QUANTUM CRYPTOGRAPHY
Master of Logic, University of Amsterdam, 2017
TEACHERS: Jan Czajkowski, Yfke Dulek, and Christian Schaffner

Homework problem set 1

Please hand in your solutions to these exercises in digital form (typed, or scanned from a neatly hand-written version) through Moodle no later than **Friday June 16, 20:00h**.

Problem 1: Purity

The purity of a quantum state is defined as $\mathrm{Tr}\rho^2$. Consider a d-dimensional quantum state $\rho \in \mathbb{C}^{d\times d}$.

(a) What is the maximal value of purity and what class of states achieves this value? Prove your answer.

(b) What is the minimal value of purity, what state achieves this value? Prove your answer.

(c) Any qubit density matrix can be represented by the Bloch vector $\vec{r}$, satisfying $|\vec{r}| \leq 1$. For any quantum state $\tau \in \mathbb{C}^{2\times 2}$ we have that $\tau = \frac{1}{2}(\mathbb{1} + \vec{r}\cdot\vec{\sigma})$, where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)^T$ is the vector of Pauli matrices. How does the purity of τ relate to $\vec{r}$?

Problem 2: Parity measurements (Exercise 1.5.1)

Use a projective measurement to measure the parity, in the Hadamard basis, of the state $|00\rangle\langle 00|$. Compute the probabilities of obtaining measurement outcomes "even" and "odd", and the resulting post-measurement states. What would the post-measurement states have been if you had first measured the qubits individually in the Hadamard basis, and then taken the parity?

Problem 3: Robustness of GHZ and W states (Problem 6.1 of Week 1 and Problem 2 of Week 2)

Remember that $|W_N\rangle := \frac{1}{\sqrt{N}}\sum_{i=1}^{N} \underbrace{|0\cdots 010\cdots 0\rangle}_{1 \text{ at the } i\text{-th place}}$ is an equal superposition of all N-bit strings with exactly one 1 and N-1 0's and $|GHZ_N\rangle := \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$.

In the second module you learned to distinguish product states from (pure) entangled states by calculating the Schmidt rank of $|\Psi\rangle_{AB}$, i.e. the rank of the reduced state $\rho_A = \mathrm{Tr}_B|\Psi\rangle\langle\Psi|$. In particular $|\Psi\rangle$ is pure if and only if its Schmidt rank is 1. In the following, we denote by Tr_N the operation of tracing out only the last of N qubits.

(a) What is the overlap $\mathrm{Tr}\Big(|GHZ_{N-1}\rangle\langle GHZ_{N-1}|\,\mathrm{Tr}_N(|GHZ_N\rangle\langle GHZ_N|)\Big)$ in the limit $N\to\infty$?

(b) What is the overlap $\mathrm{Tr}\Big(|W_{N-1}\rangle\langle W_{N-1}|\,\mathrm{Tr}_N(|W_N\rangle\langle W_N|)\Big)$ in the limit $N\to\infty$?

(c) What are the ranks of $\mathrm{Tr}_N|GHZ_N\rangle\langle GHZ_N|$ and of $\mathrm{Tr}_N|W_N\rangle\langle W_N|$, respectively? (Note that these are the Schmidt ranks of $|GHZ_N\rangle$ and $|W_N\rangle$ if we partition each of them between the first $N-1$ qubits and the last qubit.)

(d) Let us now introduce a more discriminating (in fact, continuous) measure of the entanglement of a state $|\Psi\rangle_{AB}$: namely, the *purity of the reduced state* ρ_A given by $\mathrm{Tr}\rho_A^2$.

Consider again the behavior of the N-qubit GHZ and W states with one qubit discarded (i.e. traced out): What is the purity of $\mathrm{Tr}_N|GHZ_N\rangle\langle GHZ_N|$ in the limit $N\to\infty$?

(e) What is the purity of $\mathrm{Tr}_N|W_N\rangle\langle W_N|$ in the limit $N\to\infty$?

Problem 4: Relation between min-entropy and ignorance

Let K be a classical (key) register, and let E be Eve's quantum register. Prove the following statement for arbitrary classical-quantum states ρ_{KE}: Eve is ignorant about K if and only if $H_{min}(K|E) = \log|K|$.