Quantum Computations, 2016, Test 1

1. **CPHASE**. Write down a matrix for "controlled-phase" (CPHASE) gate which "flips" the phase (that is, turns $|1\rangle$ into $-|1\rangle$ and leaves $|0\rangle$ unchaged) if first bit is 1 and does nothing (I) otherwise. Show how to implement CNOT with two H's and one CPHASE.
2. **Toffoli gate**. Write down a matrix for "controlled-controlled-NOT" gate on 3 qubits: third bit of output is inverted if first two bits of input are 1 and remains unchanged otherwise. Show how to simulate classical AND and NOT gates using this. Conclude about computational power of quantum circuits in comparison with classical circuits. What is the boolean formula for third bit of output?
3. **Example for *Simon's***. Create an example of function $f\colon \{0,1\}^2 \to \{0,1\}^2$ which satisfies the condition from Simon's problem (choose some particular $\bar{s} \neq \bar{0}$, write the whole truth table for f). Justify that your example actually satisfies the condition. Right down the state of a quantum system after application of first two stages of Simon's circuit (that is, tensor of a number of H's and U_f). Show how the terms in state expression are grouped basing on the property of f (*Note*: all this was done in general form on the lecture). Likewise, right down the result of application of last $H^{\otimes 2}$. Which results may final measurement yield?
4. **One-out-of-4 search**. Let $f\colon \{0,1\}^2 \to \{0,1\}$ is such that there is only one $x \in \{0,1\}^2$ with the property: $f(x) = 1$. The task is to find out x. Show that this could be done with the sequence of transformations: $AU_f H^{\otimes 3}|001\rangle$ (for some A, see below). To do this: 1) draw corresponding quantum circuit; 2) show which 4 states could possibly be formed after $U_f H^{\otimes 3}$-part; 3) justify that there exists unitary transformation A which maps each of those 4 states onto different base states (you don't have to provide A, but you could); 4) conclude which qbuits should be measured at the end and what is the meaning of the outcome of such measurement. Finally, answer the question: what is the number of f-calls to solve this task 1) classically, 2) in quantum world.
5. **One-out-of-N search**. Can you show why the one-out-of-4 search approach fails for one-out-of-8 search? Can you count probabilities for the right answer if we still try to apply the approach? What can you say about one-out-of-N search task given the same approach?