Sample Solutions Exercise 7

Exercise 7.1: Quantum Cryptography (8P)

Encrypted communication requires that both parties share a key (a random sequence of classical bits) that can be used to encode and decode messages by bitwise XOR operations. The problem of encryption therefore reduces to safely generate identical keys on both sides. In 1992 H.C. Bennett proposed a particularly simple protocol (B92):

> Alice randomly generates a classical bit $a \in \{0,1\}$, using it to prepare a qubit
>
> $$|\psi\rangle = \begin{cases} |0\rangle & \text{if } a = 0 \\ |+\rangle & \text{if } a = 1 \end{cases}$$
>
> where $|\pm\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \pm |1\rangle\big)$. Then she sends this qubit to Bob.
>
> Likewise Bob randomly generates a classical bit $b \in \{0,1\}$. He uses this bit to select one of the two measurement apparatuses
>
> $$\mathbf{M}_0 = |0\rangle\langle 0| - |1\rangle\langle 1|\,, \qquad \mathbf{M}_1 = |+\rangle\langle +| - |-\rangle\langle -|$$
>
> which is then used to measure Alice's incoming qubit. Then he sends the measurement result $m = \pm 1$ by classical public communication to Alice. Both Alice and Bob repeat the process until they get the result $m = -1$.

(a) Show that $a = 1 - b$ if $m = -1$, that is, the locally generated bits are opposite. (2P)

(b) How many qubits are on average needed to generate a bit of the key? (1P)

(c) Suppose that Eve intercepts the communication in that she measures the transferred qubit by a projective measurement $\mathbf{E} = |\phi_+\rangle\langle\phi_+| - |\phi_-\rangle\langle\phi_-|$, where

$$|\phi_+\rangle = \alpha|0\rangle + \beta|1\rangle\,, \qquad |\phi_-\rangle = \beta^*|0\rangle - \alpha^*|1\rangle\,, \qquad |\alpha|^2 + |\beta|^2 = 1$$

are two arbitrary orthogonal states. Show that Eve's interception generally changes the measurement statistics seen from the perspective of Bob and Alice, depending effectively on two parameters $u := |\alpha|^2$ and $v := \frac{1}{2}|\alpha + \beta|^2$. (3P)

(d) Determine u and v such that Bob and Alice cannot detect the interception. (1P)

(e) In the case of (d), is it possible for Eve to get information about the key? (1P)

Sample Solution

(a) The simplest approach is to set up a table of all possibilities for the joint system (Alice+Bob)

a	$\|\psi\rangle$	b	$\mathbf{M}$	$P(m=1\|a,b)$	$P(m=-1\|a,b)$
0	$\|0\rangle$	0	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	1	0
0	$\|0\rangle$	1	$\|+\rangle\langle +\| - \|-\rangle\langle -\|$	1/2	1/2
1	$\|+\rangle$	0	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	1/2	1/2
1	$\|+\rangle$	1	$\|+\rangle\langle +\| - \|-\rangle\langle -\|$	1	0

Clearly, if $m=-1$, we have $a=1-b$ with certainty.

(b) Each line in the table takes place with probability $P(a,b)=1/4$. Therefore, the probability to get $m=-1$ is $1/4$, meaning that we need on average four qubits for generating one bit of the key.

(c) Without interception Alice will see the measurement statistics given by $P(m,a)=\sum_b P(m|a,b)P(a)P(b)$ as listed in the following table:

a	$m=1$	$m=-1$
0	3/8	1/8
1	3/8	1/8

Bobs measurement statistics $P(m,b)=\sum_a P(m|a,b)P(a)P(b)$ turns out to be given by the same table.

