Quantum Information 116031 – Homework №10
Quantum Fourier Transform and Shor's algorithm

Due date: 24-Jun-2018

1 QFT I (20 points)

1.1 (10 points) Draw explicitly the QFT circuit for 4 qubits.

1.2 (10 points) Suppose $x = (x_0, \dots, x_{N-1}) \in \mathbb{R}^N$ is a vector which is r-periodic in the following sense: there exists an integer r such that $x_k = 1$ whenever k is an integer multiple of r, and $x_k = 0$ otherwise. Let U be the unitary matrix of the Fourier transform DFT_N. Compute Ux, i.e., write down a formula for the entries $\hat{x}_j$ of the vector Ux. Assuming r divides N, write down a simple closed form for the entries. In such case, what are the entries with the largest magnitude?

Sketch a graph of x_k vs k and of $\hat{x}_j$ vs. j for the case $N = 100$ and $r = 20$.

2 QFT II (25 points)

In class we have seen that the QFT circuit over n qubits can be written using $\mathcal{O}(n^2)$ gates. Here we will show that it can be well approximate by a circuit with only $\mathcal{O}(n \log n)$ gates.

2.1 (4 points) Recall the definition of the operator norm:

$$\|A\|_{\mathrm{op}} \stackrel{\mathrm{def}}{=} \max_{|\psi\rangle} \frac{\|A\,|\psi\rangle\|}{\||\psi\rangle\|}.$$

Use this definition to show that for any operator A and any unitary U it holds that $\|AU\|_{\mathrm{op}} = \|UA\|_{\mathrm{op}} = \|A\|_{\mathrm{op}}$.

2.2 (5 points) What is the operator norm distance between the phase gate $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{smallmatrix}\right)$ and the 2×2 identity matrix? Show that it is $\mathcal{O}(\phi)$.

2.3 (3 points) Consider a product of n-qubit unitaries $U = U_L \cdot U_{L-1} \cdots U_1$, and suppose we drop the j'th gate to create the sequence $U' = U_L \cdots U_{j+1} \cdot U_{j-1} \cdots U_1$. Show that $\|U - U'\|_{\mathrm{op}} = \|U_j - \mathbb{1}\|_{\mathrm{op}}$.

2.4 (3 points) Suppose that we also drop the k'th unitary: $U'' = U_L \cdots U_{j+1} \cdot U_{j-1} \cdots U_{k+1} \cdot U_{k-1} \cdots U_1$. Show that $\|U - U''\|_{\text{op}} \le \|U_j - \mathbb{1}\|_{\text{op}} + \|U_k - \mathbb{1}\|_{\text{op}}$.

2.5 (10 points) Give a quantum circuit with $\mathcal{O}(n \log n)$ that has an operator norm distance less than $\frac{1}{n}$ from the DFT circuit $U_{\text{FT}(n)}$.

3 Finding the period in the "hard" case. (30 points)

Consider Shor's algorithm for finding the period r of some number x with respect to a large N using $2 \times \ell$ qubits, where ℓ is such that $2^\ell \le N^2 < 2^{\ell+1}$, and set $L \stackrel{\text{def}}{=} 2^\ell$. In class we saw that after the first measurement, the first register collapses to a homogeneous superposition of m states, where $m = \lceil \frac{L}{r} \rceil$ or $m = \lfloor \frac{L}{r} \rfloor$. Then we saw that the probability of measuring j in the second measurement is given by

$$\text{Prob}\,(j) = \frac{|c_j|^2}{mL},$$

where c_j is given by

$$c_j = \begin{cases} m, & \mathrm{e}^{2\pi \mathrm{i} rj/L} = 1 \\ \dfrac{1 - \mathrm{e}^{2\pi \mathrm{i} mrj/L}}{1 - \mathrm{e}^{2\pi \mathrm{i} rj/L}}, & \mathrm{e}^{2\pi \mathrm{i} rj/L} \neq 1. \end{cases}$$

We proved that in the (very unlikely) case when r divides L, the outcome of the second measurement is *always* a j that is an integer multiple of $\frac{L}{r}$, i.e., $j = k\frac{L}{r}$ for $k = 0, \ldots, r-1$. In this question, we will show that when r does not divide L, we still have high probability of measuring j that is *close* to an integer multiple of $\frac{L}{r}$. Throughout the question, we assume then that r *does not* divide L.

