ETH Zürich, Dept. Informatik
WS 03/04

Lecturer: Jonathan Poritz

Introduction to Quantum Computation
Übung 9

30.01.2004

9.1 Consider the quantized oracle for a Boolean function $f : \{0,1\}^n \to \{0,1\}$: prove that the four versions given in class:

$$Q_f(|x\rangle \otimes |b\rangle) = |x\rangle \otimes |b \oplus f(x)\rangle \qquad \text{and} \qquad U_f(|x\rangle) = (-1)^{f(x)}|x\rangle$$

for general f and

$$U = \mathrm{Id} - 2|y_0\rangle\langle y_0|$$

and

$$U = \text{“reflection in the hyperplane perpendicular to } |y_0\rangle\text{”}.$$

for f with a single solution (*i.e*, a single y_0 s.t. $f(y_0) = 1$, while $f(y) = 0$ for all other y), are all equivalent. Show that these give *unitary* transformations.

9.2 Show that when the Boolean function f has more than one solution, the oracle operator can still be thought of as reflection in the hyperplane perpendicular to the vector

$$|\bar{y}\rangle = \sum_{y | f(y)=1} |y\rangle,$$

i.e.,

$$U = \mathrm{Id} - \frac{2}{\| |\bar{y}\rangle \|^2} |\bar{y}\rangle\langle\bar{y}|.$$

9.3 Construct a quantum circuit that implements (efficiently) the operator

$$V = \mathrm{Id} - 2|\zeta\rangle\langle\zeta| \qquad \text{where} \qquad \zeta = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} |y\rangle.$$

9.4 Show that the product of two reflection operators in Euclidean space is a rotation operator – about which axis, by what angle?

9.5 If Alice transmits a 0 or a 1, encoded as the qubits $|0\rangle$ and $|1\rangle$ or as $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, and Bob (or Eve), measures with respect to the incorrect encoding basis, what will he (or she) think Alice was transmitting, and with what probability?

9.6 Consider the attack model for BB84 whereby Eve measures every qubit, with respect to a randomly chosen encoding basis, and then re-transmits whatever she received, in that same encoding, on to Bob. What fraction of the key bits will we expect Eve to have correctly in her hands? What error rate will Bob discover in the error-checking phase of the protocol?