Now let us assume that Eve measures the qubit on its way to Bob by a projective measurement $\mathbf{E}=|\phi_+\rangle\langle\phi_+|-|\phi_-\rangle\langle\phi_-|$. Eve will get a measurement result $e=\pm 1$ and the state of the qubit $|\psi\rangle$ will be mapped projectively to a different state $|\psi'\rangle$. Regarding the total system, the table therefore doubles:

a	$\|\psi\rangle$	e	$P(e\|a)$	$\|\psi'\rangle$	b	$\mathbf{M}$	$P(m=1\|a,e,b)$
0	$\|0\rangle$	+	$\|\alpha\|^2$	$\|\phi_+\rangle$	0	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\|\alpha\|^2$
0	$\|0\rangle$	-	$\|\beta\|^2$	$\|\phi_-\rangle$	0	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\|\beta\|^2$
0	$\|0\rangle$	+	$\|\alpha\|^2$	$\|\phi_+\rangle$	1	$\|+\rangle\langle +\| - \|-\rangle\langle -\|$	$\frac{1}{2}\|\alpha+\beta\|^2$
0	$\|0\rangle$	-	$\|\beta\|^2$	$\|\phi_-\rangle$	1	$\|+\rangle\langle +\| - \|-\rangle\langle -\|$	$\frac{1}{2}\|\alpha-\beta\|^2$
1	$\|+\rangle$	+	$\frac{1}{2}\|\alpha+\beta\|^2$	$\|\phi_+\rangle$	0	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\|\alpha\|^2$
1	$\|+\rangle$	-	$\frac{1}{2}\|\alpha-\beta\|^2$	$\|\phi_-\rangle$	0	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\|\beta\|^2$
1	$\|+\rangle$	+	$\frac{1}{2}\|\alpha+\beta\|^2$	$\|\phi_+\rangle$	1	$\|+\rangle\langle +\| - \|-\rangle\langle -\|$	$\frac{1}{2}\|\alpha+\beta\|^2$
1	$\|+\rangle$	-	$\frac{1}{2}\|\alpha-\beta\|^2$	$\|\phi_-\rangle$	1	$\|+\rangle\langle +\| - \|-\rangle\langle -\|$	$\frac{1}{2}\|\alpha-\beta\|^2$

Because of $|\alpha|^2+|\beta|^2=1$ and $\frac{1}{2}|\alpha+\beta|^2+\frac{1}{2}|\alpha-\beta|^2=1$ this table depends only on two real parameters, namely $u=|\alpha|^2$ and $v=\frac{1}{2}|\alpha+\beta|^2$. The probability table seen by Alice is given by

a	$m=1$	$m=-1$
0	$Q_0/2$	$(1-Q_0)/2$
1	$Q_1/2$	$(1-Q_1)/2$

where

$$Q_0=\frac{1}{2}\left(u^2+(1-u)^2+uv+(1-u)(1-v)\right),$$
$$Q_1=\frac{1}{2}\left(vu+(1-v)(1-u)+v^2+(1-v)^2\right).$$

The measurement statistics seen by Bob turns out to be given by the same table.

(d) Alice and Bob cannot detect Eve's interception if the modified probability table coincides with the unperturbed one, i.e. if $Q_0=Q_1=3/4$. These equations have two solutions, namely, $u=v=\frac{1}{4}(2\pm\sqrt{2})$.

(e) In this situation the probability for Eve to get $e = 1$ is given by u, irrespective of the values of a, b. Therefore, Eve cannot retrieve any information in this situation.

Exercise 7.2: Supremum norm of operators (4P)

The supremum norm of a bounded operator $\mathbf{M}$ is defined by

$$||\mathbf{M}|| = \sup_{|\psi\rangle} \frac{||\,\mathbf{M}|\psi\rangle\,||}{||\,|\psi\rangle||}\,,$$

where $||\,|\psi\rangle|| = \langle\psi|\psi\rangle$ is the usual vector norm in the Hilbert space.

