

Exercise Sheet 03

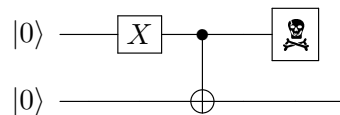
Out: 2022-03-11


Due: 2022-03-18

1 Partial trace

	Knowlets: ParTr, PauliX, CNOT	ProblemID: PTraceXCNOT
(a)	Time:	
	Difficulty:	

Consider the following quantum circuit.

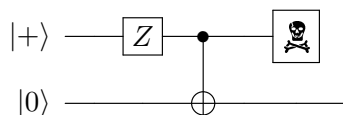



By  we mean that the corresponding register (and the information therein) is destroyed. X is the X-gate (bit flip).

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

	Knowlets: ParTr, PauliZ, CNOT	ProblemID: PTraceZCNOT
(b)	Time:	
	Difficulty:	

Consider the following quantum circuit.

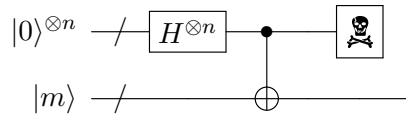



By  we mean that the corresponding register (and the information therein) is destroyed. Z is the Z-gate (i.e., $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$).

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

	Knowlets: ParTr, Hada, CNOT, ComposUni	ProblemID: PTraceHnCNOT
(c)	Time:	
	Difficulty:	

Consider the following quantum circuit.

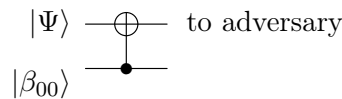


Here m is an n -bit string, the CNOT denotes bitwise CNOT (i.e., a CNOT between bit 1 of the first and the second n -qubit register, then a CNOT between bit 2 of the first and the second register, etc.). By  we mean that the corresponding register (and the information therein) is destroyed.

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

	Knowlets:	ParTr, CNOT, QOTP	ProblemID: PTraceQOTP
(d)	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 Quantum one-time pad, with Pauli matrices

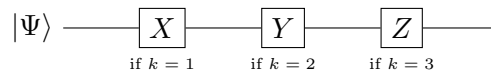
Knowlets:	QOTP, PauliX, PauliY, PauliZ	ProblemID: QOTPPauli
Time:		
Difficulty:		

Consider the following variant of the quantum one-time pad:

The secret key is $k \in \{1, 2, 3, 4\}$. (Uniformly at random.)

Then, depending on k , we apply one of the four Pauli matrices X, Y, Z, I . (It is a matter of taste whether the identity I is called a Pauli-matrix.)

That is, we compute the following circuit:



Show that this variant of the quantum one-time pad is secure but computing the density operator of the final state for $|\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. The final state should not depend on α, β .

Note: Don't forget that there is also the case $k = 4$ in which case the circuit above applies no gate.

Note: Note that α, β are complex numbers. In the lecture, we assumed for simplicity that they are real numbers, but you are not supposed to make that simplification. (At least not when full points are desired.)

3 Physical indistinguishability – the opposite direction (bonus problem)

Knowlets:	QDistr, Density, ProjMeas, DensityM	ProblemID: PhysIndReverse
Time:		
Difficulty:		

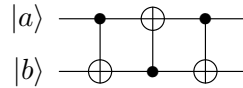
Let E_1 and E_2 be quantum state probability distributions with density matrices ρ_1 and ρ_2 . Assume that $\rho_1 \neq \rho_2$. Prove that E_1 and E_2 are physically distinguishable by specifying a measurement $M = \{Q_{\text{yes}}, Q_{\text{no}}\}$ with the following property: When measuring E_1 and E_2 with M , we get the outcome yes with different probabilities P_1 and P_2 (where $P_i := \Pr[\text{Outcome is yes when measuring } \rho_i]$).

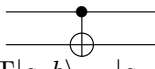
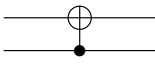
Hint: Consider the matrix $\sigma := \rho_1 - \rho_2$. Show that σ is diagonalisable and that it therefore has an eigenvector $|\Psi\rangle$ with eigenvalue $\lambda \neq 0$. Set $Q_{\text{yes}} := |\Psi\rangle\langle\Psi|$. You may use without proof the fact that a density operator is always Hermitean and nonzero.

4 Quantum circuits

(a)	Knowlets:	UniTrafo, ComposQState, CNOT	ProblemID: TripleCNOT
	Time:		
	Difficulty:		

What state comes out of the following circuit (for $a, b \in \{0, 1\}$)?



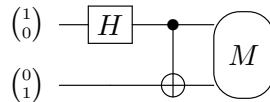
Here  denotes the controlled NOT, i.e., the operation defined by $\text{CNOT}|a, b\rangle = |a, a \oplus b\rangle$. (And  analogously denotes the operation mapping $|a, b\rangle$ to $|a \oplus b, b\rangle$.)


What useful (and simple) function does the above circuit perform?

Note: Recall that $|a\rangle$ for some bit a simply stands for one of the computational basis vectors. E.g., $|a\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ if $a = 0$. And similarly, $|a, b\rangle$ stands for one of the four basis vectors of a 2-qubit system. E.g., $|a, b\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ if $a = 0, b = 1$.

(b)	Knowlets:	ComposQState, ComposUni, Hada, CNOT, ComplMeas	ProblemID: CircHCNOTM
	Time:		
	Difficulty:		

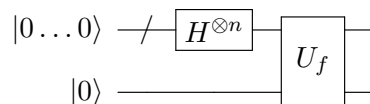
What are the possible outcomes of the measurement M ? With which probabilities do they occur?



Here  is the complete measurement in the computational basis on the first and the second qubit.

(c)	Knowlets:	ComposQState, ComposUni	ProblemID: CircHadaAllUf
	Time:		
	Difficulty:		

Let f be a function from $\{0, 1\}^n$ to $\{0, 1\}$. What is the state resulting from this circuit?

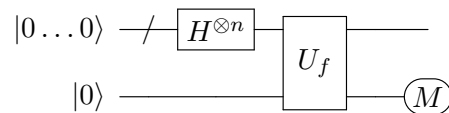


By $\text{---}/\text{---}$ we denote a wire consisting of n qubits. The unitary operation U_f is defined by $U_f|x, y\rangle := |x, y \oplus f(x)\rangle$ with \oplus being the XOR. $H^{\otimes n}$ means $H \otimes H \otimes \cdots \otimes H$ (n times).

Hint: First figure out what $H^{\otimes n}|0 \dots 0\rangle$ is as a linear combination of basis vectors $|0 \dots 0\rangle, |0 \dots 01\rangle, |0 \dots 010\rangle, \dots$

(d)	Knowlets:	ComposQState, ComposUni, ComposMeas ProblemID: CircHadaAllUfMeas
	Time:	
	Difficulty:	

Let $n := 8$ and $f(x) := 1$ iff x is a prime number (the bitstring $x \in \{0, 1\}^n$ is interpreted as an integer in binary representation). What is the probability of measuring 1 in the measurement M ?



The unitary operation U_f is defined by $U_f|x, y\rangle := |x, y \oplus f(x)\rangle$ with \oplus being the XOR.

Note: Do/recall Problem 4 (c) first.