INTRODUCTION TO QUANTUM INFORMATION SCIENCE

Problem Sheet 3
Hilary Term

ARTUR EKERT & ZHENYU CAI

Questions Label: A - Bookwork B - Standard C - Challenging/Optional

3.1.B **Entanglement and Bell.** A source repeatedly generates two entangled qubits in the state $|\Omega\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$,

$$|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

One qubit is sent to Alice and one to Bob.

(1) When Alice measures her qubit in the standard Z basis, she *instantaneously* knows whether Bob, who may be miles away, will observe outcome 0 or 1 when he measures his qubit in the Z basis. Explain why these correlations cannot be used for instantaneous communication but they can be used for generating cryptographic keys.

(2) Show that for any two operators $A, B \in \mathcal{B}(\mathbb{C}^2)$, we have

$$\langle\Omega| A \otimes B |\Omega\rangle = \frac{1}{2} \operatorname{tr} A^T B.$$

(3) Let A and B be two observables measured by Alice and Bob, respectively,

$$A = \cos\alpha Z + \sin\alpha X, \quad \text{and} \quad B = \cos\beta Z + \sin\beta X, \tag{1}$$

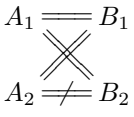
where X and Z are the Pauli operators. Show that

$$\langle\Omega| A \otimes B |\Omega\rangle = \cos(\alpha - \beta).$$

What is the probability that the results registered by Alice and Bob upon measuring these observables are identical?

Let A_1, A_2, B_1 and B_2 be the observables defined by using the angles $\alpha_1 = \frac{\pi}{2}$, $\alpha_2 = 0$, $\beta_1 = \frac{\pi}{4}$ and $\beta_2 = \frac{3\pi}{4}$ (respectively) in Eq. (1). Alice and Bob perform a statistical test (known as the CHSH test) in which Alice repeatedly measures either A_1 or A_2, and Bob either B_1 or B_2. For each run they choose, randomly and independently from each other, which observable to measure, and then check whether the following conditions are satisfied:

$$A_1 = B_1, \quad A_1 = B_2, \quad A_2 = B_1, \quad A_2 \neq B_2. \tag{2}$$



In each run they are able to check only *one* of the four conditions depending on the pair of observables they choose to measure.

(4) Show that their probability P_s of success (i.e. the asymptotic fraction of runs in which they find that the outcomes agree with the conditions in Eq. (2)) is given by $P_s = \cos^2\frac{\pi}{8}$.

The CHSH test described above can be performed using two devices, $\mathcal{A}$ and $\mathcal{B}$, with $\mathcal{A}$ being a "black box" of unknown design that has two settings A_1 and A_2, and similarly for $\mathcal{B}$ with the settings being B_1 and B_2. At each run of the device $\mathcal{A}$ or $\mathcal{B}$ for a given setting, an outcome of ± 1 is generated. The probability of success in any such CHSH test cannot exceed $P_s = \cos^2\frac{\pi}{8}$. The maximum value is achieved only when the settings correspond to the measurements on qubits in state $|\Omega\rangle$, as

described above (modulo some simple relabelling). The test is rigid — there is no other way to maximise the probability of success.

(5) An adversary, Eve, who manufactured, pre-programmed, and sold the two devices to Alice and Bob, claims that for each run of the CHSH test she has assigned numerical values ± 1 to A_1, A_2, B_1, and B_2 so that the outcomes are predetermined. Alice and Bob run the CHSH test using their unreliable devices and obtain $P_s \approx 0.85$. Is the claim from Eve true?

(6) Would the CHSH test be conclusive if Alice and Bob, in their "random" choices of measurements (A_1 or A_2 for Alice, and B_1 or B_2 for Bob), relied on random number generators supplied by their adversary Eve?

