Quantum Information Theory
Solutions 13

Exercise 13.1 One-time Pad

Consider three random variables: a message M, a secret key K and a ciphertext C. We want to encode M as a ciphertext C using K with perfect secrecy, so that no one can guess the message from the cipher: $I(C : M) = 0$.
After the transmission, we want to be able to decode the ciphertext: someone that knows the key and the cipher should be able to obtain the message perfectly, i.e. $H(M|C,K) = 0$.
Show that this is only possible if the key contains at least as much randomness as the message, namely $H(K) \geq H(M)$. Give an optimal algorithm for encoding and decoding.

First note that

$$\begin{aligned} I(C:M) - I(C:M|K) &= I(M:K) - I(M:K|C) \\ &= I(K:C) - I(K:C|M), \end{aligned}$$

and that mutual information is non-negative. We introduce $x = I(C : M|K)$, $y = I(M : K|C)$ and $z = I(K : C|M)$ and, using $I(C : M) = 0$, we get

$$x - I(C;M) = x = y - I(M;K) = z - I(K;C). \tag{1}$$

Using the two conditions, we write

$$\begin{aligned} H(M) &= H(M|C,K) + I(C:M) + I(K:M|C) = y, \quad \text{and} \\ H(K) &= H(K|M,C) + I(M:K) + I(M:C|K) \geq y - x + z. \end{aligned}$$

However, since $y \geq x$ and $z \geq x$ (from (1)), we get $H(K) \geq H(M)$.
Given a message M of m bits, an optimal encoding algorithm could first compress the message to $H(M)$ bits and then use a secret and completely random binary key of length $H(M)$ to encode it. Given a message bit M_i and a secret code bit K_i, the ciphertext bit would be generated $C_i = M_i \oplus K_i$ using XOR. The decoding would recreate the message bit $M_i = C_i \oplus K_i$ and then decompress it.

Exercise 13.2 Secret Key Agreement

The Bell basis vectors are given by the Bell states

$$|\Psi_{1,2}\rangle := \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \qquad |\Psi_{3,4}\rangle := \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{2}$$

Furthermore, let us introduce an additional step in the algorithm right after sifting: Alice and Bob agree on one of four equiprobable operations $\{\mathbb{1}, X, iY, Z\}$ that they perform on their corresponding qbit. After performing, they forget which operation they have chosen.

a) *Express the Pauli operators $X \otimes X$, $iY \otimes iY$ and $Z \otimes Z$ in the Bell basis.*

This calculation is straight-forward. Let us apply these operators onto the basis vectors $|\Psi_i\rangle$ and write the resulting vectors in terms of the $|\Psi_i\rangle$ and voilà, we have the operator in the Bell basis. For group theory enthusiasts: the Bell states are irreducible representations of the permutation group, hence operators $U^{\otimes 2} = U \otimes U$, U unitary, will not mix the symmetric subspace spanned by $|\Psi_i\rangle, i = 1 \ldots 3$ with the antisymmetric subspace $|\Psi_4\rangle$. Furthermore, the calculation shows that, in the Bell basis,

$$X \otimes X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad iY \otimes iY = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and}$$

$$Z \otimes Z = (iY \cdot X) \otimes (iY \cdot X) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

are diagonal.

b) *What is the most general shared state ρ_{AB} after these operations have been applied? Hint: The matrix ρ_{AB} will have 3 degrees of freedom.*

The most general matrix $\tilde{\rho}_{AB}$ is a positive hermitian matrix with trace 1:

$$\tilde{\rho}_{AB} = \begin{pmatrix} a & e & f & g \\ e^* & b & h & i \\ f^* & h^* & c & j \\ g^* & i^* & j^* & d \end{pmatrix}.$$

Applying one of the operations and forgetting the outcome is equivalent to producing a mixture of the different resulting states. The operation can thus be written as:

$$\tilde{\rho}_{AB} \mapsto \rho_{AB} = \frac{1}{4}\Big(\tilde{\rho}_{AB} + X^{\otimes 2}\tilde{\rho}_{AB}X^{\otimes 2} + Y^{\otimes 2}\tilde{\rho}_{AB}Y^{\otimes 2} + Z^{\otimes 2}\tilde{\rho}_{AB}Z^{\otimes 2}\Big) \tag{3}$$

and we get

$$\rho_{AB} = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{pmatrix}. \tag{4}$$

This matrix is real and positive if $a, b, c, d \geq 0$ and the trace condition $a + b + c + d = 1$ limits our degrees of freedom to 3. From another perspective, the above operation symmetrizes our density matrix in the sense that it now fulfills $\mathrm{tr}_B \rho_{AB} = \mathrm{tr}_A \rho_{AB} = \mathbb{1}/2$ as you can easily verify.

