Lecture & Proseminar 250078/250042
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2024/25

— Exercise Sheet #8 —

Problem 1: 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 2: The original Deutsch algorithm.

In the original version of his algorithm (found under this link with univie-Login), Deutsch does not use the phase kick-back technique. Instead, he applies U_f to $|+\rangle|0\rangle$, and thus obtain the state

$$|\psi_{\text{out}}\rangle = \tfrac{1}{\sqrt{2}}\big(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\big) \ .$$

1. Write down explicitly the output states $|\psi_{\text{out}}\rangle$ obtained for an f which is (i) constant (i.e., $f(0) = f(1)$), and (ii) balanced (i.e., $f(0) \neq f(1)$).
2. Devise a measurement (projective or POVM) which has three outcomes, where outcome 1 allows to conclude with certainty that f is constant, outcome 2 allows to conclude with certainty that f is balanced, and the third outcome does not allow for any definite conclusion about f.
3. Try to find a measurement which give a conclusive result with an as high as possible probability. What is the best you can achieve? (*Hint:* $\frac{1}{2}$ is possible.) Can you achieve this with a projective measurement?

Feel free to check the paper (linked above) – the solution can be found there quite explicitly, and checking papers can be very instructive.

Problem 3: Reversible classical 2-bit gates.

1. Show that all reversible classical 2-bit gates $G(x_1, x_2) = (y_1, y_2)$ can be written as a linear map over $\mathbb{Z}_2$, i.e.,
$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = M \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mod 2$$
(where $x_i, y_i \in \{0,1\}$, and M has entries 0 and 1).
2. Show that all those gates can be decomposed into only NOT and CNOT gates. (A useful identity can be that three consecutive CNOTs with opposite alignment swap the input bits.) Of course, you can solve this question before question 1, and then just show that CNOT and NOT are linear maps over $\mathbb{Z}_2$.
3. Show that this implies that any classical circuit consisting only of reversible 2-bit gates can be written as a linear transformation over $\mathbb{Z}_2$.
4. Show that the Toffoli gate is not of this form – that is, reversible classical two-bit gates are not universal for classical computation.

(*Note:* The class of problems which can be solved this way in time poly(n), with n the number of bits, defines the complexity class $\oplus$L (pronounced "Parity-L"). $\oplus$L can be simulated in time $\log(n)^2$ by a general classical circuit, and is thus indeed much more restricted than general efficient classical computations, which can have a runtime poly(n).)