Indian Institute of Science

E2: 270 Quantum Information Theory

Instructor: Shayan Srinivasa Garani

MidTerm Exam, Spring 2022

Name and SR.No:

Instructions:

- This is an in-class exam for 1.5 hours.
- There are five main questions. None of them have negative marking.
- Attempt all of them with careful reasoning and justification for partial credit.
- There is absolutely no collaboration except referring to your crib sheets and homework solutions.
- Assigned on Oct. 6th, 2022 at 11:30 hrs.
- Do not panic, do not cheat, good luck!

Question No.	Points scored
1	
2	
3	
4	
5	
Total points	

PROBLEM 1: This problem has 2 parts:

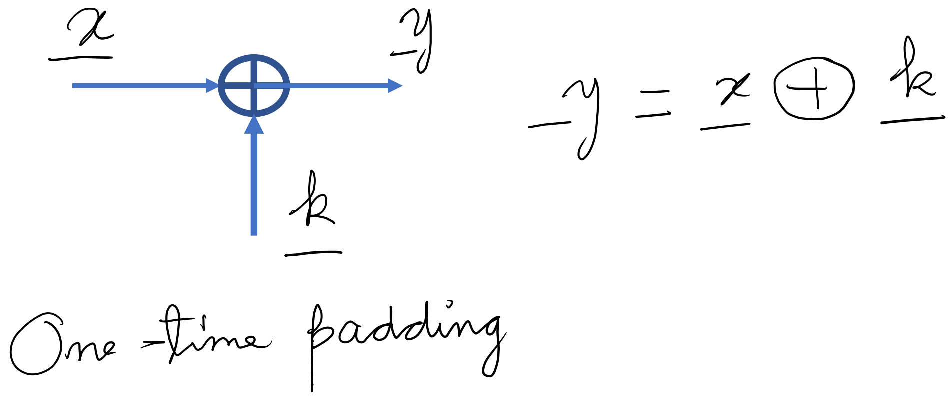

FIGURE 1. Vernam cipher for generating encrypted data.

(1) Consider a one-time padding system shown in Figure 1, where a binary message $\underline{x}$ of length n with $P(x_i = 0) = p$ is XOR-padded with a key $\underline{k}$ of the same length such that $P(k_i = 0) = \frac{1}{2}$. Is the one-time cipher system perfectly secure in the information-theoretic sense? Show all your steps carefully. How about the case if $P(x_i = 0) = p_i$? (7 pts.)

(2) Show that for a discrete random variable with d different realizations, the entropy of the random variable is upper bounded by $\log_2(d)$. (4 pts.)

PROBLEM 2: This problem has 2 parts:

(1) Let C be a CNOT gate with qubit 1 as control and qubit 2 as the target. Prove that (a) $CX_1C = X_1X_2$, (b) $CZ_1C = Z_1$ (4 pts.)

(2) Let $\rho = |\psi\rangle\langle\psi|$ be a pure state on $\mathcal{H}^A \otimes \mathcal{H}^B$. For a function f show that $f(\rho_A) \otimes \mathcal{I}_B |\psi\rangle = \mathcal{I}_A \otimes f(\rho_B) |\psi\rangle$. (7 pts.)

PROBLEM 3: Show that randomly applying the Heisenberg Weyl operators $\{X(i)Z(j)\}_{i,j\in\{0,1,\ldots,d-1\}}$ with uniform probability to any qudit density operator ρ yields a maximally mixed state. Is there any connection to this result as a quantum analog of Problem 1(a)? (10 pts.)

PROBLEM 4: Consider a noisy quantum channel $\mathcal{N}^{\mathcal{A}\to\mathcal{B}}$ acting on density matrix ρ with Kraus operators N_j. Let $\mathcal{U}_{\mathcal{N}}^{\mathcal{A}\to\mathcal{B}\mathcal{E}}$ be an isometric extension. Obtain the density operator from Eve's side. (10 pts.)

PROBLEM 5: Let $|AR_1\rangle$ and $|AR_2\rangle$ be two purifications of a quantum state ρ^A. Prove that there exists a unitary transformation U_R acting on the reference system R such that $|AR_1\rangle = (I_A \otimes U_R)\,|AR_2\rangle$. (8 pts.)