(a) Show that $||\mathbf{M}||$ is the square root of the maximal eigenvalue of $\mathbf{M}^\dagger\mathbf{M}$. (2P)

(b) Prove that the norm $||\mathbf{M}||$ is subadditive $\big(||\mathbf{M}+\mathbf{N}|| \leq ||\mathbf{M}|| + ||\mathbf{N}||\big)$ and submultiplicative $\big(||\mathbf{MN}|| \leq ||\mathbf{M}||\,||\mathbf{N}||\big)$. (2P)

Sample Solution

(a) Note that $||\mathbf{M}|| \geq 0$. Therefore, the squared supremum equals the supremum of the squares so that we can write:

$$||\mathbf{M}||^2 = \sup_{|\psi\rangle} \frac{||\,\mathbf{M}|\psi\rangle\,||^2}{||\,|\psi\rangle||^2} = \sup_{|\psi\rangle} \frac{\langle\psi|\mathbf{M}^\dagger\mathbf{M}|\psi\rangle}{\langle\psi|\psi\rangle}$$

$\mathbf{M}^\dagger\mathbf{M}$ is quadratic and Hermitean, hence it has an orthonormal eigendecomposition $\mathbf{M}^\dagger\mathbf{M} = \sum_N \lambda_n |n\rangle\langle n|$ with real eigenvalues λ_n. Let λ_{n_0} be the maximal eigenvalue. Then

$$||\mathbf{M}||^2 = \sup_{|\psi\rangle} \sum_n \underbrace{\frac{\langle\psi|n\rangle\langle n|\psi\rangle}{\langle\psi|\psi\rangle}}_{\geq 0} \lambda_n \leq \sup_{|\psi\rangle} \underbrace{\sum_n \frac{\langle\psi|n\rangle\langle n|\psi\rangle}{\langle\psi|\psi\rangle}}_{=1} \lambda_{n_0} = \lambda_{n_0}$$

On the other hand, choosing $|\psi\rangle$ to be the eigenvector $|n_0\rangle$ corresponding to the maximal eigenvalue, we get

$$||\mathbf{M}||^2 \geq \sum_n \underbrace{\frac{\langle n_0|n\rangle\langle n|n_0\rangle}{\langle n_0|n_0\rangle}}_{=\delta_{n,n_0}} \lambda_n = \lambda_{n_0}.$$

Hence $||\mathbf{M}||^2 = \lambda_{n_0}$. Since $||\mathbf{M}|| \geq 0$ we can conclude that $||\mathbf{M}|| = \sqrt{\lambda_{n_0}}$. □

(b) **Subadditivity** (triangle relation): We simply use the ordinary triangle relation for the vector norm in the nominator:

$$||\mathbf{M}+\mathbf{N}|| = \sup_{|\psi\rangle} \frac{||(\mathbf{M}+\mathbf{N})|\psi\rangle||}{\langle\psi|\psi\rangle} \leq \sup_{|\psi\rangle} \frac{||\mathbf{M}|\psi\rangle|| + ||\mathbf{N}|\psi\rangle||}{\langle\psi|\psi\rangle}$$

$$\leq \sup_{|\psi\rangle} \frac{||\mathbf{M}|\psi\rangle||}{\langle\psi|\psi\rangle} + \sup_{|\psi\rangle} \frac{||\mathbf{N}|\psi\rangle||}{\langle\psi|\psi\rangle} = ||\mathbf{M}|| + ||\mathbf{N}||$$

Submultiplicativity:

$$||\mathbf{MN}|| = \sup_{|\psi\rangle} \frac{||\mathbf{MN}|\psi\rangle||}{|||\psi\rangle||} = \sup_{|\psi\rangle} \frac{||\mathbf{MN}|\psi\rangle||}{||\mathbf{N}|\psi\rangle||} \frac{||\mathbf{N}|\psi\rangle||}{|||\psi\rangle||}$$

$$\leq \sup_{|\psi\rangle} \frac{||\mathbf{MN}|\psi\rangle||}{||\mathbf{N}|\psi\rangle||} \sup_{|\psi\rangle} \frac{||\mathbf{N}|\psi\rangle||}{|||\psi\rangle||} \leq \sup_{|\phi\rangle} \frac{||\mathbf{M}|\phi\rangle||}{|||\phi\rangle||} \sup_{|\psi\rangle} \frac{||\mathbf{N}|\psi\rangle||}{|||\psi\rangle||} = ||\mathbf{M}||\,||\mathbf{N}||$$

$(\Sigma = \mathbf{12P})$