INTRODUCTION TO QUANTUM INFORMATION SCIENCE

Solutions Set 2
HT 2020

ARTUR EKERT & JORDI MUR-PETIT

2.1. **Entangled qubits.**

(1) Alice and Bob will always obtain identical outcomes. However, since the outcomes are random and cannot be enforced this does not allow Alice and Bob to communicate instantaneously.

(2) Applying the unitary operations R_α and R_β to the entangled pair gives:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{R_\alpha \otimes R_\beta} \quad \tfrac{1}{\sqrt{2}}[(\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle)(\cos\beta\,|0\rangle + \sin\beta\,|1\rangle) + (-\sin\alpha\,|0\rangle + \cos\alpha\,|1\rangle)(-\sin\beta\,|0\rangle + \cos\beta\,|1\rangle)]]$$

Multiplying out the brackets:

$$\tfrac{1}{\sqrt{2}}[(\cos\alpha\cos\beta + \sin\alpha\sin\beta)\,|0\rangle\,|0\rangle + (\sin\alpha\sin\beta + \cos\alpha\cos\beta)\,|1\rangle\,|1\rangle + (\cos\alpha\sin\beta - \sin\alpha\cos\beta)\,|0\rangle\,|1\rangle + (\sin\alpha\cos\beta - \cos\alpha\sin\beta)\,|1\rangle\,|0\rangle]$$

and using standard trigonometric identities, we find :

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

The probability that Alice and Bob's outcomes are identical is just the square modulus of the corresponding amplitude i.e. $\cos^2(\alpha-\beta)$.

2.2. **Quantum teleportation.** Let us write the initial state of the circuit as

$$(\alpha\,|0\rangle + \beta\,|1\rangle)\,|0\rangle\,|0\rangle\,.$$

Remember that the convention is that the state of the top wire of a circuit diagram comes first. Consider the two smaller circuits

The one on the left maps the standard basis into the four Bell states

$$\begin{aligned}
|00\rangle &\mapsto |\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\\
|01\rangle &\mapsto |\psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),\\
|10\rangle &\mapsto |\psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),\\
|11\rangle &\mapsto |\psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).
\end{aligned}$$

The circuit on the right, which is the reverse image of the circuit on the left, implements the inverse of this operation and maps the Bell states $|\psi_{kl}\rangle$ into the corresponding states from the standard basis $|kl\rangle \equiv |k\rangle\,|l\rangle$. This one to one mapping allows us to implement the Bell measurement, that is, the projections on the Bell states, by first applying the circuit (on the right) and then performing the regular qubit by qubit measurement in the standard basis.

It should be clear now that after the Hadamard gate on qubit 2 and the first controlled-NOT on qubit 2 and 3 we have the total state

$$(\alpha\,|\,0\rangle + \beta\,|\,1\rangle)(|\,00\rangle + |\,11\rangle)/\sqrt{2}.$$

By regrouping the terms, but keeping the qubits in the same order, this state can be written as the sum

$$\begin{aligned}
\frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle) \quad &\otimes \quad (\alpha\,|\,0\rangle + \beta\,|\,1\rangle) + \\
\frac{1}{\sqrt{2}}(|\,01\rangle + |\,10\rangle) \quad &\otimes \quad (\alpha\,|\,1\rangle + \beta\,|\,0\rangle) + \\
\frac{1}{\sqrt{2}}(|\,00\rangle - |\,11\rangle) \quad &\otimes \quad (\alpha\,|\,0\rangle - \beta\,|\,1\rangle) + \\
\frac{1}{\sqrt{2}}(|\,01\rangle - |\,10\rangle) \quad &\otimes \quad (\alpha\,|\,1\rangle - \beta\,|\,0\rangle),
\end{aligned} \tag{1}$$

where we have dropped the normalisation factor $\frac{1}{2}$. The second controlled-NOT on qubits 1 and 2 followed by the Hadamard gate on qubit 1 maps the four Bell states of qubits 1 and 2 to the corresponding states from the computational basis

$$\begin{aligned}
|\,00\rangle \quad &\otimes \quad (\alpha\,|\,0\rangle + \beta\,|\,1\rangle) + \\
|\,01\rangle \quad &\otimes \quad (\alpha\,|\,1\rangle + \beta\,|\,0\rangle) + \\
|\,10\rangle \quad &\otimes \quad (\alpha\,|\,0\rangle - \beta\,|\,1\rangle) + \\
|\,11\rangle \quad &\otimes \quad (\alpha\,|\,1\rangle - \beta\,|\,0\rangle).
\end{aligned} \tag{2}$$

This gives the relation between outcomes x, y and the relative states of the third qubit.

Alice can save Cambridge science by teleporting the state of the first qubit. She performs the Bell measurement on the first two qubits, which gives two binary digits, x and y. She then lets Bob know what happened and broadcasts x and y. Upon learning the values of x and y Bob chooses one of the four Pauli transformations,

$$00 \to \mathbb{1}, \quad 01 \to X, \quad 10 \to Z, \quad 11 \to ZX,$$

(e.g. if $x = 0, y = 1$ he chooses X) and applies it to his qubit. This restores the original state of the first qubit, which was destroyed when Alice performed the Bell measurement.