3.1 (4 points) Let us define the "Good j's" as those j's in the range $0, 1, \ldots, L-1$ that are close to a an integer multiple of $\frac{L}{r}$. Specifically, $j \in \{0, 1, \ldots, L-1\}$ is a good j if there exists an integer k such that

$$\left| j - k\frac{L}{r} \right| \le \frac{1}{2}.$$

Show that there are at least r good j's.

3.2 (5 points) Show that $\text{Prob}\,(j)$ can be written as

$$\text{Prob}\,(j) = \frac{1}{mL} \begin{cases} m^2, & e^{2\pi \mathrm{i} rj/L} = 1 \\ \left| \dfrac{\sin(\pi mrj/L)}{\sin(\pi rj/L)} \right|^2, & e^{2\pi \mathrm{i} rj/L} \neq 1. \end{cases}$$

3.3 (4 points) Show that for every good j there exists an integer k and a real number $-\frac{1}{2} \le h \le \frac{1}{2}$ such that

$$j = k\frac{L}{r} + h.$$

3.4 (4 points) Show that if $h = 0$, then $\text{Prob}\,(j) \ge \frac{1}{r}$.

3.5 (4 points) Show that for $h \neq 0$,

$$\text{Prob}\,(j) = \frac{1}{mL}\left|\frac{\sin\left(\pi m h r/L\right)}{\sin\left(\pi h r/L\right)}\right|^2$$

3.6 (5 points) Show that $0 < m\frac{r}{L}|h| < \frac{4}{5}$, and use it to show that $\text{Prob}\,(j) \ge \frac{1}{2}\frac{m}{L}$.
Hint: you may use the fact that $\frac{3}{4}x < \sin(x) < x$ for $0 < x < \frac{5}{4}$.

3.7 (4 points) Show that the probability of measuring a good j is at least 30% (you may assume that $N > 10$).

4 Simulating Shor's algorithm (25 points)

Assume we run Shor's algorithm to find the period of the function $f(x) \stackrel{\text{def}}{=} 7^x \pmod{11}$ using a Fourier transform over $L = 128$. The algorithm uses $7 + 7$ qubits in two registers. Each of the registers can hold a number between 0 and 127 (in binary coding). The first 3 steps of the algorithm are as follows.

1. Prepare the initial state state:

$$|\psi_0\rangle = |0\rangle \otimes |0\rangle\,.$$

2. Act with $H^{\otimes 7}$ on the first register:

$$|\psi_1\rangle = \frac{1}{\sqrt{128}}\sum_{k=0}^{127}|k\rangle \otimes |0\rangle\,.$$

3. Act with U_f, where $f(x) = 7^x \pmod{11}$:

$$|\psi_2\rangle = \frac{1}{\sqrt{128}}\sum_{x=0}^{127}|x\rangle \otimes |x^7 \pmod{11}\rangle\,.$$

Let us now assume that in the next step – measuring the second register – we obtain the result 9.

4.1 (8 points) What is the resultant state $|\psi_3\rangle$ after the measurement? You may use a simple computer code to find the $|x\rangle$ components from the first register that participate in the superposition. How many components are there? What is the period r? Note that you should only consider the first register (the second register is known to be at the state $|9\rangle$).

4.2 (8 points) Write a simple computer code (MATLAB, Python, or whatever) that performs a DFT_{128} on the first register. The code should calculate $|\psi_4\rangle = \sum_{j=0}^{127} b_j |j\rangle$, i.e., it should calculate the coefficients b_j. Plot a graph of j vs. $|b_j|^2$, and write the first 4 j's for which $|b_j|^2$ peaks.

4.3 (9 points) Running the algorithm few times, the results of the second measurement were $j = 102, j = 13, j = 39$. Which of these results gave the correct order? Explain your answer using continued fractions.