Quantum Cryptography (spring 2021) Dominique Unruh

Exercise Sheet 09

Out: 2021-04-20 Due: 2021-04-27

1 Bell test, 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.)

Note that in both cases below, 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.

(a)

Knowlets:	BellTest, DensityM ProblemID: BellTestComp
Time:	
Difficulty:	

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)

Knowlets:	BellTest, DensityM ProblemID: BellTestDiag
Time:	
Difficulty:	

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.

2 Missing claims from QKD proof

(a)

Knowlets:	RawKey ProblemID: CountTError
Time:	
Difficulty:	

In the practice we showed (or will show) that in our QKD protocol, after the Bell test and after measuring the n-bit raw key, we have

$$H_\infty(K_A|E)_{\rho_{raw}} \geq -\log(N2^{-n})$$

where $N := |\{xy \in \{0,1\}^{2n} : |xy| \leq t\}|$. (Note: $|xy|$ does not refer to the Hamming weight of xy here, but to the number of non-00 bitpairs.)

Show that $N \leq (3n+1)^t$.

Hint: Think of how you can compactly describe the bitstring xy with $|xy|$ by only telling where the non-00 pairs are, and then calculate how many such descriptions there are.

(b)

Knowlets:	RawKey, RawKeyKeyDiff ProblemID: RawKeyDiff
Time:	
Difficulty:	

In the lecture, we claimed that if $\rho \in S^{\text{test}}_{\text{Ideal}}$, and we measure A's and B's system in the computational basis, then with probability 1, we have $|K_A \oplus K_B| \leq t$.

Show that this is true.

Hint: If you have trouble, start small. First show it for a state $|\widetilde{xy}\rangle$ with $|xy| \leq t$. Then show it for a pure state $|\Psi\rangle$ that is a superposition of such $|\widetilde{xy}\rangle$ (like the ones that occur in the definition of $S^{\text{test}}_{\text{Ideal}}$. And then got for $\rho \in S^{\text{test}}_{\text{Ideal}}$.