Quantum computing, Assignment 2. Due 30 September

(Dated: September 15, 2020)

- **Problem 1: Deutsch's problem. [4 points]**

  Suppose one tried to solve Deutsch's problem not by using the trick that we considered during the lecture, but by applying the standard procedure: Start with the output and input registers in the state $|0\rangle|0\rangle$, apply the Hadamard to the input register and then apply $\mathbf{U_f}$, thereby transforming to the state

  $$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|f(1)\rangle \tag{1}$$

  Given the two Qbits in this state, a direct measurement only reveals the value of f at either 0 or 1 (randomly), but gives no information about whether $f(0) = f(1)$. But there is a way (noticed by Deutsch) to do this with 50% probability by applying other unitary transformation before measuring.

  Show that if one applies Hadamard $\mathbf{H}$ to each of the Qbit prior to measurement, then regardless of which of the four possible states (1) one has been given (corresponding of the four possible choices of the function $f(x)$ that brings on bit into one bit), there is a 50% chance that measurement will enable one to conclude whether or not $f(0) = f(1)$. But the other 50% one will learn nothing whatever from the measurement outcome, neither about whether $f(0) = f(1)$ nor about the value of either $f(0)$ or $f(1)$.

- **Problem 2 [8 points]: Useful identities** Prove that

  - **[4 points]**

  $$H^{\otimes n}|\boldsymbol{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{z}\in\{0,1\}^n} (-1)^{\boldsymbol{x}\cdot\boldsymbol{z}}|\boldsymbol{z}\rangle \tag{2}$$

  - **[4 points]** Using Eq.2 show that

  $$H^{\otimes n}\left(\frac{1}{\sqrt{2}}|\boldsymbol{x}\rangle + \frac{1}{\sqrt{2}}|\boldsymbol{y}\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{z}\in\{\boldsymbol{s}\}^\perp} (-1)^{\boldsymbol{x}\cdot\boldsymbol{z}}|\boldsymbol{z}\rangle \tag{3}$$

    where $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$, $\boldsymbol{s} = \boldsymbol{x} \oplus \boldsymbol{y}$ and $\boldsymbol{s}^\perp = \{\boldsymbol{z} \in \{0,1\}^n | \boldsymbol{s}\cdot\boldsymbol{z} = 0\}$

- **Problem 3 [8 points]: Probabilities for solving Simon's problem**

  As discussed in lectures, to estimate how many times a quantum computer has to invoke the subroutine $\mathbf{U_f}$ to solve Simon's problem, on has to answer a purely mathematical question. We have an n-dimensional space of vectors whose components are either 0 or 1 whose addition and inner products are carried out with the modulo 2 arithmetic. We are interested in the $(n-1)$-dimensional subspace of vectors orthogonal to a given vector a. We have a quantum computer program which gives us a random vector y in this subspace. If we run the program $n+x$ times, what is the probability q that $n-1$ of the vector will be linearly independent ? We have discussed in the lectures that

  $$q = \left(1 - \frac{1}{2^{2+x}}\right)\left(1 - \frac{1}{2^{3+x}}\right)\dots\left(1 - \frac{1}{2^{n+x}}\right) \tag{4}$$

  Consider the case $n = 3$, $x = 1$ and $a = 111$ (in binary representation). Prove that the expression for probability (4) is correct by the direct computation.

- **Problem 4 [8 points]: Grover' search** Design and test the Grovers' search with 2 Qbits.

  - **[4 points]** Explain the basic elements of the quantum circuit including oracles and other operators.
  - **[2 points]** Design and test the algorithm with Qiskit.
  - **[2 points]** Find out what happens if one applies Grover' iterations more times than needed.