Let us denote the probability of detecting anti-correlation when measuring on the $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis by ε^+ and $\varepsilon^\times$ respectively. Henceforth, we assume that $\varepsilon^+ = \varepsilon^\times = \varepsilon$.

c) *Find the projectors P^+ and $P^\times$ that describe anti-correlation measurements.*

First, it is easy to see that

$$P^+ = |01\rangle\langle 01|01 + |10\rangle\langle 10|10 = |\Psi_3\rangle\langle\Psi_3|\Psi_3 + |\Psi_4\rangle\langle\Psi_4|\Psi_4 \tag{5}$$

in the Bell basis. If we measure in the $\{|+\rangle, |-\rangle\}$ basis, we get

$$P^\times = |+-\rangle\langle +-|+- + |-+\rangle\langle -+|-+ = H^{\otimes 2}P^+H^{\otimes 2}, \tag{6}$$

where H is the Hadamard matrix. One way to evaluate this is by expressing $H^{\otimes 2}$ in the Bell basis. This simple calculation results in

$$H^{\otimes 2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{7}$$

From this follows immediately that

$$P^{\times} = |\Psi_2\rangle\langle\Psi_2|\Psi_2 + |\Psi_4\rangle\langle\Psi_4|\Psi_4. \tag{8}$$

d) *For given ε, find the two additional constraints imposed on ρ_{AB} by*

$$\varepsilon = \mathrm{tr}(\rho_{AB}P^{+}) = \mathrm{tr}(\rho_{AB}P^{\times}). \tag{9}$$

Given the results of c), this is trivial and we get the constraints

$$c + d = \varepsilon, \quad \text{and} \quad b + d = \varepsilon. \tag{10}$$

We can now rewrite the density operator ρ_{AB} using only two parameters d and ε:

$$\rho_{AB} = \begin{pmatrix} 1 + d - 2\varepsilon & 0 & 0 & 0 \\ 0 & \varepsilon - d & 0 & 0 \\ 0 & 0 & \varepsilon - d & 0 \\ 0 & 0 & 0 & d \end{pmatrix}. \tag{11}$$

In the worst case, the adversary, Eve, holds a purification ρ_{ABE} of ρ_{AB}. The secret key rate R is defined as the number of secret bits that can be generated per shared qubit asymptotically. For our symmetric problem, it is given by $R = I(A:B) - I(A:E)$. A secret key can be generated if and only if $R > 0$.

e) *Show that $R > 0$ can only be achieved if and only if $S(A,B) < 1$.*

First, let us expand $R = I(A:B) - I(A:E) = S(A) + S(B) - S(A,B) - S(A) - S(E) + S(A,E)$. Since the state ρ_{ABE} is pure, we get $S(E) = S(A,B)$ and $S(A,E) = S(B)$ (this follows from the Schmidt decomposition). Furthermore, it can easily be verified that $S(A) = S(B) = 1$, i.e. if we trace out one system in our diagonal ρ_{AB}, we will end up with a completely mixed state. Using these properties, we find that $R = 2S(B) - 2S(A,B) = 2\big(1 - S(A,B)\big)$, which is positive if and only if $S(A,B) < 1$.

f) *For given ε, there is one degree of freedom left in ρ_{AB}. Maximize $S(A,B)$ to get rid of it.*

We want to maximize the function $f_\varepsilon(d)$ given by the entropy $S(A,B)$ (this entropy is essentially a Shannon entropy, since the density matrix is diagonal):

$$f_\varepsilon(d) = -(1 + d - 2\varepsilon)\log(1 + d - 2\varepsilon) - 2(\varepsilon - d)\log(\varepsilon - d) - d\log d. \tag{12}$$

After some simplifications, you should get

$$\frac{\partial f_\varepsilon}{\partial d} = -\log\frac{(\varepsilon - d)^2}{d(1 + d - 2\varepsilon)}, \tag{13}$$

which equals zero if and only if $(\varepsilon - d)^2 = d(1 + d - 2\epsilon)$. Finally, we get $d = \varepsilon^2$. Is this indeed a maximum? The parameter d is bounded by $0 \leq d \leq \varepsilon$ by positivity constraints on ρ_{AB}. We now compare $f_\varepsilon(\varepsilon^2)$, $f_\varepsilon(\varepsilon)$ and $f_\varepsilon(0)$ to find the maximum. Using the binary entropy function $H(\varepsilon)$, we immediately find that

$$f_\varepsilon(\varepsilon^2) = 2H(\varepsilon), \qquad f_\varepsilon(\varepsilon) = H(\varepsilon) \qquad \text{and} \tag{14}$$

$$f_\varepsilon(0) = -(1 - 2\varepsilon)\log(1 - 2\varepsilon) - 2\varepsilon \log \varepsilon. \tag{15}$$

We now try to bound $f_\varepsilon(0) \leq 2H(\varepsilon)$ for $\varepsilon \in [0, 1/2]$. First, we substitute and simplify to get

$$(1 - 2\varepsilon)\log(1 - 2\varepsilon) \geq 2(1 - \varepsilon)\log(1 - \varepsilon). \tag{16}$$

Next, we note that the the inequality holds at $\varepsilon = 0$ and differentiate with regards to ε on both sides. If the left-hand side increases faster than the right-hand side, the inequality is shown. We thus need to show that

$$-2 - 2\log(1 - 2\varepsilon) \geq -2 - 2\log(1 - \varepsilon). \tag{17}$$

Hence, $f_\varepsilon(0) \leq 2H(\varepsilon)$ holds if $\log(1 - 2\varepsilon) \leq \log(1 - \varepsilon)$, which is obviously satisfied in the required interval of ε. Thus, we have shown that $d = \epsilon^2$ maximizes the von Neumann entropy of ρ_{AB}.

g) *Find an upper limit on ε, such that we can still generate a secret key. Hint: You will either have to find ε numerically or give an approximation.*

The error parameter ε must satisfy $H(A, B) \leq 1$ or $H(\varepsilon) \leq 1/2$. The binary entropy function certainly satisfies this if

$$\varepsilon < 0.1.$$