2.3. **Playing with conditional unitaries.**

(1) Acting with S on each of the four Bell states gives us:

$$\begin{aligned}
S\frac{|\,00\rangle \pm |\,11\rangle}{\sqrt{2}} &= \frac{|\,00\rangle \pm |\,11\rangle}{\sqrt{2}} \\
S\frac{|\,01\rangle + |\,10\rangle}{\sqrt{2}} &= \frac{|\,01\rangle + |\,10\rangle}{\sqrt{2}} \\
S\frac{|\,01\rangle - |\,10\rangle}{\sqrt{2}} &= -\frac{|\,01\rangle - |\,10\rangle}{\sqrt{2}},
\end{aligned}$$

from which we deduce that eigenvectors $\{\frac{1}{\sqrt{2}}(|\,00\rangle \pm |\,11\rangle), \frac{1}{\sqrt{2}}(|\,01\rangle + |\,10\rangle)\}$ span the three-dimensional symmetric subspace. The antisymmetric subspace is one-dimensional and spanned by $\frac{1}{\sqrt{2}}(|\,01\rangle - |\,10\rangle)$. Since $S^2 = \mathbb{1}$, then S can only have two eigenvalues ± 1.

(2) Again, using $S^2 = \mathbb{1}$, we get: $P_+P_- = 0$ and $P_\pm^2 = P_\pm$, which confirms that $P_\pm$ are orthogonal projectors. Finally, it is straighforward to show that $P_+ + P_- = \mathbb{1}$, i.e., $P_\pm$ form a decomposition of the identity.
Applying them to $|\,a\rangle\,|\,b\rangle$:

$$\begin{aligned} P_+(|\,a\rangle\,|\,b\rangle) &= \frac{1}{2}(|\,a\rangle\,|\,b\rangle) + |\,b\rangle\,|\,a\rangle) \\ P_-(|\,a\rangle\,|\,b\rangle) &= \frac{1}{2}(|\,a\rangle\,|\,b\rangle) - |\,b\rangle\,|\,a\rangle). \end{aligned}$$

(3) Stepping through the network

$$\begin{aligned} |\,0\rangle\,|\,a\rangle\,|\,b\rangle &\mapsto \frac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle)\,|\,a\rangle\,|\,b\rangle && (3)\\ &\mapsto \frac{1}{\sqrt{2}}(|\,0\rangle\,|\,a\rangle\,|\,b\rangle + |\,1\rangle\,|\,b\rangle\,|\,a\rangle) && (4)\\ &\mapsto \frac{1}{2}((|\,0\rangle + |\,1\rangle)\,|\,a\rangle\,|\,b\rangle + (|\,0\rangle - |\,1\rangle)\,|\,b\rangle\,|\,a\rangle) && (5)\\ &= |\,0\rangle\,\frac{1}{2}(|\,a\rangle\,|\,b\rangle + |\,b\rangle\,|\,a\rangle) + |\,1\rangle\,\frac{1}{2}(|\,a\rangle\,|\,b\rangle - |\,b\rangle\,|\,a\rangle). && (6) \end{aligned}$$

The probability of observing the outcome s ($s \in \{0,1\}$) is obtained by calculating the modulus squared of the amplitude of the first qubit being in state s:

$$\begin{aligned} \text{Probability of } 0 &= \left|\frac{1}{2}(|\,a\rangle\,|\,b\rangle + |\,b\rangle\,|\,a\rangle)\right|^2 = \frac{1}{2}(1 + |\,\langle\,a\,|\,b\,\rangle\,|^2) \\ \text{Probability of } 1 &= \left|\frac{1}{2}(|\,a\rangle\,|\,b\rangle - |\,b\rangle\,|\,a\rangle)\right|^2 = \frac{1}{2}(1 - |\,\langle\,a\,|\,b\,\rangle\,|^2) \end{aligned}$$

(4) The output state $|\,0\rangle \otimes \frac{1}{2}(|\,a\rangle\,|\,b\rangle + |\,b\rangle\,|\,a\rangle) + |\,1\rangle \otimes \frac{1}{2}(|\,a\rangle\,|\,b\rangle - |\,b\rangle\,|\,a\rangle)$ shows clearly that outcomes 0 or 1 lead to the "collapse" of the superposition to either the symmetric or the antisymmetric component of $|\,a\rangle\,|\,b\rangle$.
(5) Operators S and $U \otimes U$ commute. $(U \otimes U)S\,|\,a\rangle\,|\,b\rangle = (U \otimes U)\,|\,b\rangle\,|\,a\rangle = |\,b'\rangle\,|\,a'\rangle$ and $S(U \otimes U)\,|\,a\rangle\,|\,b\rangle = S\,|\,a'\rangle\,|\,b'\rangle = |\,b'\rangle\,|\,a'\rangle$. Thus, the symmetric and the antisymmetric subspaces are invariant under the action of $U \otimes U$.
(6) The uncontrolled rotation of the photon polarisation angle amounts to a random unitary U as in (5). Thus, we can use symmetric and antisymmetric two-photon states to encode one bit of information. Here two photons are needed to encode one logical bit but the transmission is error free.

