INTRODUCTION TO QUANTUM INFORMATION SCIENCE

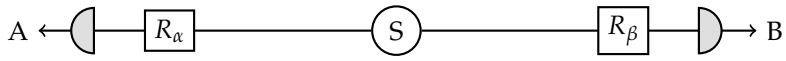
Exercise Set 2
HT 2018

ARTUR EKERT

2.1. **Entangled qubits.** Two entangled qubits in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ are generated by source S; one qubit is sent to Alice and one to Bob, who perform measurements in the computational basis.

(1) What is the probability that Alice and Bob will register identical results? Can any correlations they observe be used for instantaneous communication?

(2) Prior to the measurements in the computational basis Alice and Bob apply unitary operations R_α and R_β to their respective qubits



The gate R_θ is defined by its action on the basis states

$$\begin{aligned} |0\rangle &\rightarrow \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,, \\ |1\rangle &\rightarrow -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle\,. \end{aligned}$$

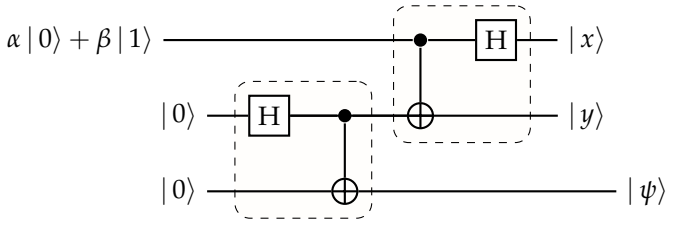
Show that the state of the two qubits prior to the measurements is

$$\cos(\alpha-\beta)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) - \sin(\alpha-\beta)\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

What is the probability that Alice and Bob's outcomes are identical?

2.2. **Quantum teleportation.** Consider the following quantum network (circuit), containing the Hadamard and the controlled-NOT gates,

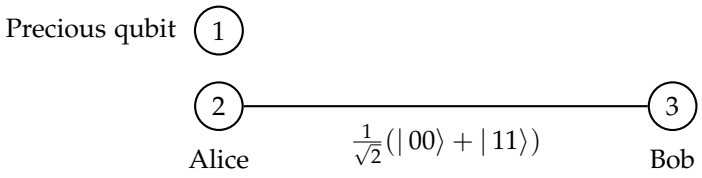
You should remember the action of the Hadamard and the controlled-NOT gates.



Divide et impera, that is, divide and conquer, a good approach to solving problems in mathematics (and in life). Start with smaller circuits, those surrounded by the dashed boxes.

The measurement on the first two qubits (counting from the top) gives two binary digits, x and y. The third qubit is not measured. How does the state of the third qubit, $|\psi\rangle$, depend on the values x and y?

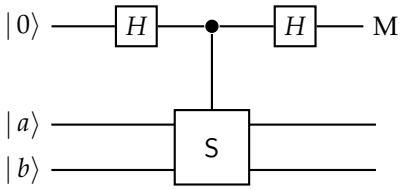
Suppose the three qubits, which look very similar, are initially in a possession of an absent-minded Oxford student Alice. The first qubit is in a precious quantum state and this state is needed urgently for an experiment in Cambridge. Alice's colleague, Bob, pops in to collect the qubit. Once he is gone Alice realises that by mistake she gave him not the first but the third qubit, the one which is entangled with the second qubit (see the figure below).



The situation seems to be hopeless – Alice does not know the quantum state of the first qubit, Bob is now miles away and her communication with him is limited to at most one tweet. However, Alice and Bob are both very clever and attended the "Introduction to Quantum Information Science" course at Oxford. Can Alice rectify her mistake and save Cambridge science?

2.3. **Playing with conditional unitaries.** The swap gate S on two qubits is defined first on product vectors, $S : |a\rangle\,|b\rangle \mapsto |b\rangle\,|a\rangle$ and then extended to sums of products vectors by linearity.

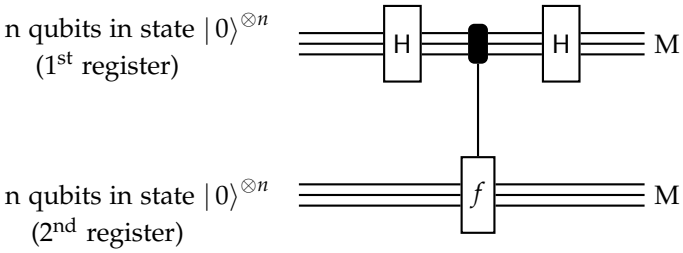
(1) Show that the four Bell states $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are eigenvectors of S which form the orthonormal basis in the Hilbert space associated with two qubits. Which Bell states span the symmetric subspace (all eigenvectors of S with eigenvalue 1) and which the antisymmetric one (all eigenvectors of S with eigenvalue -1)? Can S have any other eigenvalues except ± 1?
(2) Show that $P_\pm = \frac{1}{2}(\mathbb{1} \pm S)$ are two orthogonal projectors which form the decomposition of the identity and project on the symmetric and the antisymmetric subspaces. Decompose the state vector $|a\rangle\,|b\rangle$ of two qubits into symmetric and antisymmetric components.
(3) Consider the following quantum network composed of the two Hadamard gates, one controlled-S operation (also known as the controlled-swap or the Fredkin gate) and the measurement M in the computational basis,



The state vectors $|a\rangle$ and $|b\rangle$ are normalised but not orthogonal to each other. Step through the execution of this network, writing down quantum states of the three qubits after each computational step. What are the probabilities of observing 0 or 1 when the measurement M is performed?
(4) Explain why this quantum network implements projections on the symmetric and the antisymmetric subspaces of the two qubits.
(5) Two qubits are transmitted through a quantum channel which applies the same, randomly chosen, unitary operation U to each of them. Show that $U \otimes U$ leaves the symmetric and antisymmetric subspaces invariant.
(6) Polarised photons are transmitted through an optical fibre. Due to the variation of the refractive index along the fibre the polarisation of each photon is rotated by the same unknown angle. This makes communication based on polarisation encoding unreliable. However, if you can prepare any polarisation state of two photons you can still use the channel and communicate without any errors. How can this be achieved?

2.4. **Simon's algorithm.** Let $f : \{0,1\}^n \mapsto \{0,1\}^n$ be a 2-to-1 function such that $f(x \oplus s) = f(x)$, where s is a binary string of length n which is different from zero ($s \neq 0^n$) and $x \oplus s$ is a bit-wise addition modulo 2. In the network below the H operations denote the Hadamard transform on n qubits, M is a qubit by qubit measurement in the standard computational basis and the f operation represents a quantum evaluation of f; $|x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus f(x)\rangle$.

Recall that the Hadamard transform is defined as $|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}\,|y\rangle$, where $x, y \in \{0,1\}^n$ and the product $x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \,(\mathrm{mod} 2)$



(1) What is the state of the two registers right after the quantum function evaluation?
(2) The second register is measured qubit by qubit in the computational basis and a binary string $k \in \{0,1\}^n$ is registered. What is the state of the first register after the measurement?
(3) Subsequently the Hadamard transform is performed on the first register, followed by a measurement in the computational basis. The result is a binary string, z. Show that $z \cdot s = 0$.
(4) Suppose the function f is presented as an oracle. How many calls to the oracle are required in order to find s? How does it compare with a classical algorithm for the same problem? Provide rough estimates, detailed derivations are not required.