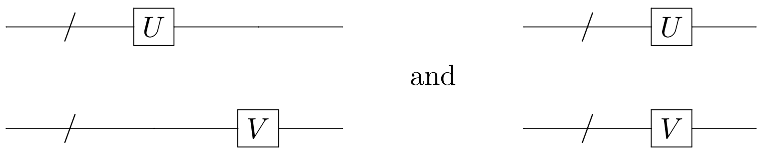
Quantum Cryptography (fall 2013)	Prof. Dr. Dominique Unruh

Exercise Sheet 4

Out: October 2, 2013 — Due: October 8, 2013

Problem 1: Composite Systems

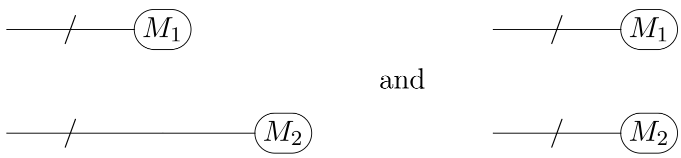
(a) Show that the following two circuits perform the same unitary operation.



By this we mean that in the first case, first U is applied to the first system while nothing is done to the second, and then V is applied to the second system while nothing is done to the first. In the second case, both operations are applied simultaneously.

(Note that this implies that on independent subsystems, it does not matter whether we first operate on the first and then the second, or vice versa.)

(b) **(Bonus question)** Assume that the measurement M_1 is given by projectors $P_1, \dots, P_n$ and that the measurement M_2 is given by projectors $Q_1, \dots, Q_m$. Show that the following two circuits have the same effect. I.e., prove that for each i, j, the probability of getting the outcomes i, j is the same in both circuits, and the state after performing the measurements is the same.



(c) Explain (shortly) why (a) and (b) imply that one cannot use quantum mechanics to transfer information faster than light. (I.e., the only way to transfer information is to actually send something.)

Problem 2: Physical indistinguishability

Consider the following experiments:

- Experiment A: A two-qubit system is initialised with probability $\frac{1}{2}$ to be in the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and with probability $\frac{1}{2}$ to be in the state $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$.

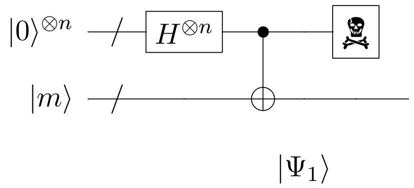
- Experiment B: A random bit r is chosen, and then both qubits are individually prepared to be in the same state $|r\rangle$.

Note that in experiment A, we have entanglement: The state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ cannot be written in the form $|\Psi_1\rangle \otimes |\Psi_2\rangle$ (same for $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$). On the other hand, in experiment B, in each of the two cases $r = 0$ and $r = 1$, a state is prepared that is separable (of the form $|\Psi_1\rangle \otimes |\Psi_2\rangle$).

Show that the states produced in the two experiments are physically indistinguishable.

Problem 3: Partial Trace

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?