Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

11. Exercise sheet
Hand in solutions until Monday, 24 January 2011, 23:59h.

Exercise 11.1 (The harmonic oscillator revisited). (14 points)

In the lecture we discussed in the context of physical realizations of quantum computers again the concept of the (quantum) harmonic oscillator. The oscillator is given by the Hamiltomian

$$H = \frac{P^2}{2m} + \frac{1}{2} m\omega^2 X^2,$$

where $P = -i\hbar \frac{\partial}{\partial x}$ and $X = x\cdot$. Write

$$\begin{array}{rcl} a & = & \frac{1}{\sqrt{2m\hbar\omega}}(m\omega X + iP) \\ a^* & = & \frac{1}{\sqrt{2m\hbar\omega}}(m\omega X - iP) \end{array}$$

(i) Compute $XP - PX$. $\boxed{2}$

(ii) Show that $H = \hbar\omega(a^* \cdot a + \frac{1}{2})$. $\boxed{3}$

In Exercise 2.4 we already showed that the energy-levels of the Hamiltonian H are $\hbar\omega\left(n + \frac{1}{2}\right)$. Call from now on the eigenstates of H simply $|n\rangle$ for $n \in \mathbb{N}$, i.e. $H|n\rangle = \hbar\omega\left(n + \frac{1}{2}\right)|n\rangle$.

(iii) Compute explicitely $|0\rangle$ from $a|0\rangle = 0$. $\boxed{2}$

(iv) Define $|n+1\rangle = \frac{1}{\sqrt{n+1}} a^* |n\rangle$. Show that the equality $\boxed{4}$

$$|n\rangle = \frac{1}{\sqrt{2^n \cdot n!}} \pi^{-1/4} \exp(-x^2/2) h_n(x)$$

holds, using the n-th Hermite polynomial $h_n(x) = (-1)^n \cdot \exp(x^2) \frac{\partial^n}{\partial x^n} \exp(-x^2)$.

(v) Show that for $n > 0$ we have $a|n\rangle = \sqrt{n}\,|n-1\rangle$. $\boxed{2}$

(vi) Conclude that $a^* a|n\rangle = n|n\rangle$. $\boxed{1}$

Exercise 11.2 (Beam splitter). (10 points)

The Bake-Campbell-Hausdorf formula says that for a complex number λ, operators A, G and C_n, where C_n is recursively defined as

$$\begin{array}{rcl} C_0 & = & A \\ C_{n+1} & = & [G, C_n], \end{array}$$

we have

$$e^{\lambda G} A e^{-\lambda G} = \sum_{n \geq 0} \frac{\lambda^n}{n!} C_n.$$

Let $G = a^* b - a b^*$, where a, b are the annihilation (or deletion) operators and a^*, b^* are the creation operators.

(i) Argue that $[a, a^*] = [b, b^*] = 1$. 2

2 (ii) Compute the values for C_0, C_1, C_2 and C_3 explicitely.

2 (iii) Write down a formula defining C_n for all n.

3 (iv) Now apply the Bake-Campbell-Hausdorf formula to show that

$$e^{\lambda G} a e^{-\lambda G} = a \cos(\lambda) + b \sin(\lambda).$$

1 (v) Argue that $e^{\lambda G} b e^{-\lambda G} = b \cos(\lambda) - a \sin(\lambda)$.

Exercise 11.3 (Optical Hadamard gate). (4 points)

4 Consider the dual-rail single photon realization of quantum computers. Show that the beam-splitter followed by a phase shift of π on the first output photon corresponds to a Hadamard gate (up to a global phase).