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

Homework problem set 1

You do not have to hand in these exercises, they are for practicing only.

Problem 1: 1

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, what class of states achieve this value.

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

(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 purity of τ relate to $\vec{r}$.

Problem 2: Minimum-error measurement of qubits

Alice is given one of the states $|\theta\rangle := \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$, $|-\theta\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle - \sin\left(\frac{\theta}{2}\right)|1\rangle$, each with probability $p := \frac{1}{2}$. Design a measurement $\{\Pi_+, \Pi_-\}$, where $\Pi_+, \Pi_- \succeq 0$ and $\Pi_+ + \Pi_- = \mathbb{1}$, such that the probability of error is minimal. The probability of error is defined as $p_e := p\mathrm{Tr}(\Pi_-|\theta\rangle\langle\theta|) + (1-p)\mathrm{Tr}(\Pi_+|-\theta\rangle\langle-\theta|)$.

Problem 3: 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 4: Partial trace (Exercise 1.6.1)

Verify that the state $\rho_A = \sum_x (\mathbb{1}\otimes\langle u_x|)\rho_{AB}(\mathbb{1}\otimes|u_x\rangle)$ does not depend on the choice of basis $\{|u_x\rangle\}$. [Hint: first argue that if two density matrices ρ, σ satisfy $\langle\phi|\rho|\phi\rangle = \langle\phi|\sigma|\phi\rangle$ for all unit vectors $|\phi\rangle$ then $\rho = \sigma$. Then compute $\langle\phi|\rho_A|\phi\rangle$, and use the POVM condition $\sum_x M_x = \mathbb{1}$ to check that you can get an expression independent of $\{|u_x\rangle\}$. Conclude that ρ_A itself does not depend on $\{|u_x\rangle\}$.]

Problem 5: Robustness of GHZ and W states (Problem 6.1)

(a) Now we generalize to the N-qubit case. As you might expect, $|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$.

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

(b) $|W_N\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^N \underbrace{|0\cdots010\cdots0\rangle}_{\text{1 at the } i\text{-th place}}$ is an equal superposition of all N-bit strings with exactly one 1 and N-1 0's

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