Quantum Cryptography (spring 2021) Dominique Unruh

Exercise Sheet 06

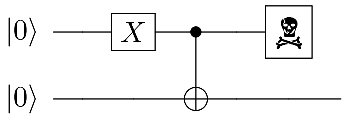
Out: 2021-03-29 Due: 2021-04-06

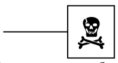
1 Partial trace

(a)

Knowlets:	ParTr, PauliX, CNOT ProblemID: PTraceXCNOT
Time:	
Difficulty:	

Consider the following quantum circuit.



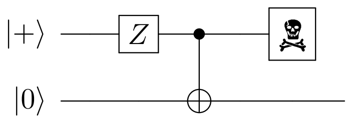
By  we mean that the corresponding register (and the information therein) is destroyed. X is the X-gate (bit flip).

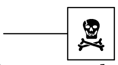
What is the density operator ρ of the state resulting from that circuit?

(b)

Knowlets:	ParTr, PauliZ, CNOT ProblemID: PTraceZCNOT
Time:	
Difficulty:	

Consider the following quantum circuit.



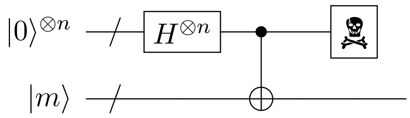
By  we mean that the corresponding register (and the information therein) is destroyed. Z is the Z-gate (i.e., $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$).

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

(c)

Knowlets:	ParTr, Hada, CNOT, ComposUni ProblemID: PTraceHnCNOT
Time:	
Difficulty:	

Consider the following quantum circuit.



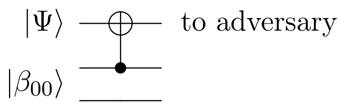
Here m is an n-bit string, the CNOT denotes bitwise CNOT (i.e., a CNOT between bit 1 of the first and the second n-qubit register, then a CNOT between bit 2 of the first and the second register, etc.). By  we mean that the corresponding register (and the information therein) is destroyed.

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

(d)

Knowlets:	ParTr, CNOT, QOTP — ProblemID: PTraceQOTP
Time:	
Difficulty:	

`(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).

2 Classical functions as quantum operations

Consider a classical function $f : \{0,1\}^n \to \{0,1\}^n$. We want to show that f can be interpreted as a quantum operation $\mathcal{E}_f$ that transforms n qubits to m qubits.

(a)

Knowlets:	QDistr, Density ProblemID: CFQOperClaSt
Time:	
Difficulty:	

Having classical value $x \in \{0,1\}^n$ means being in state $|x\rangle$ (and no superposition). Write this down as a quantum state probability distribution E_x, and write down the corresponding density operator ρ_x. (Recall that $|x\rangle$ is the vector in $\mathbb{C}^{2^n}$ that has a 1 at the x-th position.)

(b)

Knowlets:	QOper ProblemID: CFQOperSingleIn
Time:	
Difficulty:	

Find some operator/matrix E_x such that $E_x \rho_y E_x^\dagger = 0$ if $x \neq y$, and such that $E_x \rho_x E_x^\dagger$ has trace 1.

Hint: $E_x \rho_x E_x^\dagger \neq 0$ is a good start. Trace 1 (if you don't have it automatically) is then most likely easy to achieve by multiplying with a scalar.

(c)

Knowlets:	QOper ProblemID: CFQOperSingle
Time:	
Difficulty:	

Tweak your definition of E_x such that still $E_x \rho_y E_x^\dagger = 0$ if $x \neq y$, but $E_x \rho_x E_x^\dagger = \rho_{f(x)}$.

(d)

Knowlets:	QOper ProblemID: CFQOperCombine
Time:	
Difficulty:	

Using the operators E_x from Problem 2 (c), define a linear function $\mathcal{E}_f$ such that $\mathcal{E}_f(\rho_x) = \rho_{f(x)}$ for all $x \in \{0,1\}^n$.

Note: Also show that $\mathcal{E}_f$ indeed has that property.

(e)

Knowlets:	QOper ProblemID: CFQOperIsQOper
Time:	
Difficulty:	

Show that $\mathcal{E}_f$ from Problem 2 (d) is a quantum operation.

(f)

Knowlets:	QOper ProblemID: CFQOperPTr
Time:	
Difficulty:	

(Bonus problem) Consider the function $\mathcal{F}_f$ defined by $\mathcal{F}_f(\rho) = \operatorname{tr}_A\Big(U_f(\rho \otimes |0\dots0\rangle\langle 0\dots0|_B)U_f^\dagger\Big)$ where $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$. (That is, $\mathcal{F}_f$ computes the function in superposition and then discards the input.)

Show that $\mathcal{F}_f = \mathcal{E}_f$.

Hint: Show first that $\mathcal{F}_f(\rho_x) = \mathcal{E}_f(\rho_x)$.