Quantum Cryptography (fall 2013)	Prof. Dr. Dominique Unruh

Exercise Sheet 11

Out: November 20, 2013 — Due: November 26, 2013

Problem 1: Discrete Fourier Transform

In this problem, not that the indexes in the definition of the DFT start with 0. I.e., the top-left component of $D_N = N^{-1/2}\left(\!\left(e^{2i\pi kl/N}\right)\!\right)_{kl}$ is $N^{-1/2}\, e^{2i\pi 00/N} = 1$.

(a) Show that the $N \times N$-DFT D_N is unitary.

Hint: Show first that for some $\tilde\omega \in \mathbb{C}$ with $\tilde\omega^N = 1$ and $\tilde\omega \neq 1$, we have $\sum_{k=0}^{N-1} \tilde\omega^k = 0$. (What is $\tilde\omega \cdot \left(\sum_{k=0}^{N-1} \tilde\omega^k\right) = 0$?)

(b) Give a circuit for D_2 using only elementary gates (i.e., only gates given in the lecture notes in Sections 2 and 5).

(c) Let $N > 0$ be an integer. Let $r \in \{1, \dots, N\}$ with $r \mid N$. Let $x_0 \in \{0, \dots, r-1\}$. Let $|\Psi\rangle := t^{-1/2} \sum_{k=0}^{t-1} |x_0 + kr\rangle$ where δ is a normalization factor and $t := N/r$.

(If $r = \operatorname{ord} a \mid N$ for some group element a, then $|\Psi\rangle$ is the post-measurement state we have in Shor's order-finding algorithm directly before applying the DFT D_N.)

Let D_N be the $N \times N$-DFT. Let $|\Psi'\rangle := D_N|\Psi\rangle$. Consider a measurement on $|\Psi'\rangle$ in the computational basis and let γ denote the outcome. Show that $\Pr[\frac{N}{r}$ divides $\gamma] = 1$. (In other words, if $N \nmid \gamma r$ then $|\langle\gamma|\Psi'\rangle|^2 = 0$.)

(That is, at least in the case where $\operatorname{ord} a \mid N$, the order finding algorithm returns a multiple of $N/\operatorname{ord} a$.)

Hint: Show first that for some $\tilde\omega \in \mathbb{C}$ and $t \in \mathbb{N}$ with $\tilde\omega^t = 1$ and $\tilde\omega \neq 1$, we have $\sum_{k=0}^{t-1} \tilde\omega^k = 0$.

Problem 2: Inverting cyclic functions

Consider a function $H : [N] \to [N]$ where $[N] := \{0, \dots, N-1\}$. Let $H^i(x)$ denote $H(H(H(\dots H(x)\cdots)))$ (applied i times). For the sake of this problem, we call H cyclic if there exists a value p (the period) such that for all x, $H^p(x) = H(x)$.

(a) Let $U_H|x\rangle|i\rangle|0\rangle = |x\rangle|i\rangle|H^i(x)\rangle$. Give a quantum algorithm involving U_H for finding the period of H (assuming that H is cyclic).

Note: You may assume that the DFT D_N can be implemented as a polynomial-time[1] quantum circuit. (This is, in general, not true for all N. But in the general case, you would be able to use an approximately solution that is only slightly more complicated than the solution needed here.)

(b) Given $y = H(x)$ and given the period of p, show that you can find x in polynomial-time. (You may still use U_H.)

(c) The following statement is wrong:

> Given a cyclic H and a value $y \in \operatorname{range} H$, using the algorithm from (a), we can find the period p of H, and then using the algorithm from (b), we can compute $H^{-1}(y)$.[2] Moreover, all involved algorithms run in polynomial-time. Hence using quantum computers, cyclic functions can be inverted in polynomial-time.

Why?

[1] By polynomial-time, I mean that the size of the circuit is bounded by $p(\log N)$ for some polynomial p.

[2] Notice that cyclicity implies bijectivity, so H^{-1} is well-defined.