Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

4. Exercise sheet
Hand in solutions until Monday, 22 November 2010, 23:59h.

By now you should remember the six most important single qubit operations, namely the Hadamard gate H, the phase gate S, the $\pi/8$-gate T and the Pauli gates X, Y and Z as well as the rotation operators defined by them.

Exercise 4.1 (Reminder). (4 points)

Show that

(i) $XYX = -Y$ and prove $XR_y(\vartheta)X = R_y(-\vartheta)$. [2]

(ii) $HXH = Z$, $HYH = -Y$ and $HZH = X$. [2]

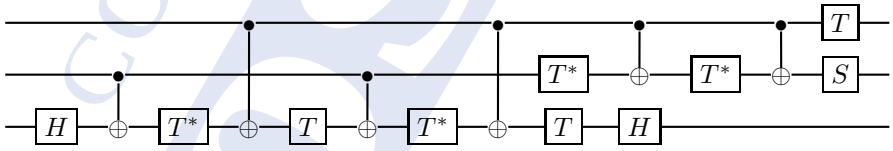
Exercise 4.2 (Toffoli gate). (9 points)

The Toffoli gate is a three-bit gate that is simply a doubly controlled NOT.

(i) Write down the matrix defining the Toffoli gate and prove that it is self inverse. [1]

(ii) Show that the Toffoli gate is classically universal, i.e. show that one can implement the classical $NAND$ operation using this gate. [3]

(iii) Prove that the Toffoli gate is equivalent to the following circuit: [5]



Exercise 4.3 (Multi-Control). (11+5 points)

(i) Compute a square root of the Pauli Z matrix. Derive a square root of the Pauli X matrix. [1]

(ii) Show that any unitary matrix U over $\mathbb{C}$ has a unitary square root, i.e. show that there is a unitary matrix V such that $U = V^2$. [5]

(iii) In the lecture we encountered a circuit implementing the $C^5(U)$ operation using four work qubits. For $U = V^2$ unitary, construct a $C^5(U)$ gate using no work qubits. You may use controlled V and controlled V^* gates. [5]

(iv) Find a circuit with $\mathcal{O}(n^2)$ gates using only Toffoli, CNOT, and single qubit gates which implements the $C^n(X)$ gate (for $n > 3$) using no work qubits. [+5]

Exercise 4.4 (Expensive operations). (0+5 points)

+5 Prove that there is a $d \times d$ unitary transformation that cannot be decomposed as a product of fewer than $d - 1$ two-level unitary matrices.

Exercise 4.5 (Irrationality). (6 points)

Suppose $\cos \vartheta = 3/5$. Give a proof by contradiction that ϑ is an irrational multiple of 2π:

3 (i) Using the fact that $\exp(i\vartheta) = (3 + 4i)/5$, show that if ϑ is rational, then there must exist a positive integer m such that $(3 + 4i)^m = 5^m$.

3 (ii) Show that $(3 + 4i)^m = 3 + 4i$ in $\mathbb{Z}_5[i]$ (that is, modulo 5) for all $m > 0$, and conclude that no m with $(3 + 4i)^m = 5^m$ can exist.