QUANTUM CRYPTOGRAPHY
Master of Logic, University of Amsterdam, June 2022
TEACHERS: Christian Schaffner, Florian Speelman and Sebastian Zur

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 Canvas no later than **Update: Friday June 17th, 2022, 20:00h**.

Problem 1: Purity

The purity of a quantum state is defined as $\text{Tr}\rho^2$. 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: A three-player game

Consider the following three-player game: Alice, Bob, and Charlie each receive one bit (x, y, and z, respectively). They are promised that the parity of the three bits is 1 (i.e., $(x,y,z) \in \{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$). Their task is to each output a single bit (a, b, and c), such that $a \oplus b \oplus c = xyz$.

(a) Find a classical strategy for Alice, Bob, and Charlie, and prove that it is optimal.

(b) As you might expect, they can do better if they are allowed to share entanglement. Suppose that the players each hold one qubit of the state $|GHZ_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Find a strategy so that the game is won with certainty.
Hint: Their first step should be to change their resource state into $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$ if and only if $(x,y,z) = (1,1,1)$.

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 $H_{min}(K|E) = \log|K|$.