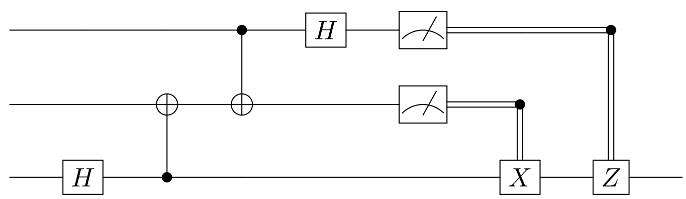
Quantum Computation & Cryptography
Lab sheet 3

Applications of entanglement

1. Recall one of the circuits from the first lab:



   This is a circuit for quantum teleportation. Alice has the first two qubits and Bob has the third one. Show that if the first input state is some qubit $|\psi\rangle$ and the other two inputs are $|00\rangle$ the circuit is equivalent to the teleportation procedure shown in the lectures. Implement it and test it with arbitrary states $|\psi\rangle$ to see that it does indeed work. As a second application, consider the task of Alice wanting to send 2 classical bits to Bob. This can be done by having Alice and Bob again share the $|\Phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ Bell state and having Alice send only one qubit to Bob (this is known as *superdense coding*). What simple modification can you make to the teleportation setup to achieve this?

2. We saw in the lectures the CHSH game. Briefly, Alice and Bob receive binary inputs x and y and need to produce the binary outputs a and b such that $xy = a \oplus b$ (importantly, Alice and Bob cannot communicate but can have preshared correlations like entanglement). We saw that the quantum strategy that Alice and Bob can use is to share many copies of the $|\Phi_+\rangle$ state and have Alice measure either the X or Z observables depending on the value of x, and Bob measure either $\frac{1}{\sqrt{2}}(X + Z)$ or $\frac{1}{\sqrt{2}}(X - Z)$ depending on the value of y. Implement the quantum strategy for the CHSH game and see (through experimentation) that it does indeed achieve a win rate of approximately 85.35% (higher than the classical maximum of 75%). You can do this as follows:

   (a) First implement measurement functions for all possible observables. You can do this using the regular computational basis measurement M and rotations on the Bloch sphere.

   (b) Implement the function *chshTest (k:Ket) (n:int)*. The function receives a Ket state k and a number of tests to be run, n. The Ket state is the state Alice and Bob will share in each round of the game (so they have n copies of k, you can mimic this by resetting the state after each measurement).

Assume the measurement settings (i.e. their inputs x and y) are chosen randomly (in $F\#$ the function $System.Random()$ returns a random number generator, call it $rand$ and you can then obtain a uniform random number between 0 and $m-1$ using $rand.Next(0, m)$).

(c) Test the function with a large number of iterations (say $n = 10000$). Display, at the end, the number of wins divided by the number of iterations (win rate). Test the function for the case when the Ket state is the $|\Phi_+\rangle$ state but also for non-entangled states. Check what happens to the win rate.

3. Implement the Ekert '91 (E91) protocol described in the lectures. As in the previous problem, assume Alice and Bob are sharing copies of some Ket state and that Alice randomly measures her qubit with either the X, Z, $\frac{1}{\sqrt{2}}(X+Z)$ observables, whereas Bob measures $\frac{1}{\sqrt{2}}(X+Z)$, $\frac{1}{\sqrt{2}}(X-Z)$, Z. You can keep the same template, i.e. *E91 (k:Ket) (n:int)*. When Alice and Bob measure the same observable count how many times their outcomes match and how many times they don't. When Alice and Bob are making the CHSH measurements, collect the statistics to compute the win rate. Test the implementation for the following cases and compare them using the data you collect in each case:

(a) **Ideal case**: The shared state of Alice and Bob is always the $|\Phi_+\rangle$ state.

(b) **Totally non-ideal case**: The shared state of Alice and Bob is always a separable state (say $|00\rangle$).

(c) **Eavesdropper case**: The shared state of Alice and Bob is always the *specialKet* state, which is provided in the source file.

(d) **Simple noise case**: The shared state of Alice and Bob is 1/4th of the time a separable state and the other times is the $|\Phi_+\rangle$ state.

(e) **Partly eavesdropping case**: The shared state of Alice and Bob is 1/4th of the time the *specialKet* state and the other times is the $|\Phi_+\rangle$ state.