Quantum Cryptography (spring 2020)	Dominique Unruh
Exercise Sheet 9	
Out: 2020-05-20	Due: 2020-05-27

Problem 1: Discrete Fourier Transform

In this problem, note 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 $\tilde\omega \cdot \left(\sum_{k=0}^{N-1} \tilde\omega^k\right)$?)

(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) **(Bonus)** 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 t 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 $\Pr[\frac{N}{r} \text{ divides } \gamma] = 1$. (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 $\sum_{k=0}^{t-1} \tilde\omega^k = 0$.

Note: This was sketched in the lecture. You only get points if your proof goes beyond the sketch in the lecture in detail/rigor.

Problem 2: Breaking a Protocol

Consider the following commitment protocol (where n is some security parameter).

- *Commit phase.* Alice wants to commit to a bit b. First, she chooses n uniformly random bits $x_1, \dots, x_n \in \{0, 1\}$. If $b = 0$ she encodes them in the computational basis; if $b = 1$, in the diagonal basis. I.e., if $b = 0, x_i = 0$, then $|\Psi_i\rangle := |0\rangle$, if $b = 0, x_i = 1$, then $|\Psi_i\rangle := |1\rangle$, if $b = 1, x_i = 0$, then $|\Psi_i\rangle := |+\rangle$, if $b = 1, x_i = 1$, then $|\Psi_i\rangle := |-\rangle$.

  Then Alice sends the qubits $|\Psi_1\rangle, \dots, |\Psi_n\rangle$ to Bob.

- For each of the qubits, Bob randomly chooses whether to measure it in the computational or the diagonal basis. Let the outcomes of these measurements be denoted $\tilde{x}_i$.

- *Unveil phase.* Alice sends $b, x_1, \dots, x_n$ to Bob.

- Bob checks whether $x_i = \tilde{x}_i$ for all i where Bob measured in the right basis (computational in the case of $b = 0$, diagonal in the case of $b = 1$).

The intuition behind this protocol is as follows: It is hiding because Bob cannot distinguish which bases Alice used. It is binding because of the following reason: If Bob measures some $|\Psi_i\rangle$ in, say, the computational basis, but $|\Psi_i\rangle$ was not one of $|0\rangle, |1\rangle$, then the outcome of the measurement is to some extend random, and Alice cannot predict the output $\tilde{x}_i$ of Bobs measurement. On the other hand, if Bob measures $|\Psi_i\rangle$ in the diagonal basis, but $|\Psi_i\rangle$ was not one of $|+\rangle, |-\rangle$, then the outcome of the measurement is again random, and Alice cannot predict the output $\tilde{x}_i$ of Bobs measurement. So whatever state $|\Psi\rangle$ Alice sends, there is some probability that she will not know $\tilde{x}_i$. And since to unveil both as $b = 0$ and as $b = 1$, Alice needs to know all $\tilde{x}_i$, she will fail.

Of course, this intuition cannot be correct since we know from the lecture that this (and any other) commitment protocol cannot be secure.

(a) Show that this protocol is perfectly hiding (i.e., ε_H-hiding for $\varepsilon_H = 0$).

(b) Show that this protocol is not ε_B-binding for any $\varepsilon_B < 1$. (I.e., it is possible for Alice to commit in a way such that she can unveil both as $b = 0$ and as $b = 1$.)

  Note: You have to actually give an attack. It is not sufficient to say that there exists an attack due to Theorem 6 in the lecture notes and (a).

  Hint: Think of Bell pairs. Try out what happens if you measure both qubits of $|\beta_{00}\rangle$ in the diagonal basis.