Lecture "Quantum Information" WS 17/18 — Exercise Sheet #5

Problem 1: The Bernstein-Vazirani algorithm.
This is a variation of the Deutsch-Jozsa problem. Suppose that the quantum black box computes one of the functions f_a, where $f_a(x) = a \cdot x$ and a is an n-bit string. The task is to determinate a. Show that Deutsch-Jozsa algorithm can solve this problem, i.e. can find the n-bit string a with probability one.

Problem 2: Grover's algorithm with multiple marked elements.
Consider the Grover search problem of finding x_0 such that $f(x_0) = 1$ for some function $f(x) \in \{0, 1\}$. In the lecture, we derived Grover's algorithm which finds x_0, given that it is unique. Now assume that there are $r > 1$ solutions to the equation $f(x) = 1$. In other words, suppose that we have N states and r of them are marked. The problem is to find one of the marked states with high probability.

Grover's algorithm with mulitple solutions is very similar to the unique solution one. First, the oracle is constructed the same way as before. Find the action of the oracle on a state $|x\rangle$. The remaining steps of the algorithm remain unchanged. Perform a step-by-step analysis of this modified Grover's algorithm, and estimate the number of iterations needed ot obtain one of the marked elements with high probability. How does the runtime of the algorithm scale in r and N? Compare this to the performance of a classical algorithm.

Problem 3: Phase estimation.
Consider a unitary U with an eigenvector $U|\phi\rangle = e^{2\pi i\phi}|\phi\rangle$. Assume that $\phi = 0.\phi_1\phi_2 \dots \phi_n = \frac{1}{2}\phi_1 + \frac{1}{4}\phi_2 + \dots$. Our goal will be to study ways to determine ϕ as accurately as possible, given that we can implement U (and are given $|\phi\rangle$).

1. First, consider that we use controlled-U operations $CU|0\rangle|\phi\rangle = |0\rangle|\phi\rangle$, $CU|1\rangle|\phi\rangle = |1\rangle e^{2\pi i\phi}|\phi\rangle$. Describe a protocol where we apply CU to $|+\rangle|\phi\rangle$, followed by a measurement, to infer information about ϕ. Which information, and to which accuracy, can we obtain with N iterations?

2. Now consider a refined scheme. To this end, assume we can also apply controlled-$U^{(2^k)} \equiv CU_k$ operations for integer k efficiently.
   a) We start by applying CU_{n-1} to $|+\rangle|\phi\rangle$. Which information can we infer? What measurement do we have to make?
   b) In the next step, we apply CU_{n-2}, *knowing* the result of step a). What information can we infer? What measurement do we have to make? Rephrase the measurement as a unitary rotation followed by a measurement in the $|\pm\rangle$ basis.
   c) Iterating the preceding steps, describe a procedure (circuit) to obtain $|\phi\rangle$ exactly. How many times do we have to evaluate controlled-$U^{(2^k)}$'s?
   (*Note:* This procedure is known as *quantum phase estimation.*)

3. An alternative way to determine ϕ is to use the quantum Fourier transform. To this end, we apply a transformation $\sum_x |x\rangle|\phi\rangle \mapsto \sum_x |x\rangle U^x|\phi\rangle$, followed by a quantum Fourier transform and a measurement. Describe the resulting protocol, its outcome, and the number of $U^{(2^k)}$'s required.

4. Compare the two protocols derived in step 2 and 3.

5. What outcome will we obtain if we apply the phase estimation algorithm to a *superposition* of different eigenstates $\sum_k w_k|\phi^k\rangle$? (It might help to first consider the case where we measure the register with the $|\phi^k\rangle$'s.)

6. Let us now consider the factoring problem. For a coprime with N (such as it appears in the factoring problem, cf. lecture), the map $U : |x\rangle \mapsto |ax \bmod N\rangle$ is unitary (no proof required). This unitary has periodicity r (with $a^r \bmod N = 1$), i.e., its eigenvalues are r's roots of unity.
   What happens if we apply phase estimation to this U, given we are provided with an eigenvector $|\lambda\rangle$ of U?

7. Consider the form of the eigenvalues of U, and show that their equal weight superposition has a simple form. Discuss how this can be used to determine r without knowing an eigenvector $|\lambda\rangle$ of U. Discuss how this relates to Shor's factoring algorithm.

Problem 4: Period finding.
In this problem, we will analyze the use of the Quantum Fourier transform for period finding in more detail.

1. We start from a state $\frac{1}{2^{n/2}}\sum|x\rangle|f(x)\rangle$, where the first register has n qubits, and $f(x)$ has a period r.

2. By measuring the second register, this collapses to $\frac{1}{\sqrt{k_0}}\sum_{k=0}^{k_0-1}|x_0+kr\rangle$. Show that $\frac{2^n}{r}-1 < k_0-1 \le \frac{2^n}{r}$.

3. By applying a QFT, we arrive at a state $\sum a_\ell|\ell\rangle$. Determine a_ℓ.

4. Plot $|a_\ell|^2$ for different n and r (in particular, check the regime where $r \ll 2^n$). Verify that the distribution is peaked around $\ell = s\frac{2^n}{r}$, where s is an integer (here, $\frac{2^n}{r}$ can be seen as the frequency of the periodic signal in $f(x)$).

5. Since $s\frac{2^n}{r}$ is not necessarily integer, the signal will be peaked around the ℓ closest to $s\frac{2^n}{r}$. Consider such an ℓ_s:
$$\ell_s = \frac{2^n}{r}s + \delta_s\ ;\quad |\delta_s| \le \tfrac{1}{2}\ .$$
Evaluate the expression for a_{ℓ_s}. Simplify the obtained expression by using that $r \ll 2^n$ and thus $k_0 r/2^n \approx 1$ given the bound on k_0 shown above.

6. Now derive a lower bound on $|a_{\ell_s}|^2$, using that $\sin(x) \ge \frac{2}{\pi}x$, and $\sin(x)\approx x$ for small x. You should find $|a_{\ell_s}|^2 \ge \frac{4}{\pi^2 r}$.

7. Use this to show that the total probability to find one of those ℓ_s, i.e., $\sum_s |a_{\ell_s}|^2$, is bounded below by $4/\pi^2 \approx 0.41$. (What is the range of s?)

8. Overall, this shows that we find an ℓ_s such that $|\ell_s - \frac{2^n}{r}s| \le \frac{1}{2}$ with sufficiently high probability. Show that this can be used to infer s/r, given that $r \ll 2^n$. (*Hint:* What is the minimum spacing of s/r and $s/(r+1)$? If this is sufficiently larger than the accuracy of $\ell/2^n \approx s/r$, this allows to uniquely determine r, and subsequently s. How much smaller than 2^n does r have to be?)