2.4. **Simon's algorithm.**

(1) The first two computational steps end up with the quantum function evaluation and generate the state

$$|\,0\rangle\,|\,0\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\rangle\,|\,0\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\,x\rangle\,|\,f(x)\rangle\,.$$

(Note: the summation is over all n-bit strings x.) This is an entangled state of the two registers. Here and in the following $|\,0\rangle$ represents a binary string of length n with all qubits showing logical 0.
(2) If $k \in \{0,1\}^n$ is the result of the bit-by-bit measurement on the second register then the state of the first register is a superposition of exactly those values of x for which $f(x) = k$. The problem statements says we are assuming $s \neq 0^n$ (i.e., f is not one-to-one). In this case, from the fact that $k \in \text{range}(f)$, it follows that there exist two strings $x, x' \in \{0,1\}^n$ such that $f(x) = f(x') = k$ and moreover $x \oplus x' = s$, or equivalently $x' = x \oplus s$.

Hence, we can write the state of the first register as

$$\frac{1}{\sqrt{2}}\left(|\,x\rangle + |\,x+s\rangle\right).$$

(3) The Hadamard transform applied to the first register after the function evaluation and the measurement on the second register gives

$$\begin{aligned}\frac{1}{\sqrt{2}}\left(|\,x\rangle + |\,x+s\rangle\right) &\mapsto \frac{1}{\sqrt{2^{n+1}}}\sum_{z\in\{0,1\}^n}\left[(-1)^{x\cdot z}+(-1)^{(x+s)\cdot z}\right]|\,z\rangle \\ &= \frac{1}{\sqrt{2^{n+1}}}\sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}\left[1+(-1)^{s\cdot z}\right]|\,z\rangle\,.\end{aligned}$$

When the first register is subsequently measured bit-by-bit in the computational basis, the probability of getting a particular binary string z is

$$\frac{1}{2^{n+1}}\left(1+(-1)^{s\cdot z}\right)^2 = \begin{cases} 1/2^{n-1} & , \quad \text{if } s\cdot z = 0 \\ 0 & , \quad \text{if } s\cdot z = 1 \end{cases}$$

The products of binary strings are non-negative integers; hence, the measured string z must satisfy $s\cdot z = 0$.

(4) Students should be able to provide estimates and plausibility arguments. More detailed explanations, as presented below, are not required.

Students should notice that running the quantum network gives us a method for extracting uniformly random strings z such that $s\cdot z = 0$ for our unknown s. If $z \neq 0$, then this cuts in half the number of possible s strings consistent with this equation. In order to find s we need $n-1$ such equations, $z_1\cdot s = 0, z_2\cdot s = 0, \ldots z_{n-1}\cdot s = 0$, with the z_i being linearly independent ($s = 0$ is always a solution but we have excluded it). The probability of obtaining $n-1$ independent binary strings of length n via random sampling can be estimated in many ways. For example, one can notice that m linearly independent vectors $z_1, z_2, \ldots z_m$, specify a subspace with 2^m bit strings. The probability that the next bit string z_{m+1} is linearly independent is $(2^n - 2^m)/2^n$. Chaining these conditional probabilities we obtain the probability of getting $n-1$ linearly independent bit strings,

$$\Pr = \left(1-\frac{1}{2^n}\right)\left(1-\frac{1}{2^{n-1}}\right)\cdots\left(1-\frac{1}{4}\right).$$

To bound this we then use the fact that $(1-a)(1-b) \geq 1-a-b$ for $0 \leq a, b \leq 1$ to turn the products into a sum,

$$\Pr \geq 1-\left(\frac{1}{2^n}+\frac{1}{2^{n-1}}+\cdots+\frac{1}{4}\right) > \frac{1}{2}.$$

Thus with probability of greater than $1/2$ we obtain $n-1$ linearly independent bit strings z_i and can solve for s. We may need to repeat this process a few times; the probability that we fail to find s decreases exponentially with the number of repetitions. Thus the number of runs for the quantum algorithm is of the order of n.

In contrast a classical algorithm randomly chooses $x_1, x_2, \ldots x_k$, evaluates $f(x_1), f(x_2), \ldots f(x_k)$ and checks for collision events where $f(x_i) = f(x_j)$ for some x_i and x_j ($s = x_i + x_j$). The probability for at least one collision can be estimated in a number of different ways (the birthday paradox type calculations) and it is not greater than $k^2/2^n$. This implies that we have to sample roughly $\sqrt{2^n}$ times in order to find a collision (and hence s).

This problem was presented in a preliminary version in D. R. Simon, "On the power of quantum computation", Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, p. 116 (1994) [DOI: 10.1109/SFCS.1994.365701] and in further detail in SIAM J. Comput. ***26****, 1474 (1997) [DOI: 10.1137/S0097539796298637].*