Homework problems, set 7:

Quantum computing

Hand in before 1/6-2018.
Maximum number of points: 28.

1 Quantum fourier transform

Given m qubits, we have $D(\mathcal{H}) = 2^m \equiv N$. Thus, we can label the N states $|x_1 x_1 \dots x_m\rangle$ in decimal representation $|0\rangle$, $|1\rangle$, ..., $|N-1\rangle$. One converts between the binary string $x_1 x_2 \dots x_m$ to the corresponding base 10 number k accordingly

$$x_1 x_2 \dots x_m \to k = \sum_{l=1}^{n} x_l 2^{m-l}. \tag{1}$$

Furthermore, the *quantum Fourier transform* is defined as

$$|n\rangle_F = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{N-1} e^{2\pi i n k/N} |k\rangle. \tag{2}$$

a) What is the quantum Fourier transform of the state $|00\dots0\rangle$? (2p)

   (Comment: if the input state $|0\rangle \equiv |00\dots0\rangle$ would represent the zero momentum state, what would one expect for its fourier transform?)

b) Prove that the quantum Fourier transform is unitary. (3p)

c) Use (1) to show that any state $|n\rangle_F$ can be written on the product form

$$|n\rangle_F = \frac{1}{\sqrt{2^m}} \bigotimes_{l=1}^{m} \left[|0\rangle + e^{2\pi i n/2^l} |1\rangle \right]. \tag{3}$$

   This implies that the quantum Fourier transform can be implemented using only Hadamard and control-phase gates. (4p)

2 Factoring

Find the period of each of the following functions and, if appropriate, use this information to factor the designated numbers:

a) 11^n (mod 133) to factor 133. (3p)

b) 2^n (mod 221) to factor 221. (3p)

3 Grover's search algorithm

This algorithm considers the problem of finding a desired entry in a data base. Assume we design a function such that $f(x) = 1$ if x is the desired entry and $f(x) = 0$ otherwise. Furthermore we assume that x can be any of the values $0, 1, \ldots, N-1$. Thus, each element can be represented by a binary string of n entries (assuming that $2^n > N$), or n qubits. Now we assume we have an oracle performing

$$|a\rangle \otimes |b\rangle \rightarrow |a\rangle \otimes |b \oplus f(a)\rangle. \tag{4}$$

It then follows

$$|a\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow (-1)^{f(a)}|a\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{5}$$

Now, if we have the initial state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$, operation with the oracle gives

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{6}$$

The idea of the Grover's algorithm is to apply the oracle and a *diffusion operator*

$$\hat{D} = 2|\psi\rangle\langle\psi| - \hat{\mathbb{1}}^{\otimes n}, \tag{7}$$

where $\hat{\mathbb{1}}^{\otimes n}$ is n-quibit identity operator.

a) If $|x_0\rangle$ is the state corresponding to the desired entry x_0, show that operating with $\hat{D}$ on the state

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{8}$$

results in

$$\left[\left(1-\frac{4}{N}\right)|\psi\rangle+\frac{2}{\sqrt{N}}|x_0\rangle\right]\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle). \qquad (3p) \qquad (9)$$

The amplitude to find the desired state x_0 has increased from $1/\sqrt{N}$ to $(3-4/N)/\sqrt{N}$ by this operation. One can show that repeating this procedure leads to an ever increased probability to find x_0. This is the idea behind the Grover's search algorithm.

4 Quantum circuit

On the cowrse web page (http://www.fysik.su.se/ jolarson/Kvantinfo/) there is a picture showing a quantum circuit, for a general input state $|\psi\rangle$ give the output state of this circuit. (The control-Z gate represents operation with $\hat{\sigma}_z$ on the target qubit.) (4p)

5 Geometry of pure quantum states

We've seen that for qubits and qutrits any state can be written

$$\hat{\rho}=\frac{1}{D}\left(\mathbb{1}+a\mathbf{R}\cdot\lambda\right). \qquad (10)$$

Here, D is the dimension, a some scaling parameter, $\mathbf{R}$ the Bloch vector and the λ's are the Pauli matrices for qubits and the Gell-Mann matrices for qutrits. It turns out that this formula can be generalized to arbitrary dimensions D, *i.e.* to *qudits*. The λ-matrices are then the *generalized Gell-Mann matrices*, and the Bloch vector $\mathbf{R}$ will be of dimension D^2-1. Thus, the expression (10) is general and not restricted to qubits ($D=2$) and qutrits ($D=3$).

Of course, $\hat{\rho}$ in Eq. (10) is valid for both pure and mixed states. Let us consider only pure states; $\hat{\rho}^2=\hat{\rho}$. Assume that $\{|\phi_i\rangle\}$ with $i=1,2,\dots,D$ is an ON-basis. To these states we construct the corresponding density operators $\hat{\rho}_i=|\phi_i\rangle\langle\phi_i|$. To each such state $\hat{\rho}_i$ we can thereby identify a Bloch vector $\mathbf{R}_i$ which fully specify our state.

a) The fact that $\langle\phi_j|\phi_i\rangle=\delta_{ji}$, does this imply orthogonality of the corresponding Bloch vectors, *i.e.* $\mathbf{R}_j\cdot\mathbf{R}_i=\delta_{ji}$? (2p)

b) For general dimension D, calculate the sum $\sum_{i=1}^{D} \mathbf{R}_i$. (4p)