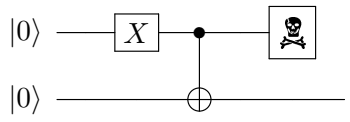
Quantum Cryptography (spring 2020) Dominique Unruh

Exercise Sheet 4

Out: 2020-03-28 Due: 2020-04-05

Problem 1: Partial Trace

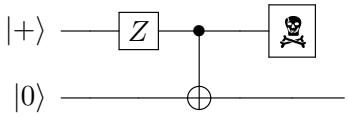
(a) Consider the following quantum circuit.



By  we mean that the corresponding register (and the information therein) is destroyed. X is the X-gate (bit flip).

What is the density operator ρ of the state resulting from that circuit?

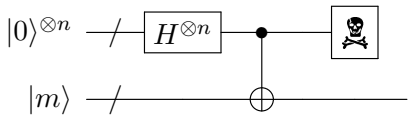
(b) Consider the following quantum circuit.



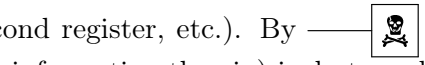
By  we mean that the corresponding register (and the information therein) is destroyed. Z is the Z-gate (i.e., $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$).

What is the density operator ρ of the state resulting from that circuit?

(c) Consider the following quantum circuit.

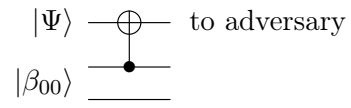


Here m is an n-bit string, the CNOT denotes bitwise CNOT (i.e., a CNOT between bit 1 of the first and the second n-qubit register, then a CNOT between bit 2 of the

first and the second register, etc.). By  we mean that the corresponding register (and the information therein) is destroyed.

What is the density operator ρ of the state resulting from that circuit?

(d) **(Bonus problem)** Consider the following encryption circuit:



Here $|\Psi\rangle$ is a qubit (assumed to be either $|0\rangle$ or $|1\rangle$), and $|\beta_{00}\rangle$ is $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. That is, we CNOT the qubit $|\Psi\rangle$ with the first half of a Bell pair.

This is a slight variant of the one-time pad encryption. Here, we do not XOR the secret qubit $|\Psi\rangle$ with a classical bit, but with a quantum bit. (Imagine that Alice holds $|\Psi\rangle$ and the first qubit of $|\beta_{00}\rangle$, i.e., the first two wires. And Bob holds the third wire.) Then Alice sends the first wire to the adversary.

Compute the density operator describing the qubit that the adversary gets, both in the case $|\Psi\rangle = |0\rangle$ and the case $|\Psi\rangle = |1\rangle$.

Your result will show that this encryption scheme is secure for encrypting classical data. (With respect to some suitable notion of secrecy.)

Hint: First compute the quantum state of the three wires (i.e., a three-qubit state) after the CNOT. Then compute the corresponding density operator. Then use the partial trace to compute the density operator corresponding to the first wire only (i.e., after destroying the second and third wire).

Problem 2: Trace Distance

(a) Let E_1 and E_2 be quantum state probability distributions. Let ρ_1 and ρ_2 be the corresponding density operators. Assume that E_1 and E_2 are physically indistinguishable. What is $\mathrm{TD}(\rho_1, \rho_2)$?

(b) Let $E_1 := \{(|+\rangle, \frac{1}{2}), (|-\rangle, \frac{1}{2})\}$ and $E_2 := \{(|0\rangle, 1)\}$ be quantum state probability distributions. Let ρ_1 and ρ_2 be the corresponding density operators. What is $\mathrm{TD}(\rho_1, \rho_2)$?

(c) Let $\rho = p\tau + q\rho'$ and $\sigma = p\tau + q\sigma'$ where τ, ρ', σ' are density operators, and $p, q \geq 0$, $p + q = 1$. Show that $\mathrm{TD}(\sigma, \rho) = q \cdot \mathrm{TD}(\sigma', \rho')$.

Note: Do not use Lemma 9 in the lecture notes.

(d) Let $E_1 := \{(|+\rangle, \frac{1}{4}), (|-\rangle, \frac{1}{4}), (|\Psi\rangle, \frac{1}{2})\}$. Let $E_2 := \{(|0\rangle, \frac{1}{2}), (|\Psi\rangle, \frac{1}{2})\}$. Here $|\Psi\rangle := \frac{1}{\sqrt{3}}|0\rangle - \sqrt{\frac{2}{3}}|1\rangle$. Let ρ_1 and ρ_2 be the corresponding density operators. What is $\mathrm{TD}(\rho_1, \rho_2)$?

Hint: Consider (c).

(e) Consider the following setup: Alice has a secret bit $b \in \{0,1\}$. Then she chooses randomly $r \in \{0,1\}$. If $r = 0$, she encodes b in the $|0\rangle, |1\rangle$ basis (i.e., she sends $|0\rangle$ for $b = 0$ and $|1\rangle$ for $b = 1$). If $r = 1$, she encodes b in the $|+\rangle, |-\rangle$ basis. Then she sends the resulting state $|\Psi_b\rangle$ to Eve. Show that the trace distance between the mixed states ρ_0 and ρ_1 corresponding to $b = 0$ and $b = 1$, respectively, is $\mathrm{TD}(\rho_0, \rho_1) = \frac{1}{\sqrt{2}}$.

Hint: The eigenvalues of $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$ are $\frac{1}{\sqrt{2}}$ and $-\frac{1}{\sqrt{2}}$. Note that this is not the toy protocol from the lecture, in the toy protocol b selected the basis, not r.

(f) **(Bonus problem)** In the experiment described in (e), assume that the bit b is chosen uniformly at random. Show that Eve cannot guess b with probability larger than $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 85\%$.

Hint: Try to express the probability that Eve guesses correctly in terms of $\Pr[G = x | b = y]$ for various $x, y \in \{0,1\}$ (here G denotes Eve's guess) and then use (e).