QUANTUM INFORMATION

MFF UK

Recall the Toffoli gate T and the controlled negation gate CNOT are defined as follows:

$$T : (a, b, c) \mapsto (a, b, c \oplus ab), \;\; \text{CNOT} : (a, b) \mapsto (a, b \oplus a).$$

(0) Show that NAND is complete and then show that the Toffoli gate is complete and reversible.

(1) Compute matrix representations of the CNOT gate and the Toffoli gate. Are both of these gates valid from the QM perspective? Show that the Toffoli gate is able to clone basis states but not the general state.

(2) * Provide an (informal) argument showing that is is, indeed, necessary to have at least $2^{n-1} + 1$ queries to solve Deutsch-Jozsa problem on a deterministic non-quantum machine and thus the problem is provably not in P. Show that, on the other hand, the problem is in NP. Does this result provide an affirmative answer to the famous conjecture that $P \neq NP$?

(3) Assume you are given a function $f : \{0, 1\}^n \to \{0, 1\}$ and a quantum oracle for computing U_f where, as usual, U_f is defined as:

$$U_f : (\overline{x}, y) \mapsto (\overline{x}, y \oplus f(\overline{x})).$$

Let I_0 be the set of n-bit strings which start with 0 and I_1 its complement.

You are given a promise that f can be either of the following two types:

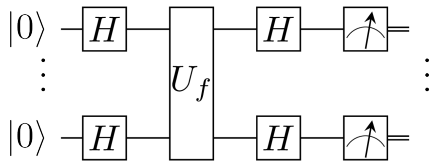
(a) $f(\overline{x}) = 0$ for all $\overline{x} \in I_0$ and 1 for all $\overline{x} \in I_1$;

(b) the total number of strings from I_0 for which $f(\overline{x})$ is 1 plus the total number of strings from I_1 for which $f(\overline{x})$ is 0 is exactly 2^{n-1}.

Design an algorithm which distinguishes between those two types making just a single query to U_f.

(4) The Bernstein-Vazirani problem (1992) is stated as follows: given a boolean function $f : \{0, 1\}^n \to \{0, 1\}$ which is a dot product of $\overline{x}$ and some fixed string $\overline{s}$, i.e. $f(\overline{x}) = x_1 s_1 \oplus ... \oplus x_n s_n$, and given U_f, compute $\overline{s}$ by querying U_f just once.

The quantum circuit solving this problem is as follows (the ancilla cubit is omitted from the picture):



Show that measuring the output of this circuit in the standard basis yields the desired string $\overline{s}$.