Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

3. Exercise sheet
Hand in solutions until Monday, 15 November 2010, 23:59h.

In the lecture we encountered a number of single-qubit gates. Important are the Hadamard gate H, the phase gate S and the $\pi/8$-gate (denoted by T):

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}.$$

Also the Pauli gates X, Y and Z are of central importance:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Exercise 3.1 ($\pi/8$???). (1 points)

Find a reasonable explanation why the T gate is called the $\pi/8$-gate. $\boxed{1}$

Exercise 3.2 (Rotation matrices). (14+5 points)

(i) Restate the eigenvalues of the Pauli matrices and find the points on the Bloch-sphere which correspond to the normalized eigenvectors. $\boxed{3}$

(ii) The Pauli matrices give rise to three rotation operators $\boxed{5}$

$$R_x(\vartheta) = \exp(-i\vartheta X/2) = \cos\frac{\vartheta}{2} \cdot I - i \sin\frac{\vartheta}{2} \cdot X$$
$$R_y(\vartheta) = \exp(-i\vartheta Y/2) = \cos\frac{\vartheta}{2} \cdot I - i \sin\frac{\vartheta}{2} \cdot Y$$
$$R_z(\vartheta) = \exp(-i\vartheta Z/2) = \cos\frac{\vartheta}{2} \cdot I - i \sin\frac{\vartheta}{2} \cdot Z.$$

Let $x \in \mathbb{R}$ and A a matrix such the $A^2 = I$. Show that then

$$\exp(iAx) = \cos x \cdot I + i \sin x \cdot A$$

and, using this, verify the above three equations for the rotation operators. Hint: Remember $\cos x = \sum_{k\geq 0} \frac{(-1)^k}{(2k)!} x^{2k}$ and $\sin x = \sum_{k\geq 0} \frac{(-1)^k}{(2k+1)!} x^{2k+1}$.

(iii) Show that up to a global phase we have $T = R_z(\pi/4)$. $\boxed{2}$

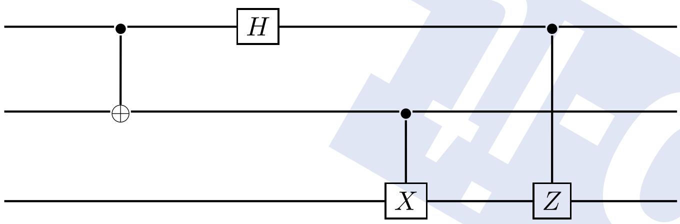
(iv) Express the Hadmard-gate H as a product of $R_x(\vartheta_1)$, $R_z(\vartheta_2)$ and $\exp(i\varphi)$ for some ϑ_1, ϑ_2 and φ. $\boxed{4}$

(v) Prove in general that if U is a unitary operation on a single qubit then there exist real numbers $\alpha, \beta, \gamma, \delta$ such that $\boxed{+5}$

$$U = \exp(i\alpha) R_z(\beta) R_y(\gamma) R_z(\delta).$$

Exercise 3.3 (Quantum teleporation). (11 points)

In the lecture we encountered a nice quantum circuit that performs quantum teleportation. We are now to prove that the following modified circuit also teleports a qubit:



5 (i) Write down the unitary transformation that describes the circuit. Hint: Proceed step by step. A computer algebra system might be of big help!

3 (ii) Prove that if $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ then on input $|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ the output of the circuit is $H^{\otimes 2}\,|00\rangle \otimes |\psi\rangle$.

3 (iii) How can you now get rid of the first two qubits?

Exercise 3.4 (Experimental Quantum teleportation). (0+10 points)

+10 Read and report on the article

`http://www.nature.com/nature/journal/v390/n6660/full/390575a0.html`