Quantum Computing Exercises # 11

Ronald de Wolf

Apr 19, 2011
(to be handed in before or at the start of the lecture on Apr 26)

1. Prove that classical deterministic protocols with one message (from Alice to Bob), need to send n bits to solve the equality problem. *Hint: Argue that if Alice sends the same message for distinct inputs x and x', then Bob doesn't know what to output if his input is $y = x$.*

2. (a) Show that if $|\phi\rangle$ and $|\psi\rangle$ are non-orthogonal states (i.e., $\langle\phi|\psi\rangle \neq 0$), then there is no two-outcome projective measurement that perfectly distinguishes these two states, in the sense that applying the measurement on $|\phi\rangle$ always gives a different outcome from applying the same measurement to $|\psi\rangle$. *Hint: Argue that if P is a projector then we can't have both $P|\phi\rangle = |\phi\rangle$ and $P|\psi\rangle = 0$.*

   (b) Prove that quantum protocols with one message (from Alice to Bob), need to send $\log n$ qubits to solve the distributed Deutsch-Jozsa problem with success probability 1 on every input. *Hint: Observe that among Alice's possible n-bit inputs are the n codewords of the Hadamard code that encodes $\log n$ bits; each pair of distinct Hadamard codewords is at Hamming distance exactly $n/2$. Use part (a) to argue that Alice needs to send pairwise orthogonal states for those n inputs, and hence her message-space must have dimension at least n.*

3. Consider an error-correcting code $C : \{0,1\}^n \to \{0,1\}^N$ where $N = O(n)$, N is a square, and any two distinct codewords are at Hamming distance $d(C(x), C(y)) \in [0.49N, 0.51N]$ (such codes exist, but you don't have to prove that).

   (a) View the codeword $C(x)$ as a $\sqrt{N} \times \sqrt{N}$ matrix. Show that if you choose a row uniformly at random, and choose a column uniformly at random, then these intersect in a bit $C(x)_i$ for uniformly random $i \in \{1, \ldots, N\}$.

   (b) Give a classical bounded-error SMP-protocol for the equality problem where Alice and Bob each send $O(\sqrt{n})$ bits to the Referee. *Hint: Let Alice send a random row of $C(x)$ (with the row-index) and let Bob send a random column of $C(y)$ (with the column-index).*

4. Suppose Alice and Bob each have n-bit agendas, and they know that for exactly 25% of the timeslots they are both free. Give a quantum protocol that finds such a timeslot with probability 1, using only $O(\log n)$ qubits of communication.