Quantum Computing Exercises # 3

Ronald de Wolf

Feb 15, 2011
(to be handed in before or at the start of the lecture on Feb 22)

1. Prove that an EPR-pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is an *entangled* state, i.e., that it cannot be written as the tensor product of two separate qubits.

2. Show that every unitary one-qubit gate with real entries can be written as a rotation matrix, possibly preceded and followed by Z-gates. In other words, show that for every 2×2 real unitary U, there exist signs $s_1, s_2, s_3 \in \{1, -1\}$ and angle $\theta \in [0, 2\pi)$ such that
$$U = s_1 \begin{pmatrix} 1 & 0 \\ 0 & s_2 \end{pmatrix} \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & s_3 \end{pmatrix}$$

3. Suppose we run Simon's algorithm on the following input x (with $N = 8$ and hence $n = 3$):
$$x_{000} = x_{111} = 000$$
$$x_{001} = x_{110} = 001$$
$$x_{010} = x_{101} = 010$$
$$x_{011} = x_{100} = 011$$
Note that x is 2-to-1 and $x_i = x_{i \oplus 111}$ for all $i \in \{0,1\}^3$, so $s = 111$.
   (a) Give the starting state of Simon's algorithm.
   (b) Give the state after the first Hadamard transforms on the first 3 qubits.
   (c) Give the state after applying the oracle.
   (d) Give the state after measuring the second register (suppose the measurement gave $|001\rangle$).
   (e) Using $H^{\otimes n}|i\rangle = \frac{1}{\sqrt{2^n}} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} |j\rangle$, give the state after the final Hadamards.
   (f) Why does a measurement of the first 3 qubits of the final state give information about s?
   (g) Suppose the first run of the algorithm gives $j = 011$ and a second run gives $j = 101$. Show that, assuming $s \neq 000$, those two runs of the algorithm already determine s.

4. Given a string $x \in \{0,1\}^N$ ($N = 2^n$) with the promise that there exists a string $s \in \{0,1\}^n$ such that $x_i = i \cdot s \pmod 2$ for all $i \in \{0,1\}^n$. We would like to learn what s is.
   (a) Give a quantum algorithm that makes only 1 query to x and that computes s with success probability 1. *Hint:* Use the Deutsch-Jozsa algorithm.
   (b) Argue that any classical algorithm to compute s needs to query x at least n times.