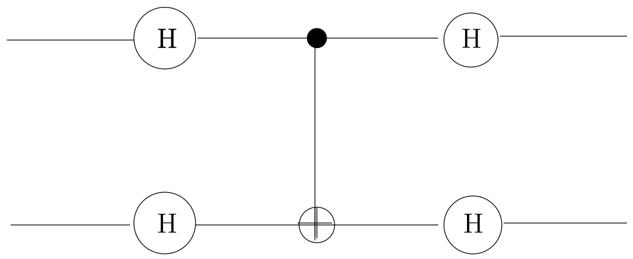
Find a unitary matrix $U$, that permutes the Bell states as follows:

$$\left|\Phi^+\right\rangle \to \left|\Phi^-\right\rangle \to \left|\Psi^+\right\rangle \to \left|\Psi^-\right\rangle \to \left|\Phi^+\right\rangle$$

(i.e. $U\left|\Phi^+\right\rangle = \left|\Phi^-\right\rangle$, etc.).

## 2. Quantum Circuits

Calculate what the following circuit does on input standard basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$:




Can you describe the combined operation in a meaningful way?

## 3. GHZ Game

Consider the GHZ (Greenberger- Horne- Zeilinger) state, of three qubits:

$$\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$

Suppose that three parties, Alice, Bob and Charlie, are given three random bits $X_A, X_B, X_C$, respectively, with the constraint $X_A \oplus X_B \oplus X_C = 0$. They have to output three bits, $a, b, c$, such that $a \oplus b \oplus c = X_A \vee X_B \vee X_C$. Show that if Alice, Bob and Charlie share a GHZ state, then this can be done with certainty (i.e with probability 1). **Hint:** you will need the Hadamard matrix,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

which takes

$$\begin{aligned} |0\rangle &\rightarrow |+\rangle \\ |1\rangle &\rightarrow |-\rangle . \end{aligned}$$

## 4. Circuits With Erroneous Gates

Let $Q$ be a quantum circuit with $m$ gates, $G_1, \ldots, G_m$, and let $Q'$ be a circuit which we get by replacing in $Q$ the gate $G_i$ by the gate $G'_i$, such that for every $i$ $\| G'_i - G_i \| \leq \frac{\epsilon}{m}$. Show that for every $|\alpha\rangle$ we have $\| Q |\alpha\rangle - Q' |\alpha\rangle \| \leq \epsilon$.

## 5. Universal Reversible Computation

5.1. Show that the Toffoli gate is a universal gate with respect to reversible classical computation.

5.2. Show that there is no set of 2 bit gates which is universal with respect to reversible classical computation.

## 6. Order Of Application Of Gates Within A Circuit

A quantum circuit is a directed graph, which contains no cycles, and in which each node represents a unitary gate from some universal set of unitary gates. It has inputs (some of which may be constant states) and outputs (i.e., marked qubits to be measured at the end.)

Show that the order in which the gates are operated on the input state of the circuit does not affect the final output state of the circuit, as long as this order corresponds to a topological order of the nodes in the graph.