# Problem Sheet 3

## 1.1 Bernstein-Vazirani Problem

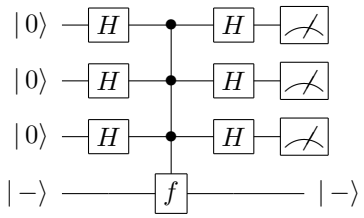
Suppose you are presented with an oracle (i.e. a black box whose internal processes we don't care about) which takes input $|x\rangle|y\rangle$, for $x \in \{0,1\}^n$ and $y \in \{0,1\}$, and produces output $|x\rangle|y \oplus f(x)\rangle$ where

$$f(x) = a \cdot x = a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n.$$

It is our task to determine the value of the $n$-bit string $a$ while minimising the number of calls to the oracle.

(i) Explain how you would complete the task classically.

(ii) The quantum network shown below can accomplish the task with only a single call to the oracle.




The central gate in the network represents the oracle. The second register, to which the value $f(x)$ is added, contains a single qubit, initially prepared in state $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

Explain how this is done by evaluating the network step by step.

## 1.2 Quantum Fourier transform and phase estimation

(a) The quantum Fourier transform (QFT) on n qubits is defined as

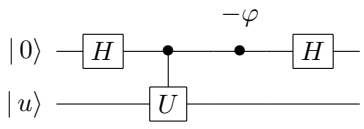
$$|x\rangle \mapsto \frac{1}{2^n} \sum_y e^{i\frac{2\pi}{2^n}xy} |y\rangle,$$

where $|x\rangle = |x_{n-1}\rangle|x_{n-2}\rangle \ldots |x_0\rangle$ and $|y\rangle = |y_{n-1}\rangle|y_{n-2}\rangle \ldots |y_0\rangle$ are elements of the computational basis and $x = \sum_{k=0}^{n-1} x_k 2^k$, $y = \sum_{k=0}^{n-1} y_k 2^k$. Show that this expression can be written in tensor product form

$$\frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i 0.x_0}|1\rangle)(|0\rangle + e^{2\pi i 0.x_1 x_0}|1\rangle)\ldots(|0\rangle + e^{2\pi i 0.x_{n-1}\ldots x_1 x_0}|1\rangle).$$

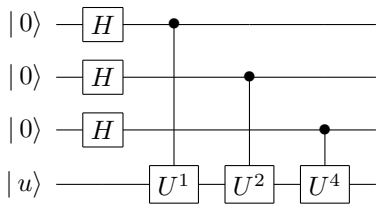
Remember the definition of the binary point notation, e.g., $0.x_1x_0 = x_1/2 + x_2/4$.

(b) Suppose you use the following network, where $|u\rangle$ is some eigenstate of the unitary, $U$, and has eigenvalue $e^{i\phi}$. The controlled unitary $U$ is followed by a phase shift gate.




Evaluate the output of the network. You do not know the value of $\phi$ and your task is to estimate it for a given value of $-\varphi$. What would you do if you are promised that $\phi$ is either $\varphi$ or $\varphi + \pi$?

(c) Consider an eigenstate $|u\rangle$ of the unitary $U$ with eigenvalue $e^{i\phi}$. You are promised that the phase $\phi$ is of the form $\phi = \frac{2\pi s}{2^n}$ for some integer $0 \leq s < 2^n$. Your task is to find the value of $\phi$. You are given the controlled versions of $U^{2^0}$, $U^{2^1}$, $U^{2^2}$,..., $U^{2^{n-1}}$, one qubit in state $|u\rangle$, and as many Hadamard and controlled phase shift gates as you want. You start by constructing the network shown below (for $n = 3$):




(i) Evaluate the output state of this network. Write all phase factors using the binary point notation.

(ii) Complete this network so that it computes $s$ (and hence determines $\phi$) in a single run.

Do you remember how to implement the QFT using controlled phase shift and Hadamard gates?

(iii) Explain how your network constructed in (ii) works using the results from (b).

## 1.3 Non-local boxes and Bell's inequality

Suppose Alice and Bob were given two coins each. Alice can toss either coin $A_1$ or coin $A_2$ and Bob either $B_1$ or $B_2$. Each coin is equally likely to show heads or tails, also labelled as 0 and 1. Can the results of the tosses satisfy the following four conditions

$$A_1 = B_1,\ B_1 = A_2,\ A_2 = B_2,\ \text{and}\ B_2 \neq A_1, \tag{1}$$

that is, whenever $A_1$ and $B_2$ are tossed they always come out opposite but any other pair of coins always comes out the same ?

**Classical world**. Let

$$I = \Pr[A_1 \neq B_1] + \Pr[B_1 \neq A_2] + \Pr[A_2 \neq B_2] + \Pr[B_2 = A_1]$$

be the sum of the probabilities that the coins deviate from the behaviour described by the four conditions above. What is the lowest possible value of $I$ in the case of "classical" correlations, i.e. when the random variables $A_1$, $A_2$, $B_1$ and $B_2$ have some pre-existing values, e.g. heads or tails?

If you solve this you will get what is known as Bell's inequality. It is usually expressed differently, but the meaning is the same.

**Magic world**. In a magical world where $I = 0$, i.e. the four conditions (1) are satisfied, Alice and Bob repeatedly toss their magically linked coins, choosing randomly and independently from each other which coin to toss. The coins may be high-tech marvels manufactured by their adversary Eve, but can she pre-program the coins and know in advance the outcomes of Alice's and Bob's tosses? Can such strong correlations be used by Alice and Bob for instantaneous signalling? Can they be used for a secure key distribution?

To be sure, the magic correlations have never been observed. They are, however, the subject of intense mathematical studies.

**Quantum world**. The table below describes weaker correlations. The entries are the joint probabilities of outcomes given the choices of coins. For example, if Alice tosses coin $A_1$ and Bob $B_2$ then the probability that Alice sees 1 and Bob 0 is $(1 - \varepsilon)/2$.

| Alice | | $A_1$ | | $A_2$ | |
|---|---|---|---|---|---|
| Bob | | 0 | 1 | 0 | 1 |
| $B_1$ | 0 | $\frac{1-\varepsilon}{2}$ | $\frac{\varepsilon}{2}$ | $\frac{1-\varepsilon}{2}$ | $\frac{\varepsilon}{2}$ |
| | 1 | $\frac{\varepsilon}{2}$ | $\frac{1-\varepsilon}{2}$ | $\frac{\varepsilon}{2}$ | $\frac{1-\varepsilon}{2}$ |
| $B_2$ | 0 | $\frac{\varepsilon}{2}$ | $\frac{1-\varepsilon}{2}$ | $\frac{1-\varepsilon}{2}$ | $\frac{\varepsilon}{2}$ |
| | 1 | $\frac{1-\varepsilon}{2}$ | $\frac{\varepsilon}{2}$ | $\frac{\varepsilon}{2}$ | $\frac{1-\varepsilon}{2}$ |

Here, $\varepsilon$ can be interpreted as the probability of a deviation from the behaviour of the perfect magic coins. How does $I$ depend on $\varepsilon$? If we replace any coin toss by an appropriately chosen polarisation measurement on entangled photons we can observe correlations with $\varepsilon = \sin^2(\pi/8)$. This is gives the lowest value of $I$ that was ever observed. What is this value?

Can you figure out how this $\varepsilon = \sin^2(\pi/8)$ came about?