Quantum Cryptography (spring 2020)	Dominique Unruh
Exercise Sheet 7	
Out: 2020-04-26	Due: 2020-05-04

Problem 1: Doing the Impossible

Let $|\beta_{ab}\rangle$ for $a, b \in \{0, 1\}$ be the Bell states, and let

$$P_{bf} := |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{10}\rangle\langle\beta_{10}|,$$
$$P_{pf} := |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{01}\rangle\langle\beta_{01}|.$$

(Remember that $\{P_{bf}, 1 - P_{bf}\}$ and $\{P_{pf}, 1 - P_{pf}\}$ are the measurements that Alice and Bob need to perform on their qubit pairs during the Bell test.)

(a) Consider the following two experiments on a two qubit system.

  (i) The two qubits are (jointly) measured according to the measurement $\{P_{yes} := P_{bf}, P_{no} := 1 - P_{bf}\}$. Then the qubits are destroyed.

  (ii) The two qubits are individually measured in the computational basis $\{|0\rangle, |1\rangle\}$. If the results are equal, output *yes*, otherwise output *no*. Then the qubits are destroyed.

  Show that both experiments are equivalent. That is, show that for any two-qubit state $\rho \in S(\mathbb{C}^4)$, we have that the probability for getting outcome *yes* is the same. (Usually, one would have to also show that the post-measurement state is the same. But since here the qubits are destroyed, this is trivially the case.)

  Hint: Let P_{00}, P_{11} be the two projectors corresponding to both measuring 0 and both measuring 1, respectively, in the second experiment. Then the probability of *yes* in the second experiment is $\operatorname{tr} P_{00}\rho + \operatorname{tr} P_{11}\rho = \operatorname{tr}(P_{00} + P_{11})\rho$.

(b) Consider the following two experiments on a two qubit system.

  (i) The two qubits are (jointly) measured according to the measurement $\{P_{yes} := P_{pf}, P_{no} := 1 - P_{pf}\}$. Then the qubits are destroyed.

  (ii) The two qubits are individually measured in the diagonal basis $\{|+\rangle, |-\rangle\}$ with $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. If the results are equal, output *yes*, otherwise output *no*. Then the qubits are destroyed.

  Show that both experiments are equivalent.

Note that in both cases, experiment (ii) can be implemented even if the two qubits are in different locations and only classical communication is possible between these locations. This allows to replace the Bell test from the lecture by a procedure that can actually be implemented.

Problem 2: Techniques from the QKD proof

Consider the following (rather useless) protocol. Alice gets a state $\rho \in S(\mathbb{C}^{2^n})$ consisting of n qubits. Then Alice chooses a random $i \in \{1, \dots, n\}$ and measures the i-th qubit in ρ in the computational basis. (The qubit is not discarded after the measurement.) If this measurement returns 1, Alice aborts. Let $\tilde\rho$ denote the state that Alice has under the condition that she does not abort. Let $P_{success}$ denote the probability of *not* aborting.

In the following, by $T(\rho)$ we denote the density operator $p\tilde\rho$ where p is the probability that ρ passes Alice's test and $\tilde\rho$ is the state that results after passing Alice's test. (In particular, $\tilde\rho = \frac{T(\rho)}{\operatorname{tr} T(\rho)}$ and $p = \operatorname{tr} T(\rho)$.) For any projector P, we write short $P(\rho)$ for $P\rho P^\dagger$.

Hint: The following proofs use techniques that have appeared in the proof of QKD. However, the present case is somewhat simpler.

(a) Assume that $\rho = |x\rangle\langle x|$ for some $x \in \{0,1\}^n$, $x \neq 0^n$. Show that ρ passes Alice's test with probability at most $\delta := \frac{n-1}{n}$.

(b) Assume that $\rho = \sum_{x\in\{0,1\}^n} p_x |x\rangle\langle x|$ for some $p_x \geq 0$, $\sum p_x = 1$. Let $P_{ok} := |0^n\rangle\langle 0^n|$. Show that $\operatorname{tr} P_{ok}(\tilde\rho) \geq 1 - \frac{\delta}{P_{success}} = 1 - \frac{\delta}{\operatorname{tr} T(\rho)}$.

(c) Assume that $\rho \in S(\mathbb{C}^{2^n})$ (arbitrary state). Show that $\operatorname{tr} P_{ok}(\tilde\rho) \geq 1 - \frac{\delta}{P_{success}}$.

Hint: Consider a complete measurement in the computational basis, and use the fact that it commutes with other measurements in the computational basis.

(d) Show that $\mathrm{TD}(\tilde\rho, |0^n\rangle\langle 0^n|) \cdot P_{success} \leq \sqrt{\frac{n-1}{n}}$.

Problem 3: Commuting Measurements (Bonus Problem)

Let $\mathcal{H}$ be a Hilbert space and let $|\Psi_1\rangle, \dots, |\Psi_n\rangle$ be an orthonormal basis of $\mathcal{H}$.

Let $M = \{P_1, \dots, P_a\}$ and $M' = \{P'_1, \dots, P'_b\}$ be measurements on $\mathcal{H}$. Assume that each P_i and P'_i is of the form $\sum_j \lambda_j |\Psi_j\rangle\langle\Psi_j|$. (Here the λ_j may be different for the different projectors, but the $|\Psi_j\rangle$ are the same for all projectors.)

We will show that it does not matter in which order to apply the measurements M and M' for any density operator ρ.

More precisely, consider the following two experiments:

(i) Measure ρ with measurement M and then measure the resulting post-measurement state with measurement M'. Let o and o' denote the outcomes of M and M', respectively, and let $\tilde\rho$ denote the final post-measurement state.

(ii) Measure ρ with measurement M' and then measure the resulting post-measurement state with measurement M. (I.e., the measurements are applied in inverse order.) Let o and o' denote the outcomes of M and M', respectively, and let $\tilde\rho'$ denote the final post-measurement state.

Show the following facts:

(a) For all i, j we have $\Pr[o = i \text{ and } o' = j : \text{ experiment (i)}] = \Pr[o = i \text{ and } o' = j : \text{ experiment (ii)}]$.

(b) For all i, j, we have $\tilde{\rho} = \tilde{\rho}'$ where $\tilde{\rho}$ and $\tilde{\rho}'$ are the post-measurement states in the case of $o = i$ and $o' = j$.

Hint: You may assume without loss of generality that $|\Psi_1\rangle, \dots, |\Psi_n\rangle$ is the computational basis $|1\rangle, \dots, |n\rangle$. (Since otherwise one can just do a basis transformation to transform it into that basis.) In that case, all P_i and P_i' will be diagonal.