W4281 - Introduction to Quantum Computing

Homework 4

due date: Thursday 7/14/2005

Exercise 1 (10 points):

In class we discussed the Quantum Fourier Transform

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} |k\rangle$$

and its circuit, which is shown in figure 5.1 in the textbook.

Derive a circuit for the Inverse Quantum Fourier Transform and prove its correctness.

Exercise 2 (10 points):

Prove the convolution theorem for the Quantum Fourier Transform $\mathscr{F}_{2^n}$ defined as

$$\mathscr{F}_{2^n} \sum_{j=0}^{2^n-1} \alpha_j |j\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} \sum_{j=0}^{2^n-1} \alpha_j e^{2\pi ijk/2^n} |k\rangle .$$

The *convolution* of two states $|\alpha\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle$ and $|\beta\rangle = \sum_{k=0}^{2^n-1} \beta_k |k\rangle$ is defined as

$$\frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} \sum_{l=0}^{2^n-1} \alpha_l \beta_{j-l} |j\rangle ,$$

where for $j-l<0$ we define $\beta_{j-l} := \beta_{2^n+j-l}$. It is a way to compute how much two states $|\alpha\rangle$ and $|\beta\rangle$ "have in common" and is used widely in signal processing.

Convolution theorem: Let $|\alpha\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle$ and $|\beta\rangle = \sum_{k=0}^{2^n-1} \beta_k |k\rangle$ be arbitrary n qubit states with Fourier transforms

$$\mathscr{F}_{2^n} |\alpha\rangle = \sum_{k=0}^{2^n-1} \gamma_k |k\rangle \text{ and } \mathscr{F}_{2^n} |\beta\rangle = \sum_{k=0}^{2^n-1} \delta_k |k\rangle .$$

Then

$$\mathscr{F}_{2^n} \Big[\frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} \sum_{l=0}^{2^n-1} \alpha_l \beta_{j-l} |j\rangle \Big] = \sum_{j=0}^{2^n-1} \gamma_j \delta_j |j\rangle . \tag{1}$$

Hint: instead of (1) show

$$\frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} \sum_{l=0}^{2^n-1} \alpha_l \beta_{j-l} |j\rangle = \mathscr{F}_{2^n}^{-1} \Big[\sum_{j=0}^{2^n-1} \gamma_j \delta_j |j\rangle \Big].$$

Exercise 3 (10 points):

Write a program to simulate the Quantum Phase Estimation algorithm.

The input should be given as

- The number of qubits $m \in \mathbb{N}$.
- A matrix U given by $2^m \times 2^m$ complex numbers.
- An eigenvector $|u\rangle$ of U, given by 2^m complex numbers (you do not have to check that it actually is an eigenvector).
- A precision 2^{-n} for the result given by an integer n. The phase φ_u of the eigenvalue $e^{2\pi i \varphi_u}$ of $|u\rangle$, i.e. $e^{2\pi i \varphi_u} |u\rangle = U |u\rangle$, should differ from the output $\widetilde{\varphi_u}$ of your algorithm by less than 2^{-n}, i.e.

$$|\varphi_u - \widetilde{\varphi}_u| < 2^{-n}, \tag{2}$$

- A probability $\varepsilon > 0$ of failure for which equation (2) does not have to hold.