Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

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

Exercise 5.1 (Rotations revisited). (6 points)

If $\vec{n} = (n_x, n_y, n_z)$ is a real unit vector then we generalize the definitions of our rotation operators R_x, R_y and R_z by defining a rotation by an angle ϑ around the $\vec{n}$-axis by the equation

$$(\#) \qquad \begin{aligned} R_{\vec{n}}(\vartheta) &= \exp(i\vartheta/2(n_x X + n_y Y + n_z Z)) \\ &= \cos(\vartheta/2) I - i \sin(\vartheta/2) \left(n_x X + n_y Y + n_z Z\right), \end{aligned}$$

where X, Y, Z are the three Pauli matrices.

(i) Prove that $(n_x X + n_y Y + n_z Z)^2 = I$. Derive the equality (#). 2

The Bloch sphere can be used to nicely visualize the composition of two rotations.

(ii) Prove that a rotation by an angle β_1 around the axis $\vec{n}_1$ followed by a rotation by an angle β_2 around the axis $\vec{n}_2$ is the same as a rotation by an angle β_3 around the axis $\vec{n}_3$ given by 4

$$\begin{aligned} c_3 &= c_1 c_2 - s_1 s_2 \left(\vec{n}_1 \cdot \vec{n}_2\right), \\ s_3 \vec{n}_3 &= s_1 c_2 \vec{n}_1 + c_1 s_2 \vec{n}_2 - s_1 s_2 (\vec{n}_2 \times \vec{n}_1), \end{aligned}$$

where $c_i = \cos(\beta_i/2), s_i = \sin(\beta_i/2)$ for $i \in \{1, 2, 3\}$ and for two real vectors $\vec{a}, \vec{b} \in \mathbb{R}^3$ their inner product is defined as

$$\vec{a} \cdot \vec{b} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = a_1 b_1 + a_2 b_2 + a_3 b_3$$

and their outer product is defined as

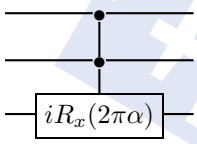
$$\vec{a} \times \vec{b} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{pmatrix}.$$

(iii) Specialize to $\beta_1 = \beta_2 = \beta$.

Exercise 5.2 (Universality). (8 points)

(i) Use the result of exercise 4.5 to show that Hadamard, phase and controlled NOT are universal for quantum computation. 4

(ii) Show that the following three qubit gate G is universal for quantum computation whenever α is irrational: 4



Exercise 5.3. (4 points)

4 Given two unit vectors $\hat{n}, \hat{m} \in \mathbb{R}^3$ which are linearly independent prove that for each $U \in U(2)$ there exist $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that

$$U = \mathrm{e}^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta).$$

Remark 5.4. (0+8 points)

+8 Actually, there is a two-to-one map

$$SU(2) \longrightarrow O(3).$$

(i) Take any matrix $U \in SU(2)$. Prove that it is given by four real parameters $(\alpha_0, \alpha_1, \beta_0, \beta_1) \in \mathbb{R}^4$ with euclidean norm 1. This defines a bijective map $SU(2) \to S^3$.

(ii) Define $F_U \colon SU(2) \to SU(2),\ V \mapsto UVU^{-1}$. Since $\mathbb{R}^3 \subset SU(2)$ by the previous, F_U defines an element of $O(3)$.