ETH Zürich, Dept. Informatik
WS 03/04

Lecturer: Jonathan Poritz

Introduction to Quantum Computation
Übung 2

14.11.2002

2.1 Prove that eigenspaces corresponding to distinct eigenvalues for a Hermitian matrix are necessarily orthogonal.

2.2 Prove that the eigenvalues of unitary matrices are all of norm one.

2.3 Show that the CNOT cannot be written as the tensor product of two single qubit gates, *i.e.*, it is not expressible as $A \otimes B$ for $A, B \in U(2)$.

2.4 Prove that if $A \in U(n)$ and $B \in U(m)$, then $A \otimes B \in U(nm)$.

Hint: Don't write it out.

2.5 Describe a way to teleport a *two* qubit state. Can you generalize?

2.6 The No-cloning Theorem

A *quantum cloning machine* would be a unitary operation on two qubits (*i.e.*, an element $U \in U(4)$) which would take one unknown input qubit $v \in \mathbb{C}^2$ and make two copies of it. More precisely, U would take v and some other qubit in a default state $|0\rangle$ and give back $v \otimes v$. Symbolically,

$$U(v \otimes |0\rangle) = v \otimes v \quad \forall v \in \mathbb{C}^2.$$

Show that no such cloning machine is possible.

2.7 Problems with No-cloning

Doesn't the No-Cloning Theorem contradict quantum teleportation? For that matter, it seems like the CNOT can be used as a copying circuit: set the target bit (the non-control bit) to 0, look at what happens to the control bit. Doesn't *this* contradict the No-cloning Theorem?

2.8 Quantum coin-flipping

a) Describe *fair coin-tossing* in the quantum context. That is, give a Hilbert space whose states will represent the value of the coin, describe the initial state (where the value of the coin is completely determined), the unitary evolution operator which realizes the *toss* itself and the measurement operator which you will use (before and after the toss) to see what the value of the coin is. Be completely specific.

b) Can you do the same thing for a *biased* coin, one where the probability of heads showing after the toss is some previously chosen number $p \in (0, 1)$, where p is not necessarily $\frac{1}{2}$?

c) Can you extend your scheme to realize a *common coin*, that is, a state shared between two parties which is in a determined state before the toss and which then is "tossed" by some unitary transformation, so that afterwards each party gets *the same* value when they measure, but heads and tails are equally likely?