8 Quantum algorithms

Preskill: *chapter 6.3*

Suppose you have a "black box" (an "oracle" in computer jargon) that evaluates a function $f(x)$. The integer x varies from 0 to $2^N - 1$. For each x the number $f(x)$ is either 0 or 1. You do not know which f has been programmed in the black box, but you do know that f belongs to one of these two classes:

- class C: f is constant, taking on the same value for each x.

- class B: f is balanced, taking on the values 0 and 1 equally often.

a) If the black box is a classical computer, how often should it be consulted to determine with certainty the class of f?

Deutsch and Jozsa have discovered that for a quantum computer one single consultation suffices. We examine in this problem a slight variation of the Deutsch-Jozsa algorithm, that needs N instead of $N+1$ qubits.

Initially all N qubits are in the state $|0\rangle$. Act with a Hadamard gate on each qubit.

b) Explain why the resulting state can be written as

$$(H|0\rangle)^N = 2^{-N/2} \sum_{x=0}^{2^N-1} |x\rangle.$$

Because the black box is quantum mechanical, you are not allowed to describe its operation by

$$\sum_x |x\rangle \rightarrow \sum_x |f(x)\rangle.$$

c) Why not?

Instead we describe its operation by

$$\sum_x |x\rangle \rightarrow \sum_x (-1)^{f(x)} |x\rangle.$$

d) Why is this allowed?

On each of the N qubits that comes out of the black box we act again with a Hadamard gate. Finally we measure them.

e) Show that they are all 0 if f is of class C.

f) Show that at least one qubit is 1 if f is of class B.

The Deutsch-Jozsa algorithm is a curiosity. It does not solve any "useful" problem. The Simon algorithm goes further. The unknown function $f : x \to y$, with $x, y \in 0, 1, 2, \ldots 2^N - 1$ is periodic and you wish to find the period a. This algorithm is at the basis of Shor's code breaker.

More precisely, for any pair $x \neq x'$ it is given that $f(x) = f(x')$ if and only if $x' = x \oplus a$, with $1 \leqslant a \leqslant 2^{N-1}$. The symbol $\oplus$ indicates that you write x and a in binary notation and then add bits modulo 2. For example $01011 \oplus 11001 = 10010$.

g) Show that $x \oplus a \oplus a = x$.

In addition to the N qubits we need a second set of N qubits (called ancilla's = female slaves, in the jargon). Initially all $2N$ qubits are 0, then the first N qubits are each sent through a Hadamard gate and subsequently they are acted upon with the following operation:

$$\sum_x |x\rangle|0\rangle \to \sum_x |x\rangle|f(x)\rangle.$$

Measure the N ancilla's.

h) Suppose you measure $f(x_0)$. In which superposition of states are the first N qubits?

Send the first N qubits through a Hadamard gate and measure them.

i) Explain that the result x_1 of that measurement is orthogonal to a, meaning that $x_1 \odot a = 0$, with $\odot$ the bitwise multiplication.

By repeating the whole algorithm some N times you obtain N independent equations from which you can solve for a.