QUANTUM INFORMATION

MFF UK

The gates T (*Toffoli gate*) and CNOT (*controlled negation*) are defined as follows:

$$T : (x, y, z) \mapsto (x, y, z \oplus (x \wedge y)), \ \ \mathsf{CNOT} : (x, y) \mapsto (x, y \oplus x),$$

where x, y, z range over $\{0, 1\}$, and $\oplus$ is a binary XOR operator (*exclusive or*).

The NAND gate (*not and*) is defined as $\mathsf{NAND} : (x, y) \mapsto \neg(x \wedge y)$.

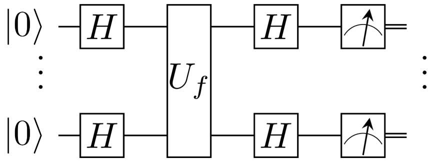
(0) Show that NAND is complete, i.e. any boolean function from $\{0, 1\}^n$ to $\{0, 1\}$ can be expressed as a suitable combination of NAND gates. Show that the Toffoli gate is reversible (i.e. bijective), and is complete (i.e., for any boolean function f from $\{0, 1\}^n$ to $\{0, 1\}$, there is a composition of T gates which takes $x_0, \ldots, x_{n-1}$ with some extra constant bits and outputs $x_0, \ldots, x_{n-1}, f(x_0, \ldots, x_{n-1})$ with some extra constant bits).

(1) Compute matrices representing CNOT and T gates. Show that the matrices are unitary.

(2) * (Deutsch-Josza problem) Provide a (possibly informal) argument that it is necessary to make at least $2^{n-1} + 1$ queries when the oracle function f takes only classical (i.e. 0/1) inputs. This means that the underlying decision problem is not in P. On the other hand, show that this problem is in coNP. Does this resolve the P versus NP conjecture?

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

The quantum circuit solving this problem is depicted below (the ancilla qubit is omitted from the picture).



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

(4) Assume you are given a function $f : \{0, 1\}^n \to \{0, 1\}$ with a quantum oracle gate U_f 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 with the first bit equal to 0, and I_1 be $\{0, 1\}^n \setminus I_0$.

You are given a promise that f fulfills one of the two conditions

(a) $f(\overline{a}) = 0$ if and only if $\overline{a} \in I_0$;

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

Design an algorithm that decides which of the two above conditions is fulfilled via just a single query to U_f.