Lecture & Proseminar 250078/250042
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2022/23

— Exercise Sheet #9 —

Problem 24: The Bernstein-Vazirani algorithm.

The Bernstein-Vazirani algorithm is a variation of the Deutsch-Jozsa problem.
Suppose that we are given an oracle

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle \ ,$$

where $f : \{0,1\}^n \to \{0,1\}$, i.e. x is an n-qubit state and y a single qubit, and where we have the promise that $f = a \cdot x$ for some unkown $a \in \{0,1\}^n$. The task is to determine a.
Show that the same circuit used for the Deutsch-Jozsa algorithm can also solve this problem, i.e., it can be used to find a with unit probability in one iteration.
Compare this to the number of classical calls to the function f required to determine a (either deterministically or with high probability).

Problem 25: Phase estimation

Consider a unitary U with an eigenvector $U|\phi\rangle = e^{2\pi i\phi}|\phi\rangle$. Assume that

$$\phi = 0.\phi_1\phi_2\ldots\phi_n = \tfrac{1}{2}\phi_1 + \tfrac{1}{4}\phi_2 + \ldots\ + \tfrac{1}{2^n}\phi_n \ ,$$

i.e. ϕ can be exactly specified with n binary digits. Our goal will be to study ways to determine ϕ as accurately as possible, given that we can implement U (and are given the state $|\phi\rangle$).

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 in the $|\pm\rangle$ basis, to infer information about ϕ. Which information, and to which accuracy, can we obtain with N iterations? (*Bonus question:* Could this scheme be refined by changing the measurement?)

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*, and is closely linked to the quantum Fourier transformation.)