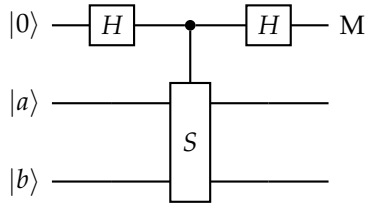
3.2.B **Playing with conditional unitaries.** The swap gate S on two qubits is defined first on product vectors, $S : |a\rangle\,|b\rangle \mapsto |b\rangle\,|a\rangle$ and then extended to sums of products vectors by linearity.

(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 $\Pi_\pm = \frac{1}{2}(\mathbb{1} \pm S)$ 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.

An operator A is a projector iff it is idempotent: $A^2 = A$.

(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?

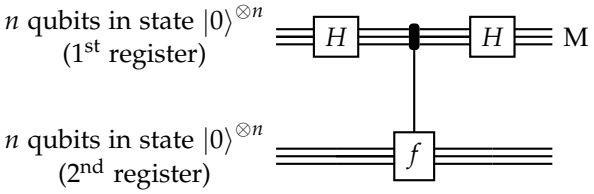
(4) Explain why this quantum network implements projections into the symmetric and the antisymmetric subspaces of the two qubits.

(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?

3.3.A **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 $x \cdot y = x_1y_1 + x_2y_2 + \ldots + x_ny_n \pmod 2$



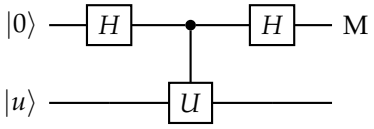
(1) What is the state of the two registers right after the quantum function evaluation?

(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.

3.4.B **Controlled unitaries revisited.** Consider the following quantum network composed of the two Hadamard gates, one controlled-U operation and the measurement M in the computational basis,



The top horizontal line represents a qubit and the bottom one an auxiliary physical system.

(1) Suppose $|u\rangle$ is an eigenvector of U, such that $U\,|u\rangle = e^{i\alpha}\,|u\rangle$. Step through the execution of this network, writing down quantum states of the qubit and the auxiliary system after each computational step. What is the probability for the qubit to be found in state $|0\rangle$?

Regardless the state of the auxiliary system, the probability P_0 for the qubit to be found in state $|0\rangle$, when the measurement M is performed, can be written as

$$P_0 = \frac{1}{2}\left(1 + v\cos\phi\right),$$

where v and ϕ depend on U and on the initial state of the auxiliary system.

(2) Show that for an arbitrary pure state $|u\rangle$ of the auxiliary system the quantities v and ϕ are given by the relation $ve^{i\phi} = \langle u|\,U\,|u\rangle$.

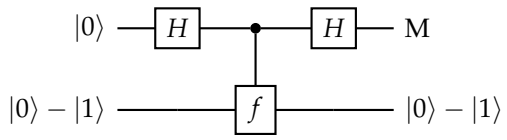
(3) Suppose the auxiliary system is prepared in a mixed state described by the density operator ρ,

$$\rho = \sum_{k=1}^{n} p_k \, |u_k\rangle\langle u_k|$$

where vectors $|u_k\rangle$ form an orthonormal basis, $p_k \geq 0$ and $\sum_{k=1}^{n} p_k = 1$. Show that v and ϕ are given by $ve^{i\phi} = \mathrm{tr}(\rho U)$.

(4) How would you modify the network in order to estimate $\mathrm{tr}(\rho U)$? How would you estimate $\mathrm{tr}\, U$?

3.5.B **Deutsch's algorithm and decoherence.** Deutsch's algorithm with an oracle $f : \{0,1\} \mapsto \{0,1\}$, is implemented by the following network



Suppose that in between the Hadamard gates the top qubit undergoes decoherence by interacting with an environment in state $|e\rangle$,

$$|0\rangle\,|e\rangle \quad \mapsto |0\rangle\,|e_0\rangle\,, \tag{3}$$

$$|1\rangle\,|e\rangle \quad \mapsto |1\rangle\,|e_1\rangle\,, \tag{4}$$

where $|e_0\rangle$ and $|e_1\rangle$ are the new states of the environment which are normalised but not necessarily orthogonal, $\langle e_0|e_1\rangle = v$ for some real v. How reliably can you tell whether f is constant or balanced?