Quantum Cryptography (spring 2022)	Dominique Unruh

Exercise Sheet 10

Out: 2022-06-06 Due: 2022-06-07

Bonus homework. Each subproblem gives 3 points. That is, a total of 27 points can be reached (not counting the typesetting bonus for nicely rendered solutions). Deadline is 3pm!

1 Quantum proofs

Knowlets:	ProofSys	ProblemID: QProofs
Time:		
Difficulty:		

Show that if (P, V) is a proof system (Definition 53 in the lecture notes), then it also is a quantum proof system as in the following definition:

Definition 1 (Quantum proof systems) *We call a pair* (P, V) *of interactive machines a* quantum proof system *for the relation* R *with* soundness-error ε *iff the following two conditions are fulfilled:*

- Completeness: *For any* $(x, w) \in R$*, we have that* $\Pr[\langle P(x, w), V(x)\rangle = 1] = 1$.
- Soundness: *For any (potentially computationally unlimited)* ***quantum*** *machine* P^**, and for any* $x \notin L_R$*, we have* $\Pr[\langle P^*(), V(x)\rangle = 1] \leq \varepsilon$.

Notice that the only difference to Definition 53 in the lecture notes is the additional word **quantum**.

2 Quantum State Probability Distributions and Density Operators

(a)

Knowlets:	QDistr, QDistrU, Density	ProblemID: URandom
Time:		
Difficulty:		

Consider the following process: First, a random value $x \in \{0, 1\}^n$ is chosen. Then an n-bit quantum register is prepared to have the value $|\Psi\rangle := |x\rangle$. Then a unitary transformation U is applied to Ψ. What is the density operator corresponding to the resulting quantum state probability distribution?

Hint: As the first step, consider the case that U is the identity.

(b)

Knowlets:	QDistr, QDistrM, Density	ProblemID: MeasureForget
Time:		
Difficulty:		

Let a measurement M consisting of projectors $P_1, \dots, P_n$ be given. Let a quantum state $|\Psi\rangle$ be given. Assume that $|\Psi\rangle$ is measured using M but the measurement outcome **is not recorded** (i.e., it is forgotten, erased). What is the quantum state probability distribution describing the state of the system after this experiment? What is the corresponding density operator?

Note: The formula in the lecture was for the case where the measurement outcome is **not** forgotten.

(c)

Knowlets:	QDistrM, QDistrM, Density ProblemID: MeasureForgetD
Time:	
Difficulty:	

Assume a quantum system is in the state described by a density operator ρ. We apply a measurement M consisting of projectors $P_1, \dots, P_n$ to the system and forget the outcome. What is the density operator describing the resulting state of the system?

(d)

Knowlets:	QDistr, Density, PhysInd, DensityPhysInd ProblemID: PhysIndBellIndep
Time:	
Difficulty:	

Consider the following experiments:

- Experiment A: A two-qubit system is initialised with probability $\frac{1}{2}$ to be in the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and with probability $\frac{1}{2}$ to be in the state $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$.
- Experiment B: A uniformly random bit r is chosen, and then both qubits are individually prepared to be in the same state $|r\rangle$.

Note that in experiment A, we have entanglement: The state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ cannot be written in the form $|\Psi_1\rangle \otimes |\Psi_2\rangle$ (same for $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$). On the other hand, in experiment B, in each of the two cases $r = 0$ and $r = 1$, a state is prepared that is separable (of the form $|\Psi_1\rangle \otimes |\Psi_2\rangle$).

Show that the states produced in the two experiments are physically indistinguishable.

(e)

Knowlets:	QDistr, Density, PhysInd, DensityPhysInd ProblemID: GlobalPh
Time:	
Difficulty:	

In the lecture, we mentioned several times that a global phase, i.e., a factor $\varphi \in \mathbb{C}$ with $|\varphi| = 1$ in front of a quantum state, is physically irrelevant.

Demonstrate this by showing that the two states $|\Psi\rangle$ and $\varphi|\Psi\rangle$ are physically indistinguishable.[1]

[1] More precisely, that the quantum state probability distributions $\{|\Psi\rangle@1\}$ and $\{\varphi|\Psi\rangle@1\}$ are physically indistinguishable.

3 Quantum Operations

Knowlets:	ParTr, QOper ProblemID: PTraceQOp
Time:	
Difficulty:	

Describe the partial trace as a quantum operation. More exactly, let $\mathcal{H}_A = \mathbb{C}^n$, $\mathcal{H}_B = \mathbb{C}^m$. Find operators $E_k : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A$ such that these define a quantum operation $\mathcal{E} = \{E_k\}_k$ with the property that $\mathcal{E}(\rho) = \operatorname{tr}_B \rho$ for all ρ. Show that $\mathcal{E}$ is indeed a quantum operation (i.e., that the E_k are valid operators for defining a quantum operation).

Hint: For density operators ρ we have $\operatorname{tr} \rho = \sum_k \langle k|\rho|k\rangle$. Note that here $\langle k|$ is a linear operator from $\mathcal{H}_B$ to $\mathbb{C}$. And $I \otimes \langle k|$ is a linear operator from $\mathcal{H}_A \otimes \mathcal{H}_B$ to $\mathcal{H}_A \otimes \mathbb{C} = \mathcal{H}_A$. Note that it is sufficient to check that $\mathcal{E}(\rho) = \operatorname{tr}_B \rho$ for $\rho = \sigma \otimes \tau$, the rest follows by linearity.

4 Universal hash functions

(a)

Knowlets:	UHF ProblemID: MatrixUHF
Time:	
Difficulty:	

Let S be the set of all binary $\ell \times m$-matrices. I.e., $S = \mathbb{F}_2^{\ell \times m}$. Let X be the set of all m-bit vectors. I.e., $X = \mathbb{F}_2^m$. Let $Y = \mathbb{F}_2^\ell$. Let $F : S \times X \to Y$ be defined as $F(s, x) := sx$.

Show that F is a universal hash function.

Note: You may use the fact that for any fixed $z \neq 0$, and uniformly distributed $s \in \mathbb{F}_2^{\ell \times m}$, sz is uniformly distributed on $\mathbb{F}_2^\ell$. (Bonus points if you prove that fact, too.)

Hint: $sx = sx'$ iff $s(x - x') = 0$.

(b)

Knowlets:	UHF ProblemID: FieldUHF
Time:	
Difficulty:	

Let $S := X := \mathbb{F}_{2^m}$ be a finite field (encoded in the standard way as an $\mathbb{F}_2$ vector space). Let $trunc_\ell(x)$ denote the first ℓ bits of x. Let $Y := \{0,1\}^\ell$. Let $F : S \times X \to Y$ be defined as $F(s, x) := trunc_\ell(sx)$.

Show that F is a universal hash function.

Note: You may use that $trunc_\ell(a - b) = trunc_\ell(a) - trunc_\ell(b)$. (This is immediate from the encoding of $\mathbb{F}_{2^m}$.)