Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

6. Exercise sheet
Hand in solutions until Monday, 06 December 2010, 23:59h.

Exercise 6.1 (Controlled Swap). (10+5 points)

The controlled swap gate (also called Fredkin gate) is given by the unitary transformation

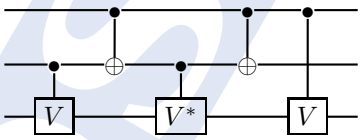
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(i) Give a quantum circuit that uses three Toffoli gates to perform the controlled swap. Hint: Think of the swap gate construction. You can control each gate, one at a time. [3]

(ii) Show that the first and the last Toffoli gate can be replaced by CNOT gates. [3]

(iii) Restate a soution V of the equation $X = V^2$, where X is the Pauli X gate. [1]

(iv) Now replace the Toffoli gate with the following circuit to obtain a controlled swap that uses only seven two-bit qubit gates. [3]



(v) How can you do better? [+5]

Exercise 6.2 (Quantum Fourier transformation). (11 points)

In the lecture we discussed the quantum Fourier transform.

(i) Show directly that the quantum Fourier transform is a unitary operation. [2]

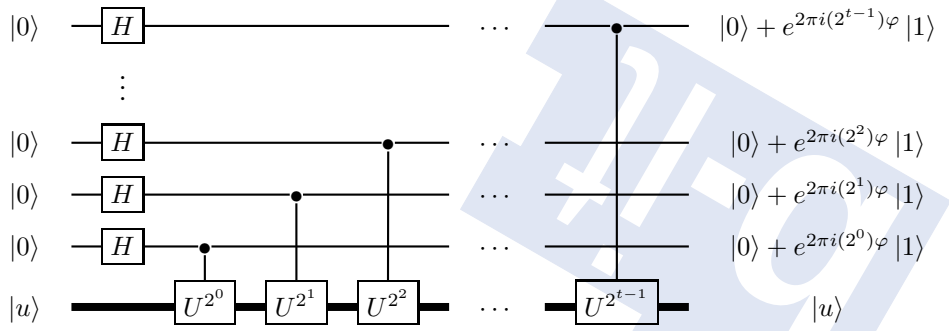
(ii) Give a quantum circuit that implements the inverse quantum Fourier transform. [3]

(iii) Explicitely state the circuit that implements the three qubit quantum Frouier transform using H, S, T and swap gates. [3]

(iv) Write down the matrix defining the circuit. It might be useful to abbreviate $\omega = \sqrt{i} = \exp(2\pi i/8)$. [3]

Exercise 6.3 (Phase estimation). (6 points)

In the lecture we encoutered the following circuit:



3 (i) Show that the sequence of the controlled U take the state $|j\rangle|u\rangle$ to the state $|j\rangle U^j|u\rangle$.

3 (ii) Why does this not depend on $|u\rangle$?

Exercise 6.4 (Decompostition). (22+5 points)

We will now explore how to decompose a controlled U when you operate on n qubits analogous to the A, B, C decomposition from the course.

2 (i) Recall that *any* matrix U can be written as VJV^{-1}, where V is invertible and J is in Jordan normal form.

4 (ii) Show that a *unitary* matrix U can be written as VJV^{-1}, where V is unitary and J is diagonal. Hint: Recall that V is built from the eigenvectors from U.

4 (iii) Show that the controlled-U operation $C(U)$ is the same as $(I \otimes V)C(J)(I \otimes V^{-1})$.

3 (iv) Prove that for $n = 1$ we can explicitly write $J = A \cdot XBX$ with $AB = I$. Hint: Due to the phase shift $\exp(i\varphi)$ you can assume that J has determinant 1.

3 (v) Show that in general we can not do this for $n > 1$ by replacing X with $X^{\otimes n}$.

3 (vi) Show that there exist matrices A, B_0, B_1 such that

$$U = \exp(i\varphi)A \cdot X_0B_0X_0 \cdot X_1B_1X_1 \text{ with } AB_0B_1 = I$$

where $X_0 = X \otimes I$ and X_1 is $I \otimes X$.

3 (vii) Conclude that we only need additional CNOT gates to implement $C(U)$ in the case $n = 2$.

+5 (viii) Generalize for $n > 2$.