Quantum Computing - Problem Set 1

Mateus de Oliveira Oliveira

School of Computer Science and Communication
KTH Royal Institute of Technology, 100-44, Stockholm, Sweden
mdeoliv@kth.se

1 Tensor Product

Let A, B and C be $k \times k$ matrices. Prove the following:

1. $cA \otimes B = A \otimes cB = cA \otimes B$
2. $A \otimes (B \otimes C) = (A \otimes B) \otimes C$.
3. $A \otimes B$ is not necessarily equal to $B \otimes A$.
4. $(A \otimes B)(v \otimes w) = (Av) \otimes (Bw)$
5. $(\otimes_{i=1}^{n} A_i)(\otimes_{i=1}^{n} v_i) = \otimes_{i=1}^{n}(A_i v_i)$
6. Let $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Write down the matrix representing $H^{\otimes 2}$ and $H^{\otimes 3}$. Give an explicit formula for the element i, j of the matrix $H^{\otimes n}$, where $i, j \in \{0,1\}^n$.

2 Dirac's Notation

Let A, B, C be matrices in $\mathbb{C}^{n \times n}$ and let $|0\rangle = (1, 0, ..., 0)^T$, $|1\rangle = (0, 1, 0, ..., 0)^T$, ... Then a vector in $\mathbb{C}^n$ can be written as $|v\rangle = \sum_i v_i |i\rangle$ and a matrix $A \in \mathbb{C}^{n \times n}$ as $A = \sum_{ij} a_{ij} |i\rangle\langle j|$.

- Prove that the identity $(\langle\varphi|\langle\psi|)(|\varphi'\rangle|\psi'\rangle) = \langle\varphi|\varphi'\rangle\langle\psi|\psi'\rangle$ is valid for any quantum states $|\varphi\rangle, |\varphi'\rangle, |\psi\rangle, |\psi'\rangle$. This identity was used in the proof of the no-cloning Theorem.
- Rewrite the proofs of items 1,2 and 4 of the last question using the bracket notation.
- Prove using Dirac's notation: For any orthonormal basis $|\phi_1\rangle, |\phi_2\rangle, ..., |\phi_n\rangle$ of $\mathbb{C}^n$ we have that $\sum_i |\phi_i\rangle\langle\phi_i| = I$.

3 Reversible Quantum Computation

The second postulate of quantum mechanics states that any closed physical system evolves according to a unitary transformation. This fact in particular implies that if we wish to compute non-injective functions using quantum computers, first we need to make them reversible. The goal of this question is to show that for any function $f : \{0,1\}^n \to \{0,1\}$ there is a quantum circuit that takes the state $|x\rangle|0\rangle$ and sends it to the state $|x\rangle|f(x)\rangle$. We will use two facts: first that any boolean function can be computed by a classical circuit consisting only of OR, AND and NOT gates. Second there exists a gate, the Toffoli gate, that sends the state $|a\rangle_1|b\rangle_1|c\rangle_1$ into the state $|a\rangle_1|b\rangle_1|c \oplus ab\rangle_1$.

1. Show how to simulate the gates OR, AND and NOT using the Toffoli gate.
2. Show that for any function $f : \{0,1\}^n \rightarrow \{0,1\}$ there is a quantum circuit that takes the state $|x\rangle_n|0\rangle_1|0\rangle_m$ and sends it to the state $|x\rangle_n|f(x)\rangle_1|garbage(x)\rangle_m$ where $garbage(x)$ is an irrelevant string on m bits generated during the computation.
3. Show that using the circuit of the previous item two times, plus one $CNOT$ gate, and one additional wire one can get rid of the garbage. In other words, there is a circuit that sends $|x\rangle_n|0\rangle_1|0\rangle_m|0\rangle_1$ into $|x\rangle_n|0\rangle_1|0\rangle_m|f(x)\rangle_1$.

4 Playing With States

The bell states are defined as

$$|\Psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\Psi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\Phi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\Phi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

1. Use the gates H, X and $CNOT$ to prepare each of the Bell states from the state $|00\rangle$.
2. Starting from the state $|000\rangle$, prepare the GHZ state $\frac{|000\rangle+|111\rangle}{\sqrt{2}}$.
3. Starting from the state $|000\rangle$, prepare the state

$$|W\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}$$

   using only $CNOT, H$ and projective measurements. Hint: Consider a function $f : \{0,1\}^3 \rightarrow \{0,1\}$ such that $f(001) = f(010) = f(100) = 1$ and $f(x) = 0$ for other strings in $\{0,1\}^3$.

5 Implications of Efficient Cloning

Assume you live in cloneland, a universe in which cloning quantum states is possible. In other words assuming that there is an efficient process CLONE that takes a quantum state $|\psi\rangle|0\rangle$ and transforms it into a state $|\psi\rangle|\psi\rangle$ for an arbitrary state $|\psi\rangle$ on n qubits. The goal of this question is to prove that life is easy for clonelanders.

1. Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a function given as a black box such that there exists a unique x for which $f(x) = 1$. Using the process CLONE, show how to determine x with high probability.

2. The requirement that f has a unique solution x for which $f(x) = 1$ is not essential. Assume that f has k solutions. How faster can you find such an x for which $f(x) = 1$?
3. Assume that $f_n : \{0,1\}^n \to \{0,1\}$ is a sequence of functions such that f_n can be computed by a circuit of size $p(n)$ for some polynomial p. Argue that clonelanders can solve NP-hard problems.